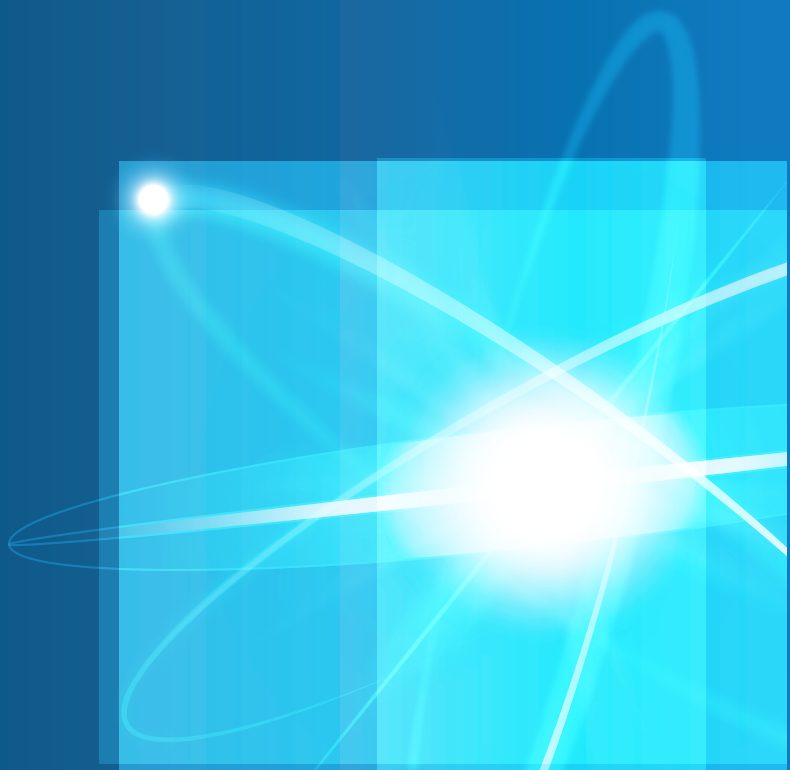


PME

1/2024

Prawo Mediów Elektronicznych

Kwartalnik Naukowy



CBiKE



Dostęp online:

<https://www.bibliotekacyfrowa.pl/publication/154584>

<https://www.repozytorium.uni.wroc.pl/publication/150558>

<https://www.pme.uni.wroc.pl>

DOI: 10.34616/150558

Prawo Mediów Elektronicznych

Kwartalnik Naukowy

pod redakcją Jacka Gołaczyńskiego

Uniwersytet Wrocławski

<https://orcid.org/0000-0002-3295-7099>

1/2024

Wrocław 2024

Redakcja

Redaktor naczelny: prof. dr hab. Jacek Gołaczyński, Uniwersytet Wrocławski

Sekretarz redakcji: dr Rafał Skibicki, Uniwersytet Wrocławski

Członek redakcji: mgr Agata Jałowicka, Uniwersytet Wrocławski

Rada Programowa

Przewodniczący: dr hab. Wojciech Wiewiórowski, Uniwersytet Gdański, EIOD

Członkowie

r.pr. Włodzimierz Chróścik

sędzia Jacek Czaja, Naczelny Sąd Administracyjny

adw. Rafał Dębowski

dr hab. Włodzimierz Gromski, emerytowany prof. UW

adw. Xawery Konarski

prof. Avv. Michele Angelo Lupoi, University of Bologna

prof. dr hab. Jacek Mazurkiewicz, Uniwersytet Zielonogórski

dr hab. Grzegorz Sibiga, prof. nadzw., Instytut Nauk Prawnych PAN

dr hab. Joanna Studzińska, prof. nadzw., Akademia Leona Koźmińskiego

prof. dr hab. Grażyna Szpor, Uniwersytet Kardynała Stefana Wyszyńskiego

prof. dr Andreas Wiebe, University of Goettingen

prof. dr hab. Krzysztof Wójtowicz, Uniwersytet Wrocławski

dr hab. Dariusz Szostek, prof. nadzw., Uniwersytet Śląski w Katowicach

dr hab. Piotr Stec, prof. nadzw., Uniwersytet Opolski

dr hab. Radim Polcak, prof. Uniwersytetu w Brnie

dr hab. Svietlana Fursa, Taras Shevchenko, National University of Kyiv

dr hab. Marlena Jankowska, prof. nadzw. UŚ

Recenzenci

prof. hab. dr Vytautas Nekrošius, Vilnius University

dr hab. Andrzej Adamski, prof. nadzw. UMK

prof. Zsolt Balogh, Corvinus University

prof. dr hab. Sławomir Cieślak, Uniwersytet Łódzki

dr hab. Kinga Flaga-Gieruszyńska, prof. nadzw. USz

prof. dr hab. Jacek Górecki, Uniwersytet Śląski

prof. em. dr Wolfgang Kilian, University of Hannover

prof. dr hab. Ryszard Markiewicz, Uniwersytet Jagielloński

dr hab. Marek Świerczyński, Uniwersytet Kardynała Stefana Wyszyńskiego

prof. Richard Warner Ph.D, Kent College of Law, Chicago

dr hab. Kazimierz Zgrzyzek, prof. nadzw. UŚ

© Copyright by Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, 2024

Czasopismo dofinansowane ze środków Ministerstwa Edukacji i Nauki

w ramach programu „Rozwój Czasopism Naukowych” (projekt nr RCN/SP/0553/2021/1)

Korekta (język polski): Sebastian Surendra

Korekta (język angielski): Rafał Skibicki

Projekt i wykonanie okładki: Agata Jałowicka

Skład i opracowanie techniczne: Munda Maciej Torz

Wydawca

E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa.

Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego

ISSN 2082-100X

Adres redakcji

Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii,

Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej

ul. Uniwersytecka 22/26, 51-145 Wrocław

e-mail: jacek.golaczynski@uwr.edu.pl

Wersją pierwotną (referencyjną) czasopisma jest wydanie elektroniczne

Spis treści

Gracjan Ciupa

Wybrane zagadnienia zobowiązań związanych z walutami wirtualnymi –
stan *de lege lata* i *de lege ferenda* 7

Justyna Doniec-Niezgoda

Zaprzepaszczone szanse Aktu o Usługach Cyfrowych? – rozważania doty-
czące definicji platformy internetowej – część I 20

dr Jarosław Greser

Access to health data for scientific research. Remarks in the light of Arti-
cle 40 DSA 34

Michał R. Kolasiński

Kwalifikacja prawna plików *cookie* jako danych osobowych oraz podstawy
prawne ich przetwarzania 49

Julia Rodakiewicz

Prawo własności intelektualnej i technologia NFT w kontekście branży
muzycznej: wyzwania i perspektywy 64

Gracjan Ciupa*

Uniwersytet Wrocławski

Wydział Prawa, Administracji i Ekonomii

ORCID: 0000-0002-5687-1732

Wybrane zagadnienia zobowiązań związanych z walutami wirtualnymi – stan *de lege lata* i *de lege ferenda*

Streszczenie

Celem niniejszego artykułu jest przedstawienie wybranych zagadnień zobowiązań związanych z walutami wirtualnymi w świetle regulacji polskiego Kodeksu cywilnego – stan *de lege lata* i *de lege ferenda*. Autor w swoich rozważaniach dokonuje analizy trzech instytucji odpowiednio ze Zobowiązań – części ogólnej oraz Zobowiązań – części szczególnej, wykorzystując metodę dogmatyczno-prawną ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny w świetle regulacji ustaw szczegółowych.

Rozpoczynając swoje rozważania od definicji waluty wirtualnej, idąc w ślad za polską definicją oraz standardem międzynarodowym, dochodzi do wniosku, że analiza przebiegała będzie jednotorowo tam, gdzie to możliwe, a dwutorowo tam, gdzie wymaga tego natura stosunku prawnego. W tym wypadku z jednej strony aspekty polskiego prawa cywilnego analizowane będą z perspektywy tzw. kryptowalut (np. *bitcoin*, *cardano*), a z drugiej strony z perspektywy tzw. coinsów występujących chociażby w FIFA 23, jednocześnie spełniających polską definicję waluty wirtualnej.

Autor kolejno rozważa następujące instytucje prawa prywatnego – zasadę swobody umów, realizację zobowiązań w walucie obcej, zasadę waloryzacji oraz umowy sprzedaży, zamiany i darowizny.

W konkluzji dochodzi do wniosku, iż instytucje polskiego Kodeksu cywilnego wymagają nowelizacji i unowocześnienia w świetle rozwoju technologicznego.

Słowa kluczowe:

waluty wirtualne, darowizna, sprzedaż, zamiana, waloryzacja, swoboda umów

Wstęp

Waluty wirtualne, a w szczególności kryptowaluty, z roku na rok zyskują w obrocie gospodarczym coraz większe znaczenie. Historycznie pierwszy raz koncept kryptowaluty znanej w dzisiejszej formie opisywać zaczął informatyk Wei Dai na

* Autor jest studentem III roku stacjonarnych studiów prawa oraz stacjonarnych studiów ekonomii (specjalizacja prawo podatkowe).

jednej z cyberpunkowych list mailingowych. Wówczas zaproponował on stworzenia idei nowego pieniądza, który zamiast centralnego organu wykorzystywać miał kryptografię – b-money¹.

Celem niniejszego artykułu jest przedstawienie wybranych zagadnień zobowiązań związanych z walutami wirtualnymi w świetle regulacji polskiego Kodeksu cywilnego – stan *de lege lata* i *de lege ferenda*. Rozważania rozpoczęte zostaną poprzez wskazanie definicji waluty wirtualnej w świetle polskiego ustawodawstwa oraz międzynarodowych standardów. Następnie analizie poddane zostaną instytucje zobowiązań – części ogólnej ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny² poprzez zestawienie ich pod kątem użyteczności w zakresie walut wirtualnych. Będą to: swoboda umów, zasady dotyczące zobowiązań wyrażonych w walucie obcej oraz zasada waloryzacji. Ponadto waluty wirtualne poddane zostaną również analizie pod kątem ich wykorzystania z trzema kodeksowymi umowami – umową sprzedaży, umową zamiany oraz umową darowizny.

1. Definicja waluty wirtualnej w świetle polskiego ustawodawstwa oraz międzynarodowych standardów

Celem uniknięcia nieścisłości związanych z wieloznacznością sformułowania kluczowego dla tegoż artykułu na wstępie należy zdefiniować pojęcie waluty wirtualnej. Pojęcie to posiada w polskim systemie prawa definicję legalną. Ustawodawca, definiując to pojęcie, posłużył się zarówno kryteriami pozytywnymi, jak i negatywnymi. Zgodnie z art. 2 ust. 2 pkt 26 ustawy z dnia 1 marca 2018 r o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu³, który definiuje pojęcie waluty wirtualnej, do pozytywnych przesłanek należy zaliczyć:

- 1) wymienialność na prawne środki płatnicze w obrocie gospodarczym;
- 2) akceptowalność jako środek wymiany;
- 3) możliwość bycia przechowaną oraz przenoszalną elektronicznie albo
- 4) możliwość bycia przedmiotem handlu elektronicznego.

Negatywną przesłanką jest zaś bycie cyfrowym odwzorowaniem wartości, które jednocześnie nie jest:

- 1) prawnym środkiem płatniczym emitowanym przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej;

¹ A. Behan, *Waluty wirtualne jako przedmiot przestępstwa*, Kraków 2022, s. 241.

² T.j. Dz. U. z 2023 r. poz. 1610, dalej jako k.c.

³ T.j. Dz. U. z 2023 r. poz. 1124.

2) międzynarodową jednostką rozrachunkową ustanawianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub z nią współpracujące;

3) pieniądzem elektronicznym w rozumieniu ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych;

4) instrumentem finansowym w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi;

5) wekslem lub czekiem.

Warto również zauważyć, że uregulowanie to daje podstawy do krytyki, co też ma miejsce w doktrynie⁴. Zdaniem jurysprudencji definicja ta jest zbyt szeroka i poza kryptowalutami *sensu stricto* obejmuje także inne środki wymiany, o mniejszym znaczeniu gospodarczym, np. „coinsy” w grze FIFA Ultimate Team⁵. Co więcej, definicja ta stworzona została nie w celu regulacji obrotu cywilnoprawnego, lecz w celu ochrony interesu państwa.

Kolejna definicja odpowiadająca częściowo na wady polskiej definicji została przedstawiona przez FATF⁶. Warto również wskazać, iż polska definicja zdaniem doktryny wzorowana była na definicji FATF⁷. Zgodnie z tą definicją „waluta wirtualna” to cyfrowa reprezentacja wartości, którą można cyfrowo obracać i która funkcjonuje jako:

1) środek wymiany; i/lub

2) jednostka rozrachunkowa; i/lub

3) zasób wartości, ale która nie ma legalnego statusu środka płatniczego w żadnej jurysdykcji⁸.

Ponadto dokonano również klasyfikacji, które z punktu widzenia polskiej definicji są relewantne. Mianowicie jest to podział na waluty wirtualne scentralizowane – są wydawane przez jeden podmiot oraz zdecentralizowane – wydawane przez więcej niż jednego wydawcę jednocześnie posiadające zabezpieczone kryptograficznie

⁴ G. Ciupa, *Commentary of confirmation to the judgement of the Voivodship Administrative Court in Łódź of 30 November 2021, Ref. No. I SA/Łd 699/21*, „Prawo Mediów Elektronicznych” 2023, nr 1, s. 38.

⁵ M. Nowakowski, *Art. 2 [Instytucje obowiązane; definicje]*, [w:] M. Nowakowski (red.), *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Warszawa 2023, s. 122.

⁶ Grupa Zadaniowa ds. Przeciwdziałania Praniu Pieniędzy, z fran. Groupe d’action financière, jest organizacją międzyrządową założoną w 1989 r. dzięki inicjatywie G7 w celu opracowania polityki zwalczania prania pieniędzy i utrzymania pewnych interesów.

⁷ W. Kapica, *Art. 2 [Katalog instytucji obowiązanych; objaśnienie pojęć ustawowych]*, [w:] W. Kapica (red.), *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Warszawa 2020, s. 38.

⁸ M. Dyl, M. Królikowski (red.), *Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Warszawa 2021.

algorytmy. Drugi podział stworzony przez FATF nastąpił ze względu na kryterium wymienialności. Waluta wirtualna wymienialna to taka, która może być wymieniona w „obie strony” na waluty fiducjarne (*bitcoin, cardano, etherum*) i niewymienialne, które są stworzone dla celów określonej, wirtualnej domeny lub funkcji, nie mogą być wymieniane na walutę fiducyjną, np. World of Warcraft Gold⁹.

O ile pierwszy z podziałów w tejże definicji bez wątpienia uznać można za trafny, tak drugi z nich wzbudza pewne wątpliwości. Przede wszystkim warto zauważyć, że podział ten nie spełnia założenia rozłączności. Podana w przykładzie została waluta w grze World of Warcraft. Bardzo często jednak waluta ta spełniać będzie przesłanki waluty wirtualnej wymienialnej, ze względu na to, że powszechnie akceptowalna (lecz nie zawsze zgodnie z regulaminem poszczególnych domen) możliwa jest wymiana w obie strony „coinsów” i waluty fiducjarnej.

Polska nauka prawa cywilnego wprowadziła także pojęcie pieniądza elektronicznego. Doktrynalna definicja tego pojęcia brzmi następująco: „pieniądz cyfrowy jest wartością pieniężną stanowiącą ekwiwalent wyborczy znaków pieniężnych. Jest on przechowywany na elektronicznych nośnikach pamięci i emitowany na podstawie umowy przez banki lub instytucje pieniądza cyfrowego w zamian za środki pieniężne o wartości nominalnej nie mniejszej niż ta wartość. Jest wyrażony w jednostkach pieniężnych i musi zostać wymieniony na gotówkę przez emitenta na żądanie. Emisja pieniądza cyfrowego przybiera formę instrumentu płatniczego, tj. spersonalizowanego urządzenia lub zestawu procedur uzgodnionych między użytkownikiem a emitentem pieniądza elektronicznego, wykorzystywanego do złożenia zlecenia płatniczego”¹⁰. Główną różnicą między walutą wirtualną a pieniądzem cyfrowym jest to, że pieniądz cyfrowy musi zostać wymieniony na każde żądanie na gotówkę. Jednakże oba te instrumenty nie są prawnym środkiem płatniczym na terenie Rzeczypospolitej Polskiej¹¹.

W związku z przedstawionymi założeniami w tym artykule prowadzona analiza będzie przebiegać jednorodowo tam, gdzie to możliwe, a dwutorowo tam, gdzie z natury stosunku zobowiązaniowego nie będzie to możliwe – z jednej strony aspekty polskiego prawa cywilnego analizowane będą z perspektywy tzw. kryptowalut¹²

⁹ *Ibidem*.

¹⁰ Z. Radwański, A. Olejniczak, J. Grykiel, *Zobowiązania – część ogólna*, Warszawa 2022, s. 64-65.

¹¹ K. Osajda (red. serii), J. Dybiński (red. tomu), *Ustawa o usługach płatniczych. Komentarz*, wyd. 2, Warszawa 2022.

¹² Na potrzeby niniejszego artykułu przez pojęcie „kryptowaluty” rozumieć należy walutę wirtualną, która wykorzystuje technologię kryptografii do zabezpieczenia transakcji oraz kontrolowania tworzenia nowych jednostek tej waluty. <https://www.infor.pl/slownik/biznes/6289545,kryptowaluta.html> [dostęp 15.12.2023].

(np. *bitcoin*, *cardano*), a z drugiej strony z perspektywy tzw. coinsów¹³ występujących chociażby w FIFA 23, a jednocześnie spełniających polską definicję waluty wirtualnej.

2. Swoboda umów z art. 353¹ k.c. a zobowiązania związane z walutami wirtualnymi

Swoboda umów w polskim ustawodawstwie zawarta została w art. 353¹ k.c. Z jej brzmienia wynika jedna z najbardziej doniosłych zasad prawa cywilnego – statuuje ona swobodę kształtowania treści zobowiązaniowych stosunków prawnych przez ich strony. Zasada swobody umów w szerokim znaczeniu obejmuje także kompetencję do swobody zawarcia umowy, tzn. do decyzji o zawarciu lub niezawarciu umowy, wyboru kontrahenta, rozwiązania istniejącego stosunku prawnego. Z praktycznej perspektywy przepis ten zawiera normę umożliwiającą tworzenie konkretnych stosunków zobowiązaniowych odpowiadających kodeksowym i pozakodeksowym typom, np. umowy sprzedaży, a także stosunków o innej treści, tzw. umów nienazwanych¹⁴.

Polskie uregulowanie swobody umów nie jest bezwzględne. Ustawodawca w art. 353¹ *in fine* uregulował trzy ograniczenia tejże zasady – właściwość (naturę) stosunku, ustawę i zasady współżycia społecznego. Każdą z tych granic analizować należy kazuistycznie, lecz już na ich podstawie można wysnuć pewne wnioski.

Przede wszystkim dokonywanie transakcji przy użyciu walut wirtualnych nie jest zakazane przez prawo. Jednakże by zweryfikować, czy każdorazowa umowa, w której jednym ze świadczeń będzie świadczenie w walucie wirtualnej, nie przekracza granicy swobody umów, należy poddać testowi świadczenie wzajemne i jego naturę oraz charakter. Chociażby umowa darowizny, której przedmiotem będzie waluta wirtualna, będzie ważna i zgodna z zasadą przy zachowaniu odpowiedniej formy oraz wszelkich aktów staranności przewidzianych przez ustawę. Patrząc z drugiej strony, apriorycznie stwierdzić można, że umowa zamiany¹⁵, w której dojdzie do zamiany waluty wirtualnej za 5 gramów marihuany, przekracza granicę swobody umów. Zgodnie z art. 59 ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii¹⁶

¹³ Na potrzeby niniejszego artykułu przez pojęcie „coinsy” rozumieć należy waluty wirtualne, które są stworzone dla celów określonej, wirtualnej domeny lub funkcji, np. gry komputerowej.

¹⁴ E. Gniewek, P. Machnikowski (red.), *Kodeks cywilny. Komentarz*, wyd. 11, Warszawa 2023.

¹⁵ W tym przypadku poczyniono założenie, że walutę wirtualną można zakwalifikować jako rzecz w kodeksowym rozumieniu tego pojęcia. Szersze rozważania poczynione zostały w części dotyczącej umowy zamiany.

¹⁶ T.j. Dz. U. z 2023 r. poz. 1939.

udzielanie innej osobie środka odurzającego celem osiągnięcia korzyści majątkowej lub osobistej jest zakazane pod groźbą kary, a w związku z tym umowa ta sprzeciwia się ustawie (jednej z granic swobody umów).

3. Zobowiązanie wyrażone w walucie obcej z art. 358 k.c. a zobowiązania związane z walutami wirtualnymi

Artykuł 358 k.c. konstytuuje zasadę, w myśl której jeżeli przedmiotem zobowiązania podlegającego wykonaniu na terytorium Rzeczypospolitej Polskiej jest suma pieniężna wyrażona w walucie obcej, dłużnik może spełnić świadczenie w walucie polskiej, chyba że ustawa, orzeczenie sądowe będące źródłem zobowiązania lub czynność prawna zastrzega spełnienie świadczenia wyłącznie w walucie obcej. Zasada ta w swoim brzmieniu jest przedmiotem licznych rozważań doktryny w związku ze swoją niejasnością oraz zbyt mało kazuistycznym uregulowaniem¹⁷.

Przechodząc do meritum – w ślad za polską doktryną *de lege lata* nie ma podstaw, by w zbiorze desygnatów „waluty obcej” znalazło się pojęcie „waluty wirtualnej”. Zdaniem autorów nie jest to „pieniądz”, a zatem w odniesieniu do świadczeń niepieniężnych art. 358 k.c. nie znajduje zastosowania¹⁸. Pogląd ten zasługuje niestety na aprobatę. W obecnym uregulowaniu z definicji legalnej „waluty wirtualnej” wynika, że nie może być ona pieniądzem. Jednakże regulacja ta z prakseologicznego punktu widzenia powinna być znowelizowana.

Waluty wirtualne w swoim społeczno-gospodarczym użyciu coraz częściej zastępują świadczenia pieniężne. Przykładowo w grze World of Warcraft walutą wirtualną jest „World of Warcraft Gold” (dalej: „Gold”). Przy użyciu Golda gracz może nabyć zawartość w grze, tzw. abonament. Gracz może nabyć go także za cenę około 10 euro, płacąc za niego przy wykorzystaniu waluty fiducjarnej. Ponadto abonament można nabyć w formie żetonu, który później można wymienić na równowartość w walucie fiducjarnej. Powoduje to, że waluta wirtualna zaczyna mieć coraz większe znaczenie społeczno-gospodarcze, a w związku z tym zobowiązania w niej zawierane powinny posiadać podobną ochronę co zobowiązania pieniężne¹⁹.

Kolejnym problemem, który pojawia się w art. 358 k.c., są § 2 oraz § 3. Obie te części przepisu na pierwszy plan przesuwają znaczenie średniego kursu waluty

¹⁷ M. Bujalski, F. Zoll, [w:] A. Olejniczak (red.), *System Prawa Prywatnego*, t. 6, Warszawa 2023.

