Uwaga! Artykuł został opublikowany w dwóch wersjach językowych – podstawą do cytowań jest wersja angielska

Natalia Karpiuk
Uniwersytet Marii Curie-Skłodowskiej w Lublinie
ORCID: 0000-0001-6861-1885
natalia.karpiuk@mail.umcs.pl

Blockchain jako niestandardowa odpowiedź na ograniczenia prawa stanowionego w środowisku social mediów

ABSTRAKT

W dzisiejszych czasach większość społeczeństwa korzysta z Internetu i rozwijających się tam social mediów. Internet jest jednak przestrzenią, w której bezsprzecznie dochodzi do różnego rodzaju naruszeń, którym trudno przeciwdziałać przy wykorzystaniu instytucji i narzędzi prawnych, często nieprzystających do dynamicznie rozwijającego się środowiska. Pandemia COVID-19, która zmusiła do przeorganizowania życia ludzi na wszystkich polach i przeniesienia go nierzadko do sieci, nasiliła negatywne zjawiska, w tym rozpowszechnianie nieprawdziwych i szkodliwych społecznie informacji. Niniejszy artykuł zawiera oryginalne rozważania na temat skuteczności polskiego ustawodawstwa na tle dotychczasowej działalności organów Unii Europejskiej ukierunkowanej na zwiększenie bezpieczeństwa użytkowników Internetu na przykładzie przeciwdziałania rozpowszechniania nieprawdziwych informacji. Zdaniem autorki zarówno organy krajowe, jak i organy unijne nie wydają się być zainteresowane poszukiwaniem alternatyw opierających się na rozwiązaniach technologicznych, które mogłyby sprzyjać zapobieganiu dalszym naruszeniom w Internecie, a raczej są skoncentrowane na udoskonaleniu konwencjonalnych modeli ochronnych, których skuteczność wydaje się dyskusyjna. Celem artykułu jest rozpoczęcie interdyscyplinarnego dyskursu na temat szansy zmniejszenia ilości negatywnych zjawisk w środowisku social mediów przy użyciu technologii blockchain, nie wyłączając podjęcia dyskusji na temat możliwości opracowania odpowiednich przepisów w tym zakresie.

Słowa kluczowe: blokchain; ograniczenia prawa stanowionego; social media; Internet; organy Unii Europejskiej; rozwiązania technologiczne

WPROWADZENIE

Definitywne określenie rozmiaru zjawiska cyberprzestępczości i skali naruszeń, jakich dopuszczają się użytkownicy Internetu, jest niemal niemożliwe. Problem niedoszacowania może być spowodowany brakiem odpowiednich narzędzi pomiarowych, które dałyby wiarygodny wynik. W Polsce badania statystyczne dotyczące cyberprzestępczości przeprowadzone przez Komendę Główną Policji kończą się na 2012 r.[1], ale publicystyka prawnicza i ekonomiczna – powołując się na dane statystyczne policji – szacuje, że zjawisko te stale narasta, co nie idzie w parze ze skutecznością wykrywania zdarzeń. Zdaniem ekspertów źródłem problemu jest m.in. nieprawidłowa kwalifikacja czynów przez organy ścigania, rezygnacja z ich zgłaszania przez pokrzywdzonych oraz nierzadko element transgraniczny[2]. Nowe technologie, a w szczególności dynamika przemian zachodzących w ich obszarze, sprawiają, że mate-

[1] *Przestępstwa w sieci*, 2013, https://statystyka.policja.pl/st/informacje/85606,Przestepstwa-w-sieci.html [dostęp: 22.10.2021].

[2] Zob. *Hakerzy mają się w Polsce dobrze. Problem policji*, 2021, https://businessinsider.com.pl/technologie/nowe-technologie/cyberprzestepstwa-w-polsce-statystyki/zrn11l7 [dostęp: 9.10.2021]; K. Kucharczyk, *Liczba ataków hakerskich rośnie a wykrywalność spada*, 2021, www.rp.pl/biznes/art8648591-liczba-atakow-hakerskich-rosnie-a-wykrywalnosc-spada [dostęp: 9.10.2021]; L. Krakowiak, *Cyberprzestępstwa w Polsce są statystycznie niewidoczne*, 2019, www.computerworld.pl/news/Cyberprzestepstwa-w-Polsce-sa-statystycznie-niewidoczne,413041.html [dostęp: 9.10.2021].

ria ta jest szczególnie trudna do normatywnego uchwycenia[3]. W prawdzie nie można odmówić ustawodawcy podjęcia inicjatywy stworzenia krajowego systemu cyberbezpieczeństwa[4], lecz zakres regulacji pozwala na stwierdzenie, że przewidziane tam narzędzia nie zapewnią skutecznej ochrony jednostce, której dobro zostało naruszone w jakikolwiek sposób. Perspektywa utworzenia stabilnego, precyzyjnego i jasnego ustawodawstwa chroniącego pojedynczego użytkownika Internetu wydaje się być zatem odległa. Niezrozumienie pewnych zjawisk i prawidłowości technologicznych nie powinno jednak prowadzić do odstąpienia od poszukiwania nowych rozwiązań, zwłaszcza kiedy dotychczas stosowane narzędzia i instytucje prawne nie wydają się dostatecznie dobre. Celem niniejszego artykułu jest rozpoczęcie interdyscyplinarnej dyskusji na temat dobrodziejstw płynących z technologii blockchain i możliwości ich zaadaptowania do stworzenia przepisów prawnych zmierzających do skuteczniejszego zapewnienia szeroko pojętej ochrony użytkowników Internetu, w tym social mediów.

W artykule wykorzystano metodę dogmatyczną. Autorka dokonała przeglądu i analizy piśmiennictwa w zakresie działania technologii sieci blockchain w jej teoretycznym zarysie oraz interpretacji wyników statystycznych pozwalających na wyciągnięcie wniosków, które następnie zestawiła z obowiązującym stanem prawnym.

