ZARZĄDZANIE MEDIAMI
Tom 6(3)2018, s. 221–234
doi:10.4467/23540214ZM.18.016.10568
www.ejournals.eu/ZM

Patrycja Hendzel

Uniwersytet Jagielloński

INTERNETOWE SIECI SPOŁECZNE OPARTE NA ZDECENTRALIZOWANEJ ARCHITEKTURZE (DOSN) A POPRAWA BEZPIECZEŃSTWA I PRYWATNOŚCI UŻYTKOWNIKÓW SOCIAL MEDIÓW

Abstract

ONLINE SOCIAL NETWORKS BASED ON DECENTRALIZED ARCHITECTURE (DOSN) AND IMPROVEMENT OF THE SECURITY AND PRIVACY OF SOCIAL MEDIA USERS

OSN (Online Social Networks), and thus "traditional" social media, are characterized by a centralized architecture. Therefore, all user data is stored logically in the servers of the service provider. This leads to many cases of abuse, such as monetization of users' data, violations of the security and privacy of individuals. The search for alternative solutions combined with the development of information technology has led to the creation of a new type of social media that distinguishes the decentralized structure. DOSN (Decentralized Online Social Networks) are created using P2P technology, a Web-based network or with a Blockchain protocol. Decentralized portals use additional encryption tools and cryptography, so they can ensure better control of users' privacy and increase their autonomy. The aim of this article is to present DOSN as sites providing better mechanisms to protect the privacy and security of users than social media with centralized architecture.

Key words: OSN, DOSN, decentralization, privacy, security, social media, social networks

Wstęp

Na przestrzeni ostatnich lat media społecznościowe zyskały status fenomenu o charakterze globalnym, stając się tym samym immanentnym elementem codzienności milionów użytkowników. Można je uznać za narzędzia internetowe pozwalające na zawieranie i podtrzymywanie relacji społecznych, a także przechowywanie

i udostępnianie treści. Platformy SNS (*Social Network Services*) zarządzają i oferują dostęp online do OSN (*Online Social Networks*)[1]. OSN definiuje się jako usługi internetowe umożliwiające: „1) skonstruowanie publicznego lub półpublicznego profilu w ramach ograniczonego systemu i określenie relacji między własnym profilem a wizytówkami pozostałych użytkowników; 2) udostępnianie informacji i treści wybranym użytkownikom; 3) nawiązywanie interakcji zarówno z »przyjaciółmi«, jak i nieznajomymi"[2]. Internetowe sieci społeczne wspierają działania społeczne zachodzące w Internecie. Oferowane przez nie funkcjonalności można podzielić na trzy kategorie: „wymiana wiadomości umożliwia wysyłanie i odbieranie krótkich tekstów za pomocą czatu, bloga, forum; udostępnianie zasobów pozwala użytkownikom na przesyłanie i pobieranie danych multimedialnych, jak zdjęcia, wideo lub e-booki; czynność przeglądania pozwala użytkownikom wyszukiwać dane, nawiązywać znajomości, grać w gry społecznościowe"[3].

SNS w swojej „tradycyjnej", opartej na ideologii i technologii Web 2.0 formie wyróżnia przede wszystkim scentralizowana struktura działania. Serwisy społecznościowe posiadają wyłączne prawo nie tylko do decydowania o kształcie portalu i panujących w jego granicach zasadach, ale także do kontrolowania wszystkich danych udostępnionych przez użytkowników[4]. W konsekwencji infrastruktura nadzorowana jest przez pojedynczy, autorytatywny organ, co implikuje wielopłaszczyznową „nierównowagę w ekosystemie Internetu"[5].

Budulcem portali społecznościowych pozostają dane użytkowników, którzy są gotowi je udostępniać, by nawiązywać i podtrzymywać relacje z jednostkami należącymi do serwisu. Opisywany model funkcjonowania aplikacji Web 2.0 sprawia, że „coraz więcej danych z sieci społecznościowych jest publicznie dostępnych i analizowanych w celach komercyjnych i badawczych"[6]. Prowadzi to do wielu nadużyć związanych z wykorzystywaniem użytkowników i eksploracją ich informacji. Struktura social mediów połączona z modelem biznesowym opartym na reklamach implikuje bowiem między innymi monetyzowanie i przywłaszczenie wartości, wyzyskiwanie darmowej pracy *userów*, ich dehumanizację oraz zwiększoną inwigilację[7].

Wydarzenia ostatnich miesięcy, a więc wyciek PII (*Personally Identifiable Information*) pond 87 milionów użytkowników portalu społecznościowego Facebook

[1] T. Paul, S. Buchegger, T. Strufe, *Decentralizing Social Networking Services*, [w:] N. Blefari-Melazzi, G. Bianchi, L. Salgarelli (eds.), *Trustworthy Internet*, Springer-Verlag, Milan 2011, s. 187.

[2] Tamże.

[3] Tamże.

[4] C.A. Yeung, I. Liccardi, K. Lu, O. Seneviratne, T. Berners-Lee, *Decentralization: The Future of Online Social Networking*, „W3C Workshop on the Future of Social Networking Position Papers" 2009, s. 1.

[5] S.R. Chowdhury, A.R. Roy, M. Shaikh, K. Daudjee, *A Taxonomy of Decentralized Online Social Networks*, „Peer-to-Peer Networking and Applications" 2014, s. 1.

[6] Y. Xie, M. Zheng, *A Differentiated Anonymity Algorithm for Social Network Privacy Preservation*, „Algorithms" 2016, t. 9, nr 4, s. 85.