¹⁸ K. Osajda (red. serii), W. Borysiak (red. tomu), *Kodeks cywilny. Komentarz*, wyd. 31, Warszawa 2023.

¹⁹ Zob. Ł. Klimczyk, M. Leciak (red.), *E-sport. Aspekty prawne*, Warszawa 2020.

obecnej według Narodowego Banku Polskiego. Powoduje to, że aby móc stosować ten przepis chociażby *per analogiam*, do waluty wirtualnej należałoby ustalić średni kurs waluty wirtualnej przy wykorzystaniu niezależnego organu. W chwili obecnej, jeśli chodzi o walutę wirtualną pod postacią bitcoina to ustalenie takiego kursu byłoby trudne, lecz nie niemożliwe. Obecnie możliwe byłoby to, chociażby ze względu na liczbę transakcji zawieranych na świecie. Z drugiej zaś strony stworzenie niezależnego państwowego organu, który określałby taki kurs, byłoby niezgodne z celem jego stworzenia. Niestety, jeśli chodzi o waluty wirtualne używane w grach to ze względów technicznych jest to niemożliwe – przede wszystkim z uwagi na brak odpowiedniej liczby transakcji, na podstawie których można ustalić jednoznaczny kurs kupna bądź sprzedaży waluty.

4. Zasada waloryzacji z art. 358¹ § 2 k.c. a waluty wirtualne

Kodeksowa zasada waloryzacji jest wyjątkiem od zasady nominalizmu z art. 358¹ § 1 k.c., w myśl której jeżeli przedmiotem zobowiązania od chwili jego powstania jest suma pieniężna, spełnienie świadczenia następuje przez zapłatę sumy nominalnej, chyba że przepisy szczególne stanowią inaczej. Zasada waloryzacji stosowana jest przez strony w celu zabezpieczenia się przed ryzykiem związanym ze zmianą siły nabywczej pieniądza poprzez zastosowanie tzw. umownej klauzuli waloryzacyjnej. Dzięki zastosowaniu tejże klauzuli wysokość świadczenia w zobowiązaniu pieniężnym ustalana jest w sposób pośredni – nie przy użyciu konkretnej liczby jednostek pieniężnych, lecz przez opisanie wartości innego przedmiotu²⁰.

Kodeksowe uregulowanie w tym jest dość łaskawe, jeśli chodzi o zastosowanie walut wirtualnych. Klauzula weryfikacyjna bowiem może być ustalona według innego niż pieniądź miernika wartości. Bez wątpienia przyznać należy, iż waluta wirtualna spełnia wymóg miernika wartości²¹, na co wskazuje chociażby jej definicja przedstawiona przez FATF. Przykładowa klauzula mogłaby brzmieć następująco:

„§ X. Cena 1 kilograma jabłek wynosi 3 zł pomnożone przez równowartość 1500 coinsów z gry FIFA Ultimate Team przeliczone na złotówki według kursu z dnia poprzedzającego transakcję według średniego kursu zamieszczonego na stronie [XYZ.pl](#)”.

²⁰ M. Załucki (red.), *Kodeks cywilny. Komentarz*, wyd. 3, Warszawa 2023.

²¹ M. Michna, *Bitcoin jako przedmiot stosunków cywilnoprawnych*, Warszawa 2018, s. 84.

Wobec aktualnej sytuacji społeczno-gospodarczej stosowanie takich klauzul w umowach wszelkiego rodzaju może zyskiwać na popularności, lecz niekoniecznie w celu ustalonym przez ustawodawcę. Przede wszystkim warto zwrócić uwagę na zmiany kursowe, np. bitcoina, który wyznacza trend na rynku kryptowalut.



Rys. 1. Średnia wartość 1 BTC w USD

Źródło: opracowanie własne na podstawie <https://pl.investing.com/crypto/bitcoin/historical-data> [dostęp 30.12.2023].

Jak widać z wykresu, 1 stycznia 2023 r. średnia wartość 1 bitcoina w USD wynosiła 16 618, zaś 30 grudnia 2023 r. 42 000 – tylko w ciągu roku wartość ta wzrosła o 152%. Z jednej strony pokazuje to, że bitcoin tak jak każda inna waluta jest podatny na zmiany, a co za tym idzie – nie będzie spełniał swojej funkcji utrzymania wartości. Z drugiej zaś strony takie zmiany kursowe wykorzystywane mogą być chociażby do inwestowania i czerpania z nich korzyści.

5. Umowa sprzedaży z art. 535 k.c. oraz umowa zamiany z art. 603 k.c. a waluty wirtualne

Umowa sprzedaży jest umową dwustronnie zobowiązującą wzajemną, odpłatną, konsensualną, co do zasady wywołującą skutek zobowiązująco-rozporządzający. Polega ona na zobowiązaniu się sprzedawcy do przeniesienia na kupującego własności rzeczy i wydania mu jej, a kupujący zobowiązuje się rzecz odebrać i zapłacić sprzedawcy cenę²².

²² B. Gliniecki, [w:] M. Balwicka-Szczyrba, A. Sylwestrzak (red.), *Kodeks cywilny. Komentarz aktualizowany*, LEX/el. 2023, art. 535.

Rozważania umowy sprzedaży będą przebiegać w związku z tym dwutorowo – z perspektywy kupującego, którego świadczenie wzajemne wobec sprzedawcy wyrażone jest w walucie wirtualnej i w odwrotnej sytuacji. Inaczej mówiąc – analizie poddane zostanie, czy w rozumieniu art. 535 waluta wirtualna może stać się rzeczą oraz czy możliwe jest zapłacenie ceny przy użyciu wspomnianej waluty.

Rozpoczynając od ceny – zdanie doktryny w tym wypadku jest dość jednoznaczne. „Cena musi stanowić świadczenie pieniężne. W przypadku gdy przedmiot świadczenia wzajemnego kupującego nie ma charakteru świadczenia pieniężnego (np. jest to rzecz lub prawo), umowa stanowi umowę zamiany”²³. Jednakże na tym nie kończy się wykorzystanie waluty wirtualnej w związku z umową sprzedaży. Zgodnie z art. 536 k.c. cenę można określić przez wskazanie podstaw do jej ustalenia. W tym wypadku klauzula ustalająca może brzmieć następująco: „§ X. Cena 1 kilograma jabłek wynosi równowartość 1500 coinsów z gry FIFA Ultimate Team przeliczonych na złotówki według kursu z dnia poprzedzającego transakcję według średniego kursu zamieszczonego na stronie XYZ.pl”.

Przechodząc do rzeczy – na wstępie warto zaznaczyć, że zgodnie z art. 555 k.c. przepisy o sprzedaży rzeczy stosuje się odpowiednio do sprzedaży energii, praw oraz wody. W związku z tym w doktrynie oraz środowisku bankowym przyjmuje się pogląd, iż waluty wirtualne kwalifikować należy jako wierzytelności i przy dokonaniu charakterystycznych dla ich natury czynności przekazania, możliwe jest zastosowanie do ich sprzedaży art. 535 k.c. w zw. z art. 555 oraz art. 510 k.c.²⁴

Jeśli zaś chodzi o umowę zamiany, to polega ona na tym, że każda ze stron zobowiązuje się przenieść na drugą stronę własność rzeczy w zamian za zobowiązanie się do przeniesienia własności innej rzeczy. W związku z poczynionymi rozważaniami z łatwością można dojść do wniosku, iż waluta wirtualna może być przedmiotem umowy zamiany, ze względu na odesłanie znajdujące się w art. 604 k.c.

Po ogólnych rozważaniach dotyczących kwestii umowy sprzedaży oraz zamiany warto zwrócić jeszcze uwagę na kwestię *stricte* związaną z walutami wirtualnymi pod postacią „coinsów”, a mianowicie nabywanie przedmiotów w poszczególnych grach za „coinsy”.

Przykładowo FIFA Ultimate Team umożliwia nabywanie przy pomocy coinsów zawartości w grze, takich jak karty zawodników, stroje czy stadiony. Sam schemat nabywania tychże przedmiotów odbywa się w wolnorynkowych warunkach. Gracz

²³ *Ibidem*.

²⁴ Polskie Stowarzyszenie Bitcoin, *Aspekty prawno-podatkowe w Polsce*, <https://bitcoin.org.pl/prawno-podatkowe-aspekty-kryptowalut/> [dostęp 5.12.2023].

posiadający pożądaną kartę wystawia na licytację posiadaną przez siebie kartę, ustalając jej cenę minimalną oraz „kup teraz”. Gracze, którzy chcą nabyć, mogą to zrobić wyłącznie w drodze licytacji.

Schemat nabywania kart w grze FIFA Ultimate Team bardzo przypomina kodeksową regulację jednego z trybu zawarcia umowy – aukcji (art. 70¹ k.c. i n.). Kwestią wartą odnotowania jest także fakt, że większość tychże transakcji ma charakter transgraniczny, a więc zastosowanie do wymienionych umów powinno mieć tzw. rozporządzenie Rzym I²⁵. Co do zasady główną regułą rządzącą tymże rozporządzeniem jest tzw. wybór prawa. Oznacza to, że strony mogą dokonać wyboru, jakiemu podlegać będzie dana umowa. W przypadku braku jego wyboru zastosowanie mieć będzie art. 4 ust. 1 lit. g, zgodnie z którym umowa sprzedaży towarów w drodze licytacji podlega prawu państwa, w którym odbywa się licytacja, jeżeli miejsce to można ustalić. Niestety, zastosowanie tychże przepisów może sprawiać trudności, gdyż gracze ze swojej pozycji (widoku gry) obecnie nie są w stanie ustalić, od kogo *de facto* kupują powyższe karty, ze względu na anonimowość aukcji, która na celu ma ograniczenie celowego przekazywania coinsów pomiędzy kontami. Jednakże z pozycji administratora gry jest to możliwe. W związku z tym, aby ustalić prawo właściwe, potrzebne jest współdziałanie z tymże podmiotem.

6. Umowa darowizny z art. 888 k.c. a waluty wirtualne

Umowa darowizny jest umową konsensualną, zobowiązującą oraz bezpłatną. Polega ona na tym, że darczyńca zobowiązuje się do bezpłatnego świadczenia na rzecz obdarowanego kosztem swego majątku²⁶. Kluczowym aspektem z perspektywy waluty wirtualnej jest określenie przedmiotu darowizny. Doktryna charakteryzuje go bardzo szeroko oraz zróżnicowanie²⁷. Co najważniejsze dla kwestii waluty wirtualnej, mogą być nim także prawa, a w szczególności wierzytelności, co przy przyjętych w poprzednich akapitach założeniach bezdyskusyjnie rozwiązuje tę kwestię – waluty wirtualne mogą być przedmiotem darowizny.

Co do formy darowizny, to przepisy szczególne nie przewidują formy szczególnej dla czynności prawnej przeniesienia własności waluty wirtualnej. W związku z tym zastosowanie będzie miał art. 890 k.c., w myśl którego umowa ta powinna

²⁵ Rozporządzenie Parlamentu Europejskiego i Rady (WE) Nr 593/2008 z dnia 17 czerwca 2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Rzym I), Dz. Urz. UE L 177/6 z 4.07.2008 r.

²⁶ Z. Radwański, J. Panowicz-Lipska, *Zobowiązania – część szczegółowa*, Warszawa 2022, s. 71.

²⁷ M. Bączyk, L. Stecki, [w:] J. Rajski (red.), *System Prawa Prywatnego*, t. 7, Warszawa 2018, s. 352.

zostać zawarta w formie aktu notarialnego, jednakże umowa darowizny zawarta bez zachowania tej formy staje się ważna, jeżeli przyrzeczone świadczenie zostało spełnione. Praktyka obrotu pokazuje jednak, że zdecydowanie częściej podmioty umowy wybierają formę umowy inną niż akt notarialny.

Wychodząc poza ramy polskiego prawa prywatnego i przechodząc do prawa publicznego, darowiznę waluty wirtualnej dopuszcza się również w ustawodawstwie podatkowym. Zgodnie ze stanowiskiem Dyrektora Krajowej Informacji Skarbowej w interpretacji z 19 lipca 2021 r., nr 0111-KDIB2-3.4015.78.2021.3.BD, darowizna waluty wirtualnej równoznaczna jest z darowizną prawa majątkowego, co oznacza, że podlega ona opodatkowaniu podatkiem od spadków i darowizn.

Podsumowanie

Polski Kodeks cywilny został uchwalony w 1964 r., ma już zatem 60 lat. Komisja kodyfikacyjna pracująca nad jego brzmieniem osadzona była w Polskiej Rzeczypospolitej Ludowej nieznającej internetu, kart płatniczych, a co dopiero walut wirtualnych. Z pewnością stwierdzić trzeba, że w dzisiejszych czasach waluty wirtualne posiadają coraz większe znaczenie społeczno-gospodarcze, a co za tym idzie, prawo prywatne powinno również iść z duchem czasu i starać się dogonić w swojej regulacji rozwój technologiczny²⁸. Uwaga ta dotyczy jednak znacznej części uregulowań.

Przeanalizowane instytucje prawa prywatnego mają co prawda kluczowe znaczenie dla obrotu gospodarczego, lecz już na tym etapie na prawie każdym kroku natrafia się na trudności ich zastosowania w kontekście walut wirtualnych.

Jednakże warto wspomnieć, że prawo cywilne w swej naturze daje szerokie możliwości dostosowywania swych instytucji do zmieniającego się świata, głównie dzięki swobodzie umów. Niemniej tak szeroka interpretacja i wyłączone bazowanie na tejże regulacji może mieć negatywne skutki dla stabilności obrotu gospodarczego. Co więcej, instytucją, która poprzez odpowiednią wykładnię może być zastosowana w obecnym brzmieniu, jest zasada waloryzacji z art. 358¹ § 2 k.c. Jednakże w obecnej sytuacji ekonomicznej praktyczne zastosowanie tejże instytucji może mieć dwojakie rezultaty – z jednej strony ze względu na wahania wartości bitcoina może być ona wykorzystywana jako pewnego rodzaju spekulacja, z drugiej zaś jako zabezpieczenie przed inflacją przy wykorzystaniu innych walut wirtualnych.

²⁸ Por. pogląd przeciwny W. Srokosz, *Obszary regulacji prawnej wymagające definicji kryptowaluty*, [w:] W. Rogowski (red.), *Regulacje finansowe FinTech – nowe instrumenty finansowe – resolution*, Warszawa 2017, s. 39-40.

Głównym wnioskiem *de lege ferenda* na podstawie niniejszych rozważań jest potrzeba rozszerzenia desygnatów „ceny” w kodeksowej umowie sprzedaży, tak aby znalazły się tam również waluty wirtualne. Ma to przede wszystkim prakseologiczne znaczenie – dzięki możliwości zakwalifikowania umowy jako umowy sprzedaży obu stronom przysługuje kodeksowa ochrona, np. rękojmia.

Co do zasady walutowości to wprowadzenie możliwości korzystania z niej przy pomocy walut wirtualnych byłoby możliwe, lecz utrudnione. Wymagałoby to stworzenia pewnego rodzaju organu, którego zadaniem i kompetencją byłoby tworzenie wiążących kursów walut wirtualnych.

Reasumując – waluty wirtualne w dzisiejszej sytuacji społeczno-gospodarczej nabierają coraz większego znaczenia, przez co powinny zostać uregulowane bardziej kazuistycznie.

Bibliografia

Akty prawne

Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2023 r. poz. 1610).

Ustawa z dnia 1 marca 2018 r o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2023 r. poz. 1124).

Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (t.j. Dz. U. z 2023 r. poz. 1939).

Literatura

Bączyk M., Stecki L., [w:] J. Rajski (red.), *System Prawa Prywatnego*, t. 7, Warszawa 2018.

Behan A., *Waluty wirtualne jako przedmiot przestępstwa*, Kraków 2022.

Bujalski M., Zoll F., [w:] A. Olejniczak (red.), *System Prawa Prywatnego*, t. 6, Warszawa 2023.

Ciupa G., *Commentary of confirmation to the judgement of the Voivodship Administrative Court in Łódź of 30 November 2021, Ref. No. I SA/Łd 699/21*, „Prawo Mediów Elektronicznych” 2023, nr 1.

Dyl M., Królikowski M. (red.), *Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Warszawa 2021.

Gliniecki B., [w:] M. Bałwicka-Szczyrba, A. Sylwestrzak (red.), *Kodeks cywilny. Komentarz aktualizowany*, LEX/el. 2023, art. 535.

Gniewek E., Machnikowski P. (red.), *Kodeks cywilny. Komentarz*, wyd. 11, Warszawa 2023.

Kapica W., *Art. 2 [Katalog instytucji obowiązanych; objaśnienie pojęć ustawowych]*, [w:] W. Kapica (red.), *Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Warszawa 2020.

Kiszka J., *Obrót walutami wirtualnymi – regulacja zasad i problemy opodatkowania*, „Biuletyn Instytutu Studiów Podatkowych” 2022, nr 7.

Klimczyk Ł., Leciak M. (red.), *E-sport. Aspekty prawne*, Warszawa 2020.

- Michna M., *Bitcoin jako przedmiot stosunków cywilnoprawnych*, Warszawa 2018.
- Nowakowski M., *Art. 2 [Instytucje obowiązane; definicje]*, [w:] M. Nowakowski (red.), *Przeciw-działanie praniu pieniędzy oraz finansowaniu terroryzmu. Komentarz*, Warszawa 2023.
- Osajda K. (red. serii), Borysiak W. (red. tomu), *Kodeks cywilny. Komentarz*, wyd. 31, Warszawa 2023.
- Osajda K. (red. serii), Dybiński J. (red. tomu), *Ustawa o usługach płatniczych. Komentarz*, wyd. 2, Warszawa 2022.
- Radwański Z., Olejniczak A., Grykiel J., *Zobowiązania – część ogólna*, Warszawa 2022.
- Radwański Z., Panowicz-Lipska J., *Zobowiązania – część szczegółowa*, Warszawa 2022.
- Srokosz W., *Obszary regulacji prawnej wymagające definicji kryptowaluty*, [w:] W. Rogowski (red.), *Regulacje finansowe FinTech – nowe instrumenty finansowe – resolution*, Warszawa 2017.
- Wnęk M., *Natura prawna kryptowaluty*, Warszawa 2023.
- Załucki M. (red.), *Kodeks cywilny. Komentarz*, wyd. 3, Warszawa 2023.

Źródła internetowe

- Aspekty prawno-podatkowe w Polsce, <https://bitcoin.org.pl/prawno-podatkowe-aspekty-kryptowalut/>, [dostęp 5.12.2023].
- Kryptowaluta, <https://www.infor.pl/slownik/biznes/6289545,kryptowaluta.html>, [dostęp 15.12.2023].
- Średni kurs bitcoina, <https://pl.investing.com/crypto/bitcoin/historical-data>, [dostęp 30.12.2023].

Selected issues of obligations related to virtual currencies – *state de lege lata* and *de lege ferenda*

Abstract

The purpose of this article is to present selected issues of obligations related to virtual currencies in the light of the regulations of the Polish Civil Code – the *state de lege lata* and *de lege ferenda*. In his considerations, the author analyzes three institutions, respectively Obligations – general part and Obligations – special part using the dogmatic-legal method of the Act of April 23, 1964. – Civil Code in light of the regulations of specific laws.

Starting his considerations with the definition of virtual currency. Following the Polish definition and the international standard, he concludes that the analysis will proceed on one track where possible, and on two tracks where the nature of the legal relationship requires it. In this case, on the one hand, aspects of Polish civil law will be analyzed from the perspective of the so-called cryptocurrencies (e.g., Bitcoin, Cardano, etc.), and on the other hand from the perspective of the so-called coins appearing, for example, in FIFA 23, while meeting the Polish definition of virtual currency.

The author considers the following institutions of private law in turn – the principle of freedom of contract, the performance of obligations in foreign currency, the principle of valorization, and contracts of sale, exchange and donation.

He concludes that the institutions of the Polish Civil Code need to be amended and modernized in light of technological developments.

Keywords

virtual currencies, donation, sale, exchange, valorization, freedom of contract

Justyna Doniec-Niezgoda

Uniwersytet Jagielloński

ORCID: 0000-0003-0817-3945

Zaprzepaszczone szanse Aktu o Usługach Cyfrowych? – rozważania dotyczące definicji platformy internetowej – część I

Streszczenie

Artykuł został podzielony na dwie części. W pierwszej z nich autorka omawia cele Aktu o Usługach Cyfrowych, które są istotne w kontekście rozumienia definicji platformy internetowej oraz oceny wprowadzonych regulacji. Następnie autorka rozpoczyna analizę składowych definicji platformy internetowej, do których należą pojęcia: usługi społeczeństwa informacyjnego (1) oraz usługi hostingu, która przechowuje i rozpowszechnia publicznie informacje (2). Druga ze składowych definicji platformy internetowej została omówiona w sposób szczegółowy w kolejnej części artykułu. Rozwinięte zostało znaczenie pojęcia publicznego rozpowszechniania informacji w rozumieniu DSA oraz świadczenia usługi na „indywidualne żądanie odbiorcy” tej usługi. Dla całościowej analizy konieczne było także przyjrzenie się wyłączeniu wynikającemu z definicji platformy internetowej z art. 3 lit. i) DSA, dotyczące nieznaczności czy poboczności usługi przechowywania i rozpowszechniania publicznie informacji na żądanie odbiorcy usługi wobec innych usług oferowanych przez danego dostawcę. Na koniec drugiej części artykułu autorka formułuje wnioski dotyczące całości wywodu.

Słowa kluczowe

Akt o Usługach Cyfrowych, DSA, platforma internetowa, usługa pośrednia, usługa hostingu

1. Uwagi wstępne

Akt o Usługach Cyfrowych¹ nie zmieni całego internetu. Gdy opadły już emocje i przestały brzmieć fanfary zwiastujące nastanie „Konstytucji internetu”, można przyjrzeć się bliżej zakresowi zastosowania DSA, który po dokonaniu rzetelnej analizy może wydać się nieco zaskakujący. DSA będzie miało zastosowanie tylko do usług pośrednich, które z kolei obejmują wyłącznie usługi: zwykłego przekazu,

¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), Dz. Urz. UE L 277/1 z 27.10.2022 r., dalej: „DSA” lub „Rozporządzenie”.

cachingu i hostingu, znane już z Dyrektywy o handlu elektronicznym². Już z tego stwierdzenia można wywnioskować, że DSA nie będzie regulować całego internetu, a jedynie jego wycinek obejmujący usługi pośrednie. Pojęciem, które jednak znacząco wpływa na zakres podmiotowy Rozporządzenia, jest definicja „platformy internetowej”, która będzie stanowić przedmiot niniejszego opracowania. Rozszyfrowanie znaczenia pojęcia platformy internetowej stanowi istotny krok w określeniu zakresu zastosowania DSA³. Najistotniejsze bowiem regulacje z punktu widzenia DSA dotyczą właśnie dostawców usług platform internetowych, tj. regulacje dot. wewnętrznego rozpatrywania skarg i pozasądowego rozstrzygania sporów (art. 20 i 21 DSA), zawieszenia świadczenia usług na rzecz podmiotów przekazujących oczywiście nielegalne treści (art. 23 DSA), obowiązki sprawozdawcze (art. 24 DSA), regulacje dotyczące interfejsów internetowych (art. 25 DSA), reklamy (art. 26 DSA), systemów rekomendacji (art. 27 DSA) i ochrony małoletnich (art. 28 DSA). Właściwe zrozumienie, kiedy mamy do czynienia z platformą internetową, stanowi punkt wyjścia do interpretacji wskazanych przepisów oraz ich adresatów.