ISTOTA PROBLEMU BADAWCZEGO

Technologia blockchain (block-chain) jest jednym z wariantów technologii rozproszonego rejestru[5] i kojarzona jest powszechnie z obrotem kryptowalut w sieci Internet, co nie powinno dziwić, po raz pierwszy została bowiem użyta w 2009 r.[6] do księgowania transakcji przy użyciu cyfrowej waluty bitcoin w oparciu o koncepcję zaprezentowaną przez S. Nakamoto w 2008 r.[7] Zgodnie z pierwotnym zamysłem S. Nakamoto sieć zbudowana z niemodyfikowalnych bloków miała być gwarancją bezpieczeństwa transakcji dokonywanych w Internecie pomiędzy wirtualnymi kontrahentami, dla których największym zagrożeniem była niepewność płatności w związku z zagrożeniem możliwości podwójnego wydatkowania udostępnionych środków[8].

---

[3] Szerzej: W. Konaszczuk, *Cybersecurity Threats in the Sectors of Oil, Natural Gas and Electric Power in the Context of Technological Evolution*, „Studia Iuridica Lublinensia" 2021, vol. 30(4); I.A. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017, s. 23.

[4] Szerzej: M. Karpiuk, *Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, vol. 30(2); idem, *The Local Government's Position in the Polish Cybersecurity System*, "Lex localis – Journal of Local Self-Government" 2021, vol. 19(3); K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The Legal Status of Public Entities in the Field of Cybersecurity in Poland*, Maribor 2021; M. Rogalski, *Projekt ustawy Prawo komunikacji elektronicznej – zagadnienia wybrane*, „Krytyka Prawa. Niezależne Studia nad Prawem" 2021, vol. 13(2).

[5] K. Ciupa, *Warianty zastosowania koncepcji blockchain a modele ich doboru*, „Studia i Prace Kolegium Zarządzania i Finansów SGH" 2019, nr 173, s. 91.

[6] *Leksykon pojęć na temat technologii blockchain i kryptowalut*, red. K. Piech, 2016, www.gov.pl/documents/31305/0/leksykon_pojec_na_temat_technologii_blockchain_i_kryptowalut.pdf [dostęp: 20.10.2021]; D. Ginsberg, *The Building Blocks of Blockchain*, "North Carolina Journal of Law and Technology" 2020, vol. 4, s. 5, 472.

[7] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf [dostęp: 20.10.2021].

[8] *Ibidem*, s. 1.

Obecnie nie ma żadnych wątpliwości, że technologia blockchain jest technologią uniwersalną, a jej praktyczne zastosowanie znacznie wykracza poza wykorzystanie jej wyłącznie do dokonywania operacji finansowych w przestrzeni cyfrowej, stąd też słusznie nie brakuje głosów, że powinna ona uchodzić za „technologię przyszłości", która ma potencjał przełomowej innowacji odmieniającej oblicze współczesnego Internetu na wielu obszarach[9].

Istota tego konstruktu kryje się w specyficznej architekturze, stanowiącej w pewnym sensie zaprzeczenie dominującej w Internecie sieci scentralizowanej. Już na początku lat 60. XX w. P. Baran w ramach raportu przygotowanego dla RAND Corporation dostrzegł przewagę sieci rozproszonych nad całkowicie (scentralizowanymi) lub częściowo (zdecentralizowanymi) zhierarchizowanymi strukturami, uznając je za stabilniejsze i odporniejsze na zewnętrzną ingerencję, powodującą np. przerwanie sieci, tj. specyficznego połączenia istniejącego pomiędzy jej uczestnikami[10]. W swojej publikacji wyróżnił trzy podstawowe typy sieci: scentralizowaną, zdecentralizowaną i rozproszoną. W założeniu P. Barana fundamentem sieci scentralizowanej był jeden wspólny centralny węzeł (*node*), którego zadaniem było dystrybuowanie danych pomiędzy uczestnikami sieci (pozostałymi węzłami). Sieć rozproszona natomiast była siecią, dla której nie przewidziano „nadrzędnie" sterującego węzła. Sieć zdecentralizowana to z kolei w pewnym sensie wersja pośrednia pomiędzy dwiema poprzednimi, w której występowało wiele węzłów o funkcjach jedynie zbliżonych do węzła centralnego, ale niebędących w istocie węzłami centralnymi.

Początkowo rozważania P. Barana były osadzone wyłącznie w kontekście wykorzystania sieci rozproszonej dla celów militarnych, tj. gromadzenia i przetwarzania danych, jednak z czasem dostrzegł on potencjał konceptu nowej architektury jako ogólnospołecznej szansy na zbudowanie międzynarodowych systemów poczty elektronicznej jako tańszej alternatywy dla tradycyjnej poczty, wskazując przy tym na inne funkcjonalne zastosowanie sieci rozproszonej[11].

Poszukiwania nowych wariantów adaptacji nowej technologii doprowadziły do praktycznego już dzisiaj wykorzystania jej w różnych sektorach i branżach, w tym we wcześniej zasygnalizowanym obszarze usług finansowych, ale też logistycznych i przepływu towarów[12]. Technologia ta jest również fundamentem coraz popularniejszych smart contractów. Jak wskazuje K. Piech, dane zebrane w ramach rozproszonych baz danych mogą być traktowane jako nieswoiste nośniki oświadczeń woli uczestników obrotu[13]. Nie jest to jednak zamknięty katalog możliwych rozwiązań i właściwości technologii blockchain, dlatego coraz częściej formułowane są nowe i bardziej śmiałe pomysły wdrożenia tej architektury, w tym choćby do