[7] C. Fuchs, *Social Media: A Critical Introduction*, Sage Publications, Los Angeles–London 2014.

na rzecz zewnętrznego podmiotu, unaoczniły niewystarczające i łatwe do obejścia protokoły zabezpieczające prywatność użytkowników, a także brak transparentności funkcjonowania portali tego typu[8]. W konsekwencji uzasadnione wydaje się podawanie w wątpliwość możliwości zapewnienia jednostkom wystarczającego bezpieczeństwa przez scentralizowane media społecznościowe.

Utrata zaufania użytkowników do dostawców witryn jest jedną z przyczyn poszukiwania nowych rozwiązań w dziedzinie portali społecznościowych[9]. Ograniczenia „tradycyjnych" OSN połączone z zastrzeżeniami dotyczącymi bezpieczeństwa doprowadziły do pojawienia się witryn o zdecentralizowanej strukturze bez nadrzędnego operatora[10]. PeerSoN, pierwsza kompletna, dwuwarstwowa architektura DOSN obejmująca pełne szyfrowanie i podejście P2P (*Peer-to-Peer*), czyli rozproszoną, autonomiczną sieć współpracujących ze sobą użytkowników[11], stworzona została jeszcze w 2009 roku jako odpowiedź na nasilające się problemy z bezpieczeństwem w OSN[12].

DOSN (*Decentralized Online Social Networks*), alternatywa dla dostępnych dotychczas serwisów społecznościowych, dzięki oparciu na schemacie zdecentralizowanym pozwalają na „zwiększenie autonomii użytkowników w zakresie przechowywania i kontrolowania praw dostępu do ich treści"[13]. Jako że zdecentralizowane media społecznościowe cieszą się coraz większą popularnością, analizie należy poddać schemat ich działania oraz oferowane przez nie możliwości zabezpieczenia użytkowników i ich danych. Celem tego artykułu jest zatem charakterystyka DOSN jako witryn zapewnianiających lepsze mechanizmy ochrony prywatności i bezpieczeństwa użytkowników od mediów społecznościowych o scentralizowanej architekturze.

Rezultaty: DOSN a poprawa bezpieczeństwa i prywatności użytkowników

DOSN określa się jako „OSN wdrożony w rozproszony i zdecentralizowany sposób"[14]. Istnieje kilka metod tworzenia witryny o strukturze rozproszonej. DOSN można osiągnąć, „dodając właściwość *social* lub *decentralized* do istniejącego już

[8] J. Isaak, M.J. Hanna, *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection*, „Computer. IEEE Computer Society" 2018, t. 51, nr 8, s. 56.

[9] A. Datta, S. Buchegger, L.H. Vu, T. Strufe, K. Rzadca, *Decentralized Online Social Networks*, [w:] B. Furht (ed.), *Handbook of Social Network Technologies and Applications*, Springer-Verlag, New York 2010, s. 351.

[10] S.R. Chowdhury, A.R. Roy, M. Shaikh, K. Daudjee, *A Taxonomy...*, dz. cyt., s. 2.

[11] Tamże.

[12] S. Buchegger, D. Schiöberg, L.H. Vu, A. Datta, *PeerSoN: P2P Social Networking: Early Experiences and Insights*, „Proceedings of the Second ACM EuroSys Workshop on Social Network Systems" 2009, s. 46.

[13] Tamże, s. 2.

[14] A. De Salve, P. Mori, L. Ricci, *A Survey on Privacy in Decentralized Online Social Networks*, „Computer Science Review" 2018, nr 27, s. 156.

systemu, tym samym dokonując jego przekształcenia na przykład poprzez przejęcie scentralizowanych OSN i ich zdecentralizowanie"[15]. Możliwe jest również „dodanie składnika *social* do zdecentralizowanych aplikacji, które nie posiadają jeszcze komponentu społecznościowego"[16]. DOSN mogą być także tworzone „po jednoczesnym dodaniu do scentralizowanych aplikacji komponentu *decentralized* i *social*"[17].

Zdecentralizowane sieci społeczne zapewniają „różne usługi w zakresie komputerów społecznych w rozproszonym środowisku". Dają one większe możliwości niż te, które oferowane były przez dostępne dotychczas OSN. By uzyskać niezależność od scentralizowanego operatora, witryny DOSN oparte są najczęściej na modelach sieci zaufanych serwerów (*Web-based Decentralized OSN*), P2P (*Peer-to-Peer*), a od niedawna także zdecentralizowanej bazy danych (*Blockchain*). Dzięki temu DOSN cechuje „obniżenie kosztów dostawcy", „lepsza kontrola prywatności użytkowników" oraz „nieustanny rozwój innowacyjności"[18]. Oznacza to, że każdy użytkownik, w zależności od architektury, kontekstu lub określonej sytuacji, może działać zarówno jako serwer, jak i jako klient[19].

Mechanizm ochrony danych użytkowników DOSN opiera się na implementacji dwóch elementów: szyfrowania oraz decentralizacji. Szyfrowanie, które pozostaje niezależne od operatora, „umożliwia użytkownikowi ochronę danych przed nieautoryzowanym dostępem"[20]. Dzięki protokołom takim jak ABE (*Attribute Based Encryption*) klienci zyskują wyłączne prawo „definiowania dostępu do swoich danych" – może być on przyznany na podstawie określonych kryteriów, na przykład społecznych, „jak bycie znajomym lub członkiem pewnej grupy"[21]. Decentralizacja tworzonych, przechowywanych i udostępnianych danych zapobiega natomiast sytuacji, w której „pojedynczy, nadrzędny podmiot może obserwować profil i dostęp do niego, a także ma możliwość kontrolowania przepływu danych w sieci społecznościowej"[22].