Tezą niniejszego artykułu jest założenie, że definicja platformy internetowej została ukształtowana w Rozporządzeniu w sposób niezwykle wąski, czego skutkiem będzie objęcie regulacjami DSA wyłącznie części usług dostępnych w internecie. W przypadku bowiem, gdy nie będziemy mogli uznać, że dany podmiot jest dostawcą usługi pośredniej lub platformy internetowej, która stanowi rodzaj usługi pośredniej, nie będzie obowiązku zastosowania przepisów DSA. Będzie to oznaczać, że nie wszyscy usługodawcy stron internetowych będą objęci zakresem zastosowania DSA, mimo że zagrożenia wynikające z oferowanych przez nich usług będą w niektórych przypadkach możliwe do identyfikacji dla ich użytkowników końcowych dokładnie w ten sam sposób dla dostawców platform internetowych w rozumieniu DSA i tych, którzy pod to pojęcie nie podpadają. Dla przykładu: reklamy prezentowane w serwisach kontentowych, jak np. gazeta internetowa, nie będą musiały być oznaczane zgodnie z art. 26 DSA, a reklamy prezentowane w serwisach społecznościowych czy marketplace'ach już tak. Podobnie, zakaz dotyczący projektowania interfejsów w sposób wprowadzający w błąd lub manipulujący odbiorców będzie stosowany wyłącznie do podmiotów, które będą świadczyć usługi platformy inter-

² Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), Dz. Urz. WE L 178/1 z 17.07.2000 r., dalej: „Dyrektywa E-commerce”.

³ Przepisy dotyczące platform internetowych i bardzo dużych platform internetowych rozpoczynają się już w art. 19 DSA, a kończą na art. 43 DSA, co stanowi większość przepisów DSA.

netowej. Oznacza to, że serwisy, które będą sprzedawać na swojej stronie produkty oferowane bezpośrednio przez siebie, a nie przez podmioty trzecie, nie będą objęte regulacjami DSA dotyczącymi platform internetowych i nie będą musiały projektować swoich interfejsów w sposób określony w art. 25 DSA. Wyłącznie te podmioty, które będą jednocześnie lub wyłącznie umożliwiać umieszczanie ofert przez innych użytkowników internetu (np. eBay), będą musiały projektować swoje interfejsy w sposób określony w DSA. Użytkownik końcowy może być jednak przecież narażony na wprowadzenie go w błąd, niezależnie od kogo nabywa produkt przez internet. Taka sytuacja może prowadzić do pesymistycznego stwierdzenia o braku możliwości objęcia „Konstytucją” zakresu całego „terytorium” internetu lub nałożenia określonych obowiązków na niektóre podmioty istniejące na rynku, mimo wniosku o istnieniu tych samych zagrożeń bez względu na rodzaj dostawcy usługi. Wniosek, jaki zostanie przedstawiony w niniejszym artykule, sprowadza się do stwierdzenia, że potencjał DSA jest znaczący, lecz ze względu na zakres adresatów omawianej regulacji nie został w pełni wykorzystany.

2. Cele DSA

Cele DSA zostały określone w preambule Rozporządzenia. Jego motyw 9 preambuły wskazuje, że harmonizacja przepisów ma na celu zapewnienie „bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego, przeciwdziałania rozpowszechnianiu nielegalnych treści w internecie oraz zagrożeniom społecznym, jakie może stwarzać rozpowszechnianie dezinformacji lub innych treści, w którym to środowisku prawa podstawowe zapisane w Karcie są skutecznie chronione, a innowacje są wspierane. Motyw ten podkreśla zakaz ustanowienia odmiennych regulacji na poziomie krajowym, które mogłyby prowadzić do rozbieżności w zakresie jednolitego stosowania przepisów. W motywie 67 preambuły DSA wskazane jest uzasadnienie dotyczące wprowadzenia regulacji zakazujących praktyk dotyczących zwodniczych interfejsów internetowych zakłócających zdolność odbiorców usługi do dokonywania niezależnych i świadomych wyborów lub podejmowania takich decyzji. Jako przykłady wymieniono w DSA przypadki bliskie platformom zakupowym takie jak utrudnianie rezygnacji z zakupów czy wypisania się z platformy, zachęcanie do podejmowania decyzji dotyczących zakupu czy też używanie domyślnych ustawień w sposób sugerujący czy ograniczający świadome podejmowanie decyzji przez użytkownika takiej platformy sprzedażowej.

Szerokie uzasadnienie co do wprowadzenia przepisów DSA opisuje motyw 68 preambuły, który stanowi o zagrożeniach związanych z reklamą internetową. Wskazuje on, że reklama może być źródłem nielegalnych treści, poprzez zapewnianie zachęt finansowych do publikowania lub akcentowania nielegalnych lub w inny sposób szkodliwych treści i działań w internecie, aż po dyskryminujące prezentowanie reklam, które ma wpływ na równe traktowanie i równość szans obywateli. Motyw 69 preambuły DSA wskazuje na zagrożenia związane z praktykami targetowania użytkowników, które dążą do dopasowania reklamy do rozpoznanych wcześniej preferencji użytkownika, tak aby zwiększyć prawdopodobieństwo dotarcia do użytkowników zainteresowanych zakupem danego produktu. W konsekwencji art. 26 ust. 3 i 28 DSA zakazują targetowania użytkowników na podstawie danych osobowych szczególnych kategorii, a także zakazują prezentowania reklam w oparciu o profilowanie w przypadku, gdy można z wystarczającą pewnością ustalić, że użytkownik jest małoletni.

Wymienione przykładowo zakazy i ograniczenia wynikające z DSA stanowią znaczący postęp w odniesieniu do obecnego stanu regulacji internetu, który wciąż pozostaje przestrzenią dużo mniej sformalizowaną prawnie niż przestrzeń „pozainternetowa” i po raz pierwszy zostały w sposób tak wyraźny zaakcentowane w prawie europejskim. Dodatkowo nie sposób nie zgodzić się, że zagrożenia wymieniane przez ustawodawcę europejskiego w preambule DSA występują, są dla wszystkich łatwo dostrzegalne i wprowadzenie zakazów, o których mowa, przyczyniłoby się do zwiększenia bezpieczeństwa w sieci. Z przytoczonymi argumentami dotyczącymi ochrony użytkowników należy oczywiście się zgodzić. Internet potrzebuje regulacji, a praktyki, które prowadzą do nadużyć czy braku wystarczającej informacji do podjęcia decyzji przez użytkowników końcowych, powinny być zakazane.

Mimo tego należy zauważyć, że fakt występowania zagrożeń opisywanych w DSA jest dużo szerszy niż krąg adresatów, którzy zostali objęci regulacjami. Jak zostanie dokładnie przedstawione w dalszej części tekstu, definicja platformy internetowej będzie w praktyce rozgraniczać dostawców usług internetowych na dwie grupy⁴: tych, którzy będą uznani za dostawcę platformy internetowej i będą zobowiązani do przestrzegania standardów wynikających z DSA, w tym dotyczących reklamy i zwodniczych interfejsów, i tych, którzy nie będą zobowiązani do projektowania interfejsów i oznaczania prezentowanych reklam w sposób uregulowany w DSA. Dojdzie zatem

⁴ Oczywiście takie dwie grupy można także wskazać poprzez rozróżnienie dostawcy usługi pośredniej i niedostawcy usługi pośredniej, jednak niniejsze opracowanie dotyczy zagadnienia platformy internetowej, stąd dokonane rozróżnienie opiera się na tym pojęciu.

do sytuacji, w której niecałe środowisko internetowe, o którym stanowi motyw 9 preambuły DSA, stanie się „bezpieczne, przewidywalne i budzące zaufanie”. Wyłącznie ci usługodawcy, którzy będą mogli zostać zakwalifikowani jako świadczący usługę pośrednią oraz platformy internetowej, będą objęci regulacjami z art. 19-43 DSA. W pozostałym zakresie, tj. podmiotów, które nie będą mogły zostać zdefiniowane jako platformy internetowe, regulacje dot. reklamy czy zwodniczych interfejsów, ale także systemów rekomendacji czy ochrony małoletnich nie będą miały zastosowania. Wniosek ten jest o tyle znamieny, że w praktyce wyłącznie nieliczne podmioty będą spełniać wszystkie przesłanki platformy internetowej.

Konkluzja ta, dotycząca fragmentarycznej regulacji internetu, mimo szeroko wskazanych celów Rozporządzenia jest oczywiście spójna z zakresem prezentowanym w poszczególnych artykułach DSA. Rozporządzenie już w art. 1 wyraźnie precyzuje, że swoim zakresem obejmuje „rynek wewnętrzny usług pośrednich”, a zatem nie rynek wszystkich usług dostępnych w internecie, a wyłącznie tych, które świadczą usługi pośrednie. F. Hofman zwraca uwagę na konieczną ochronę praw podstawowych jak prawa do informacji czy do wyrażania opinii, które stoją w opozycji do wprowadzanych regulacji przez DSA⁵. W motywie 69 preambuły Rozporządzenia stanowiącym o zagrożeniach wynikających z reklamy internetowej możemy znaleźć następujące stwierdzenie: „Platformy internetowe są szczególnie wrażliwym środowiskiem, jeżeli chodzi o takie praktyki i stwarzają większe zagrożenie społeczne”. Potwierdza to tezę, że nie wszystkie strony internetowe dostępne w internecie, które prezentują reklamy na swoich interfejsach internetowych, będą adresatami obowiązków wynikających z DSA, a wyłącznie te, które będą spełniać definicję platformy internetowej, gdyż zdaniem ustawodawcy europejskiego korzystanie z nich wiąże się z większymi zagrożeniami w porównaniu z pozostałymi kategoriami usługodawców.

Zakres zastosowania przepisów DSA wynika także jasno z literatury zagranicznej. Mając na uwadze wymóg interpretacji przepisów DSA w sposób spójny, konieczne jest przyjrzenie się wykładni przepisów DSA w innych krajach Unii Europejskiej. F. Hofman wskazuje, że to usługi pośrednie stanowią szczególny rodzaj usług, który powinien być bardziej szczegółowo uregulowany niż reszta usług pozostających na rynku, z uwagi na ich funkcję, która pozwala na tworzenie i publikowanie treści przez samych użytkowników⁶. Zdaniem tego autora należy wyraźnie rozróżnić podmioty będące serwisami contentowymi, ale posiadającymi pełną kon-

⁵ F. Hofman, B. Raue, *Digital Services Act: Gesetz über digitale Dienste*, Baden-Baden 2023, s. 50.

⁶ *Ibidem*, s. 88.

trolę nad treścią, która się na takich serwisach znajduje (np. Spotify), oraz podmioty świadczące usługi pośrednie, w tym platformy internetowe, które nie są w stanie kontrolować treści udostępnianych przez ich użytkowników (np. YouTube)⁷. Takie uzasadnienie pozwala rozgraniczyć celowościowo konieczność stosowania DSA wyłącznie do podmiotów, które nie są w stanie kontrolować treści dodawanych przez samych użytkowników takiego serwisu i z tego powodu ryzyko wystąpienia naruszeń jest większe.

Zaskakujące może być jednak to, że uzasadnienie celowościowe wymienionych przykładowo regulacji z art. 25 i 26 DSA jest znacznie szersze niż wyłącznie to, które wyznacza definicja platformy internetowej. Z punktu widzenia użytkownika może wydawać się to bez znaczenia, czy reklama targetowana wyświetla mu się na interfejsie platformy internetowej w rozumieniu DSA, tj. np. Facebooku, czy stronie gazety internetowej bądź innej stronie internetowej, która nie będzie objęta DSA. W obu przypadkach następuje zagrożenie związane z tym, że użytkownik będzie poddany praktykom manipulacyjnym lub że zostanie on sprofilowany z wykorzystaniem szczególnych kategorii danych osobowych i na tej podstawie zostanie wyświetlona mu reklama. Z DSA wynika jednak wniosek, że wyłącznie na portalach stanowiących platformę internetową w rozumieniu Rozporządzenia taki zakaz będzie musiał być przestrzegany, a na innych stronach internetowych takie praktyki będą dalej dozwolone.

Stąd niezwykle istotna jest właściwa interpretacja przesłanek definicji platformy internetowej. Zdaniem autorki bowiem jedynie nieliczne strony internetowe dostępne na rynku będą mogły zostać uznane za spełniające przesłanki platformy internetowej, a tym samym będą zobowiązane do przestrzegania przepisów DSA. Pozostały obszar dostawców usług pośrednich, które nie będą objęte definicją platformy internetowej, pozostanie całkowicie poza regulacjami z art. 19-43 DSA.

Oczywiście ta konstatacja nie wyklucza możliwości zastosowania innych, istniejących już aktów prawnych takich jak Dyrektywa E-commerce, o czym stanowi wprost art. 2 ust. 3 DSA. Rozporządzenie stanowi rozwinięcie regulacji wprowadzonych Dyrektywą E-commerce, a nie całkowicie je zastępuje, i tak też należy interpretować rolę DSA⁸. Dodatkowo, DSA bezpośrednio w art. 2 ust. 4 stanowi, że akt ten „nie pozostaje

⁷ Także w ten sposób: X. Konarski, *Status prawny platform internetowych na podstawie projektu Aktu o usługach cyfrowych (AUC)*, „Prawo Nowych Technologii” 2021, nr 1, s. 63.

⁸ F. Hofman, B. Raue, *op. cit.*, s. 67. Autorzy ci wskazują także, że w odniesieniu do regulacji wynikających z Dyrektywy E-commerce dalej obowiązywać będzie zasada państwa pochodzenia, podczas gdy DSA nie uzależnia zastosowania swoich regulacji od państwa pochodzenia usługodawcy, lecz terytorium odbiorców usługi pośredniej (art. 2 ust. 1 DSA).

bez uszczerbku dla przepisów ustanowionych w innych aktach prawnych Unii regulujących inne aspekty świadczenia usług pośrednich na rynku wewnętrznym lub określających i uzupełniających niniejsze rozporządzenie”. W cytowanym przepisie podkreślono, że DSA nie stanowi regulacji wyłączającej stosowanie wymienionych regulacji do innych aspektów usług pośrednich poza tymi wskazanymi w DSA. Przykładem takiego zastosowania będą przepisy konsumenckie, regulujące prawa autorskie oraz dane osobowe, tj. te zawarte np. odpowiednio w: rozporządzeniu 2017/2394⁹, dyrektywie 2001/29/WE¹⁰ czy RODO¹¹. W zakresie nieuregulowanym w DSA możliwe są także przepisy krajowe państw członkowskich Unii Europejskiej.

3. Składowe definicji platformy internetowej w DSA

Definicja platformy internetowej jest złożona i zostanie odtworzona od najszerszego do najwęższego pojęcia, w które została ujęta. Złożoność pojęcia zostanie zaprezentowana od strony negatywnej, poprzez położenie akcentu na ilość wyłączeń spod rozumienia pojęcia platformy internetowej na gruncie DSA, która wynika z ukształtowania definicji opartej na utrwalonych wcześniej pojęciach istniejących w prawie UE lub orzecznictwie TSUE.

Po pierwsze, platforma internetowa to usługa społeczeństwa informacyjnego, której definicja przypisana jest do pojęcia „usługi” w art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535, zgodnie z którą: „jest to każda usługa normalnie świadczona za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usługi”¹². Po drugie, DSA wprowadza nowe pojęcie usługi pośredniej, do której następnie w wielu miejscach odwołuje się DSA. Pojęcie to zostało zdefiniowane przez odesłanie

⁹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2394 z dnia 12 grudnia 2017 r. w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów i uchylające rozporządzenie (WE) nr 2006/2004, Dz. Urz. UE L 345/1 z 27.12.2017 r. z późn. zm.

¹⁰ Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym, Dz. Urz. WE L 167/10 z 22.06.2001 r. z późn. zm.

¹¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE L 119/1 z 4.05.2016 r. z późn. zm.

¹² Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego, dalej: „Dyrektywa 2015/1535”, Dz. Urz. UE L 241 z 17.09.2015 r.

do innych definicji, bowiem na gruncie art. 3 lit. g) DSA, usługa pośrednia to jedna z wymienionych usług społeczeństwa informacyjnego: „zwykłego przekazu”, „cachingu” lub „hostingu”, które zostały zdefiniowane w DSA i stanowią katalog zamknięty. W zakresie niniejszego opracowania znaczenie będzie miała ostatnia z nich – usługa hostingu, w której mieści się pojęcie platformy internetowej. Po trzecie, usługa hostingu polega na: „przechowywaniu informacji przekazanych przez odbiorcę usługi oraz na jego żądanie”. Po czwarte, w definicji „platformy internetowej” z art. 3 lit. i) DSA, ustawodawca europejski stanowi, że platforma internetowa to usługa hostingu w rozumieniu jak wskazano powyżej, jednak, oprócz przechowywania na żądanie odbiorcy informacji przez niego przekazanych (jak w przypadku usługi hostingu), usługa ta powinna także rozpowszechniać publicznie te informacje na żądanie odbiorcy usługi, tj. udostępniać je potencjalnie nieograniczonej liczbie osób trzecich (art. 3 lit. k) DSA).

Wskazane przesłanki zostały określone w sposób pozytywny. Definicja platformy internetowej zawiera także wyłączenie ze swojego zakresu dostawców platform internetowych, których działanie polegające na przechowywaniu i rozpowszechnianiu informacji na żądanie odbiorcy jest nieznaczną lub wyłącznie poboczną cechą innej usługi lub nieznaczną funkcją głównej usługi, i ze względów obiektywnych i technicznych nie można z niej skorzystać bez takiej innej usługi, a włączenie takiej cechy lub funkcji w taką inną usługę nie jest sposobem na obejście stosowania niniejszego rozporządzenia.

Dopiero spełnienie wszystkich wskazanych przesłanek pozytywnych i brak wejścia w zakres przesłanki negatywnej pozwala na zakwalifikowanie danego podmiotu pod reżim DSA i konieczność zastosowania się do jego zasad dotyczących platform internetowych. Wyliczenie to nie uwzględnia dodatkowo istniejących wyłączeń przewidzianych np. w art. 19 DSA stanowiącym o braku zastosowania DSA do mikroprzedsiębiorstw lub małych przedsiębiorstw zgodnie z definicją w zaleceniu 2003/361/WE¹³ i innych przepisach Rozporządzenia.

3.1. Usługa społeczeństwa informacyjnego w DSA

Usługa społeczeństwa informacyjnego powinna być definiowana zgodnie z art. 1 ust. 1 lit. b) dyrektywy (UE) 2015/1535: „usługa” oznacza każdą usługę społeczeństwa informacyjnego, tj. każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług.

¹³ Zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Tekst mający znaczenie dla EOG) (notyfikowane jako dokument nr C(2003) 1422).

Dla niniejszych rozważań definicja usługi społeczeństwa informacyjnego jest o tyle istotna, że w przypadku, gdy dana usługa nie zostanie zakwalifikowana w zakres definicji usługi społeczeństwa informacyjnego, nie będzie mogła zostać uznana za usługę platformy internetowej.

Zakres rozumienia pojęcia usługi społeczeństwa informacyjnego był wielokrotnie poddawany pod osąd Trybunału Sprawiedliwości Unii Europejskiej¹⁴. Skupiając się jednak tylko na wyłączeniach spod tego pojęcia, należy zwrócić uwagę na orzeczenie TSUE z dnia 20 grudnia 2017 r., C-434/15 w sprawie *Asociación Profesional Elite Taxi przeciwko Uber Systems Spain SL*¹⁵, które dotyczy usług mieszanych, tj. świadczonych w części drogą elektroniczną i nieświadczonych w części tą drogą¹⁶. W przedmiotowym orzeczeniu TSUE zwrócił uwagę na konieczny warunek kwalifikacji danej usługi za usługę społeczeństwa informacyjnego, która zgodnie z art. 1 lit. b (ii) Dyrektywy 2015/1535 musi być „całkowicie przesyłana, kierowana i otrzymywana za pomocą kabla, fal radiowych, środków optycznych lub innych środków elektromagnetycznych”. Znamienne było zatem dla TSUE wyznaczenie sytuacji, w których usługa mieszana będzie mogła zostać uznana za całkowicie świadczoną drogą elektroniczną w przypadkach usług mieszanych, tj. takich, w których niektóre z usług wchodzących w zakres umowy zawartej z użytkownikiem końcowym nie były świadczone drogą elektroniczną.

Na podstawie wskazanego wyroku i opinii M. Szpunara przedstawionej 11 maja 2017 r. do omówionej sprawy należy sformułować następujące wnioski w zakresie podlegania pod definicję usługi społeczeństwa informacyjnego. Analizę należy przeprowadzać dwustopniowo, tj. (1) w pierwszej kolejności zbadać, czy usługa jest w ogóle świadczona drogą elektroniczną, do czego będzie konieczne wyodrębnienie głównego elementu tej usługi, który musi być świadczony drogą elektroniczną; a następnie ewentualnie dodatkowo określić, (2) czy część usługi mieszanej w zakresie nieświadczonym drogą elektroniczną jest niezależna gospodarczo od usługi świadczonej drogą elektroniczną.

Po pierwsze, aby ustalić, czy usługa jest świadczona drogą elektroniczną w rozumieniu Dyrektywy E-commerce, w przypadku usług mieszanych, w części świadczonych drogą elektroniczną i w części nieświadczonych drogą elektroniczną, konieczne

¹⁴ Dalej: „TSUE”.

¹⁵ Dalej: „sprawa Uber”. Podobna argumentacja znajduje się także w wyroku TSUE z 10.04.2018 r., C-320/16, *Uber France*.

¹⁶ Problem prawny rozpatrywany przez TSUE w omawianym wyroku powstał na gruncie usługi mieszanej, jaką świadczy Uber. Użytkownicy za pomocą aplikacji mogą zamawiać przejazdy (usługa świadczona drogą elektroniczną), jednak sam przewóz osoby jest dokonywany na podstawie usługi przewozu, która w oczywisty sposób nie stanowi usługi świadczonej drogą elektroniczną.

jest, aby główny element wykonywanej usługi był świadczony drogą elektroniczną¹⁷. Na przykład w przypadku sprzedaży internetowej, gdy umowa sprzedaży jest zawierana drogą elektroniczną, lecz towar jest dostarczany do kupującego w zakresie usługi przesłania go do zamawiającego, tj. usługi dostawy, należałoby uznać, że głównym elementem takiej usługi jest umowa sprzedaży zawarta za pośrednictwem usługodawcy świadczącego usługi drogą elektroniczną. Istotą takiej transakcji jest bowiem dokonanie sprzedaży towaru przez internet, a nie jego dostarczenie, które stanowi wyłącznie efekt tego, że sprzedający i kupujący nie znajdują się w jednym miejscu w tym samym czasie. W tym przypadku należałoby zatem uznać, że usługa sprzedaży online jest świadczona drogą elektroniczną, gdyż umowa sprzedaży, która stanowi główny element takiej usługi, jest zawierana drogą elektroniczną.