[9] Por. W. Szpringer, *Fintech i blockchain – kierunki rozwoju gospodarki cyfrowej*, „Studia BAS" 2019, nr 1, s. 10; K. Ciupa, *op. cit.*, s. 90; J. Gosh, *The Blockchain: Opportunities for Research in Information Systems and Information technology*, "Journal of Global Information Technology Management" 2019, vol. 22.
[10] Szerzej: P. Baran, *On Distributed Communications: I. Introduction to Distributed Communications Network*, August 1964, www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf [dostęp: 20.10.2021], s. 1.
[11] Idem, *Some Perspectives on Networks – Past, Present and Future*, Palo Alto 1977.
[12] K. Ciupa, *op. cit.*, s. 90
[13] *Leksykon pojęć na temat technologii blockchain…*, s. 9.

wspierania demokratyzacji społeczeństwa, wspierania kształtowania ruchów wolnościowych[14] czy dla celów stworzenia nowych, alternatywnych social mediów.

Pandemia COVID-19 ogłoszona 11 marca 2020 r. przez Światową Organizację Zdrowia (WHO) zmusiła do przeniesienia przez społeczeństwo wielu obszarów swojego życia do sieci. To zaś spowodowało zwiększenie liczby niepożądanych incydentów, w tym wyeksponowało rozmiar zagrożenia, jakie niesie za sobą narastające od lat zjawisko świadomego rozpowszechniania przez użytkowników Internetu nieprawdziwych informacji[15] (fake news) w sieci, co Komisja Europejska w realiach pandemii określiła mianem „infodemii"[16].

Jak się wydaje, wdrożenie adekwatnych rozwiązań technologicznych (architektury sieciowej), zwłaszcza w obszarach, w których inne instrumenty zdają się być nie w pełni skuteczne, może stanowić kluczowe wsparcie dla konwencjonalnych (prawnych) form ochrony szeroko pojętego bezpieczeństwa w Internecie, których skuteczność jest przecież uzależniona np. od wykrycia sprawcy danej operacji, rodzaju operacji i innych kluczowych danych. W wielu przypadkach trudność w prześledzeniu czynności podjętych przez sprawcę czy niemożność ich określenia może decydować o nieskuteczności zastosowania modeli przewidzianych w obowiązującym prawie.

BLOCKCHAIN JAKO TECHNOLOGIA SIECI ROZPROSZONEJ

Koncepcja blockchain zakłada gromadzenie danych w ramach zdecentralizowanej, rozproszonej i zsynchronizowanej bazy danych, której spektrum działania opiera się na normach ogólnodostępnego protokołu określającego normy techniczne i ogólne zasady obowiązujące wszystkich użytkowników[17]. Jak już wspomniano, założenia sieci rozproszonej stanowią alternatywę dla scentralizowanej architektury opierającej się na opozycyjnych wartościach i sposobie działania. Abstrahując od rozbudowanych typologii i klasyfikacji porządkujących modele mieszczące się w szeroko ujętej „technologii blockchain"[18], jej istota kryje się w specyficznej formule skonstruowanej w oparciu o wzajemnie połączone kryptograficznie bloki, będące podstawowym budulcem łańcucha bloków. Blok jako podstawowe ogniwo łańcucha strukturalnie składa się z nagłówka (znacznika czasu oraz korzenia haszy, ang. *hash*), które w pewnym sensie dokumentuje moment jego utworzenia i nawiązuje do poprzedzającego go bloku oraz do danych pozwalających na jednoznaczne zdefiniowanie operacji zawar-

[14] K. Piech, *Blockchain a ludzie*, „Magazyn Polskiej Akademii Nauk" 2020, nr 1. Szerzej: M. Friedlmaier, A. Tumasjan, I.M. Welpe, *Disrupting Industries with Blockchain: The Industry, Venture Capital Funding, and Regional Distribution of Blockchain Ventures*, 2018, https://scholarspace.manoa.hawaii.edu/bitstream/10125/50333/1/paper0446.pdf [dostęp: 20.10.2021].
[15] Zob. J. Jabłońska-Bonca, *„Wciskanie kitu" (w rozumieniu H.G. Frankfurta) na temat prawa w mediach. Z problematyki komunikacji erystycznej*, „Krytyka Prawa. Niezależne studia nad prawem" 2021, vol. 13(2), s. 253.
[16] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego Komitetu Regionów. Wytyczne Komisji Europejskiej w sprawie wzmocnienia kodeksu postępowania w zakresie dezinformacji, COM(2021) 262 final, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2021:0262:FIN:PL:PDF [dostęp: 16.10.2021].
[17] B. Bodó, J.K. Brekke, J.-H. Hoepman, *Decentralisation: A multidisciplinary perspective*, "Internet Policy Review" 2021, vol. 10(2).
[18] Por. K. Ciupa, *op. cit.*, s. 91.

tych w bloku. Rodzaj danych zależny jest od rodzaju łańcucha (jego przeznaczenia) i może zawierać rozmaite informacje determinowane typem transakcji[19].

Charakter połączenia istniejącego pomiędzy blokami powoduje, że nowo dołączone bloki są trwale związane ze wszystkimi wcześniej dodanymi blokami, które wyznaczają jego treść, ponieważ treść nowego bloku charakteryzowana jest treścią bloków poprzedzających. Nawet najmniejsza ingerencja czy modyfikacja danych ujawnionych w danym bloku automatycznie powoduje ponowne obliczenie i wygenerowanie w ten sposób nowego skrótu dla wszystkich następujących po nim bloków, co czyni zmianę w zapisach historycznych bez zmiany całej historii transakcji niemożliwą[20]. Bloki tworzą zatem integralną i nierozerwalną całość celowo określaną jako „łańcuch".