Na strukturę DOSN składają się zazwyczaj trzy główne poziomy: sieć społeczna (*social network*) wytworzona między użytkownikami, narzędzia wykorzystywane przez użytkowników (laptopy, PC, tablety, urządzenia mobilne) oraz infrastruktura, na której zbudowany jest serwis[23]. Dodatkowo model funkcjonowania DOSN implikuje powstanie „wielu poziomów architektonicznych", przy czym każdy z nich

[15] A. Datta, S. Buchegger, L.H. Vu, T. Strufe, K. Rzadca, *Decentralized Online...*, dz. cyt., s. 352.
[16] Tamże.
[17] Tamże.
[18] Tamże, s. 350.
[19] A. De Salve, P. Mori, L. Ricci, *A Survey...*, dz. cyt., s. 156.
[20] F. Tegeler, D. Koll, X. Fu, *Gemstone: Empowering Decentralized Social Networking with High Data Availability*, „Global Telecommunications Conference – GLOBECOM" 2011, s. 1.
[21] Tamże.
[22] Tamże.
[23] D. Koll, J. Li, X. Fu, *The Good Left Undone: Advances and Challenges in Decentralizing Online Social Networks*, „Computer Communications" 2017, t. 108.

cechuje się odrębnymi funkcjami[24]. Portale zapewniające niezależność od nadrzędnego podmiotu mogą więc posiadać strukturę w całości zdecentralizowaną – „architektura ta nie narzuca żadnych szczególnych warunków dotyczących miejsca przechowywania danych, ponieważ *content* użytkowników znajduje się w losowych węzłach sieci"[25]. W architekturze częściowo zdecentralizowanej (*semi-decentralized*) grupa użytkowników (super-hosty) staje się odpowiedzialna za „przechowywanie i zarządzanie danymi wszystkich użytkowników" wewnątrz sieci[26]. Tym sposobem zarządzaniem danymi nie zajmuje się cała społeczność, lecz grupa *userów* posiadająca narzędzia o zwiększonej mocy obliczeniowej – rozwiązanie to pozwala na odciążenie części użytkowników bez konieczności posiadania centralnego organu organizującego i przechowującego dane. Natomiast DOSN o architekturze hybrydowej co do zasady „stosują podejście P2P", ale ich funkcjonowanie wspierane jest także przez dodatkowe, „zewnętrzne usługi zapewniane przez scentralizowaną jednostkę (takie jak chmury, prywatne serwery, Dropbox itp.)"[27]. Architektura ta może być stosowana na przykład wtedy, gdy użytkowanie gotowych rozwiązań jest bardziej opłacalne niż tworzenie ich od podstaw. Takie rozwiązanie z jednej strony umożliwia i gwarantuje użytkownikom „korzystanie ze stale dostępnych zasobów", z drugiej zaś wiąże się ze zwiększeniem kosztów eksploatacji[28].

Powstaniu zdecentralizowanych mediów społecznościowych towarzyszy potrzeba bezwzględnej ochrony użytkowników, ich praw, prywatności, wartości oraz danych. Zamiar ten realizuje się przez „dążenie do stworzenia systemu, który czyni technologicznie trudniejszym (lub niemożliwym) naruszanie prywatności użytkowników i eksplorację ich danych na dużą skalę, nawet jeśli jednostki nadal korzystają z zalet sieci społecznych"[29]. Mając w pamięci nadużycia scentralizowanych monopolistów społecznościowych, za zrozumiałą należy uznać oddolną „motywację do przekazania kontroli nad danymi z powrotem użytkownikom"[30].

Scentralizowane media społecznościowe oferują użytkownikom „bezpłatną" usługę „z iluzją nieskończonej przestrzeni dyskowej zapewnianej przez dostawcę"[31]. Portale te funkcjonują w oparciu o model reklamowy, co prowadzi do nieustannej monetyzacji danych użytkowników. Właściwością odróżniającą DOSN od typowych social mediów jest między innymi redefinicja wybranego modelu biznesowego – powstaniu DOSN przyświecała bowiem idea „stworzenia społeczności internetowej dobrowolnego uczestnictwa użytkowników"[32]. Zdecentralizowana sieć to „nieskomercjalizowana, samoregulująca się usługa", która pozwala użytkownikom

[24] A. De Salve, P. Mori, L. Ricci, *A Survey...*, dz. cyt., s. 156.
[25] Tamże.
[26] Tamże.
[27] Tamże.
[28] Tamże.
[29] A. Datta, S. Buchegger, L.H. Vu, T. Strufe, K. Rzadca, *Decentralized Online...*, dz. cyt., s. 357.
[30] Tamże.
[31] S.R. Chowdhury, A.R. Roy, M. Shaikh, K. Daudjee, *A Taxonomy...*, dz. cyt.
[32] Tamże.

na utrzymywanie relacji społecznych bez wykorzystywania finansowego ze strony nadrzędnego operatora[33]. *User*, dołączając do DOSN, w zależności od architektury portalu „przechowuje dane użytkowników i wykonuje dla nich obliczenia, ponieważ w zamian otrzymuje te same usługi od innych uczestników sieci"[34]. Ponadto dobrowolny model serwisu zdecentralizowanego może ulec rozszerzeniu, gdy „użytkownicy posiadający narzędzia o wyższej pojemności pamięci masowej i obliczeniowej oraz przepustowości sieci zaczną oferować usługi dla sieci społecznościowej"[35]. Pozostali użytkownicy, zgadzając się na reklamy lub dokonując opłaty, mogą zatem korzystać z serwisu bez konieczności zarządzania węzłem sieciowym[36].