Po drugie, dla ostatecznego wniosku należy zbadać, czy taka złożona usługa, w części nieświadczona drogą elektroniczną, jest w części „nieelektronicznej” niezależna gospodarczo od usługi świadczonej drogą elektroniczną i ma charakter samodzielny. Przykładem podnoszonym w opinii M. Szpunara do sprawy C-434/15 jest relacja pomiędzy liniami lotniczymi czy hotelami a pośrednikami internetowymi sprzedającymi bilety lotnicze¹⁸. Wówczas należałoby uznać, że linie lotnicze czy hotele, których działalność jest niezależna od funkcjonowania platform internetowych i którzy wykorzystują platformy sprzedażowe pośredników jako jedno z form sprzedaży swoich usług, nie będą stanowić usługi zależnej gospodarczo od usługi świadczonej drogą elektroniczną.

Warty zaznaczenia w zakresie niniejszych rozważań jest także podkreślany w omawianym wyroku cel Dyrektywy 2015/1535, zauważany także w opinii M. Szpunara do wyroku TSUE w sprawie C-434/15¹⁹. Zasada liberalizacji usług społeczeństwa informacyjnego obecna w Dyrektywie 2015/1535 stałaby w sprzeczności z koniecznością objęcia zakresem zastosowania Dyrektywy części usług mieszanych, w zakresie których przeważająca część usługi mieszanej nie spełniałaby definicji usługi społeczeństwa informacyjnego. Inna wykładnia prowadziłaby do konieczności objęcia zakresem zastosowania Dyrektywy także tej części usługi mieszanej, która nie jest świadczona drogą elektroniczną.

¹⁷ *Ibidem*, pkt 35.

¹⁸ E. Bagińska, S. Majkowska-Szulc, *Granice prawne „uberyzacji”*. Glosa do wyroku TS z dnia 20 grudnia 2017 r., C-434/15, „Europejski Przegląd Sądowy” 2018, nr 5, s. 32, za opinią rzecznika generalnego TSUE, M. Szpunara, przedstawioną 11 maja 2017 r., sprawa C-434/15 *Asociación Profesional Elite Taxi przeciwko Uber Systems Spain SL*, pkt 32-35 oraz 57-60.

¹⁹ Opinia rzecznika generalnego TSUE, M. Szpunara, przedstawiona w dniu 11 maja 2017 r., sprawa C-434/15 *Asociación Profesional Elite Taxi przeciwko Uber Systems Spain SL*, pkt 31.

Jak skonkludował M. Szpunar w opinii do przywoływanego wyroku TSUE w sprawie C-434/15, nie każda działalność online związana z transakcjami handlowymi sama w sobie stanowi usługę społeczeństwa informacyjnego, w szczególności, gdy ma ona charakter jedynie pomocniczy, drugorzędny lub przygotowawczy i nie jest gospodarczo samodzielna²⁰. W tym kontekście usługa świadczona przez Uber, która została zakwalifikowana jak usługa przewozu, oderwana od usługi samego zamawiania pojazdu przez aplikację online, została zakwalifikowana w wyroku TSUE 434/15 jako niewchodząca w zakres pojęcia usługi społeczeństwa informacyjnego.

W kontekście wąskiej granicy wyznaczonej wyrokiem w sprawie Uber co do rozumienia pojęcia usługi społeczeństwa informacyjnego warto przywołać wyrok TSUE z dnia 19.12.2019 r., C-390/18 w sprawie *Airbnb Ireland*. TSUE w przedmiotowym wyroku argumentuje, że platforma Airbnb Ireland oferująca usługi pośrednictwa w zakwaterowaniu nie ma decydującego wpływu na warunki świadczenia usług zakwaterowania, do których odnosi się jej usługa pośrednictwa, ponieważ Airbnb Ireland nie ma wpływu na ceny czynszów, wybór wynajmujących czy nieruchomości, które są oferowane na platformie, w przeciwieństwie do wpływu, jaki Uber ma na usługi, w których pośredniczy. Oceniając powyższy wyrok, po lekturze jego uzasadnienia, nie sposób nie zgodzić się z przedstawianą tam argumentacją. Jednak z drugiej strony, z łatwością można wyobrazić sobie zupełnie inne rozłożenie akcentów niż w prezentowanych uzasadnieniach, które mogłyby prowadzić do zupełnie odmiennych wniosków, tj. tych, które byłyby bliższe prezentowanym w sprawie Uber. W zakresie wyroku dot. Airbnb mogłoby to być zwrócenie większej uwagi na usługi dodatkowe oferowane przez Airbnb, które są charakterystyczne dla usług pośrednika nieruchomości regulowanej innymi przepisami²¹, czy też możliwości wykluczania użytkowników z platformy, na co wskazuje się w doktrynie²².

Mając na uwadze powyższe rozumienie usługi społeczeństwa informacyjnego, należy powziąć następujące wnioski na gruncie DSA. W przypadku gdy dana usługa nie będzie mogła zostać uznana za usługę społeczeństwa informacyjnego, będzie pozostawać poza zakresem DSA²³. Oznacza to dla przykładu, że usługa oferowana przez Uber nie będzie mogła zostać uznana za usługę pośrednią, a co za tym idzie

²⁰ *Ibidem*, pkt 37.

²¹ Wyrok TS z dnia 19 grudnia 2019 r., C-390/18, *Postępowanie Karne Przeciwko X*, LEX nr 2753786, pkt 23.

²² A. Jabłonowska, *Pośrednictwo w zawieraniu umów najmu krótkoterminowego jako świadczenie usług społeczeństwa informacyjnego. Glosa do wyroku TS z dnia 19 grudnia 2019 r., C-390/18*, „Europejski Przegląd Sądowy” 2021, nr 4, s. 37.

²³ F. Hofman, B. Raue, *op. cit.*, s. 65.

usługę platformy internetowej²⁴. Za tym podąża kolejny wniosek: zasady z art. 28 DSA dotyczące projektowania i organizacji interfejsów internetowych nie będą miały zastosowania do aplikacji oferowanych przez Uber, gdyż usługa świadczona przez Uber została w sposób jednoznaczny zakwalifikowana jako niewchodząca w zakres pojęcia usługi społeczeństwa informacyjnego. W każdym przypadku zatem, aby określić zakres zastosowania DSA, należy na wstępie stwierdzić, czy usługodawca, który taką analizę wobec swoich usług przeprowadza, świadczy usługi społeczeństwa informacyjnego. Jeśli wniosek będzie negatywny, będzie to oznaczać, że zapisy DSA nie będą miały do takich usług zastosowania.

Do wskazanego wniosku należy dodać na marginesie kolejne zawężenie zastosowania przepisów DSA, które jednak należy oceniać pozytywnie. Art. 2 ust. 2 DSA, a szerzej motyw 6 preambuły DSA precyzuje: „W praktyce niektórzy dostawcy usług pośrednich pośredniczą w zakresie usług, które mogą, ale nie muszą być świadczone drogą elektroniczną, takich jak zdalne usługi technologii informacyjnej, transport, zakwaterowanie lub usługi doręczeń”.

4. Wnioski

Mając na uwadze poczynione rozważania, wydaje się, że DSA odnosi się we wskazanym zakresie do usług mieszanych, które w części stanowią usługę świadczoną drogą elektroniczną i mogą być uznane za taką usługę, lecz w części faktycznie jej nie stanowią, ale wobec właściwej wykładni prowadzonej w sposób jak wskazano powyżej, stosuje się do nich przepisy Dyrektywy E-commerce dot. usług społeczeństwa informacyjnego. Wobec tego w dalszej części motywu 6 preambuły DSA wprost stanowi: „Niniejsze rozporządzenie powinno mieć zastosowanie wyłącznie do usług pośrednich i nie powinno mieć wpływu na wymogi określone w prawie Unii lub prawie krajowym dotyczące produktów lub usług, których świadczenie odbywa się poprzez usługi pośrednie, w tym w sytuacjach, w których usługa pośrednia stanowi integralną część innej usługi, która nie jest usługą pośrednią zgodnie z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej”. W omawianym motywie ustawodawca europejski zakreśla zatem zakres zastosowania DSA wyłącznie do części usługi, która będzie usługą pośrednią na gruncie DSA, stano-

²⁴ Tak: C. Cauffman, C. Goanta, *A New Order: The Digital Services Act and Consumer Protection*, „European Journal of Risk Regulation” 2021, vol. 12, s. 764, w odniesieniu do możliwości skorzystania z wyłączeń określonych w art. 5 ust. 1 DSA, jednak wniosek ten można rozumieć szerzej, także w odniesieniu do zastosowania DSA *per se*.

wiąc, że do innych usług wchodzących w zakres usługi mieszanej DSA nie będzie miało zastosowania. Jako implikację w praktyce można przytoczyć przykład usługi *marketplace* i jej pobocznej usługi dostawy produktu do kupującego. Oczywisty jest wobec poczynionego wyводу wniosek, że choć możliwość korzystania z *marketplace* będzie usługą pośrednią, do części tej usługi dotyczącej dostawy nie będzie można zastosować przepisów DSA.

Bibliografia

I. Źródła (spis aktów prawnych, orzeczeń sądowych, trybunałów)

A. Akty prawne

Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz. Urz. WE L 167/10 z 22.06.2001 r. późn. zm.).

Zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Tekst mający znaczenie dla EOG) (notyfikowane jako dokument nr C(2003) 1422).

Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119/1 z 4.05.2016 r. z późn. zm.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065, z dnia 19 października 2022 r., w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), (Dz. Urz. UE L 277/1 z 27.10.2022 r.).

Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), (Dz. Urz. WE L 178/1 z 17.07.2000 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2394 z dnia 12 grudnia 2017 r. w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów i uchylające rozporządzenie (WE) nr 2006/2004 (Dz. Urz. UE L 345/1 z 27.12.2017 r. z późn. zm.).

B. Orzeczenia TSUE oraz opinia rzecznika generalnego TSUE

Wyrok TSUE z dnia 20 grudnia 2017 r., C-434/15, *Asociación Profesional Elite Taxi V. Uber Systems Spain Sl*, ZOTSiS 2017, nr 12, poz. I-981.

Wyrok TSUE z dnia 10 kwietnia 2018 r., C-320/16, *Uber France*.

Wyrok TSUE z dnia 19 grudnia 2019 r., C-390/18, *Postępowanie Karne Przeciwko X przy udziale YA, Airbnb Ireland UC, Hôtelière Turenne SAS, Association pour un hébergement et un tourisme professionnels (AHTOP), Valhotel*.

Opinia rzecznika generalnego TSUE, M. Szpunara przedstawiona w dniu 11 maja 2017 r., sprawa C-434/15 *Asociación Profesional Elite Taxi przeciwko Uber Systems Spain SL*.

II. Literatura (opracowania o charakterze naukowym)

Bagińska E., Majkowska-Szulc S., *Granice prawne „uberyzacji”*. Glosa do wyroku TS z dnia 20 grudnia 2017 r., C-434/15, „Europejski Przegląd Sądowy” 2018, nr 5.

Cauffman C., Goanta C., *A New Order: The Digital Services Act and Consumer Protection*, „European Journal of Risk Regulation” 2021, vol. 12.

Hofman F., Raue B., *Digital Services Act: Gesetz über digitale Dienste*, Baden-Baden 2023.

Jabłonowska A., *Pośrednictwo w zawieraniu umów najmu krótkoterminowego jako świadczenie usług społeczeństwa informacyjnego*. Glosa do wyroku TS z dnia 19 grudnia 2019 r., C-390/18, „Europejski Przegląd Sądowy” 2021, nr 4.

Konarski X., *Status prawny platform internetowych na podstawie projektu Aktu o usługach cyfrowych (AUC)*, „Prawo Nowych Technologii” 2021, nr 1.

Lost opportunities of the Digital Services Act? – considerations on the definition of an online platform – part I

Abstract

The article is divided into two parts. In the first one, the author discusses the objectives of the Digital Services Act, which are relevant to understanding the definition of an “online platform” and evaluating the regulations introduced. The author then begins to analyze the component definitions of an “online platform”, which include the concepts of an information society service (1) and a hosting service that stores and disseminates information to the public (2). The second of the component definitions of an “online platform”, is discussed in detail in the next part of the article. The meaning of the concept of dissemination to the public of information within the meaning of the DSA and the provision of a service at the “individual request of the recipient” of this service was developed. For a comprehensive analysis, it was also necessary to look at the exclusion implicit in the definition of an „online platform” in Article 3(i) of the DSA, concerning the minor and purely ancillary feature of the service of storing and disseminating information to the public at the request of the recipient of the service comparing to other services offered by the provider in question. At the end of the second part of the article, the author draws conclusions about the whole two parts of the article.

Keywords

Digital Services Act, DSA, online platform, intermediary service, hosting service

Dr Jarosław Greser

Politechnika Warszawska, Wydział Nauk Społecznych i Administracji

Vrije Universiteit Brussel, Cyber and Data Security Lab

ORCID: 0000-0002-1021-6142

Access to health data for scientific research. Remarks in the light of Article 40 DSA

Abstract

The primary objective of the Digital Services Act is to enhance the transparency of the operations of VLOPs and VLOSEs. This is achieved by ensuring the possibility of effective control by public entities and by preventing negative phenomena covered by systemic risks through research by independent researchers. However, the data that VLOPs and VLOSEs collect as part of their services can also be used for research for public good. This is particularly relevant in the case of information on the health status of their users. This data can be important in the development of new health products and services and for the planning of public policies in this area. This article explores whether the access to data provided for in Article 40 of the Digital Services Act allows for research in health-related areas.

The article is divided into four parts. The first part examines the concept of health data, and the second considers whether medical data falls within the purposes of allowing data sharing. The third part of the article analyses the conditions that limit the release of data for research purposes. The final part of the article contains conclusions and points out that the Digital Services Act allows health information to be made available for scientific research in this area, but that this is very limited by the conditions contained in the act. However, the interpretation of these conditions can vary, and it largely determines how much and what data researchers can receive in practice. Consequently, the role of the Digital Services Coordinators is of great importance in shaping the practice of fulfilling data access requests.

Keywords

health data, open science, VLOP, VLOSE, Digital Service Act, access to data

The role of user-generated data in medical research

The slogan ‘data is the new oil’ aptly reflects its importance in modern society. The development of the internet has led to an unprecedented opportunity in human history to generate and analyse data. According to some forecasts, the total amount of data generated by humans will reach 175 zettabytes per year by 2025, an increase of 530% compared to 2018¹, which seems to be a significant underestimate. The main sources

¹ *Europejska strategia w zakresie danych. Prognozy na 2025 r.* https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_pl [access 1.03.2024].

are the Internet of Things² and online platforms. In the case of the latter, the scale can be illustrated by the example of Facebook, which generates 510,000 comments and 136,000 photos every minute³, totalling 4 petabytes of data per day⁴.

This data includes various pieces of information that can be used in medical research, such as eating habits, well-being, side effects of drugs or medical devices, and treatment effectiveness⁵. This information offers more alternatives compared to traditional research that relied solely on medical records⁶. In the era of machine learning, opportunities have arisen to analyse data more accurately and combine it with information from other sources. This can lead to more precise analyses⁷ and a better understanding of the underlying structure and patterns in the data⁸. This has practical applications in medical research, including the treatment of chronic diseases⁹, improving the functioning of patients with neurodegenerative diseases¹⁰, predicting the occurrence and spread of infectious diseases¹¹, and finding new ways to treat mental illness¹². Additionally, it may have wide applications in evidence-based policy-making in such areas as national defence, public health, tackling climate change and improving public services¹³.

² J. Greser, *Wybrane problemy funkcjonowania Internetu Rzeczy w relacji do praw człowieka*, [in:] B. Gronowska, P. Sadowski (red.), *25-lecie wejścia w życie Europejskiej Konwencji Praw Człowieka w Polsce*, Toruń 2022.

³ O. Maddy, *Wild and Interesting Facebook Statistics and Facts*, <https://kinsta.com/blog/facebook-statistics/> [access 1.03.2024].

⁴ *Facebook Research*, <https://research.facebook.com/blog/facebook-s-top-open-data-problems/> [dostęp 1.03.2024].

⁵ J. Greser, *Etyczne problemy wdrażania medycznego Internetu Rzeczy*, „Prawo Mediów Elektronicznych” 2020 nr 3, p. 4–5.

⁶ R.I. Horwitz, *Comparison of epidemiologic data from multiple sources*, „Journal of Chronic Diseases” 1986, no 11, p. 889-896.

⁷ N. Peek, J.H. Holmes, J. Sun, *Technical Challenges for Big Data in Biomedicine and Health: Data Sources, Infrastructure, and Analytics*, „Yearbook Medical Informatics” 2014, no 1, p. 42-47.

⁸ L. Brady, W. Ting, *Chatting about ChatGPT: how may AI and GPT impact academia and libraries?*, „Library Hi Tech News Volume” 2023, no 3, p. 26.

⁹ D. Su *et al.*, *Does telemedicine improve treatment outcomes for diabetes? A meta-analysis of results from 55 randomized controlled trials*, „Diabetes Research and Clinical Practice” 2016, no 116, p. 136-148.

¹⁰ J. Greser, *A step forward in health-related IoT cybersecurity: remarks on the proposal for a liability for defective products directive*, „Frontiers Digital Health” 2023, no 5, <https://www.frontiersin.org/journals/digital-health/articles/10.3389/fdgth.2023.1193255/full> [access 1.03.2024].

¹¹ S. Yanga, M. Santillanab, S. C. Koua, *Accurate estimation of influenza epidemics using Google search data via ARG0*, „Proceedings of the National Academy of Sciences” 2015, no 47, p. 14473-14478.

¹² J. Ive *Leveraging the potential of synthetic text for AI in mental healthcare*, „Frontiers Digital Health” 2022, no 4, <https://doi.org/10.3389/fdgth.2022.1010202> [access 1.03.2024].

¹³ E. Hazelkorn, A. Gibson, *Public goods and public policy: what is public good, and who and what decides?*, „Higher Education” 2019, no 78, p. 260.

Access to data collected by private entities is often restricted due to the assumption that the data becomes the private property of the company upon collection¹⁴. As a result, the data falls under the protection of private law provisions such as trade secrets or database protection, and is excluded from the framework of provisions allowing access and re-use of public data¹⁵. This makes it very challenging, and in many cases impossible, to conduct research based on such data. However, new legal frameworks are emerging at the European Union level that may allow greater access to data held by private parties. One such framework is the European Health Data Space¹⁶, which is yet to be implemented. In the case of IoT devices, the Data Act¹⁷ regulates access to non-personal data and will play a significant role. The Digital Service Act¹⁸, one of the initiatives regulating the digital market in the EU, plays a crucial role for online platforms.

The purpose of this article is to examine the extent to which health data can be shared in compliance with Article 40 of the DSA, which establishes the normative framework for data sharing by online platforms. The article is divided into four sections. The first part analyses the concept of health data, followed by an analysis of whether medical data falls within the scope of purposes that allow data sharing. Thirdly, other conditions for data sharing outlined in the Digital Service Act are explored. The final part presents conclusions and recommendations.

The concept of health data

To define the concept of health data, it is necessary to refer to the General Data Protection Regulation (GDPR)¹⁹. This regulation provides a legal definition of ‘per-

¹⁴ P. Kyung, *Data as Public Goods or Private Properties?: A Way Out of Conflict Between Data Protection and Free Speech*, „Irvine Journal of International, Transnational, and Comparative Law” 2021, no 77, <https://scholarship.law.uci.edu/ucijil/vol6/iss1/5> [access 1.03.2024].

¹⁵ Communication from The Commission A European strategy for data, COM(2020) 66 final, p. 7.

¹⁶ Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM/2022/197 final.

¹⁷ Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), Dz. Urz. UE L 2023/2854 from 22.12.2023.

¹⁸ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), Dz. Urz. UE L 277 from 27.10.2022.

¹⁹ Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Dz. Urz. UE L 119 from 4.5.2016.

sonal data’, ‘data concerning health’, and related ‘biometric data’ and ‘genetic data’, which are subsets of ‘personal data’.

According to Article 4(1) of the GDPR, personal data means any information relating to an identified or identifiable natural person. It is crucial to note that any information, regardless of its expression, can be considered personal data²⁰. However, there is a tendency to classify information too broadly as personal data²¹. In practice, it can be challenging to distinguish between personal and non-personal information, especially when dealing with data collected from online platforms. When in doubt, it is advisable to apply the data protection regulations to such data, especially when personal and non-personal data sets are linked²². This provision enhances the legal certainty for researchers while also enabling access to data.

It is important to note that article 40(8)(d) of the DSA clearly states that both personal and non-personal data may be accessed, subject to specific data security and confidentiality requirements for each type of data. Additional conditions must be met for the former, which are directly derived from the data protection legislation. This includes Article 40(8)(g), which concerns the protection of data cited in the publication of research results. Therefore, researchers do not have to limit their research to just one type of data, nor is applying for personal data the sole reason for not gaining access.

The term ‘data concerning health’ is equally broad in scope. Pursuant to Article 4 (15) of GDPR, it refers to personal data that pertains to the physical or mental health of an individual, including the provision of healthcare services, and which discloses information about their health status. Recital 35 GDPR provides examples of such data, including information related to the registration and provision of healthcare services, as well as any information regarding a disease, disability, disease risk, medical history, clinical treatment, or the physiological or biomedical state of the data subject. Furthermore, the recital highlights that the information pertains to the data subject’s physical or mental health status in the past, present, or future, and can originate from various sources, including online platforms. The European Court of Justice²³ sup-

²⁰ P. Litwinski, *Komentarz do art. 4*, [in:] P. Litwinski (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2018, Legalis, NB 4.

²¹ N. Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, „Law, Innovation and Technology” 2018, no 1.

²² L. Brygave, L. Tossoni, *Commentary to article 4*, [in:] Ch. Kuner et al. (red.), *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford 2020, p. 113

²³ European Court of Justice judgment of 6.11.2033 case C-101/01, *Criminal proceedings against Bodil Lindqvist*, European Court Reports 2003, I-12971.

ports the trend towards a comprehensive interpretation of health data, as evidenced by its recognition of sick leave as such information. It is important to note that, under Article 9(1) of the GDPR, data concerning health is considered a special category of personal data. From the point of view of the requirements under the DSA, this will be relevant in determining the higher level of protection of the data received, which must be provided by the researcher, and the burden of proof that he or she is able to do so lies with the researcher²⁴.

Health data may also encompass ‘biometric data’ and ‘genetic data’. Biometric data refers to the physical, physiological, or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person. These include, but are not limited to, the characteristics of the iris of the eye, the colour of the voice, the pattern of blood vessels. Furthermore, the literature indicates that biometric data encompasses behavioural characteristics, including the manner in which a person moves²⁵. Generally, biometric data remains constant throughout an individual’s life²⁶. Biometric data is obtained through technical methods that allow for the unique identification of an individual. This may include data related to health status, but further analysis is required in this area. The literature suggests that processing biometric data carries the risk of discriminatory misidentifications²⁷, bias²⁸, or other violations of individual rights²⁹. It is important to note that the DSA does not impose an obligation to process data in a way that avoids these issues. Therefore, the mere suspicion of such conduct is not sufficient grounds for denying access to data. However, such actions are in clear violation of research ethics, and may breach national and EU laws and results obtained through such means cannot be considered reliable.