Technologia blockchain, będąca formułą opozycyjną do sieci scentralizowanej, daje możliwość dostępu do ogółu informacji wygenerowanych dla bloków, a zgromadzonych w rozproszonym rejestrze, każdemu jej użytkownikowi, nie zaś jedynie centralnie sterującemu bytowi, który jednostronnie kontroluje i ustala odgórnie obowiązujące wszystkich warunki dostępu do danych i korzystania z sieci[21]. W literaturze sygnalizuje się wady działania sieci rozproszonych, które są związane ze specyfiką architektury, ujawniające się w problemach z późniejszym jej koordynowaniem i bardzo ograniczoną przepustowością w stosunku do sieci scentralizowanej. Tym niemniej prawidłowo działająca sieć rozproszona znacznie zmniejsza ryzyko przejęcia kontroli przez jakikolwiek podmiot, co stanowi niekwestionowaną zaletę i daje przewagę nad systemami scentralizowanymi. Sieci rozproszone i zdecentralizowane jako zbudowane z pominięciem centralnie sterującego bytu są więc lepszym rozwiązaniem dla tworzenia struktur, których skuteczność działania zależy od gwarantowania prywatności, odporności na cenzurę, dostępności i integralności informacji o właściwościach bezpieczeństwa informacji[22].

Opracowanie konstrukcji sieciowej o takich przymiotach jest bardzo ważne. Już ponad dekadę temu J. von Dijk zasygnalizował, że Internet XXI w. jest „w coraz mniejszym stopniu kontrolowany przez prawo i wspólnotę internetową, a w coraz większym przez rynek i standardy techniczne, których w żadnym razie nie można nazwać neutralnymi technologiami i za którymi stoją nowe regulacje prawne"[23]. Jak podkreślił, może to wywoływać nieuniknione kolizje w obszarze prawa do informacji i komunikacji, prawa własności i prawa do prywatności[24]. Powyższe wydaje się naturalną konsekwencją dynamiki przemian oraz skomplikowaną materią, którą ciężko jest ująć w ścisłe normatywne ramy.

---

[19] J. Gosh, *op. cit.*; A. Rot, R. Zygała, *Technologia blochchain jako rewolucja w transakcjach cyfrowych. Aspekty technologiczne i potencjalne zastosowania*, „Informatyka Ekonomiczna. Business Informatics" 2018, vol. 4(50), s. 124.

[20] *Leksykon pojęć na temat technologii blockchain…*, s. 5; P. Opitek, *Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego*, „Prokuratura i Prawo" 2017, nr 6, s. 37. Por. J. Gosh, *op. cit.*; F. Knirsch, A. Unterweger, D. Engel, *Implementing a blockchain from scratch: Why, how, and what we learned*, "EURASIP J. on Info. Security" 2019, vol. 2.

[21] B. Bodó, J.K. Brekke, J.H. Hoepman, *op. cit.*

[22] Zob. *ibidem*; J.H. Hoepman, *Privacy Design Strategies*, [w:] *ICT Systems Security and Privacy Protection. SEC 2014. IFIP Advances in Information and Communication Technology*, eds. N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, vol. 428.

[23] J. van Dijk, *Społeczne aspekty nowych mediów. Analiza społeczeństwa sieci*, Warszawa 2010, s. 186.

[24] Por. R. Maciąg, *Paradygmatyka Internetu. Web 2.0 jako środowisko*, Kraków 2013, s. 96–97.

W związku z tym nie powinien dziwić wzrost zainteresowania możliwością zaimplementowania rozwiązań technologicznych zakładających równość praw i obowiązków wszystkich użytkowników na jednolitych zasadach do budowania nowych social mediów. Skoro za opracowaniem blockchain stała w istocie chęć stworzenia konstrukcji spełniającej funkcję bazy danych, która gwarantuje monitorowanie i śledzenie losów tych danych, to czy nie warto byłoby wykorzystać jej jako budulca dla przestrzeni, w której dochodzi do rozmaitych naruszeń, a których ze względu na specyficzne środowisko skuteczne ściganie jest szczególne trudne?

CHARAKTERYSTYKA SOCIAL MEDIÓW W ŚWIETLE BADAŃ KOMISJI EUROPEJSKIEJ

Ze statystyk przygotowanych przez Eurostat wynika, że w 2020 r. 57% obywateli Unii Europejskiej zadeklarowało uczestnictwo w sieciach społecznościowych (tworzenie profili użytkowników, zamieszczanie wiadomości lub innych wpisów na Facebooku i Twitterze itp.), przy czym w przedziale wiekowym od 16 do 24 lat odsetek zaangażowanych wynosił 87%[25]. Poza wykorzystywaniem social mediów do celów prywatnych, równie chętnie sięgają się po nie przedsiębiorcy do prowadzenia działalności gospodarczej, o czym świadczy fakt, że niemal co drugie przedsiębiorstwo (43%) w Unii Europejskiej korzystało przynajmniej z jednej formuły portalu społecznościowego w celach bezpośrednio związanych z prowadzeniem działalności gospodarczej[26], jak budowanie wizerunku przedsiębiorstwa lub wprowadzanie na rynek produktów (w 2019 r. – 45%) czy też pozyskiwanie opinii i recenzji lub kierowanie pytań do klientów czy udzialnie odpowiedzi na pytania od klientów (w 2019 r. – 29%). Niektóre przedsiębiorstwa wykorzystywały social media do celów wewnatrzkomunikacyjnych, wymiany poglądów, opinii lub wiedzy w przedsiębiorstwie (w 2019 r. – 14%)[27].