Zdecentralizowane media społecznościowe rozwiązują dodatkowo problem kontroli treści i własności intelektualnej użytkownika w środowisku OSN. W DOSN użytkownik zyskuje kontrolę nad tym, kto posiada dostęp do jego *contentu* oraz co może z nim zrobić. Weryfikacja ta może być połączona z modelami licencjonowania wybranymi przez *usera*, na przykład licencjami Creative Commons[37]. Innymi słowy, to użytkownik dokona wyboru zakresu ochrony prawnej, która będzie obejmować udostępniane treści. Tym samym głównym beneficjentem tej ochrony stanie się podmiot bezpośrednio zainteresowany – twórca, a nie – jak dotychczas – dostawca usługi. Stanowi to wyraźne odejście od opresyjnego, rozpowszechnionego obecnie modelu licencjonowania treści i przywłaszczania wartości przez OSN. Jednocześnie użytkownik zyskuje możliwość samodzielnego określenia swoich potrzeb oraz najbardziej przydatnego w danej sytuacji modelu zabezpieczenia praw związanych z udostępnianymi treściami.

Dyskusja: Architektura OSN a DOSN. Różnice w mechanizmach prywatności i bezpieczeństwa użytkowników

Typowe media społecznościowe, takie jak Facebook, MySpace, Twitter, Flickr czy YouTube, bazują na technologii sieciowej w ramach architektury klient–serwer[38]. Oznacza to, że w scentralizowanych OSN wszystkie dane użytkowników przechowywane są w sposób logiczny w jednym miejscu. Dane udostępniane przez klientów stanowią podstawowy sposób finansowania serwisu. Za zarządzanie „magazynem danych" w OSN odpowiadać musi więc jeden operator, który zapewnia zasoby

[33] A. Datta, S. Buchegger, L.H. Vu, T. Strufe, K. Rzadca, *Decentralized Online...*, dz. cyt., s. 359.
[34] S.R. Chowdhury, A.R. Roy, M. Shaikh, K. Daudjee, *A Taxonomy...*, dz. cyt.
[35] Tamże.
[36] Tamże.
[37] Tamże, s. 589.
[38] M.H. Tran, V.S. Nguyen, S.V. Uyen Ha, *Decentralized Online Social Network Using Peer-to-Peer Technology*, „REV: Journal on Electronics and Communications" 2015, t. 5, nr 1–2, s. 30.

dla stałości i niezawodności usługi[39]. Centralizacja ta prowadzi jednak do wielu patologii mających związek zarówno ze strukturą serwisów, jak i wynikającego z niej braku transparentności[40].

OSN posiadają pozbawiony elastyczności interfejs, do którego muszą się dostosować użytkownicy i programiści. Ograniczenia te sprawiają, że zanika poczucie kreatywności i wolności – „programiści muszą się ograniczyć do zestawu funkcji oferowanych przez bazowy interfejs API (*Application Programming Interface*)"[41]. Równocześnie klienci, by korzystać z poszczególnych witryn, są zmuszeni zaakceptować politykę serwisów, która skutkuje między innymi monetyzowaniem ich danych i wartości do celów reklamowych[42]. Na podstawie zapisów regulaminowych osoby te przekazują zatem prawo do zarządzania swoimi danymi zewnętrznemu podmiotowi. Agregacja informacji zbieranych przez dostawców usługi sprawia natomiast, że operatorzy platform „uzyskują głęboki wgląd w relacje społeczne użytkownika, osobiste opinie, preferencje ekonomiczne lub polityczne i na tych danych opierają swój model biznesowy"[43]. Co więcej, udostępniane przez użytkowników wrażliwe informacje typu PII nie są zabezpieczane w należyty sposób. Z tego powodu dane klientów mogą być narażone na wewnętrzne nadużycia, wycieki lub zewnętrzne ataki hakerskie[44]. Biorąc powyższe pod uwagę, można uznać, że kwestie prywatności i bezpieczeństwa użytkowników to zasadnicze problemy w środowisku scentralizowanych OSN.

Polityka prywatności większości scentralizowanych portali społecznościowych składa się z czterech różnych warstw danych, które zostają udostępnione przez klienta serwisu. Pierwszy typ danych jest tworzony podczas rejestracji użytkownika i obejmuje informacje pozwalające na „identyfikację dostawcy danych w unikatowy sposób spośród wszystkich innych użytkowników sieci społecznościowej"[45]. W ramach *networkingu* kreowana jest następnie sieć danych, „która udostępniana ma być innym użytkownikom w celu skonstruowania sieci społecznej dla dostawcy informacji"[46]. *Content* stanowi tę warstwę danych, która budowana jest na podstawie rzeczywistej treści tworzonej przez uczestnika sieci społecznej" – jednostki korzystające z serwisu mają możliwość wyboru stopnia widoczności publikowanych przez siebie postów[47]. Na warstwę danych o aktywnościach użytkownika w portalu składają się natomiast między innymi „logowania do serwerów, pliki *cookies*, a także inne informacje na temat działań dostawcy danych w serwisie

[39] T. Paul, S. Buchegger, T. Strufe, *Decentralizing Social...*, dz. cyt., s. 188.

[40] C. Fuchs, *Social Media*…, dz. cyt.