When it comes to genetic data, the matter is more complicated. According to Article 4(13) GDPR, this includes ‘personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from

²⁴ J. Greser, *Zasady dostępu i wykorzystania danych posiadanych przez VLOP i VLOSE przez Komisję Europejską i Koordynatorów do spraw usług cyfrowych*, „Prawo Nowych Technologii” 2023, no 3-4, p. 147.

²⁵ P. Litwinski, *Komentarz do art. 4...*, NB 137.

²⁶ L. Brygave, L. Tossoni, *op. cit.*, p. 208.

²⁷ J. Buolamwini, T. Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, „Proceedings of Machine Learning Research” 2018, no 81, p. 1-15.

²⁸ C. Schwemmer, C. Knight, E. D. Bello-Pardo, S. Oklobdzija, M. Schoonvelde, J. W. Lockhart, *Diagnosing Gender Bias in Image Recognition Systems*, „Socius” 2020, no 6, p. 1-17.

²⁹ V. Eubanks, *Automating Inequality. How High-Tech Tools Profile, Police, and Punish the Poor*, New York 2018, p. 17.

an analysis of a biological sample from the natural person in question'. One of the conditions for classifying information as genetic data is that it provides unique information about the individual's health³⁰, which automatically categorises it as health data³¹. Although there is no automatic classification for physiological traits, they may also fall under the scope of health data due to the broad definition. It is important to note that obtaining such information requires specialised technical means. However, recital 34 GDPR states that any means leading to equivalent information from DNA or RNA samples can be used. As an example, it is possible to obtain genetic data through image analysis³². It is possible that the platform may process genetic test of images posted by users for instance on social media. This is especially true since genetic tests have applications beyond medical purposes. It is important to note that if the analysis does not pertain to physiology or health, the data will not be considered genetic data³³.

General rules on access to data for scientific purposes

Article 40 of the Digital Services Act outlines the principles for data sharing. These principles can be divided into three groups: defining who can receive and share data, specifying what data can be transferred, and establishing the procedure for requesting and terminating access to data. This article will focus on the first two premises, which are central to the problem under analysis.

Scope of subject matter

Under Article 40, the only entities obliged to share data are very large online platforms (VLOP) and very large online search engines (VLOSE). The criteria for determining these categories are defined in Article 33 of the DSA and are based on the ratio of users to the population in the EU. The Commission designated 23 VLOPs and VLOSEs. The first 19 entities were designated on 25 April 2023³⁴,

³⁰ P. Litwinski, *Komentarz do art. 4, op. cit.*, NB 132.

³¹ L. Brygave, L. Tossoni, *op. cit.*, p. 203.

³² Y. Gurovich *et al.*, *Identifying facial phenotypes of genetic disorders using deep learning*, „Nature Medicine” 2019, no 25, p. 60–64.

³³ L. Brygave, L. Tossoni, *op. cit.*, p. 202.

³⁴ *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413 [access 1.03.2024].

three additional VLOPs were designated on 20 December 2023³⁵, and the last one was designated on 26 April 2024³⁶. Two of designated VLOP have appealed against the Commission's decision to the ECJ³⁷. Given the criteria for recognition as VLOP and VLOSE, no significant change in the number of compliant companies is expected. Such a regime excludes other online platforms, including those that are independent entities under commercial law but under the effective control of VLOP and VLOSE. This could include start-ups or companies that benefit from preferential access to data, computing power or infrastructure in exchange for services to these entities. This appears to be a loophole that creates the possibility of circumventing the provisions of the Regulation, despite the fact that the issue of attributing liability to the entity exercising effective control has been advocated in both public³⁸ and private law³⁹ doctrine for many years. This should be seen as a significant shortcoming of the Regulation. It seems that a better criterion for assessing whether a platform should exchange information is the systemic risk it poses. The analysis of DSA recitals 76 and 79 shows that this concept has been used to justify the automatic inclusion of VLOP and VLOSE in additional obligations. At the same time, there is no tool to examine whether such risks are created by other actors.

Those who may request access to data are divided into two groups: vetted researchers referred to in Article 40(8) and researchers referred to in Article 40(12). For the first group, the decision to grant this status is taken by the Digital Services Coordinator of the institution, after a number of conditions set out in this article have been met. These include being part of a research organisation, acting independently from commercial interests, disclosing the funders of the research, being able to meet specific data security and confidentiality requirements, demonstrating that the research is carried out for the purposes set out in Article 40(4) and that the results will contribute to the achievement of those purposes, using the necessary and proportionate amount of data to carry it out, and making the results of its research publicly available free

³⁵ Supervision of the designated very large online platforms and search engines under DSA, <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> [access 1.03.2024].

³⁶ Commission designates Shein as Very Large Online Platform under the Digital Services Act, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2326 [access 30.04.2024].

³⁷ J. Tar, *Amazon joins Zalando in challenging very large online platform designation*, <https://www.euractiv.com/section/platforms/news/amazon-joins-zalando-in-challenging-very-large-online-platform-designation/> [access 1.03.2024].

³⁸ A. Clapham, S. Jerbi, *Categories of Corporate Complicity in Human Rights Abuses*, „Hastings International and Comparative Law Review” 2001, no 24, p. 339-349.

³⁹ P. Muchlinski, *Multinational Enterprises and the Law*, Blackwell 1999, p. 336-338.

of charge. The cumulative fulfilment of these conditions is required, which may be difficult given their evaluative nature and uncertainties in their interpretation⁴⁰. At the same time, achieving this status is rewarded by the opportunity to access data that is not publicly available and is legally protected, for example, by trade secret or personal data protection rules. In addition, they may carry out research for the detection, identification and understanding of systemic risks in the Union, as referred to in Article 34(1) DSA, and for the assessment of the adequacy, effectiveness and impact of risk mitigation measures, as referred to in Article 35 DSA.

The decision to grant the status of researcher is a matter for the VLOP or VLOSE, which will independently assess the fulfilment of the conditions set out in Article 40(12). These include independence from commercial interests, disclosure of the funders of the research, ability to meet the specific data security and confidentiality requirements, demonstration that the research is carried out for the sole purpose of detecting, identifying and understanding systemic risk in the Union, as referred to in Article 34(1), and that the results obtained will contribute to the achievement of that objective, using the necessary and proportionate amount of data to carry out the research. Fewer requirements to be met will result in limited access to information, which only cover data publicly available in the VLOP or VLOSE online interface. However, the data should be available in real time. It should be noted that both the wording of the provision itself and recital 97 DSA indicate that the status of researcher can be obtained by individuals who are not affiliated to a research organisation. This leaves considerable scope for the development of research within citizen science⁴¹.

Scope of data shared

The authors of the DSA have opted for an open catalogue of data that can be requested by researchers, but the scope of which is determined by the purposes for which they are to be used. As mentioned above, they relate to the issues identified in Articles 34 and 35 of the DSA. From the perspective of access to health information, the key question is whether it falls within the scope of systemic risk, which is a central concept used in these provisions. It should be noted that it is not defined, so it is necessary to refer to the definitions developed by researchers specialising in risk studies. According

⁴⁰ J. Greser, *Access to data for academic purposes under the Digital Services Act*, „Przegląd Europejski” [in print].

⁴¹ B. Balázs et al., *Data Quality in Citizen Science*, [w:] K. Vohland et al. (red.), *The science of citizen science*, Berlin 2021, p. 139-199.

to the literature, systemic risk refers to “risk or probability of breakdowns in an entire system, as opposed to breakdowns in individual parts or components, and is evidenced by co-movements (correlation) among most or all parts”⁴². It also has the potential for a threat or hazard to propagate disruptions or losses to multiple interconnected parts of complex systems⁴³. It is used in a similar context in legislation regulating the financial system, for example in Article 2(c) of Regulation 1092/2010⁴⁴. In view of this and the content of the recitals of the DSA, it must be assumed that the analysis goes far beyond effects that are merely infringements of the law. It is also necessary to analyse the legal content that may increase the level of systemic risk⁴⁵.

In addition, Article 34(1) identifies the areas of systemic risk to be taken into account in the risk analysis. In addition to Article 34(1)(d), issues related to the health of individuals have not been directly identified, but the interpretation of the provisions makes it possible to identify areas that will touch on it. The first is the risks associated with the dissemination of illegal content through VLOP and VLOSE services. In particular, this will concern matters that are explicitly prohibited by criminal law of individual Member States. These include offers for the sale of counterfeit medicines or information on the production of medicines. At the same time, it appears that misinformation and fake news will not be covered by this provision, as long as they are not prohibited by national law.

The second area is the risk of ‘actual or foreseeable negative effects for the exercise of fundamental rights’. In the Charter of Fundamental Rights⁴⁶ we find references to health in Article 3, which refers to the right to the integrity of the person, in Article 31 on fair and just working conditions, and in Article 35, which states that a high level of human health protection shall be ensured. It should be noted that this area is very broad and will include other rights contained in the Charter, in line with the concept of interdependence of human rights⁴⁷.

⁴² G. Kaufman, S. Kenneth, *What is systemic risk, and do bank regulators retard or contribute to it?*, „Independent Review” 2003, no 7, p. 372.

⁴³ O. Renn *et al.*, *Systemic Risks from Different Perspectives*, „Risk Analysis” 2022, no 42, p. 1903, <https://doi.org/10.1111/risa.13657> [access 1.03.2024]; International Risk Governance Council, *Guidelines for the governance of systemic risks*, Lausanne 2018.

⁴⁴ Regulation (EU) No 1092/2010 of the European Parliament and of the Council of 24 November 2010 on European Union macro-prudential oversight of the financial system and establishing a European Systemic Risk Board, Dz. Urz. UE L 331 from 15.12.2010.

⁴⁵ P. Podrecki, *Komentarz do art. 34*, [in:] M. Grochowski (red.), *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, Warszawa 2024, NB 10.

⁴⁶ Charter of Fundamental Rights of the European Union, Dz. Urz. UE C 326/02 from 26.10.2012.

⁴⁷ M. Nowak, *Introduction to the International Human Rights Regime*, The Hague 2003, p. 70.

As mentioned above, Article 34(1)(d) requires the assessment of risks associated with serious negative consequences for the physical and mental well-being of the person. As stated in the literature, the potential harm to mental health is significant⁴⁸. It is important to note the evaluative nature of the term “serious”. It seems to be interpreted as referring to effects that are occurring now. However, it is worth highlighting that many services provided by online platforms are reported to have a negative impact on mental health in the distant future⁴⁹.

A separate area is that of public health information. This concept has no legal definition and is said to cover a wide range of activities such as education, promotion of healthy lifestyles, research into the prevention of disease and injury, and the detection, prevention and response to infectious diseases⁵⁰. It should be noted that, according to Article 4(2)(k) of the Treaty on the Functioning of the European Union, public health is a shared competence between the Union and the Member States. As explained in the doctrine, this makes it possible to distinguish the following areas of Union action: patients’ rights in cross-border healthcare, including the coordination of social security systems; combating health risks, including those related to communicable diseases; blood transfusions; transplantation of human tissues and organs; control of the quality and safety of medicinal products, medical devices and cosmetics; mutual recognition of professional qualifications, including in the health professions; biotechnologies and cell banks; promotion of healthy lifestyles⁵¹. It is therefore reasonable to assume that at least these issues should be covered by the systemic risk analysis carried out by VLOP and VLOSE, and thus fall within the scope of data to which vetted researchers can apply for access. It also seems that such a broad public health perspective provides a basis for analyses of misinformation and fake news, all the more so as they have very acute effects in this area and online services, especially social media, are one of the main sources of their dissemination⁵².

⁴⁸ J. Gao *et al.*, *Mental health problems and social media exposure during COVID-19 outbreak*, „PLOS one”, 2020, <https://doi.org/10.1371/journal.pone.0231924> [access 1.03.2024].

⁴⁹ S. Chancellor, M. De Choudhury, *Methods in predictive techniques for mental health status on social media: a critical review*, „npj Digital Medicine” 2020, no 3, <https://doi.org/10.1038/s41746-020-0233-7> [access 1.03.2024].

⁵⁰ *What is public health?*, <https://www.hsph.harvard.edu/communications-guide/what-is-public-health/> [access 1.03.2024].

⁵¹ J. Barcik, *Odpowiedzialność publicznoprawna*, [in:] A. Barczak-Oplustil, T. Sroka (red.), *System Prawa Medycznego*, vol. 6, Warszawa 2023, p. 194-195.

⁵² C. Melchior, M. Oliveira, *Health-related fake news on social media platforms: A systematic literature review*, „New Media&Society” 2021, no 6, <https://journals.sagepub.com/doi/abs/10.1177/14614448211038762> [access 1.03.2024].

In the case of Article 35 DSA on risk reduction measures, it is not possible to distinguish directly between areas relating to individual health and those relating to public health. However, this does not mean that such information is not available. On the contrary, it seems that any of the measures mentioned in this article may apply to a health-related area. In the case of this provision, the focus is on the functional aspect and the effectiveness of the solutions used by VLOP and VLOSE to reduce the risks defined in Article 34 of DSA. Therefore, the scope of the shared data will include all the information that can be requested under this Article.

Conclusions

There is no doubt that the data collected by online platforms is a very valuable source of analysis for researchers working in both individual and public health. It can provide new insights or complement conclusions drawn from other information. Its importance is growing with the development of machine learning algorithms and their increasing use in medicine. At the same time, access to information held by private parties is very limited. Against this background, the Digital Services Act was passed, which explicitly formulates rules for data sharing. The analysis of the DSA allows us to answer the first part of the research question posed in the introduction in the affirmative, as the DSA allows health information collected by online platforms to be extracted and used for research purposes. This should be seen as a step in the right direction and a clearly positive solution that will benefit society as a whole.

On the other hand, when assessing the scope of the data to be exchanged by VLOP and VLOSE, it should be noted that their scope will cover all data, i.e. both personal and non-personal data, and in the case of the former, also biometric and genetic data. The absence of restrictions in this respect is to be well appreciated. Similarly, the requirement for researchers to meet certain criteria for the protection of such data should be welcomed. However, care must be taken to ensure that this requirement does not become a barrier to access. In this respect, the practice of the Digital Services Coordinator of Establishment for vetted researchers and VLOP and VLOSE for researchers will play an important role.

On the other hand, the restriction of data sharing to VLOP and VLOSE can only be assessed negatively. Especially in the case of health research, it could be useful for researchers to obtain information from online platforms that do not have this status. These could be, for example, blog sites or specialised online forums. Similarly,

the vague requirements for obtaining the status of vetted researcher and researcher and, in the case of the latter, the restriction on the scope of the research conducted, should be evaluated. Nevertheless, compared to the legal situation prior to the adoption of the DSA, at least we have a defined circle of institutions that can submit applications and a procedure for their examination by bodies independent of VLOP and VLOSE, which is a significant step forward.

Regarding the scope of data to be shared, the design of the legislation allows for both individual and public health information. Limiting the scope by specifying objectives related to research and systemic risk mitigation does not seem particularly restrictive if a research-friendly interpretation is adopted. This is particularly the case given the broad scope of the rights covered by the Charter of Fundamental Rights and the variety of aspects covered by public health.

In conclusion, the Digital Service Act is an important step towards making privately collected data more accessible. Its adoption and consideration should be seen as clearly positive. However, it is important to highlight the limitations that arise from it. These are the result of the area it regulates, i.e. the creation of a safe, predictable and trustworthy online environment, and not the direct regulation of access to data. However, it seems to open the way for further regulations that will allow access to data by more actors and for more purposes.

Bibliography

- Balázs B. *et. al.*, *Data Quality in Citizen Science*, [in:] K. Vohland *et al.* (red.), *The science of citizen science*, Berlin 2021.
- Barcik J., *Odpowiedzialność publicznoprawna*, [in:] A. Barczak-Oplustil, T. Sroka (red.), *System Prawa Medycznego*, vol. 6, Warszawa 2023.
- Brady L., Ting W., *Chatting about ChatGPT: how may AI and GPT impact academia and libraries?*, „Library Hi Tech News Volume” 2023, no 3, p. 26.
- Brygave L., Tossoni L., *Commentary to article 4*, [in:] Ch. Kuner *et al.* (red.), *The EU General Data Protection Regulation (GDPR). A commentary*, Oxford 2020.
- Buolamwini J., Gebru T., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, „Proceedings of Machine Learning Research” 2018, no 81.
- Chancellor S., De Choudhury M., *Methods in predictive techniques for mental health status on social media: a critical review*, „npj Digital Medicine” 2020, no 3.
- Clapham A., Jerbi S., *Categories of Corporate Complicity in Human Rights Abuses*, „Hastings International and Comparative Law Review” 2001, no 24.
- Eubanks V., *Automating Inequality. How High-Tech Tools Profile, Police, and Punish the Poor*, New York 2018.

- Facebook Research, <https://research.facebook.com/blog/facebook-s-top-open-data-problems/>.
- Gao J. et al., *Mental health problems and social media exposure during COVID-19 outbreak*, „PLOS one” 2020, <https://doi.org/10.1371/journal.pone.0231924>.
- Greser J., *A step forward in health-related IoT cybersecurity: remarks on the proposal for a liability for defective products directive*, „Frontiers Digital Health” 2023, no 5 <https://www.frontiersin.org/journals/digital-health/articles/10.3389/fdgh.2023.1193255/full>.
- Greser J., *Access to data for academic purposes under the Digital Services Act*, „Przegląd Europejski” (in printing).
- Greser J., *Etyczne problemy wdrażania medycznego Internetu Rzeczy*, „Prawo Mediów Elektronicznych” 2020 nr 3, p. 4–5.
- Greser J., *Wybrane problemy funkcjonowania Internetu Rzeczy w relacji do praw człowieka*, [in:] B. Gronowska, P. Sadowski (red.), *25-lecie wejścia w życie Europejskiej Konwencji Praw Człowieka w Polsce*, Toruń 2022.
- Greser J., *Zasady dostępu i wykorzystania danych posiadanych przez VLOP i VLOSE przez Komisję Europejską i Koordynatorów do spraw usług cyfrowych*, „Prawo Nowych Technologii” 2023, no 3-4.
- Gurovich Y. et al., *Identifying facial phenotypes of genetic disorders using deep learning*, „Nature Medicine” 2019, no 25.
- Hazelkorn E., Gibson A., *Public goods and public policy: what is public good, and who and what decides?*, „Higher Education” 2019, no 78.
- Horwitz R.I., *Comparison of epidemiologic data from multiple sources*, „Journal of Chronic Diseases” 1986, no 11, p. 889-896.
- Europejska strategia w zakresie danych. Prognozy na 2025 r.*, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_pl.
- International Risk Governance Council, *Guidelines for the governance of systemic risks*, Lausanne 2018 International Risk Governance Council, *Guidelines for the governance of systemic risks*, Lausanne 2018.
- Ive J., *Leveraging the potential of synthetic text for AI in mental healthcare*, „Frontiers Digital Health” 2022, no 4, <https://doi.org/10.3389/fdgh.2022.1010202>.
- Kaufman G., Kenneth S., *What is systemic risk, and do bank regulators retard or contribute to it?*, „Independent Review” 2003, no 7.
- Kyung P., *Data as Public Goods or Private Properties?: A Way Out of Conflict Between Data Protection and Free Speech*, „Irvine Journal of International, Transnational, and Comparative Law” 2021, no 77, <https://scholarship.law.uci.edu/ucijil/vol6/iss1/5>.
- Litwiński P., *Komentarz do art. 4*, [in:] P. Litwiński (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2018.
- Maddy O., *Wild and Interesting Facebook Statistics and Facts*, <https://kinsta.com/blog/facebook-statistics/>.
- Melchior C., Oliveira M., *Health-related fake news on social media platforms: A systematic literature review*, „New Media&Society” 2021, no 6, <https://journals.sagepub.com/doi/abs/10.1177/14614448211038762>.

- Muchlinski P., *Multinational Enterprises and the Law*, Blackwell 1999.
- Nowak M., *Introduction to the International Human Rights Regime*, The Hague 2003.
- Peek N., Holmes J.H., Sun J., *Technical Challenges for Big Data in Biomedicine and Health: Data Sources, Infrastructure, and Analytics*, „Yearbook Medical Informatics” 2014, no 1, p. 42-47.
- Podrecki P., *Komentarz do art. 34*, [in:] M. Grochowski (red.), *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, Warszawa 2024.
- Purtova N., *The law of everything. Broad concept of personal data and future of EU data protection law*, „Law, Innovation and Technology” 2018, no 1.
- Renn O. et al., *Systemic Risks from Different Perspectives*, „Risk Analysis” 2022, no 42, <https://doi.org/10.1111/risa.13657>.
- Schwemmer C., Knight C., Bello-Pardo E.D., Oklobdzija S., Schoonvelde M., Lockhart J.W., *Diagnosing Gender Bias in Image Recognition Systems*, „Socius” 2020, no 6.
- Su D. et al., *Does telemedicine improve treatment outcomes for diabetes? A meta-analysis of results from 55 randomized controlled trials*, „Diabetes Research and Clinical Practice” 2016, no 116.
- Tar J., *Amazon joins Zalando in challenging very large online platform designation*, <https://www.euractiv.com/section/platforms/news/amazon-joins-zalando-in-challenging-very-large-online-platform-designation>.
- Yanga S., Santillanab M., Koua S.C., *Accurate estimation of influenza epidemics using Google search data via ARGO*, „Proceedings of the National Academy of Sciences” 2015, no 47.

Dostęp do danych o stanie zdrowia do celów badań naukowych. Uwagi na tle art. 40 Aktu o usługach cyfrowych

Streszczenie

Głównym celem umożliwienia dostępu do danych w oparciu o Akt o usługach cyfrowych jest zwiększenie transparentności działania VLOP i VLOSE, w szczególności poprzez zapewnienie możliwości skutecznej kontroli przez podmioty publiczne oraz zapobieganie negatywnym zjawiskom objętym ryzykami systemowymi poprzez prowadzenie badań przez niezależnych badaczy. Jednocześnie dane, które zbierają VLOP i VLOSE w ramach świadczonych przez siebie usług, bardzo często obejmują informacje o stanie zdrowia swoich użytkowników. Dane te mogą mieć istotne znaczenie w tworzeniu nowych produktów i usług zdrowotnych oraz dla planowania polityk publicznych w tym obszarze. Celem artykułu jest udzielenie odpowiedzi na pytanie, czy dostęp do danych przewidziany w art. 40 Aktu o usługach cyfrowych pozwala na prowadzenie badań w obszarach dotyczących zdrowia. Artykuł podzielony jest na cztery części. W pierwszej przeanalizowano pojęcie danych dotyczących zdrowia, w drugiej zaś rozważano, czy dane medyczne wchodzą w zakres celów umożliwiających udostępnianie danych w oparciu o art. 40 Aktu o usługach cyfrowych. W trzeciej części analizie poddano warunki ograniczające udostępnienie danych do celów badań naukowych. Ostatnia część zawiera wnioski, zgodnie z którymi Akt o usługach cyfrowych pozwala na udostępnianie informacji o stanie zdrowia na potrzeby badań naukowych w tym obszarze, ale jest to bardzo ograniczone przez

warunki zawarte w tym akcie. Jednocześnie interpretacja tych warunków może być różnorodna, a od niej w dużej mierze zależy, ile i jakie dane mogą otrzymać naukowcy. Stąd istotną rolę odgrywać będą Koordynatorzy ds. usług cyfrowych, którzy ukształtują praktykę w zakresie realizowania wniosków o dostęp do danych.