Media społecznościowe stanowią platformę do szybkiej i bezpośredniej komunikacji, co pozwala na błyskawiczny przepływ informacji pomiędzy niemal nieograniczoną liczbą połączonych ze sobą użytkowników[28]. Z uwagi na te właściwości media społecznościowe mogą być i często są chętnie wykorzystywane jako idealne środowisko także do rozpowszechniania nieprawdziwych informacji. Badania wyraźnie wskazują na postępujący trend, zgodnie z którym media społecznościowe przestały być wykorzystywane wyłącznie do za-

[25] Eurostat, *Individuals – internet activities*, last update: 9.06.2021, https://appsso.eurostat.ec.europa.eu/nui/show.do?query=BOOKMARK_DS-053730_QID_-758A9195_UID_-3F171EB0&layout=IND_TYPE,L,X,0;GEO,L,Y,0;TIME,C,Z,0;UNIT,L,Z,1;INDIC_IS,L,Z,2;INDICATORS,C,Z,3;&zSelection=DS-053730INDICATORS,OBS_FLAG;DS-053730UNIT,PC_IND;DS-053730INDIC_IS,I_IUSNET;DS-053730TIME,2019;&rankName1=UNIT_1_2_-1_2&rankName2=INDICATORS_1_2_-1_2&rankName3=TIME_1_0_0_0&rankName4=INDIC-IS_1_2_0_0&rankName5=IND-TYPE_1_2_0_0&rankName6=GEO_1_2_0_1&rStp=&cStp=&rDCh=&cDCh=&rDM=true&cDM=true&footnes=false&empty=false&wai=false&time_mode=ROLLING&time_most_recent=true&lang=EN&cfo=%23%23%23%2C%23%23%23.%23%23%23 [dostęp: 12.10.2021].

[26] Eurostat, *Social media use by purpose*, last update: 23.09.2021, https://ec.europa.eu/eurostat/databrowser/view/isoc_cismp/default/table?lang=en%20European%20Commission:%20DG%20Communications%20Networks%20Content%20and%20Technology [dostęp: 12.10.2021].

[27] Eurostat, *Social media – statistics on the use by enterprises*, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Social_media_-_statistics_on_the_use_by_enterprises#Use_of_social_media_by_enterprises [dostęp: 12.10.2021].

[28] Szerzej: M. Radvan, *Taxation of Instagram Influencers*, „Studia Iuridica Lublinensia" 2021, vol. 30(2), s. 340.

spokojenia potrzeb społecznych i stały się obszarem rozwoju gospodarczego, platformą dla funkcjonowania różnego typu organizacji oraz kształtowania życia politycznego.

Zjawisko dezinformacji zostało dostrzeżone przez Parlament Europejski już w 2017 r. Komisja Europejska została wezwana do zbadania tego problemu, przede wszystkim celem było określenie jego skali i perspektyw legislacyjnych w obszarze ograniczenia rozpowszechniania fałszywych treści. Badania, które zostały przeprowadzone na zlecenie Komisji Europejskiej w styczniu 2018 r., ujawniły jedną z socjodemograficznych prawidłowości. Otóż respondenci w wieku od 14 do 24 lat korzystający na co dzień z internetowych sieci społecznościowych wyrazili większe zaufanie do treści pochodzących ze źródeł internetowych (60% badanych)[29]. Korelacja istniejąca pomiędzy częstotliwością korzystania z portali społecznościowych a stopniem zaufania do informacji udostępnionych w Internecie pozwala na postawienie tezy, że w najbliższych latach internetowe źródła informacji będą źródłami dominującymi w Unii Europejskiej.

W dniu 26 maja 2021 r. Komisja Europejska wydała komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów[30], skierowany także do rządów i parlamentów narodowych oraz do innych organów krajowych, partii politycznych, mediów, społeczeństwa obywatelskiego i platform internetowych. Zawarte w nim wytyczne w sprawie wzmocnienia kodeksu postępowania w zakresie dezinformacji miały być formą zachęcenia do podjęcia zintegrowanych działań w sferze walki z ogólnie postępującą dezinformacją i jednocześnie odpowiedzią na niedostatki „najważniejszego elementu starań podjętych przez Unię Europejską, jakim jest samoregulacyjny kodeks postępowania w zakresie zwalczania dezinformacji", który obowiązuje od października 2018 r., a sygnowany został przez największe platformy internetowe działające w Unii. Nie jest to jedyna inicjatywa Komisji Europejskiej w tym przedmiocie[31]. Zdaniem Komisji kodeks, mimo że nie jest wolny od wad[32], stanowi innowacyjne narzędzie zapewniające większą przejrzystość i odpowiedzialność platform internetowych, jak również ustrukturyzowane ramy monitorowania i ulepszania polityki platform w zakresie zwalczania dezinformacji[33].

---

[29] Eurobarometer, *Fake news and disinformation online*, March 2018, https://europa.eu/eurobarometer/surveys/detail/2183 [dostęp: 18.10.2021], s. 10.

[30] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego Komitetu Regionów. Wytyczne Komisji Europejskiej w sprawie wzmocnienia kodeksu postępowania w zakresie dezinformacji, COM(2021) 262 final.

[31] Por. A. Jaskiernia, *Problemy mediów w nowej strategii Unii Europejskiej „wzmocnienia odporności demokratycznej"*, „Studia Medioznawcze" 2021, vol. 1(84), s. 885. Według informacji podanych przez Krajową Radę Radiofonii i Telewizji sygnatariuszami są m.in. Facebook, Google, Mozilla, Twitter, Microsoft, Tik-Tok. Zob. Krajowa Rada Radiofonii i Telewizji, *Zwalczanie dezinformacji w mediach – zalecenia ERGA na podstawie kontroli przestrzegania „Kodeksu postępowania w zakresie dezinformacji"*, 2021, www.gov.pl/web/krrit/zwalczanie-dezinformacji-w-mediach---zalecenia-erga-na-podstawie-kontroli-przestrzegania-kodeku-postepowania-w-zakresie-dezinformacji [dostęp: 16.10.2021]. Jak podaje Komisja Europejska, do potencjalnych sygnatariuszy mają należeć również: Vimeo, Clubhouse, Avaaz, Globsec, Logically, NewsGuard i WhoTargetsMe. Zob. *Kolejne podmioty chcą zwalczać dezinformację*, 2021, https://ec.europa.eu/poland/news/211004_deinformation_pl [dostęp: 16.10.2021].