[41] C.A. Yeung, I. Liccardi, K. Lu, O. Seneviratne, T. Berners-Lee, *Decentralization...*, dz. cyt., s. 1.

[42] Tamże.

[43] F. Tegeler, D. Koll, X. Fu, *Gemstone...*, dz. cyt., s. 1.

[44] Tamże.

[45] L. Wu, M. Madei, K. Ghazinour, K. Baker, *Analysis of Social Networking Privacy Policies*, „Proceedings of the 2010 EDBT/ICDT Workshops" 2010.

[46] Tamże.

[47] Tamże.

społecznościowym"[48]. W dalszej kolejności są one zwykle „agregowane i dostarczane podmiotom zewnętrznym"[49] w celach analitycznych i biznesowych.

Należy zauważyć, że chęć partycypowania w danej sieci społecznej jest związana z koniecznością udostępniania zewnętrznemu podmiotowi wielu szczegółowych informacji typu PII. Scentralizowana architektura mediów społecznościowych zdaje się jednak nie zapewniać im należytej ochrony. System weryfikacji użytkownika nie eliminuje tworzenia fałszywych kont mających na celu atak na innych *userów*[50]. Co prawda użytkownicy OSN mogą decydować o stopniu widoczności niektórych informacji i postów znajdujących się wewnątrz ich osobistego profilu, ale w pełni publiczny charakter podejmowanych aktywności w witrynie sprawia, że osoba postronna może z łatwością „zrekonstruować siatkę znajomych danego użytkownika"[51]. Zasadniczym i alarmującym problemem mediów społecznościowych o scentralizowanej strukturze pozostaje także przekazywanie danych użytkowników zewnętrznym podmiotom bez ich zgody i wiedzy.

W opozycji do opisywanych serwisów pozostają witryny typu DOSN. Tworzone mogą być one na przykład na podstawie sieci zaufanych serwerów (*Web-based Decentralized OSN*), które wykorzystują infrastrukturę rozproszonego serwera sieciowego[52]. W tym celu niezbędne jest „nabycie przestrzeni internetowej lub wdrożenie dodatkowych serwerów sieciowych za pośrednictwem użytkowników" portalu[53]. Dzięki tej zależności użytkownicy zyskują możliwość publikacji w sposób analogiczny do stron internetowych „w swojej własnej przestrzeni internetowej i mogą lokalnie zarządzać regułami dostępu tak, aby regulować i pobierać ograniczone atrybuty oraz zasoby dla wybranych użytkowników"[54]. Trzeba wspomnieć, *że* partycypowanie w tego rodzaju sieci wymusza na użytkownikach nie tylko „potrzebę dostępu do niezawodnej przestrzeni internetowej, w której wizytówki odpowiednich osób nie są dostępne", lecz również posiadanie umiejętności technicznych związanych z „samodzielnym skonfigurowaniem serwera WWW"[55].

Z kolei model P2P wykorzystywany w budowaniu DOSN pozwala na osiągnięcie w rozproszonym środowisku „niezawodności w dystrybucji treści i autonomii w administrowaniu"[56]. Architektura niweluje problem heterogeniczności, w swoje działania angażując „hosty z wystarczającą pamięcią, przepustowością i mocą przetwarzania, aby wspierać innych użytkowników w złożonych operacjach"[57].

[48] Tamże.

[49] Tamże.

[50] S. Mahmood, *Online Social Networks: Privacy Threats and Defenses*, [w:] R. Chbeir, B. Al Bouna (eds.), *Security and Privacy Preserving in Social Networks*, Springer, Vienna 2013, s. 55.

[51] Tamże, s. 54.

[52] T. Paul, S. Buchegger, T. Strufe, *Decentralizing Social...*, dz. cyt., s. 191.

[53] Tamże.

[54] Tamże.

[55] Tamże.

[56] M.H. Tran, V.S. Nguyen, S.V. Uyen Ha, *Decentralized Online...*, dz. cyt., s. 31.

[57] Tamże.

W granicach witryny znajdują się dwa rodzaje odbiorców: host i super-host. Super-hosty dzięki zwiększonym mocom obliczeniowym „działają jako *proxy* dla zwykłych hostów i angażują się w mechanizmy *routingu* wiadomości”[58].

Podkreślenia wymaga fakt, iż architektura P2P pierwotnie została stworzona w celu udostępniania i pobierania „porównywalnie niewielu dużych obiektów danych, takich jak pliki muzyczne i filmy”[59]. Profile użytkowników OSN oparte na protokole P2P zawierają natomiast wiele atrybutów – „ich replikacja i dostarczenie danych podczas pobierania stron wymaga osobnej rejestracji każdego zasobu w celu znalezienia repliki, co biorąc pod uwagę liczbę atrybutów, staje się zadaniem skomplikowanym i czasochłonnym”[60]. Oznacza to, że zbudowanie DOSN opartych wyłącznie na protokole P2P „z rozproszoną pamięcią masową, systemami replikacji i potencjalną potrzebą skalowalności”[61], w których uczestniczy wiele użytkowników, wymaga nie tylko dużej mocy obliczeniowej, ale także „rozwoju parametrów bezpieczeństwa w mechanizmie *publish*/*subscribe*”[62].