Słowa kluczowe

dane o stanie zdrowia, dostęp do danych, VLOP, VLOSE, Akt o usługach cyfrowych, otwarta nauka

Michał R. Kolasiński

Uniwersytet Wrocławski

Wydział Prawa, Administracji i Ekonomii

Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej

ORCID: 0000-0003-2148-8116

Kwalifikacja prawna plików *cookie* jako danych osobowych oraz podstawy prawne ich przetwarzania

Streszczenie

Pliki *cookie* stanowią niezwykle istotne zagadnienie prawne związane m.in. z danymi osobowymi oraz marketingiem bezpośrednim. Niejasna kwalifikacja prawna plików *cookie* powoduje znaczne rozbieżności interpretacyjne oraz brak przestrzegania obowiązków prawnych w tym zakresie. Niniejsza publikacja poświęcona jest przede wszystkim ustaleniu, w jakich okolicznościach i w jakim zakresie pliki *cookie* mogą stanowić dane osobowe, poprzez omówienie przesłanek za tym stojących. Zagadnienie to zostanie przedstawione w kontekście orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej¹, wytycznych Europejskiej Rady Ochrony Danych i Grupy Roboczej Art. 29 oraz polskiego wymiaru sprawiedliwości, w tym w postępowaniach przed Prezesem Urzędu Ochrony Danych Osobowych². Celem tekstu jest przedstawienie praktycznego podsumowania rozważań Trybunału Sprawiedliwości Unii Europejskiej, wytycznych Europejskiej Rady Ochrony Danych i Grupy Roboczej Art. 29, rozważań Wojewódzkiego Sądu Administracyjnego w Warszawie oraz postępowania przed PUODO. Pliki *cookie* zostaną również przeanalizowane pod względem podstaw prawnych przetwarzania danych osobowych w nich zawartych. Podstawy legalizujące przetwarzanie danych osobowych zawartych w plikach *cookie* zostaną zaprezentowane w zestawieniu poszczególnych funkcji plików *cookie*.

Słowa kluczowe

pliki *cookie*, Prawo telekomunikacyjne, RODO, prawo Unii Europejskiej, prawo nowych technologii, e-prywatność, marketing bezpośredni, Trybunał Sprawiedliwości Unii Europejskiej, Urząd Ochrony Danych Osobowych.

Wstęp

Praktyka, orzecznictwo sądów powszechnych oraz postępowania przed Prezesem Urzędu Ochrony Danych Osobowych wykazują, że pliki *cookie* są zagadnieniem budzącym wątpliwości. W szczególności rozbieżności poglądów osadzają się

¹ Trybunał Sprawiedliwości Unii Europejskiej (dalej: „TSUE”).

² Prezes Urzędu Ochrony Danych Osobowych (dalej: „PUODO”).

na kwalifikacji plików *cookie* jako danych osobowych, co ma istotne znaczenie dla działalności każdego z administratorów danych osobowych, którzy posługują się narzędziami wykorzystującymi pliki *cookie*. Co więcej, skupienie się przez sądy i organy wyłącznie na tematyce ochrony danych osobowych oddała praktykę od najistotniejszej kwestii dotyczącej plików *cookie*, tj. od prywatności w łączności elektronicznej. Kolejną przeszkodą w ukształtowaniu się spójnej linii orzeczniczej jest fakt, że rozważania sądów oraz organów pozbawione są niestety analizy technicznego aspektu omawianych plików. Przedmiotem niniejszej pracy jest wykazanie, w jakich okolicznościach informacje zawarte w plikach *cookie* będą mogły nosić miano danych osobowych, oraz wskazanie podstaw prawnych ich przetwarzania.

Kwalifikacja prawna plików *cookie*

Nieodzownym elementem budowy stron internetowych, a także aplikacji mobilnych są pewne małe dane informatyczne zapisywane na urządzeniach końcowych użytkowników w określonych celach. Cele te mogą być związane z prowadzeniem bieżącej analityki stron www, tworzeniem statystyk, ułatwianiem korzystania ze stron internetowych czy stosowaniem marketingu bezpośredniego³. Wspomnianymi danymi informatycznymi są oczywiście pliki *cookie*. Nawet na podstawie tak wąskiego opisu technicznego możemy przyjąć, że pliki *cookie* są danymi informatycznymi zapisywanymi w postaci plików tekstowych umieszczanych w urządzeniach końcowych użytkowników, w określonych celach⁴. Ilekroć w niniejszej publikacji będzie mowa o plikach *cookie*, należy rozumieć je tak, jak przedstawiono w zdaniu poprzedzającym.

Na gruncie rodzimego prawa, a nawet prawa wspólnotowego nie znajdziemy definicji legalnej plików *cookie*. Należy zatem ustalić przepisy, które będą miały zastosowanie do niniejszej problematyki. Z poziomu przepisów krajowych nasuwają się dwie ustawy: o świadczeniu usług drogą elektroniczną⁵ oraz o prawie telekomunikacyjnym⁶.

³ X. Konarski, *Podstawy prawne korzystania z „ciasteczek” internetowych (cookies) jako przykład wzajemnej relacji przepisów RODO oraz przepisów o ochronie prywatności w sektorze łączności elektronicznej*, „Monitor Prawniczy” 2018, nr 22.

⁴ X. Konarski, *Część II rozdział VI punkt 3 litera c Podstawa prawna przetwarzania „ciasteczek” internetowych (Cookies)*, [w:] D. Lubasz (red.), *Meritum. Ochrona danych osobowych*, Warszawa 2020, s. 742.

⁵ Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz. U. z 2002 r. Nr 144, poz. 1204, t.j. Dz. U. z 2020 r. poz. 344 (dalej: „u.ś.u.d.e.”).

⁶ Ustawa z dnia 16 lipca 2004 r. o prawie telekomunikacyjnym, Dz. U. z 2004 r. Nr 171, poz. 1800, t.j. Dz. U. z 2024 r. poz. 34 (dalej: „pr. telkom”).

Zestawiając przepisy art. 5 ust. 3 Dyrektywy 2002/58/WE⁷, art. 6 pkt 2 u.ś.u.d.e. oraz art. 173 ust. 1 pr. telkom., możemy zauważyć pewne podobieństwa. Przede wszystkim można spostrzec, pomijając oczywiście różnice redakcyjne, że przepisy te dotyczą pewnego rodzaju *informacji zapisywanych na urządzeniach końcowych użytkowników*. Przez *urządzenia końcowe* należy rozumieć komputery, telefony, laptopy oraz inne urządzenia z wbudowaną pamięcią RAM lub trwałą zdolne do zapisywania informacji oraz pracy w internecie. *Zapisywane informacje* należy rozumieć m.in. jako pliki *cookie*.

Ze względu na swoje funkcje pliki *cookie* możemy podzielić na pięć rodzajów:

- 1) *cookie niezbędne* – umożliwiają poprawne funkcjonowanie strony oraz korzystanie z jej usług przez użytkowników;
- 2) *cookie analityczne* – służą zbieraniu informacji o sposobie wykorzystywania strony internetowej przez użytkowników;
- 3) *cookie funkcjonalne* – zapamiętują ustawienia użytkowników na stronach internetowych (kolor tła, język, koszyk zakupowy);
- 4) *cookie marketingowe/reklamowe* – służą dostarczaniu zindywidualizowanych reklam dla użytkownika. Reklamy są dostosowywane na podstawie preferencji oraz zainteresowań poszczególnych użytkowników;
- 5) *cookie społecznościowe* – umożliwiają łączenie się z mediami społecznościowymi oraz udostępnianie tam treści ze strony internetowej⁸.

Pojawienie się przepisów w polskim systemie prawnym odnoszących się do omawianej problematyki związanej z ochroną prywatności w cyberprzestrzeni wynika z implementacji Dyrektywy 2002/58/WE w ustawie o świadczeniu usług drogą elektroniczną i ustawie o prawie telekomunikacyjnym. Mając na uwadze, że aktualnie w polskim porządku prawnym istnieją dwie regulacje odnoszące się do problematyki plików *cookie*, należy zdecydować, która z nich powinna mieć zastosowanie. Powielenie przy transpozycji ma miejsce przede wszystkim przy art. 6 u.ś.u.d.e. oraz art. 173 pr. telkom. Warto zauważyć, że regulacje w ustawie o prawie telekomunikacyjnym zostały przyjęte później niż te w ustawie o świadczeniu usług drogą elektroniczną. Odpowiednie będzie zatem zastosowanie reguły kolizyjnej *lex posteriori derogat legi priori*⁹. Co więcej, warto odnotować, że przepisy prawa telekomunikacyjnego w znacznie szer-

⁷ Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (dalej: „Dyrektywa 2002/58/WE”).

⁸ M. Kolasiński, *Ciasteczkowe RODO – czyli pliki cookies a ochrona danych osobowych*, artykuł niepublikowany, 2020 r.

⁹ A. Bator, S. Kaźmierczak, *Rozdział V, chronologiczna reguła kolizyjna*, [w:] A. Bator (red.), *Wprowadzenie do nauk prawnych*, Warszawa 2016, s. 195.

szy zakresowo sposób implementują przepisy Dyrektywy 2002/58/WE. W kontekście plików *cookie* najistotniejsze znaczenie ma art. 5 ust. 3 Dyrektywy 2002/58/WE i to jego sposób implementacji powinien mieć kluczowe znaczenie¹⁰. Reguluje on bowiem przechowywane informacje na urządzeniu końcowym (tj. pliki *cookie*), obowiązek informacyjny oraz obowiązek uzyskania zgody (przyjmując system *opt-in*¹¹). Nie ulega wątpliwości, że art. 6 u.s.u.d.e. w niezwykle lakoniczny sposób transponuje przepis Dyrektywy 2002/58/WE, a w znakomitej większości tego po prostu nie dokonuje (*vide* brak obowiązku uzyskania zgody). Analizując natomiast art. 173 pr. telkom., możemy dojść do konkluzji, że przepis ten, w związku z art. 174 pr. telkom., w zadowalający sposób implementuje przepisy wspólnotowe. W związku z poczynionymi rozważaniami należy przyjąć kolejną regułę kolizyjną pomiędzy art. 6 u.s.u.d.e. a art. 173 pr. telkom., tj. *lex specialis derogat legi generali*¹². Mając na uwadze przeprowadzoną analizę konkurujących ze sobą przepisów oraz zastosowane reguły kolizyjne, należy w pełni przyjąć, że podstawowe zastosowanie w kontekście plików *cookie* powinien mieć art. 173 pr. telkom., a art. 6 u.s.u.d.e. wyłącznie uzupełniające.

Przesłanka trwałości – plik *cookie* jako stała informacja

Zgodnie z art. 4 ust. 2 pkt 1 RODO¹³ dane osobowe to wszelkie informacje, które w sposób bezpośredni lub pośredni pozwalają na zidentyfikowanie osoby fizycznej. Przepis ten w otwartym katalogu przedstawia rodzaje identyfikatorów, które umożliwiają identyfikację osób fizycznych. Między innymi ustawodawca unijny wskazuje na identyfikatory internetowe. Rozwinięcie tego pojęcia znajduje się w motywie 30 RODO. Przedstawia on identyfikatory plików *cookie* jako jeden z identyfikatorów internetowych. Należy jednak wskazać, że nie powinno się z tego wyciągnąć wniosku, że każdorazowo informacje zawarte w plikach *cookie* należy poczytywać za dane osobowe¹⁴.

¹⁰ X. Konarski, *Podstawy prawne korzystania z „ciasteczek” internetowych (cookies) jako przykład wzajemnej relacji przepisów RODO oraz przepisów o ochronie prywatności w sektorze łączności elektronicznej*, „Monitor Prawniczy” 2018, nr 22.

¹¹ T. Pałak, *Zgoda na cookies – RODO, eprivacy i nie tylko*, www.tomaszpalak.pl [dostęp 7.04.2022].

¹² A. Bator, S. Kaźmierczak, *op. cit.*, s. 218-219.

¹³ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (dalej: „RODO”), Dz. Urz. UE L 119 z 2016 r., str. 1.

¹⁴ J. Byrski, H. Hoser, *Social media oraz technologie umożliwiające śledzenie użytkowników Internetu a współadministrowanie danymi osobowymi*, „Monitor Prawniczy” 2019, nr 21, s. 3006 oraz wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 11 lipca 2022 r., II SA/Wa 3993/21.

Charakterystyczną cechą dla identyfikatorów internetowych jest ich potencjalna zmienność, a tym samym brak trwałości¹⁵. Z perspektywy danych osobowych w postaci imienia i nazwiska czy pseudonimu, tj. takich, które w znacznym stopniu przedstawiają osobowy charakter informacji, aktualność tych informacji nie będzie miała istotnego znaczenia. Takie informacje wciąż będą możliwe do uznania za dane osobowe pomimo potencjalnego braku prawdziwości. Najistotniejsze – a zarazem konieczne – dla uznania danej informacji za dane osobowe jest przypisanie tej informacji do konkretnej osoby fizycznej, możliwej do zidentyfikowania. Dodatkowo warto zauważyć, że adres IP, jako identyfikator internetowy, jest przypisany do konkretnego urządzenia (komputer, smartfon), a nie do zindywidualizowanej osoby fizycznej¹⁶. Z perspektywy identyfikatorów internetowych do uznania ich za dane osobowe kluczowa jest ich *trwałość*. Ślad pozostawiony przez użytkownika sieci, w postaci *statycznego* adresu IP, pozwala na identyfikację urządzenia, co pośrednio umożliwia ustalenie konkretnej osoby fizycznej¹⁷. Adres IP przypisany do konkretnego urządzenia na dłuższy okres może zostać uznany za daną osobową, jeżeli równocześnie określone urządzenie jest związane z określoną osobą fizyczną¹⁸. Analogicznie wnioski dotyczące statycznych adresów IP należy przenieść do plików *cookie*¹⁹.

Pliki *cookie* ze względu na okres przechowywania na urządzeniu końcowym możemy podzielić na dwa rodzaje: *cookie* sesyjne oraz *cookie* stałe²⁰. *Cookie* stałe znane są również jako „pliki śledzące”. Pliki *cookie*, co zostało wykazane we wcześniejszej części tekstu, instalowane są m.in. na urządzeniach końcowych użytkowników. Okres przechowywania *cookie* stałych może być różny w zależności od celu działania i charakterystyki takiego pliku²¹. Na tym etapie sam plik *cookie* stanowi wyłącznie nośnik, którego dopiero treść (zawartość) może zawierać dane osobo-

¹⁵ D. Nowak, *Ochrona danych osobowych i prywatności podczas stosowania plików cookie w świetle wytycznych i opinii Grupy Roboczej Art. 29 oraz Europejskiej Rady Ochrony Danych*, „Monitor Prawniczy” 2021, nr 23, s. 1568, oraz wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 19 października 2016 r. w sprawie C-582/14 *Breyer* (pkt 36).

¹⁶ Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 19 października 2016 r. w sprawie C-582/14 *Breyer* (pkt 36) oraz wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 11 lipca 2022 r., II SA/Wa 3993/21.

¹⁷ Wyrok Naczelnego Sądu Administracyjnego z dnia 19 maja 2011 r., I OSK 1079/10.

¹⁸ *Ibidem*.

¹⁹ Należy jednak zaznaczyć, że na mocy orzeczenia o sygn. C-582/14, w określonych okolicznościach dynamiczny adres IP, tak samo jak statyczny, również może zostać poczytany za dane osobowe – przyp. autora.

²⁰ M.E. Whitman, J. Perez, C. Beise, *A Study of User Attitudes toward Persistent Cookies*, „Journal of Computer Information Systems” 2001, 41(3), s. 1-7, DOI: [10.1080/08874417.2001.11647000](https://doi.org/10.1080/08874417.2001.11647000).

²¹ M. Kolasiński, *op. cit.*

we²². Dopiero stale zainstalowany plik *cookie* zbierający informacje (np. analityczne czy marketingowe) z urządzenia może stać się nośnikiem zawierającym dane osobowe o możliwej do zidentyfikowania osobie fizycznej (np. skutek budowania szczegółowych profili użytkowników²³). Pliki *cookie* sesyjne przechowywane są najczęściej w pamięci przeglądarki do momentu zakończenia sesji²⁴ – nie są zatem zapisywane w pamięci urządzenia, toteż nie można ich uznać za „pliki śledzące”. Ten rodzaj *cookie* co do zasady nie stanowi nośnika danych, zdolnego do zbierania informacji stanowiących potencjalnie dane osobowe²⁵. Służą przede wszystkim utrzymywaniu sesji i *stricte* technicznej możliwości łączenia użytkownika (*client*) z serwisem internetowym (*server*)²⁶. Najczęściej sesyjne pliki *cookie* ze względu na swoją funkcjonalność stanowią pliki „niezbędne” (będzie to co do zasady chociażby plik *cookie* odpowiedzialny za zapamiętywanie produktów dodanych do koszyka w sklepie internetowym). W związku z poczynionymi rozważaniami dotyczącymi *trwałości* informacji identyfikatorów internetowych i technicznego aspektu plików *cookie* należy przyjąć, że wyłącznie w przypadku *trwałych* plików *cookie* będzie możliwe uznanie informacji w nich zawartych za dane osobowe.

Przesłanka *identyfikowalności* osoby fizycznej – test możliwości identyfikacji osoby fizycznej z motywu 26 RODO

Jedną z przesłanek kwalifikujących określone informacje jako dane osobowe jest przesłanka identyfikowalności osoby fizycznej wyrażona w art. 4 pkt 1 RODO²⁷. Należy zaznaczyć, że identyfikacja konkretnej osoby fizycznej nie musi polegać wyłącznie na dotarciu do jej imienia i nazwiska czy miejsca zamieszkania. Osoba fizyczna jest zidentyfikowana, jeżeli możemy ją wyodrębnić z szerszego grona osób lub grupy²⁸. Identyfikacja osoby fizycznej może mieć zatem charakter bezpośredni lub pośredni²⁹.

²² J. Byrski, H. Hoser, *op. cit.*, s. 3006 oraz M. Kaczorowski, *Przetwarzanie danych osobowych w działaniach marketingowych prowadzonych on-line*, „Monitor Prawniczy” 2014, nr 9, s. 1034.

²³ D. Nowak, *op. cit.*, s. 1568.

²⁴ *Po co są Ciasteczka?, Czym są Cookies (ciasteczka)?*, wszystkooociasteczkach.pl/po-co-sa-ciasteczka/.

²⁵ *What are session cookies? Do they need consent?*, www.cookieeyes.com/blog/session-cookies, [dostęp 27.10.2021 r.]

²⁶ *Ibidem*.

²⁷ P. Litwiński, [w:] P. Litwiński (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe*, Warszawa 2021.

²⁸ Opinia 4/2007 Grupy Roboczej ds. ochrony danych powołanej na mocy art. 29 w sprawie pojęcia danych osobowych, 20.06.2007 r.

²⁹ *Ibidem*.

Wynika to m.in. z samej treści definicji danych osobowych w RODO. Drugim znaczącym zagadnieniem przy identyfikacji osób fizycznych są dwie koncepcje przesłanki identyfikowalności: koncepcja obiektywna i subiektywna.

Motyw 26 RODO oraz uprzednio motyw 26 Dyrektywy 95/46/WE³⁰ dostarczają niezwykle istotnych wytycznych związanych z identyfikacją osób fizycznych – wprowadzają one niejako test możliwości identyfikacji osoby fizycznej. Wynik tego testu powinien stanowić kolejną przesłankę do uznania zawartości plików *cookie* za dane osobowe lub nie. W pierwszej kolejności należy pochylić się nad zdaniem drugim *in fine* motywu 26 RODO oraz rozstrzygnąć, która z koncepcji przesłanki identyfikowalności będzie miała zastosowanie: obiektywna czy subiektywna. Motyw 26 stanowi, że dla stwierdzenia, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę środki/sposoby identyfikacji, jakimi może się posłużyć zarówno administrator, jak i inna osoba. Granice tych sposobów wyznacza Trybunał Sprawiedliwości Unii Europejskiej, przyjmując złagodzoną koncepcję obiektywną w orzeczeniu odnoszącym się do dynamicznego adresu IP³¹. TSUE tym samym podtrzymał tezę postawioną przez Rzecznika Generalnego³². W doktrynie podnosi się, że omawiana koncepcja nosi nazwę zrelatywizowanej koncepcji obiektywnej³³. Zgodnie z nią stosowane przez administratora sposoby należy ograniczyć wyłącznie do tych, którymi można się „racjonalnie rzecz biorąc posłużyć”, oraz do osób trzecich, do których administrator może się w tym celu „racjonalnie rzecz biorąc” odwołać³⁴. Na ową racjonalność składają się m.in. koszt, skuteczność, realna możliwość kontaktu z podmiotami trzecimi i czas.

Powyższe rozstrzygnięcia – pomimo że dotyczyły dynamicznego adresu IP – powinny znaleźć zastosowanie do plików *cookie*. Administratorzy stosujący pliki *cookie* powinni szczegółowo przeanalizować ich stosowanie pod względem wykorzystywanych technologii i narzędzi, a następnie zbadać, czy istnieją sposoby, którymi, mogąc się racjonalnie posłużyć, są w stanie na podstawie informacji zawartych

³⁰ Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (dalej: „Dyrektywa 95/46/WE”).

³¹ Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 19 października 2016 r. w sprawie C-582/14 *Breyer* (pkt 45 i 46).

³² Opinia Rzecznika Generalnego M. Composa Sancheza-Borodny z dnia 12.05.2016 r. ws. C-582/14 *Breyer* (pkt 68).

³³ D. Lubasz, A. Szkurłat, *Relatywizacja pojęcia danych osobowych w świetle orzecznictwa polskich sądów administracyjnych i powszechnych*, „Monitor Prawniczy” 2021, nr 23, s. 1575.

³⁴ Opinia Rzecznika Generalnego M. Composa Sancheza-Borodny z dnia 12.05.2016 r. ws. C-582/14 *Breyer* (pkt 68).

w tych plikach oraz innych informacji zidentyfikować konkretną osobę fizyczną. Duże znaczenie będzie miał zatem charakter działalności administratora i zakres (wolumen) przetwarzanych danych osobowych. Im większy wolumen, tym większe prawdopodobieństwo pośredniego zidentyfikowania osoby fizycznej w zestawieniu z informacjami wynikającymi z plików *cookie*³⁵. Dodatkowo, mając na względzie, że trwałe pliki *cookie* są najczęściej związane z wykorzystywaniem narzędzi od zewnętrznych dostawców, administrator powinien ustalić, czy z jego perspektywy kontakt z dostawcą takiej technologii jako osoby trzeciej w celach identyfikacji osób fizycznych jest przynajmniej potencjalnie wykonalny. Przykładowo – z pewnością nie sposób przyjąć, że administrator prowadzący drobny sklep internetowy korzystający na stronie sklepu z narzędzia Google Analytics od Google Ireland Ltd. (lub odpowiednio Google LLC) może racjonalnie odwołać się do dostawcy tego narzędzia w celu identyfikacji osób fizycznych, którym zainstalowały się pliki *cookie* związane z tym narzędziem. Warto w tym zakresie zauważyć, że w postępowaniu przed Prezesem Urzędu Ochrony Danych Osobowych, którego decyzja została zaskarżona do Wojewódzkiego Sądu Administracyjnego, strona postępowania podnosiła, że stosowanie jednego z narzędzi analitycznych na stronie www wykorzystującego pliki *cookie* (*cookie* id) w żaden sposób nie umożliwiała jej identyfikacji konkretnej osoby fizycznej, tj. uczestnika postępowania, nawet pomimo nadania unikalnego identyfikatora użytkownikowi końcowemu³⁶.