[32] W 2020 r. Komisja przeprowadziła bieżącą ocenę kodeksu. Ujawniła ona niedociągnięcia, które zaowocowały niespójnym i niepełnym stosowaniem kodeksu przez sygnatariuszy, brakiem odpowiedniego mechanizmu monitorowania przestrzegania norm. Por. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego Komitetu Regionów. Wytyczne Komisji Europejskiej w sprawie wzmocnienia kodeksu postępowania w zakresie dezinformacji, COM(2021) 262 final, s. 1–2.

[33] *Ibidem*, s. 1.

W związku z zaobserwowanymi przez Komisję wadami postanowiono sformułować wytyczne, które zdaniem Komisji przyczynią się do stworzenia silnego, stabilnego i elastycznego instrumentu, za pomocą którego platformy internetowe staną się bardziej przejrzyste, rozliczalne i odpowiedzialne[34]. Wytyczne nawołują m.in. do zwiększenia udziału innych platform, które nie zadeklarowały jeszcze „akcesu" do unijnego kodeksu, a także przedstawicieli branż reklam internetowych, które mogłyby wnieść fachową wiedzę pozwalającą na dalsze udoskonalanie kodeksu. Ponadto zaproponowano demonetyzację dezinformacji (ograniczenie możliwości zarabiania pieniędzy na dezinformacji), wypracowanie wspólnego rozumienia niedozwolonych zachowań manipulacyjnych i reakcji w przypadku ich wystąpienia. W ramach wytycznych wyeksponowano również konieczność wzmocnienia pozycji użytkowników, w tym poprzez projektowanie architektury usług przez właścicieli platform internetowych „w taki sposób, aby zminimalizować ryzyko związane z rozprzestrzenianiem się i nasileniem zjawisk dezinformacyjnych", co wydaje się szczególnie ważne, biorąc pod uwagę specyfikę środowiska, które można uznać za peryferyjne obszary legislacji[35].

Kodeks nie ma waloru normatywnego, a jego skuteczność jest w pełni zależna od woluntarystycznych postaw sygnatariuszy. Rzecz ma się podobnie w odniesieniu do wytycznych sformułowanych przez Komisję, które mogą być przez władze krajów członkowskich interpretowane wybiórczo. Należy jednak podkreślić, że dezinformacja nie jest jedynym problemem, z jakim zmagają się użytkownicy mediów społecznościowych.

PODSUMOWANIE

Blockchain wydaje się być dobrą odpowiedzią na współczesne problemy związane z funkcjonowaniem mediów społecznościowych, daje bowiem możliwość prześledzenia losów poszczególnych danych umieszczonych w sieci przez każdego użytkownika, który ma do niej dostęp na równych zasadach.

Wśród użytkowników Internetu pojawia się coraz więcej głosów za decentralizacją mediów. Głoszenie postulatów o konieczności zbudowania nowych mediów w oparciu o niezależność sieci nie jest jednak domeną wyłącznie użytkowników portali społecznościowych, którzy dostrzegają zagrożenia płynące z funkcjonowania w obszarze czy środowisku, w którym mają ograniczone możliwości weryfikowania treści, jakie do nich docierają oraz decydowania o ich dalszym losie. Już w grudniu 2019 r. J. Dorsey, założyciel i dyrektor generalny Twittera, na łamach platformy Twitter podzielił się opinią dotyczącą konieczności decentralizacji mediów. Jak stwierdził, pomocna będzie tu technologia rejestrów rozproszonych blockchain, może się bowiem przyczynić do zmiany koncepcji dotychczasowej moderacji treści trafiających do użytkowników[36].

[34] *Ibidem*, s. 2.
[35] Por. Krajowa Rada Radiofonii i Telewizji, *Fake news – dezinformacja online. Próby przeciwdziałania tym zjawiskom z perspektywy instytucji międzynarodowych oraz wybranych państw UE, w tym Polski*, Warszawa 2020, www.gov.pl/web/krrit/fake-news--dezinformacja-online [dostęp: 19.06.2021].
[36] A. Palmer, *Twitter CEO Jack Dorsey has an idealistic vision for the future of social media and is funding a small team to chase it*, 2019, www.cnbc.com/2019/12/11/twitter-ceo-jack-dorsey-announces-bluesky-social-media-standards-push.html [dostęp: 20.10.2021].

Dobrowolne przemodelowanie dotychczasowego systemu budowania platform internetowych przez ich właścicieli wydaje się najskuteczniejszym wariantem projektowania nowych mediów. Potrzeba autoregulacji może wynikać z wewnętrznego imperatywu zagwarantowania użytkownikom sieci podstawowych praw w środowisku nieuchwytnym dla prawa stanowionego. Niedostatki legislatury są więc bodźcem do wykształcenia się naturalnego dążenia do poszukiwania alternatywnych form zabezpieczenia słusznych racji użytkowników Internetu. Wewnętrznie pojawiające się impulsy wśród użytkowników Internetu nie mogą być jednak uzasadnieniem dla kompetentnych organów państwowych do odstąpienia od podjęcia próby normatywnego uregulowania przedmiotowej materii, chociaż w literaturze przedmiotu sygnalizowane są trudności w stanowczym unormowaniu wciąż dynamicznie zmieniających się praktyk kreowanych przez użytkowników globalnej sieci komputerowej[37]. Upowszechnienie zastosowania technologii blockchain pozwoliłoby użytkownikowi na prześledzenie przepływu informacji oraz być może ułatwiłoby wykorzystanie dostępnych narzędzi i instytucji prawnych pozwalających na walkę z szerzeniem nieprawdziwych informacji, które dla swej skuteczności wymagają pozyskania konkretnych informacji, których użytkownik często nie może otrzymać ze względu na specyfikę sieci scentralizowanej i niemożność wykrycia sprawcy. Ponadto technologia blockchain pozwala na bezpieczne przechowywanie danych z gwarancją dalszego ich nieprzetwarzania[38].