Obecnie można obserwować coraz częstsze powstawanie zdecentralizowanych sieci społecznych opartych na architekturze Blockchain. Jest to „połączony łańcuch bloków”, przy czym każdy blok „zawiera odpowiadający mu rekord oraz znacznik czasu (*timestamp*)”[63]. Blockchain bazuje na sieci P2P, w której „tworzona jest chronologiczna baza danych transakcji zgrupowanych w bloku i zatwierdzonych przez sieć komputerów, z wieloma blokami dodawanymi jeden po drugim w łańcuchu”[64]. Kontrola i dodawanie bloków do łańcucha odbywa się dzięki mechanizmom takim jak PoW (*Proof-of-work*) oraz PoS (*Proof-of-stake*)[65]. Rozwiązanie to uniemożliwia „nieuprawnioną modyfikację danych” znajdujących się wewnątrz bloku[66].

W odróżnieniu od scentralizowanych OSN, w których korzyści finansowe wynikające z aktywności użytkowników uzyskiwał jedynie serwis, portale oparte na protokole Blockchain przewidują gratyfikację dla użytkowników za tworzone przez nich treści[67]. Wkład użytkownika w rozwój sieci społecznej jest więc monitorowany i synchronizowany z odpowiednim systemem nagradzania[68]. Dodatkowo sieci społeczne zbudowane na technologii Blockchain dzięki rozproszeniu pozwalają

[58] Tamże.

[59] T. Paul, S. Buchegger, T. Strufe, *Decentralizing Social...*, dz. cyt., s. 192.

[60] Tamże.

[61] A. Datta, S. Buchegger, L.H. Vu, T. Strufe, K. Rzadca, *Decentralized Online...*, dz. cyt., s. 353.

[62] Tamże.

[63] Y. Chen, Q. Li, H. Wang, *Towards Trusted Social Networks with Blockchain Technology*, „Symposium on Foundations and Applications of Blockchain” 2018.

[64] A. Chakravorty, C. Rong, *Ushare: User Controlled Social Media Based on Blockchain*, „ACM IMCOM: 12th International Conference on Ubiquitous Information Management and Communication” 2018.

[65] Tamże.

[66] Y. Chen, Q. Li, H. Wang, *Towards Trusted...*, dz. cyt.

[67] A. Asharaf, A. Adarsh, *Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities*, IGI Global, Hershey 2017, s. 83.

[68] Tamże.

na koncentrację na użytkowniku (*user centric SN*), co daje mu możliwość „kontrolowania, śledzenia i bezpiecznego udostępniania treści”[69]. Platformy tego typu, ze względu na zdecentralizowaną architekturę Blockchain, ma ponadto cechować udoskonalony system dbania o prywatność użytkownika, anonimowość oraz brak wewnętrznej cenzury[70].

Na strukturę ochrony prywatności użytkownika w DOSN składają się dwa elementy: model prywatności oraz zarządzanie polityką prywatności. Model prywatności jest to „zdolność DOSN do zapewnienia userowi różnych rodzajów polityk prywatności, umożliwiając przy tym użytkownikowi określenie zbioru członków, którzy będą posiadać dostęp do jego treści”[71]. Wybór ten dokonywany jest na podstawie funkcji typowych dla OSN, takich jak „typ przyjaźni, zainteresowania, szkoła itp.”[72]. Zarządzanie polityką prywatności opiera się natomiast na „gwarancji DOSN co do egzekwowania określonych przez użytkownika zasad dla każdej treści przy użyciu odpowiednich mechanizmów bezpieczeństwa”[73]. Dzięki temu jednostki posiadają całkowitą kontrolę nad treściami udostępnionymi w portalu, zachowując jednocześnie pełnię praw autorskich.

W celu zwiększenia bezpieczeństwa i ochrony prywatności użytkowników zdecentralizowane portale stosują rozwiązania obejmujące szyfrowanie lub kryptografię[74]. Implementacja kryptografii w DOSN opiera się na „mechanizmach szyfrowania wykonujących transformację danych tak, aby jedynie autoryzowani użytkownicy [posiadający odpowiedni klucz dostępu – przyp. P.H.] mogli zrozumieć *content*”[75]. Wiąże się to jednak ze znacznym obciążeniem całego systemu z powodu liczby tworzonych kluczy oraz wolumenu kolejnych szyfrowań. Za każdym razem, gdy użytkownik definiuje lub zmienia politykę prywatności swoich treści, musi zainicjować te działania przez „wygenerowanie struktury danych szyfrowania, np. kluczy kryptograficznych wymaganych do ochrony informacji, dystrybucję ich wśród odpowiedniego zestawu *userów* i zaszyfrowanie *contentu* przed zapisem na dedykowanym hoście”[76]. Mechanizm ten może obniżać wydajność całego systemu, zwłaszcza gdy „zestaw autoryzowanych użytkowników określonych w polityce prywatności jest duży i często aktualizowany”[77].

W tradycyjnych OSN dane użytkowników przechowywane są na serwerach dostawcy usługi społecznościowej. Oznacza to, że *user* nie ma możliwości pełnego zarządzania informacjami, które zostały wprowadzone do serwisu. Użytkownik

[69] A. Chakravorty, C. Rong, *Ushare: User Controlled...*, dz. cyt.

[70] Tamże.

[71] A. De Salve, P. Mori, L. Ricci, *A Survey...*, dz. cyt., s. 157.

[72] Tamże.

[73] Tamże.

[74] M.C. Jyoti, *Privacy Policy in Decentralized Online Social Networks: Cryptography*, „International Journal of Recent Research Aspects” 2017, t. 4, nr 2, s. 210.

[75] Tamże.

[76] Tamże.