Przesłanka celu wykorzystywania plików *cookie* – zawartość pliku

Tak jak zostało już wielokrotnie wspomniane, pliki *cookie* ze względu na swój charakter mają wiele różnych zastosowań. Fakt, że dany serwis www korzysta z plików *cookie*, jest przeważnie wypadkową stosowania określonych funkcjonalności lub narzędzi, np. Google Analytics (narzędzie służące analityki strony) czy TikTok Pixel (narzędzie służące do remarketingu). Przetwarzanie danych osobowych jest związane z zasadą wyrażoną w art. 5 lit. b RODO, tj. zasadą ograniczonego celu. Każda czynność przetwarzania powinna być związana z określonymi i wyrażonymi celami bądź celem. To, jakie informacje będą gromadziły się w pliku *cookie*, jest uzależnione od jego charakterystyki i z góry zaprogramowanych funkcji. Inne informacje będą gromadzone w plikach *cookie* związanych z funkcjonowaniem narzę-

³⁵ Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 11 lipca 2022 r., II SA/Wa 3993/21.

³⁶ *Ibidem*.

dzia Google Analytics³⁷, a inne w związku ze stosowaniem narzędzia TikTok Pixel³⁸. W związku z tym należy przyjąć, że w celu zakwalifikowania informacji zawartych w plikach *cookie* jako danych osobowych konieczne będzie przeanalizowanie przez administratora stosowanych funkcjonalności oraz narzędzi pod względem celów ich stosowania oraz zakresu informacji zbieranych przez pliki *cookie*.

Trybunał Sprawiedliwości Unii Europejskiej w punkcie 45 w zakresie rozważań dotyczących pierwszego pytania prejudycjalnego w wyroku ws. *Planet 49*³⁹ przedstawia opis stosowania określonych plików *cookie* przez spółkę Planet 49. Pliki *cookie* w tym konkretnym przypadku służyły identyfikacji określonych użytkowników biorących udział w loterii promocyjnej. Zawierały one numer identyfikacyjny, który z kolei był przypisany do innych danych podanych przez użytkownika w trakcie rejestracji, tj. imienia, nazwiska oraz adresu. W związku z tym TSUE w punkcie 67 omawianego wyroku słusznie uznał, że instalowanie plików *cookie* wiąże się przetwarzaniem danych osobowych. Do powyższych rozważań – w bardzo wąskim zakresie – odwołał się również Prezes Urzędu Ochrony Danych Osobowych w swojej decyzji, która była przedmiotem zaskarżenia przed Wojewódzkim Sądem Administracyjnym w Warszawie. PUODO ograniczył się wyłącznie do twierdzenia przedstawionego w punkcie 67 wyroku ws. *Planet 49*⁴⁰. Sąd Administracyjny słusznie zauważył, że PUODO, powołując się na punkt 67, całkowicie pominął kluczowy punkt 45 wyroku. Uczestnik postępowania w stanie faktycznym będącym przedmiotem postępowania nie wypełnił żadnych formularzy, które umożliwiałyby podanie informacji takich jak imię, nazwisko czy adres e-mail. Sąd Administracyjny słusznie postawił tezę, że powołany przez PUODO punkt 67 wyroku ws. *Planet 49* nie mógł przesądzać o tym, że w stanie faktycznym postępowania przed PUODO mogło dojść do uznania plików *cookie* (*cookie id*) za dane osobowe.

Grupa Robocza ds. ochrony danych w swojej opinii 2/2010 w sprawie internetowej reklamy behawioralnej odniosła się do plików *cookie*⁴¹. Grupa słusznie przyjęła, że budowanie szczegółowych profili użytkowników w internecie wiąże się z przetwarza-

³⁷ *Our advertising and measurement cookies*, <https://business.safety.google/adscookies/>, [dostęp 29.04.2024].

³⁸ *Using Cookies with TikTok Pixel*, <https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en>, [dostęp 29.04.2024].

³⁹ Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 1 października 2019 r. ws. C-673/17 (dalej: „Wyrok ws. Planet 49”).

⁴⁰ Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 11 lipca 2022 r., II SA/Wa 3993/21.

⁴¹ Opinia 2/2010 Grupy Roboczej ds. Ochrony Danych powołana na mocy art. 29 w sprawie internetowej reklamy behawioralnej z dnia 22 czerwca 2010 r., s. 3.

niem danych osobowych⁴², m.in. za pośrednictwem takich narzędzi jak śledzące pliki *cookie*. Warto jednak zauważyć, że Grupa Robocza Art. 29 nie przesądza o tym, że zawartość plików *cookie* każdorazowo będzie stanowiła dane osobowe⁴³. Z omawianej opinii z pewnością można natomiast wyciągnąć wniosek, że stosowanie plików *cookie* marketingowych w kontekście reklamy behawioralnej będzie immanentnie związane z przetwarzaniem danych osobowych – administrator będzie bowiem przetwarzał informacje takie jak: charakterystyka zachowania określonych osób czy niepowtarzalny identyfikator marketingowy (*cookie id*)⁴⁴. Elementem kwalifikacyjnym w tym zakresie jest zatem techniczny aspekt i funkcjonalność stosowanych plików *cookie*.

W wyniku poczynionych rozważań należy przyjąć, że pozostawiona w *próżni* zawartość pliku *cookie* oraz nadany *cookie id* nie mogą zostać uznane za dane osobowe bez ustaleń w zakresie technologicznych i funkcjonalnych aspektów (celów wykorzystywania) konkretnych narzędzi i rozwiązań stosujących pliki *cookie*.

Podstawy prawne przetwarzania danych osobowych w ramach wykorzystywania plików *cookie*

W przypadku gdy administrator uzna zawartość stosowanych plików *cookie* (przynajmniej potencjalnie) za dane osobowe, następnym krokiem powinno być ustalenie podstawy prawnej przetwarzania danych osobowych z art. 6 ust. 1 RODO. W zakresie przetwarzania danych osobowych w kontekście stosowanych plików *cookie* administrator będzie mógł przyjąć – w zależności od kontekstu, celu stosowania i rodzaju plików *cookie* – następujące podstawy prawne:

- 1) art. 6 ust. 1 lit. a RODO, tj. zgoda osoby, której dane dotyczą,
- 2) art. 6 ust. 1 lit. b RODO, tj. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą,
- 3) art. 6 ust. 1 lit. f RODO, tj. prawnie uzasadniony interes administratora⁴⁵.

Podstawa prawna w postaci zgody osoby, której dane dotyczą, powinna mieć w szczególności zastosowanie w zakresie stosowania plików *cookie* zewnętrznych i trwałych o następujących funkcjach:

- 1) *cookie* analitycznych,
- 2) *cookie* marketingowych,

⁴² D. Nowak, *op. cit.*, s. 1568.

⁴³ Opinia 2/2010 Grupy Roboczej ds. Ochrony Danych..., s. 10.

⁴⁴ *Ibidem*, s. 10-11.

⁴⁵ J. Byrski, H. Hoser, *op. cit.*, s. 3006.

3) *cookie* odpowiadających za prowadzenie kampanii marketingowych (tworzenie profili użytkowników),

4) *cookie* społecznościowych (np. wtyczki zewnętrznych portali społecznościowych)⁴⁶.

Powyższa podstawa prawna z art. 6 ust. 1 a RODO nie może zostać zastąpiona podstawą z litery f omawianego przepisu. Uzasadniony interes administratora – jak wskazuje Europejska Rada Ochrony Danych w swoich wytycznych – w postaci przetwarzania danych w ramach stosowania *cookie* analitycznych, społecznościowych oraz *cookie* marketingowych nie może stanowić odpowiedniej podstawy prawnej legalizującej przetwarzanie danych osobowych w tym zakresie⁴⁷. Wyrażona przez osobę, której dane dotyczą zgoda, powinna również spełniać wszelkie rygory, jakie wynikają z RODO, a w szczególności te z art. 7 RODO.

Podstawa prawna wynikająca z art. 6 ust. 1 lit. b RODO będzie miała zastosowanie w przypadku, gdy istotą przetwarzania danych osobowych za pośrednictwem plików *cookie* jest zawarcie umowy z osobą, której dane dotyczą, lub jej realizacja czy podjęcie działań na żądanie osoby przed zawarciem umowy⁴⁸. Podstawa prawna litery b art. 6 ust. 1 RODO może zatem dotyczyć przetwarzania danych osobowych zawartych w plikach *cookie* m.in. w zakresie:

- 1) funkcjonowania koszyka w sklepie internetowym,
- 2) prowadzenia formularzy elektronicznych do realizacji zamówień,
- 3) realizacji i wysyłki zamówień,
- 4) świadczenia usług drogą elektroniczną,
- 5) funkcjonowania narzędzi związanych z prowadzeniem rekrutacji.

Warto zauważyć, że podstawa prawna z litery b art. 6 ust. 1 RODO będzie mogła mieć zastosowanie do plików *cookie* wykorzystywanych na wyraźne żądanie (interakcję) osoby, której dane dotyczą z elementem interfejsu strony internetowej, co spowoduje zainstalowanie pliku *cookie*⁴⁹. Aby administrator mógł zastosować omawianą przesłankę, musi istnieć *oczywista zależność* pomiędzy wyrażonym w określony sposób „żądaniem osoby, której dane dotyczą”, docelowo związanym z zawarciem lub realizacją umowy, a instalacją i przetwarzaniem danych w zakresie określonych plików *cookie*.

⁴⁶ D. Nowak, *op. cit.*, s. 1568.

⁴⁷ Wytyczne Europejskiej Rady Ochrony Danych dotyczące zgody na mocy rozporządzenia 2016/769 przyjęte w dniu 4.05.2020 r., s. 27.

⁴⁸ P. Litwiński (red.), *op. cit.*

⁴⁹ D. Nowak, *op. cit.*, s. 1568 – w zakresie plików *cookie* wyłączonych spod obowiązku uzyskania zgody.

Ostatnia podstawa prawna legalizująca przetwarzanie danych osobowych w postaci uzasadnionego interesu administratora powinna mieć co do zasady zastosowanie w zakresie plików *cookie* niezbędnych oraz funkcjonalnych⁵⁰. Art. 6 ust. 1 lit. f RODO dla jego zastosowania wymaga uprzedniej analizy, czy w stosunku do określonych czynności przetwarzania prawa i wolności osób, których dane dotyczą, nie mają charakteru nadrzędnego względem interesu administratora. Z pewnością administrator powinien zatem przeprowadzić test równowagi (proporcjonalności)⁵¹. Test powinien uwzględniać treść motywu 47 RODO, w tym weryfikację ewentualnej nadrzędności praw i wolności osób, których dane dotyczą nad celami przetwarzania administratora⁵². W związku z tym należy przyjąć, że stosowanie przesłanki uzasadnionego interesu administratora będzie odpowiednie w zakresie stosowania plików *cookie* niezbędnych oraz funkcjonalnych takich jak:

- 1) *cookie* odpowiedzialnych za bezpieczeństwo przesyłu informacji w obrębie strony www,
- 2) *cookie* związanych z utrzymywaniem sesji użytkownika,
- 3) *cookie* odpowiedzialnych za modyfikacje interfejsu przez użytkownika w postaci wielkości czy koloru czcionki,
- 4) *cookie* uwierzytelniających (identyfikujących użytkownika)⁵³.

Warto jednak zaznaczyć, że tak jak już zostało wykazane, wykorzystywanie plików *cookie* niezbędnych co do zasady nie będzie wiązało się z przetwarzaniem danych osobowych.

Podsumowanie

Pliki *cookie* nie zostały dotychczas bezpośrednio zdefiniowane w żadnym akcie prawnym. Należy je jednak rozumieć jako dane informatyczne, zapisywane na urządzeniach końcowych użytkowników trwale lub sesyjnie w określonych celach. W zakresie polskiego ustawodawstwa, gdzie dochodzi do kolizji norm odnoszących się do plików *cookie*, powinniśmy jako akt wyjściowy w zakresie kwalifikacji prawnej plików *cookie* stosować ustawę o prawie telekomunikacyjnym, a ustawę o świadczeniu usług drogą elektroniczną wyłącznie uzupełniająco.

⁵⁰ *Ibidem*, s. 1568 oraz J. Byrski, H. Hoser, *op. cit.*, s. 3006.

⁵¹ J. Byrski, H. Hoser, *op. cit.*, s. 3006.

⁵² M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, komentarz do art. 6.

⁵³ D. Nowak, *op. cit.*, s. 1568 – w zakresie plików *cookie* wyłączonych spod obowiązku uzyskania zgody.

Jeszcze istotniejszym praktycznie zagadnieniem jest ustalenie, czy pliki *cookie*, a raczej ich zawartości, stanowią dane osobowe. W tym celu należy przeprowadzić analizę oraz ustalić, czy są spełnione trzy przesłanki szczególne do uznania zawartości plików *cookie* za dane osobowe, tj. przesłanka trwałości, przesłanka identyfikowalności osoby fizycznej (test z motywu 26 RODO) oraz przesłanka celu wykorzystywania plików *cookie* (zawartość plików). Wskazane przesłanki mają charakter szczególny względem przesłanek ogólnych wynikających z art. 4 pkt 1 RODO kwalifikujących określone informacje jako dane osobowe. Warto również zauważyć, że ze względu na charakterystykę plików *cookie* wskazane przesłanki szczególne nie muszą zostać kumulatywnie spełnione, aby można było uznać informacje w nich zawarte za dane osobowe. W pewnych okolicznościach spełnienie nawet jednej przesłanki szczególnej może doprowadzić do uznania informacji zawartych w plikach *cookie* za dane osobowe. W praktyce zdaje się jednak, że spełnienie się jednej z przesłanek szczególnych będzie pociągało za sobą spełnianie się pozostałych. Nieodzownym elementem związanym z ustaleniami w zakresie przesłanek szczególnych będzie weryfikacja narzędzi i technologii stosujących pliki *cookie*.

Równie istotnym zagadnieniem – w przypadku uznania informacji zawartych w plikach *cookie* (przynajmniej potencjalnie) za dane osobowe – jest ustalenie odpowiedniej podstawy prawnej z art. 6 ust. 1 RODO legalizującej przetwarzanie danych osobowych w tym zakresie. Ustalenie właściwej podstawy prawnej będzie wiązało się z przeanalizowaniem narzędzi i technologii stosujących pliki *cookie* oraz celu przetwarzania danych osobowych za ich pomocą.

W praktyce zdaje się, że w zakresie plików *cookie* oprócz znajomości przepisów prawnych znaczną rolę – a wręcz kluczową – odgrywa wiedza z zakresu informatyki i nowych technologii. Bez znajomości podstaw odnoszących się do funkcjonowania konkretnych narzędzi czy rozwiązań niemożliwe będzie przeprowadzenie odpowiedniej wykładni w celu uznania zawartości plików *cookie* za dane osobowe oraz ewentualne ustalenie podstaw prawnych ich przetwarzania.

Bibliografia

Źródła

Akty prawne

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz. U. z 2002 r. Nr 144, poz. 1204, t.j. Dz. U. z 2020 r. poz. 344.

Ustawa z dnia 16 lipca 2004 r. o prawie telekomunikacyjnym, Dz. U. z 2004 r. Nr 171, poz. 1800, t.j. Dz. U. z 2024 r. poz. 34.

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz. Urz. UE L 201 z 2002 r., str. 37.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE L 119 z 2016 r., str. 1.

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. Urz. UE L 281 z 1995 r., str. 31.

Orzeczenia

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 11 lipca 2022 r., II SA/Wa 3993/21.

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 19 października 2016 r. w sprawie C-582/14 *Breyer*.

Wyrok Naczelnego Sądu Administracyjnego z dnia 19 maja 2011 r., I OSK 1079/10.

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 1 października 2019 r. ws. C-673/17.

Wytyczne i opinie

Opinia 4/2007 Grupy Roboczej ds. ochrony danych powołanej na mocy art. 29 w sprawie pojęcia danych osobowych, 20.06.2007 r.

Opinia Rzecznika Generalnego M. Composa Sancheza-Borodny z dnia 12.05.2016 r. ws. C-582/14 *Breyer*.

Opinia 2/2010 Grupy Roboczej ds. Ochrony Danych powołana na mocy art. 29 w sprawie internetowej reklamy behawioralnej z dnia 22 czerwca 2010 r.

Wytyczne Europejskiej Rady Ochrony Danych dotyczące zgody na mocy rozporządzenia 2016/769 przyjęte w dniu 04.05.2020 r.

Źródła internetowe/inne

Kolański M., *Ciasteczkowe RODO – Czyli pliki cookies a ochrona danych osobowych*, artykuł niepublikowany, 2020 r.

Palak T., *Zgoda na cookies – RODO, eprivacy i nie tylko*, www.tomaszpalak.pl, 07.04.2022 r.

Po co są Ciasteczka?, Czym są Cookies (ciasteczka)?, wszystkooociasteczkach.pl/po-co-sa-ciasteczka/.

Google Business Data Responsibility “Our advertising and measurement cookies”, <https://business.safety.google/adscokies/>.

TikTok Business Help Center, “Using Cookies with TikTok Pixel”, <https://ads.tiktok.com/help/article/using-cookies-with-tiktok-pixel?lang=en>.

What are session cookies? Do they need consent?, www.cookieeyes.com/blog/session-cookies, 2023 r.

Literatura

- Bator A. (red.), *Wprowadzenie do nauk prawnych*, Warszawa 2016.
- Byrski J., Hoser H., *Social media oraz technologie umożliwiające śledzenie użytkowników Internetu a współadministrowanie danymi osobowymi*, „Monitor Prawniczy” 2019, nr 21.
- Kaczorowski M., *Przetwarzanie danych osobowych w działaniach marketingowych prowadzonych on-line*, „Monitor Prawniczy” 2014, nr 9.
- Konarski X., *Podstawy prawne korzystania z „ciasteczek” internetowych (cookies) jako przykład wzajemnej relacji przepisów RODO oraz przepisów o ochronie prywatności w sektorze łączności elektronicznej*, „Monitor Prawniczy” 2018, nr 22.
- Litwiński P. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021.
- Lubasz D., Szkurlat A., *Relatywizacja pojęcia danych osobowych w świetle orzecznictwa polskich sądów administracyjnych i powszechnych*, „Monitor Prawniczy” 2021, nr 23.
- Lubasz D. (red.), *Meritum. Ochrona danych osobowych*, Warszawa 2020.
- Whitman M.E, Perez J., Beise C., *A Study of User Attitudes toward Persistent Cookies*, „Journal of Computer Information Systems” 2001, 4 (3), DOI: [10.1080/08874417.2001.11647000](https://doi.org/10.1080/08874417.2001.11647000).
- Nowak D., *Ochrona danych osobowych i prywatności podczas stosowania plików *cookie* w świetle wytycznych i opinii Grupy Roboczej Art. 29 oraz Europejskiej Rady Ochrony Danych*, „Monitor Prawniczy” 2021, nr 23.
- Sakowska-Baryła M. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Legal qualification of cookies as personal data and legal basis for their processing

Abstract

Cookies are a crucial and significant legal issue related to, among others, personal data and direct marketing. Unclear legal classification of Cookies results in strong discrepancies in interpretation and non-compliance with legal obligations in that regard. This publication is primarily devoted to determining in what circumstances and to what extent *cookies* may constitute personal data by discussing the rationale behind them. This issue will be presented in the context of the case law of the Court of Justice of the European Union, guidelines of European Data Protection Board and Art. 29 Working Party and considerations of Polish judiciary, including proceedings before Polish Supervisory Authority. The main purpose of the publication is to present a practical summary of the considerations of the Court of Justice of the European Union, guidelines of the European Data Protection Board and Art. 29 Working Party, considerations of Polish Administrative Court in Warsaw and Polish Supervisory Authority. *Cookies* will also be analyzed in terms of the legal basis for the processing of personal data contained therein. The legal basis for the processing of personal data contained in *Cookies* will be presented in the list of individual *Cookies* functions.

Keywords

Cookies, Telecommunications law, GDPR, European Union Law, New technologies law, e-privacy, direct marketing, The Court of Justice of the European Union, Polish Supervisory Authority.

Julia Rodakiewicz*
ORCID: 0009-0006-0748-4230

Prawo własności intelektualnej i technologia NFT w kontekście branży muzycznej: wyzwania i perspektywy

Streszczenie

Celem niniejszego opracowania jest dostarczenie kompleksowej analizy kwestii związanych z prawem własności intelektualnej przy wykorzystaniu technologii NFT w branży muzycznej. Rozwijająca się w szybkim tempie technologia NFT otwiera nowe możliwości zarówno dla twórców, jak i dla odbiorców muzyki. Jednocześnie nowa technologia niesie ze sobą wiele wyzwań zwłaszcza na tle regulacji prawnych. W tekście poruszono także aspekty etyczne oraz ekonomiczne, co pozwala na lepsze zrozumienie problemu i wskazanie odpowiedniej drogi rozwoju regulacji.

Słowa kluczowe

prawo własności intelektualnej, prawo autorskie, NFT (Non-Fungible Token), branża muzyczna, technologia blockchain, smart kontrakt, transformacja cyfrowa.

Uwagi wstępne

Technologia blockchain, która u części ludzi, widzących w niej nieograniczony potencjał na zmianę przestarzałych modeli biznesowych, budzi zachwyt, przez innych zaś jest szeroko krytykowana lub nierozumiana, stanowi przedmiot wielu debat, w wyniku których zazwyczaj pojawia się więcej pytań niż odpowiedzi. Wraz z jej nieustannym rozwojem w 2021 r. zauważyć można było ogromny wzrost popularności NFT (ang. *non-fungible token*), czyli niewymienialnych tokenów. Całkowity wolumen obrotu tego niezwykle wpływowego trendu wyniósł w 2021 r. około 25 mld dolarów¹. Rok 2023 przyniósł jednak znacznie niższe wyniki², a obecnie szacuje się, że liczba właścicieli NFT wynosi około 370 000³.

* Autorka jest studentką V roku prawa na Uniwersytecie Wrocławskim. Odbyła roczne stypendium na Freie Universität Berlin. ORCID: 0009-0006-0748-4230.

¹ S. Gherghelas, *Dapp Industry Report 2022*, <https://dappradar.com/blog/dapp-industry-report-2022-dapp-industry-proves-resilient-in-crypto-winter> [dostęp 20.08.2023].

² S. Gherghelas, *State of the Dapp Industry in Q2 2023*, <https://dappradar.com/blog/state-of-the-dapp-industry-in-q2-2023> [dostęp 20.08.2023].

³ D. Ruby, *39+ Detailed NFT Statistics In 2023*, <https://www.demandsage.com/nft-statistics> [dostęp 20.08.2023].