Niniejszy artykuł może stanowić bodziec do rozważenia możliwości wprowadzenia stanowczych regulacji, które wykorzystają w pełni potencjał technologii blockchain w polskim systemie prawnym. Jak zauważa W. Szpringer, technologia blockchain – opierając się na bezpiecznej i odpornej na manipulacje architekturze – daje szansę na przekształcenie „Internetu informacji" w „Internet wartości"[39], co organy stanowiące powinny wykorzystać. Obecnie wszystkie dotychczasowe starania koncentrują się na udoskonaleniu istniejących rozwiązań znanych nauce przedmiotu, ale nie są poszukiwane nowe rozwiązania, które mogłyby okazać się skuteczniejsze.

BIBLIOGRAFIA

LITERATURA

Baran P., *Some Perspectives on Networks – Past, Present and Future*, Palo Alto 1977.

Bodó B., Brekke J.K., Hoepman J.-H., *Decentralisation: A multidisciplinary perspective*, "Internet Policy Review" 2021, vol. 10(2), **DOI: https://doi.org/10.14763/2021.2.1560**.

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The Legal Status of Public Entities in the Field of Cybersecurity in Poland*, Maribor 2021, **DOI: https://doi.org/10.4335/2021.5**.

Ciupa K., *Warianty zastosowania koncepcji blockchain a modele ich doboru*, „Studia i Prace Kolegium Zarządzania i Finansów SGH" 2019, nr 173.

Dijk J. van, *Społeczne aspekty nowych mediów. Analiza społeczeństwa sieci*, Warszawa 2010.

Funta R., *Social Networks and Potential Competition Issues*, „Krytyka Prawa" 2020, vol. 12(1), **DOI: https://doi.org/10.7206/kp.2080-1084.369**.

[37] Por. T. Kaczmarek, *Polskie prawo karne wobec przestępczości komputerowej*, „Nowa Kodyfikacja Prawa Karnego" 2001, vol. 8, s. 57. Szerzej: A. Haręża, *Naturalnoprawne sfery regulacji technologii informacyjnych. Zarys teorii fenomenu dynamiki korelacji danych i informacji w cyberprzestrzeni*, „e-Biuletyn CBKE" 2007, nr 4.

[38] Zob. R. Funta, *Social Networks and Potential Competition Issues*, „Krytyka Prawa" 2020, vol. 12(1).

[39] W. Szpringer, *op. cit.*, s. 10.

Ginsberg D., *The Building Blocks of Blockchain*, "North Carolina Journal of Law and Technology" 2020, vol. 4.

Gosh J., *The Blockchain: Opportunities for Research in Information Systems and Information technology*, "Journal of Global Information Technology Management" 2019, vol. 22.

Haręża A., *Naturalnoprawne sfery regulacji technologii informacyjnych. Zarys teorii fenomenu dynamiki korelacji danych i informacji w cyberprzestrzeni*, „e-Biuletyn CBKE" 2007, nr 4.

Hoepman J.H., *Privacy Design Strategies*, [w:] *ICT Systems Security and Privacy Protection. SEC 2014. IFIP Advances in Information and Communication Technology*, eds. N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, vol. 428, **DOI: https://doi.org/10.1007/978-3-642-55415-5_38**.

Jabłońska-Bonca J., *„Wciskanie kitu" (w rozumieniu H.G. Frankfurta) na temat prawa w mediach. Z problematyki komunikacji erystycznej*, „Krytyka Prawa. Niezależne studia nad prawem" 2021, vol. 13(2), **DOI: https://doi.org/10.7206/kp.2080-1084.460**.

Jaroszewska I.A., *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017.

Jaskiernia A., *Problemy mediów w nowej strategii Unii Europejskiej „wzmocnienia odporności demokratycznej"*, „Studia Medioznawcze" 2021, vol. 1(84).

Kaczmarek T., *Polskie prawo karne wobec przestępczości komputerowej*, „Nowa Kodyfikacja Prawa Karnego" 2001, vol. 8.

Karpiuk M., *Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, vol. 30(2), **DOI: http://dx.doi.org/10.17951/sil.2021.30.2.233-244**.

Karpiuk M., *The Local Government's Position in the Polish Cybersecurity System*, "Lex localis – Journal of Local Self-Government" 2021, vol. 19(3), **DOI: https://doi.org/10.4335/19.3.609-620(2021)**.

Knirsch F., Unterweger A., Engel D., *Implementing a blockchain from scratch: Why, how, and what we learned*, "EURASIP J. on Info. Security" 2019, vol. 2.

Konaszczuk W., *Cybersecurity Threats in the Sectors of Oil, Natural Gas and Electric Power in the Context of Technological Evolution*, „Studia Iuridica Lublinensia" 2021, vol. 30(4), **DOI: http://dx.doi.org/10.17951/sil.2021.30.4.333-351**.

Maciąg R., *Paradygmatyka Internetu. Web 2.0 jako środowisko*, Kraków 2013.

Opitek P., *Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego*, „Prokuratura i Prawo" 2017, nr 6.

Piech K., *Blockchain a ludzie*, „Magazyn Polskiej Akademii Nauk" 2020, nr 1.

Radvan M., *Taxation of Instagram Influencers*, „Studia Iuridica Lublinensia" 2021, vol. 30(2), **DOI: http://dx.doi.org/10.17951/sil.2021.30.2.339-356**.