[77] Tamże.

jest pozbawiony kontroli nad swoimi informacjami – „nie może dokonać transferu treści na inną platformę lub całkowicie ich usunąć”[78]. Dodatkowo scentralizowana architektura OSN jest „bardziej podatna na rozprzestrzenianie się wirusów bądź złośliwego oprogramowania”[79]. Centralizacja agregacji danych prowadzi do wielu problemów związanych z niewystarczającą ochroną prywatności i bezpieczeństwa użytkowników.

Zdecentralizowane sieci społeczne rozwiązują główne obawy dotyczące nadzoru nad danymi, gdyż są one „przechowywane na hostach użytkowników należących do DOSN lub wybranych przez użytkowników serwerach bez centralnego organu kontrolującego i przechowującego dane”[80]. Co więcej, to użytkownicy DOSN mogą definiować politykę prywatności serwisu, która ma zazwyczaj formę „prostej instrukcji określającej, kto może uzyskać dostęp do ich *contentu*”[81]. Skutkuje to przeniesieniem kontroli nad danymi użytkownika na należący do niego host, który jednocześnie współtworzy dany system[82]. W rezultacie „prywatność w DOSN gwarantowana jest poprzez umożliwienie użytkownikom określenia swoich preferencji co do tego, które informacje powinny zostać ujawnione innym *userom*”, natomiast schemat ten chroniony jest dodatkowo przez „odpowiednie mechanizmy bezpieczeństwa przeznaczone do ochrony poufności tych treści”[83].

Typowe OSN sprawiają, że dane użytkowników są scentralizowane lub rozproszone (lecz wciąż połączone) – tym sposobem zarówno dostawca serwisu społecznościowego, jak i podmioty zewnętrzne są w posiadaniu PII i treści tworzonych przez *usera*, które mogą być narażone na nadmierną eksplorację, reklamę bezpośrednią czy nawet cenzurę[84]. Podejście zdecentralizowane ma z kolei wspierać wolność słowa użytkowników. Struktura DOSN pozwala bowiem na swobodny przepływ informacji, co powinno wpływać na zmniejszenie cenzury wewnątrz systemu. Sam proces tworzenia i udostępniania danych przez jednostki lepiej wpisuje się natomiast „w architekturę P2P niż dotychczasowy model klient–serwer”[85]. Użytkownicy, wybierając zdecentralizowane sieci społeczne, pozostają również wolni od „ograniczeń nałożonych przez dostawcę usług – teraz, a także w przyszłości”[86].

Aby jednak zdecentralizowane media społecznościowe zostały zaadaptowane przez użytkowników na szeroką, porównywalną z tradycyjnymi OSN skalę, muszą spełniać określone wymogi funkcjonalne. Przejście *userów* z OSN do środowisk

[78] G. Groh, S. Birnkammerer, *Privacy and Information Markets: Controlling Information Flows in Decentralized Social Networking*, „IEEE International Conference on Privacy, Security, Risk, and Trust” 2011, s. 856.

[79] A. Datta, S. Buchegger, L.H. Vu, T. Strufe, K. Rzadca, *Decentralized Online...*, dz. cyt., s. 358.

[80] A. De Salve, P. Mori, L. Ricci, *A Survey...*, dz. cyt., s. 157.

[81] Tamże.

[82] Tamże.

[83] Tamże.

[84] A. Datta, S. Buchegger, L.H. Vu, T. Strufe, K. Rzadca, *Decentralized Online...*, dz. cyt., s. 358.

[85] Tamże.

[86] Tamże.

DOSN będzie możliwe dzięki uzyskaniu chociażby przejrzystego i nietrudnego w obsłudze interfejsu serwisu. W ramach „pojedynczego interfejsu integracyjnego" użytkownik nieposiadający statusu eksperta w dziedzinie informatyki powinien mieć dostęp do tych danych i funkcji, „które pozwolą mu na łatwą publikację, wyszukiwanie, pobieranie profili i atrybutów"[87]. Co więcej, konieczne jest „umożliwienie rekonstrukcji społecznego wykresu relacji między użytkownikami, pozwalającego na uproszczoną komunikację typu *publish*/*subscribe*, jasną kontrolę dostępu i zawieranie relacji"[88]. Funkcjonowanie serwisu DOSN musi mieć charakter stabilny – „rozproszona architektura portalu nie może prowadzić do przerwanej dostępności danych lub usług"[89]. Dodatkowej ochronie powinny także podlegać prywatność i bezpieczeństwo jednostek korzystających ze strony[90].

Konkluzje

Mimo że pierwsze portale o zdecentralizowanej architekturze zaczęły się pojawiać w 2009 roku, a więc kilka lat po powstaniu serwisów takich jak MySpace, Facebook czy YouTube, strony te wciąż pozostają w początkowej fazie rozwoju. Kilka miesięcy temu Steemit, jedna z największych witryn o rozproszonej strukturze, ogłosiła, że w jej granicach pozostaje zarejestrowanych ponad milion aktywnych użytkowników[91]. W porównaniu ze społecznością Facebooka, liczącą ponad 2,27 miliarda aktywnych użytkowników miesięcznie[92], statystyki te nie napawają optymizmem. DOSN, charakteryzujące się lepszymi rozwiązaniami technologicznymi oraz bardziej zaawansowanymi protokołami ochrony bezpieczeństwa i prywatności użytkowników, wciąż nie przeniknęły do masowej świadomości odbiorców. Przeszkodami w akceptacji portali o zdecentralizowanej architekturze mogą być: nieczytelny i skomplikowany w obsłudze interfejs, wymóg posiadania specjalistycznej wiedzy, spełnienie określonych warunków technicznych, a od niedawna także konieczność otwarcia portfela kryptowalutowego. To z jednej strony.