Rogalski M., *Projekt ustawy Prawo komunikacji elektronicznej – zagadnienia wybrane*, „Krytyka Prawa. Niezależne Studia nad Prawem" 2021, vol. 13(2), **DOI: https://doi.org/10.7206/kp.2080-1084.453**.

Rot A., Zygała R., *Technologia blochchain jako rewolucja w transakcjach cyfrowych. Aspekty technologiczne i potencjalne zastosowania*, „Informatyka Ekonomiczna. Business Informatics" 2018, vol. 4(50).

Szpringer W., *Fintech i blockchain – kierunki rozwoju gospodarki cyfrowej*, „Studia BAS" 2019, nr 1.

NETOGRAFIA

Baran P., *On Distributed Communications: I. Introduction to Distributed Communications Network*, August 1964, www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf [dostęp: 20.10.2021].

Eurobarometer, *Fake news and disinformation online*, March 2018, https://europa.eu/eurobarometer/surveys/detail/2183 [dostęp: 18.10.2021].

Eurostat, *Individuals – internet activities*, last update: 9.06.2021, https://appsso.eurostat.ec.europa.eu/nui/show.do?query=BOOKMARK_DS-053730_QID_-758A9195_UID_-3F171EB0&layout=IND_TYPE,L,X,0;GEO,L,Y,0;TIME,C,Z,0;UNIT,L,Z,1;INDIC_IS,L,Z,2;INDICATORS,C,Z,3;&zSelection=DS-053730INDICATORS,OBS_FLAG;DS-053730UNIT,PC_IND;DS-053730INDIC_IS,I_IUSNET;DS-053730TIME,2019;&rankName1=UNIT_1_2_-1_2&rankName2=INDICATORS_1_2_-1_2&rankName3=TIME_1_0_0_0&rankName4=INDIC-IS_1_2_0_0&rankName5=IND-

TYPE_1_2_0_0&rankName6=GEO_1_2_0_1&rStp=&cStp=&rDCh=&cDCh=&rDM=true&cDM=true&footnes=false&empty=false&wai=false&time_mode=ROLLING&time_most_recent=true&lang=EN&cfo=%23%23%23%2C%23%23%23.%23%23%23 [dostęp: 12.10.2021].

Eurostat, *Social media – statistics on the use by enterprises*, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Social_media_-_statistics_on_the_use_by_enterprises#Use_of_social_media_by_enterprises [dostęp: 12.10.2021].

Eurostat, *Social media use by purpose*, last update: 23.09.2021, https://ec.europa.eu/eurostat/databrowser/view/isoc_cismp/default/table?lang=en%20European%20Commission:%20DG%20Communications%20Networks%20Content%20and%20Technology [dostęp: 12.10.2021].

Friedlmaier M., Tumasjan A., Welpe I.M., *Disrupting Industries with Blockchain: The Industry, Venture Capital Funding, and Regional Distribution of Blockchain Ventures*, 2018, https://scholarspace.manoa.hawaii.edu/bitstream/10125/50333/1/paper0446.pdf [dostęp: 20.10.2021].

Hakerzy mają się w Polsce dobrze. Problem policji, 2021, https://businessinsider.com.pl/technologie/nowe-technologie/cyberprzestepstwa-w-polsce-statystyki/zrn11l7 [dostęp: 9.10.2021].

Kolejne podmioty chcą zwalczać dezinformację, 2021, https://ec.europa.eu/poland/news/211004_deinformation_pl [dostęp: 16.10.2021].

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego Komitetu Regionów. Wytyczne Komisji Europejskiej w sprawie wzmocnienia kodeksu postępowania w zakresie dezinformacji, COM(2021) 262 final, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2021:0262:FIN:PL:PDF [dostęp: 16.10.2021].

Krajowa Rada Radiofonii i Telewizji, *Fake news – dezinformacja online. Próby przeciwdziałania tym zjawiskom z perspektywy instytucji międzynarodowych oraz wybranych państw UE, w tym Polski*, Warszawa 2020, www.gov.pl/web/krrit/fake-news--dezinformacja-online [dostęp: 19.06.2021].

Krajowa Rada Radiofonii i Telewizji, *Zwalczanie dezinformacji w mediach – zalecenia ERGA na podstawie kontroli przestrzegania „Kodeksu postępowania w zakresie dezinformacji”*, 2021, www.gov.pl/web/krrit/zwalczanie-dezinformacji-w-mediach---zalecenia-erga-na-podstawie-kontroli-przestrzegania-kodeku-postepowania-w-zakresie-dezinformacji [dostęp: 16.10.2021].

Krakowiak L., *Cyberprzestępstwa w Polsce są statystycznie niewidoczne*, 2019, www.computerworld.pl/news/Cyberprzestepstwa-w-Polsce-sa-statystycznie-niewidoczne,413041.html [dostęp: 9.10.2021].

Kucharczyk K., *Liczba ataków hakerskich rośnie a wykrywalność spada*, 2021, www.rp.pl/biznes/art8648591-liczba-atakow-hakerskich-rosnie-a-wykrywalnosc-spada [dostęp: 9.10.2021].

Leksykon pojęć na temat technologii blockchain i kryptowalut, red. K. Piech, 2016, www.gov.pl/documents/31305/0/leksykon_pojec_na_temat_technologii_blockchain_i_kryptowalut.pdf [dostęp: 20.10.2021].

Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf [dostęp: 20.10.2021].

Palmer A., *Twitter CEO Jack Dorsey has an idealistic vision for the future of social media and is funding a small team to chase it*, 2019, www.cnbc.com/2019/12/11/twitter-ceo-jack-dorsey-announces-bluesky-social-media-standards-push.html [dostęp: 20.10.2021].

Przestępstwa w sieci, 2013, https://statystyka.policja.pl/st/informacje/85606,Przestepstwa-w-sieci.html [dostęp: 22.10.2021].