Z drugiej zdecentralizowane portale społecznościowe nowej generacji coraz częściej w swoim działaniu wykorzystują technologię Blockchain oraz mechanizmy kryptograficzne – czyli narzędzia tożsame z rynkiem kryptowalutowym. Co ciekawe, ponad 74% „zamożnych" milenialsów w Stanach Zjednoczonych uważa

[87] T. Paul, S. Buchegger, T. Strufe, *Decentralizing Social...*, dz. cyt., s. 189.

[88] Tamże.

[89] Tamże.

[90] Tamże.

[91] Steemitblog, *1,000,000 Steem Accounts*, https://steemit.com/steem/@steemitblog/1-000-000-steem-accounts (dostęp: 10.11.2018).

[92] Statista, *Number of Monthly Active Facebook Users Worldwide as of 3rd Quarter 2018 (in Millions)*, https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (dostęp: 10.11.2018).

technologię Blockchain za instrument poprawiający bezpieczeństwo, a kolejne 25% jest w posiadaniu kryptowalut[93]. Wskazuje to na krystalizowanie się nowej grupy odbiorców dla portali typu DOSN, która może zachowywać potencjał wzrostowy. Jednostki te mogą bowiem poszukiwać alternatywnych rozwiązań bez organów centralnego sterowania zarówno w systemie monetarnym, jak i, być może, w dotychczasowych, scentralizowanych social mediach.

Bibliografia

Asharaf A., Adarsh A., *Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities*, IGI Global, Hershey 2017.

Buchegger S., Schiöberg D., Vu L.H., Datta A., *PeerSoN: P2P Social Networking: Early Experiences and Insights*, „Proceedings of the Second ACM EuroSys Workshop on Social Network Systems" 2009, s. 46–52.

Chakravorty A., Rong C., *Ushare: User Controlled Social Media Based on Blockchain*, „ACM IMCOM: 12th International Conference on Ubiquitous Information Management and Communication" 2018.

Chen Y., Li Q., Wang H., *Towards Trusted Social Networks with Blockchain Technology*, „Symposium on Foundations and Applications of Blockchain" 2018.

Chowdhury S.R., Roy A.R., Shaikh M., Daudjee K., *A Taxonomy of Decentralized Online Social Networks*, „Peer-to-Peer Networking and Applications" 2014.

Datta A., Buchegger S., Vu L.H., Strufe T., Rzadca K., *Decentralized Online Social Networks*, [w:] Furht B. (ed.), *Handbook of Social Network Technologies and Applications*, Springer-Verlag, New York 2010.

De Salve A., Mori P., Ricci L., *A Survey on Privacy in Decentralized Online Social Networks*, „Computer Science Review" 2018, nr 27, s. 154–176.

Edelman, *Millennials with Money. October 2018*, https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/Millennials-With-Money-2018.pdf.

Fuchs C., *Social Media: A Critical Introduction*, Sage Publications, Los Angeles–London 2014.

Groh G., Birnkammerer S., *Privacy and Information Markets: Controlling Information Flows in Decentralized Social Networking*, „IEEE International Conference on Privacy, Security, Risk, and Trust" 2011, s. 856–861.

Isaak J., Hanna M.J., *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection*, „Computer. IEEE Computer Society" 2018, t. 51, nr 8, s. 56–59.

Jyoti M.C., *Privacy Policy in Decentralized Online Social Networks: Cryptography*, „International Journal of Recent Research Aspects" 2017, t. 4, nr 2, s. 207–217.

Koll D., Li J., Fu X., *The Good Left Undone: Advances and Challenges in Decentralizing Online Social Networks*, „Computer Communications" 2017, t. 108, s. 36–51.

Mahmood S., *Online Social Networks: Privacy Threats and Defenses*, [w:] R. Chbeir, B. Al Bouna (eds.), *Security and Privacy Preserving in Social Networks*, Springer, Vienna 2013.

Paul T., Buchegger S., Strufe T., *Decentralizing Social Networking Services*, [w:] N. Blefari-Melazzi, G. Bianchi, L. Salgarelli (eds.), *Trustworthy Internet*, Springer-Verlag, Milan 2011.

[93] Edelman, *Millennials with Money. October 2018*, https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/Millennials-With-Money-2018.pdf (dostęp: 10.11.2018).

Statista, *Number of Monthly Active Facebook Users Worldwide as of 3rd Quarter 2018 (in Millions)*, https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

Steemitblog, *1,000,000 Steem Accounts*, https://steemit.com/steem/@steemitblog/1-000-000-steem-accounts.

Tegeler F., Koll D., Fu X., *Gemstone: Empowering Decentralized Social Networking with High Data Availability*, „Global Telecommunications Conference – GLOBECOM" 2011, s. 1–6.

Tran M.H., Nguyen V.S., Uyen Ha S.V., *Decentralized Online Social Network Using Peer-to-Peer Technology*, „REV: Journal on Electronics and Communications" 2015, t. 5, nr 1–2, s. 29–36.

Wu L., Madei M., Ghazinour K., Baker K., *Analysis of Social Networking Privacy Policies*, „Proceedings of the 2010 EDBT/ICDT Workshops" 2010.

Xie Y., Zheng M., *A Differentiated Anonymity Algorithm for Social Network Privacy Preservation*, „Algorithms" 2016, t. 9, nr 4, s. 85.

Yeung C.A., Liccardi I., Lu K., Seneviratne O., Berners-Lee T., *Decentralization: The Future of Online Social Networking*, „W3C Workshop on the Future of Social Networking Position Papers" 2009.