Od 2014 r., kiedy technologia NFT zaczynała raczkować⁴, pasjonaci nowinek technologicznych mogli obserwować powstawanie, a niekiedy także upadki takich projektów jak CryptoPunks, czyli kolekcję losowo wygenerowanych pikselowych awatarów, spośród których najbardziej unikatowe zostały sprzedane za ponad milion dolarów, a których średnia cena w lipcu 2023 r. wynosiła około 53 ETH, (cena 1 ETH w lipcu 2023 r. wynosiła około 2000 dolarów)⁵, czy Merge, dynamiczną kolekcję NFT, która w grudniu 2021 r. wygenerowała rekordową sprzedaż o wartości ponad 91,8 mln dolarów netto podczas 48-godzinnej aukcji⁶. Natomiast na jednej z pierwszych aukcji NFT w Polsce obraz „Dlaczego jest raczej coś niż nic” autorstwa Pawła Kowalewskiego został sprzedany za 552 000 zł. Oryginalna forma obrazu została zniszczona na skutek powodzi w 1997 r., więc obraz występuje dziś jedynie w wersji cyfrowej⁷. W efekcie wzrostu zainteresowania tą technologiczną nowinką oprócz ekstrawaganckich inicjatyw zaczęto także dostrzegać jej potencjał w niezliczonych branżach wychodzących poza najczęściej kojarzonymi z NFT sztukami wizualnymi i finansami, upatrując nowych rozwiązań, które mogą mieć zastosowanie w sporcie, rozrywce, modzie, grach komputerowych, a nawet na rynku nieruchomości⁸. Zwłaszcza w kontekście przemysłu muzycznego technologia NFT stanowi dynamiczną platformę pozwalającą na rewolucję w sposobie dystrybucji, konsumpcji i zarządzania własnością muzycznych dzieł. Przemysł muzyczny wart ok. 50 mld dolarów zdaje się wykorzystywać nowoczesne rozwiązania w niemalże każdym możliwym sposobie związany z produkcją. Niestety nowe technologie są rzadko implementowane w kwestiach zarządzania prawami muzycznymi czy dystrybucją tantiem. Ekspertki szacują, że muzycy zarabiają średnio 2% (23,40 na każde 1000 dolarów) ze sprzedaży swojej muzyki⁹. Innowacyjne start-upy, które

⁴ LCX Team, *The History of NFTs*, 2023, <https://www.lcx.com/the-history-of-nfts> [dostęp 20.08.2023].

⁵ A. Hayward, *What Are CryptoPunks? The Ethereum NFT Sensation's Wild Ride*, „Decrypt” 2023, <https://decrypt.co/resources/what-are-cryptopunks-ethereum-nft-avatars> [dostęp 20.08.2023].

⁶ P. Compare, *The Merge NFT: Ethereum Collection That Raised \$90,000,000+*, „CoinCodex” 2023, <https://coincodex.com/article/24706/the-merge-nft> [dostęp 20.08.2023].

⁷ M. Szymaniak, *Zniszczyła go powódź tysiąclecia. Obraz polskiego artysty nie tylko ożył dzięki NFT. Dziś trafia też na aukcję, „Spider's Web”* 2021, <https://spidersweb.pl/plus/2021/12/nft-aukcja-sztuka-licytacja-kowalewski-libera> [dostęp 1.10.2023].

⁸ Zob. J. Wilser, *15 NFT Use Cases That Could Go Mainstream*, „CoinDesk” 2021, <https://www.coindesk.com/business/2021/10/14/15-nft-use-cases-that-could-go-mainstream> [dostęp 20.08.2023].

⁹ A. Taghdiri, *How Blockchain Technology Can Revolutionize the Music Industry*, „Harvard Journal of Sports & Entertainment Law” 2019, t. 10, s. 180, <https://theblockchaintest.com/uploads/resources/Arya%20taghdiri%20-%20How%20blockchain%20Technology%20Can%20revolutionize%20the%20Music%20Industry%20-%20Ona.pdf> [dostęp 20.08.2023]. Cyt. za: C. Byun, *The Economics of the Popular Music Industry: Modelling from Microeconomic Theory and Industrial Organization*, 2014, vol. 95.

nie godzą się na taki *status quo*, proponują alternatywne rozwiązania przy użyciu technologii blockchain i NFT, które mają zapewnić wzmocnienie pozycji zarówno artystów, jak i słuchaczy, transparentność i demokratyzację w dostępie do zysków w branży muzycznej. Na obecnym etapie implementacja tych górnolotnych idei pozostaje nadal w toku, choć można zauważyć powolny wzrost zainteresowania tym tematem w mainstreamie muzycznym¹⁰. Omawiane narzędzia podważają obowiązujące paradygmaty i redefiniują sposób, w który myślimy o własności, aktywach i ich wartości. Panuje powszechne niezrozumienie, a niekiedy nawet strach przed tymi wyrafinowanymi technologicznie innowacjami. Również wielu zwolenników ma błędne przekonanie o tym, czym NFT tak naprawdę jest i jakie prawa nabywa się wraz z jego kupnem. Te niewłaściwe pojmowania związane są w dużej mierze z brakiem regulacji prawnych, które w przyszłości mogą okazać się niezbędne.

Technologia blockchain i NFT

W zrozumieniu rewolucyjnego wpływu, jaki ta technologia może wywrzeć w branży muzycznej, istotne jest poznanie podstawowych koncepcji związanych z blockchainem oraz niewymienialnymi (NFT) i wymienialnymi (FT) tokenami.

Technologia blockchain, będąca bazą dla kryptowalut, rozumiana jest jako rozproszony elektroniczny rejestr, w którym chronologicznie przechowywane są informacje o wszystkich transakcjach pomiędzy użytkownikami. Wszyscy użytkownicy posiadają dostęp do tej listy na równych prawach i nie ma jednej instytucji sprawującej władzę, co określane jest mianem decentralizacji. Transakcje zapisywane są w rejestrze według określonego algorytmu jako blok (*block*), który zawiera dane o wartości i czasie zawarcia transakcji, a następnie blok jest dołączany do poprzednich, tworząc łańcuch (*chain*). W bloku można zapisywać również inne informacje, takie jak dane osobowe. Próba zmiany jednego bloku powoduje zmianę całego łańcucha, który za nim podąża. Nie ma zatem możliwości skopiowania tak podpisanego bloku, co oznacza, że nie istnieje możliwość zmiany zapisanych w ten sposób danych, co zapewnia nieodwracalność każdego bloku i transakcji¹¹.

¹⁰ Zespół rockowy Kings of Leon wydał własne cyfrowe gadżety kolekcjonerskie w postaci NFT, takie jak albumy i bilety na koncerty. Zob. S. Hisson, *Kings of Leon Will Be the First Band to Release an Album as an NFT*, „Rolling Stone” 2021, <https://www.rollingstone.com/pro/news/kings-of-leon-when-you-see-yourself-album-nft-crypto-1135192> [dostęp 26.08.2023].

¹¹ A. Rot, R. Zygala, *Technologia blockchain jako rewolucja w transakcjach cyfrowych. Aspekty technologiczne i potencjalne zastosowania*, „Informatyka Ekonomiczna” 2018, nr 4 (50), s. 123, https://dbc.wroc.pl/Content/72987/Rot_Zygala_Technologia_blockchain_jako_rewolucja.pdf [dostęp 27.08.2023].

Satoshi Nakamoto opracował rejestr blockchain w ramach stworzenia wirtualnej waluty bitcoin. Bitcoin działa na platformie blockchain, jednak oba te elementy różnią się całkowicie pod względem funkcjonalnym¹². Europejski Bank Centralny przyjął w 2012 r., że wirtualna waluta jest rodzajem nieuregulowanego, cyfrowego pieniądza emitowanego przez jego twórców, wykorzystywanym i akceptowanym przez uczestników danej społeczności¹³. Natomiast Europejski Urząd Nadzoru Bankowego zdefiniował walutę wirtualną jako cyfrową reprezentację wartości, która może być przekazywana za pomocą technologii informatycznych i stosowana jako środek wymiany, jednostka rozrachunkowa czy środek przechowywania wartości, jednakże niemająca statusu oficjalnego środka płatniczego, tj. jej wartość nie jest gwarantowana przez żaden rząd czy bank centralny, niemniej może podlegać regulacjom państwa¹⁴. Przy pomocy technologii blockchain użytkownicy mogą przysyłać aktywa bez ingerencji czy zgody banku lub innego scentralizowanego podmiotu. Ta koncepcja stanowi podłoże dla nowej sieci Web3, której głównym założeniem jest osiągnięcie demokratyzacji danych¹⁵. Kryptowaluty to wymienne tokeny, co oznacza, że każdy token kryptowaluty jest wart tyle samo, co każdy inny token tej samej kryptowaluty¹⁶, podobnie jak wszystkie złotówki mają taką samą wartość i są wymienialne.

Natomiast NFT w przeciwieństwie do kryptowalut są niewymienne. Każdy NFT jest unikatowy i nie można go zastąpić innym NFT¹⁷. NFT odgrywają rolę cyfrowych certyfikatów własności, mogą reprezentować zarówno aktywa wirtualne, jak i fizyczne, a bezpieczeństwo ich własności zapewniane jest przez leżącą u podłoża NFT technologię blockchain, która umożliwia śledzenie transakcji oraz nie pozwala na dokonywanie zmian. Technologia ta oprócz umożliwienia transferu i śledzenia

¹² A. Taghdiri, *op. cit.*, s. 176.

¹³ P. Marszałek, *Kryptowaluty – pojęcie, cechy, kontrowersje*, „Studia BAS” 2019, nr 1(57), s. 108-110, [https://orka.sejm.gov.pl/WydBAS.nsf/0/F8F4218303461D74C12583E10037EC68/\\$file/5.Marszalek.pdf](https://orka.sejm.gov.pl/WydBAS.nsf/0/F8F4218303461D74C12583E10037EC68/$file/5.Marszalek.pdf) [dostęp 27.08.2023]. Cyt. za: European Central Bank, *Virtual Currency Schemes*, Frankfurt am Main 2012.

¹⁴ *Ibidem*. Cyt. za: Europejski Urząd Nadzoru Bankowego, *EBA Opinion on „virtualcurrencies”*, 2014, <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> [dostęp 1.06.2018]

¹⁵ B. Kazenoff, *NFTs, Blockchain Technology, and Copyrights: How the Future of the Music Industry Will Be Decentralized*, „Entertainment, Arts and Sports Law Journal” 2021, t. 32, nr 3, s. 16, https://nysba.org/app/uploads/2021/11/EASL-Journal-2021-Vol-32-No-3_8.5X11_WEB.pdf [dostęp 30.08.2023]. Cyt. za: D. Tapscott, A. Tapscott, *How This Worldwide Ledger Works, in Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World*, 2018, 6-7.

¹⁶ F. Teomete Yalabik, *Future of NFTs in the entertainment industry: No longer the ‘Wild West’ of intellectual property law?*, „European Journal of Law and Technology” 2023, t. 14, nr 1, s. 3, <https://ejlt.org/index.php/ejlt/article/view/949/1066> [dostęp 31.08.2023]. Cyt. za: S. Mackenzie, D. Berzina, *NFTs: Digital things and their criminal lives*, „Crime Media Culture” 2021.

¹⁷ *Ibidem*, s. 3.

własności zapobiega także reprodukcji, jako że NFT może mieć tylko jednego właściciela. Inteligentne kontrakty (ang. *smart contracts*) powiązane z NFT ustalają zasady zarządzania własnością i zbywalnością NFT przy użyciu unikalnych identyfikatorów i metadanych¹⁸. NFT można określić jako unikalny numer seryjny stanowiący cyfrowy certyfikat własności potwierdzony za pomocą technologii blockchain. Relacja między tradycyjnym aktem notarialnym a nieruchomością jest pod pewnymi względami podobna do relacji między NFT a aktywem, który on reprezentuje, z tym że NFT nie ogranicza się jedynie do fizycznych dóbr, a sprawowanie kontroli i dokonywanie transakcji odbywa się na warunkach inteligentnego kontraktu (ang. *smart contract*)¹⁹.

Smart contract to skomplikowane oprogramowanie, przy pomocy którego zawierane są umowy cechujące się samowykonalnością oraz autonomicznym charakterem postanowień. To narzędzie technologiczne wykorzystuje zdecentralizowane mechanizmy kryptograficzne do egzekwowania postanowień umownych²⁰. Zasadniczo jest to określenie używane do opisanego warunków, które mogą być zakodowane w każdym bloku i zaprogramowane są tak, aby automatycznie egzekwowały postanowienia umowne²¹. Zauważono już, że największą zaletą tej technologii jest szansa na uniknięcie ambiwalentności języka naturalnego, jednak takie rozwiązanie nie pozwala na wprowadzenie klauzul generalnych odwołujących się do powszechnie obowiązującego systemu prawa i wartości²². Przeświadczenie, że *smart contract* to umowa w rozumieniu cywilnoprawnym, jest mylne²³, a niektóre głosy w doktrynie podnoszą, że określenie „inteligentne” jest nie do końca trafione, skoro „wykonanie kodu następuje mechanicznie i bezrefleksyjnie”²⁴.

¹⁸ *Ibidem*, s. 1.

¹⁹ B. Kazenoff, *op. cit.*, s. 16–17. Cyt. za: C.A. Kessler, *NFTs Are Reshaping Artists' IP Rights*, 2021, <https://news.bloomberglaw.com/us-law-week/nfts-are-reshaping-artists-ip-rights>; A. Solomon, *Songwriter U: What are NFTs and Why Do They Matter?*, American Songwriter 2021, <https://americansongwriter.com/songwriter-u-what-are-nfts-and-why-do-they-matter>; L. Shin *et al.*, *What Exactly Do You Get When You Buy an NFT? Three Lawyers Discuss—Episode 224 Unchained Podcast*, 2021, <https://www.youtube.com/watch?v=frvwQAMEa8E>.

²⁰ M. Krzemińska, M. Rzeszutek, *Stosowanie smart kontraktów w obrocie konsumenckim – wybrane problemy*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny” 2021, nr 6(10), s. 51, https://ikar.wz.uw.edu.pl/images/numery/ikar_6_10/iKAR_610-21.pdf [dostęp z 2.09.2023]. Cyt. za: M. Pecyna, A. Behan, *Smart contracts – nowa technologia prawa umów?*, „Transformacje Prawa Prywatnego” 2020, nr 3, s. 187-216; M. Buchwald, *Smart Contract dispute resolution: the inescapable flaws of blockchain-based arbitration*, „University of Pennsylvania Law Review” 2020, t. 168, s. 1369-1423.

²¹ B. Kazenoff, *op. cit.* s. 16. Cyt. za: C. Hoskinson, *The Future Will Be Decentralized | Charles Hoskinson | Tedxbermuda, TEDx Talks, 2014*, <https://www.youtube.com/watch?v=97ufCT6lQcY>.

²² M. Krzemińska, M. Rzeszutek, *op. cit.*, s. 51. Cyt. za: K. Kowacz, K. Wielgus. *Smart kontrakty w prawie umów*, Kraków 2021.

²³ *Ibidem*. Cyt. za: D. Szostek, *Blockchain a prawo*, Warszawa 2018.

²⁴ *Ibidem*. Cyt. za: K. Kowacz, K. Wielgus, *op. cit.*, s. 58.

Technologia NFT w branży muzycznej. Jak to „działa”?

W tym dynamicznym krajobrazie niezliczone organizacje próbują wprowadzać innowacje technologiczne, które mają zrewolucjonizować branżę muzyczną. Jedną z organizacji wykorzystujących technologię NFT jest start-up NEWM. Projektowi przyświeca wizja stworzenia ekosystemu, w którym platformy streamingowe i wytwórnie płytowe nie przejmują głównej części przychodów, zamiast tego artyści mają większą kontrolę nad swoją twórczością, a konsumenci mogą „kolekcjonować muzykę” i czerpać z tego korzyści materialne. Aby zrealizować swoją wizję, organizacja buduje wielopoziomową i zdecentralizowaną platformę, która umożliwić będzie artystom publikację, dystrybucję, promocję i finansowanie twórczości muzycznej. W miejsce platform streamingowych i wytwórni płytowych wkracza obiektywne oprogramowanie, które nie jest ukierunkowane na osiągnięcie zysków²⁵.

Platforma ma opierać się na technologii blockchain, przy pomocy której twórcy będą mogli bezpiecznie sprzedawać lub licytować prawa własności intelektualnej do swoich dzieł bezpośrednio słuchaczom, wytwórniom muzycznym czy inwestorom poprzez połączenie NFT i FT (ang. *fungible token*, czyli wymiernialnych tokenów). Co ciekawe, im większy sukces odnoszą artyści, tym bardziej rośnie wartość NFT. Platforma ma pełnić funkcję giełdy muzycznej, ale również umożliwiać gromadzenie i przekazywanie tantiem²⁶. Pięć głównych założeń przewiduje:

1) fragmentaryzację praw własności intelektualnej do muzyki poprzez połączenie NFT i FT oraz smart kontrakty, dzięki czemu artyści przejmują kontrolę nad dystrybucją swojej twórczości,

2) kupno, sprzedaż, handel i licytacje muzycznych praw własności intelektualnej w formie NFT w aplikacji NEWM,

3) zautomatyzowany proces pobierania i dystrybucji tantiem dla właścicieli muzyki, zapewniający sprawiedliwy podział między wszystkich posiadaczy FT²⁷,

4) platformę strumieniową muzyki Hi-Fi z możliwością sprzedaży biletów w aplikacji i funkcją napiwków w trosce o zwiększenie przejrzystości w sektorze muzycznym poprzez pokazanie przepływu pieniędzy na łańcuchu,

²⁵ NEWM Whitepaper (biała księga), s. 3, https://newm.io/wp-content/uploads/2022/06/project-NEWM_Whitepaper_V1.pdf [dostęp 2.09.2023].

²⁶ *Ibidem*, s. 5.

²⁷ Zob. działanie w praktyce – *ibidem*, s. 10-11.

5) zdecentralizowaną autonomiczną organizację (DAO)²⁸ oraz tokeny użytkowe²⁹, które dają każdemu członkowi społeczności głos w sprawie przyszłości platformy.

Platforma może być wykorzystywana na wiele sposobów. Jednym z planów jest wdrożenie protokołu, który pozwala artystcie na wykorzystanie FT jako zastawu do uzyskania pożyczki od inwestorów np. w celu wyruszenia w trasę koncertową. Technologia zautomatyzowanego procesu pobierania i dystrybucji tantiem może pozwolić na wykorzystanie przyszłych opłat licencyjnych do spłaty pożyczki³⁰.

Polskie prawo własności intelektualnej w branży muzycznej

Polskie prawo własności intelektualnej reguluje ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych³¹. Zgodnie z art. 1 ust. 1 pr. aut. przedmiotem regulacji jest utwór, czyli każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiegokolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia. Utwory to dobra niematerialne, które muszą przybrać materialną postać, aby mogły podlegać percepcji. Dla prawa autorskiego nośnik, czyli rodzaj tej materii, nie ma znaczenia, natomiast prawo autorskie nie obejmuje ochroną nośników materialnych utworu³². Z kolei w ust. 2 ustawodawca wprost wskazuje utwory muzyczne i słowno-muzyczne jako przedmiot prawa autorskiego. Najczęstszym rodzajem utworów muzycznych i słowno-muzycznych są piosenki i pieśni. Jednak w definicji utworów muzycznych i słowno-muzycznych mieści się szeroka gama wytworów intelektu, które mogą być odbierane słuchowo czy też wzrokowo jako zapis nutowy³³. Podmiotem regulacji jest twórca, któremu przysługuje prawo autorskie (art. 8 pr. aut.). Twórca to autor utworu, może nim być jedynie człowiek – osoba fizyczna³⁴. Twórcy na mocy art. 16 pr. aut. przysługują prawa o charakterze osobistym, które chronią nieograniczoną w czasie i niepodlegającą zrzeczeniu się lub zbyciu więź twórcy z utworem oraz prawa o charakterze

²⁸ Zob. definicję – K. Piech, *Leksykon pojęć na temat technologii blockchain oraz kryptowalut*, s. 15, https://bitcoin.org.pl/wp-content/uploads/2023/06/leksykon_pojec_na_temat_tehnologii_blockchain_i_kryptowalut.pdf [dostęp 2.09.2023].

²⁹ Zob. definicję – *Utility Token*, „CoinMarketCap”, <https://coinmarketcap.com/alexandria/glossary/utility-token> [dostęp 2.09.2023].

³⁰ NEM Whitepaper, *op. cit.*, s. 11.

³¹ T.j. Dz. U. z 2022 r. poz. 2509; dalej jako: pr. aut.

³² J. Szyjewska-Bagińska, [w:] E. Ferenc-Szydełko (red.), *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, wyd. 4, Warszawa 2021, Legalis, art. 1, pkt 1-4.

³³ *Ibidem*, pkt 82.

³⁴ E. Ferenc-Szydełko (red.), *op. cit.*, wyd. 4, Warszawa 2021, Legalis, art. 8.

majątkowym, co stosownie do treści art. 17 pr. aut. oznacza, że twórcy przysługuje wyłączne prawo do korzystania z utworu i rozporządzania nim na wszystkich polach eksploatacji oraz do wynagrodzenia za korzystanie z utworu. Z punktu widzenia niniejszego opracowania niezwykle istotne jest wskazanie na wspomniane pola eksploatacji, które zgodnie z art. 50 pr. aut. stanowią w szczególności, lecz nie tylko:

1) w zakresie utrwalania i zwielokrotniania utworu – wytwarzanie określoną techniką egzemplarzy utworu, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;

2) w zakresie obrotu oryginałem albo egzemplarzami, na których utwór utrwalono – wprowadzanie do obrotu, użyczenie lub najem oryginału albo egzemplarzy;

3) w zakresie rozpowszechniania utworu w sposób inny niż określony w pkt 2 – publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także publiczne udostępnianie utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym.

Za pomocą licencji, czyli umowy o przeniesienie majątkowych praw autorskich lub umowy o korzystanie z utworu, nabywca uzyskuje określone w umowie prawa na umownie wyraźnie wymienionych polach eksploatacji. Na marginesie warto wskazać, że polski ustawodawca nie przewiduje możliwości zawierania umów prawnoautorskich, w których dopuszczona byłaby możliwość objęcia ich zakresem także nowych pól eksploatacji, w przeciwieństwie do ustawodawcy amerykańskiego, który dopuszcza klauzule *future media* umożliwiające korzystanie z utworu na nowych polach eksploatacji, jeżeli takowe się pojawiają³⁵.

Co istotne, art. 53 pr. aut. przewiduje, że przeniesienie autorskich praw majątkowych wymaga zachowania formy pisemnej pod rygorem nieważności. Natomiast z punktu widzenia omawianego rozwiązania przenoszenie praw za pomocą NFT nie powinno stanowić problemu, jako że zgodnie z art. 78¹ Kodeksu cywilnego oświadczenie woli złożone w formie elektronicznej jest równoważne z oświadczeniem woli złożonym w formie pisemnej, a do zachowania elektronicznej formy czynności prawnej wystarcza złożenie oświadczenia woli w postaci elektronicznej i opatrzenie go kwalifikowanym podpisem elektronicznym³⁶.

³⁵ A. Flegel, *Powstanie nowych pól eksploatacji utworów i ich wpływ na treść umów prawnoautorskich w perspektywie prawno-porównawczej*, „Folia Iuridica Universitatis Wratislaviensis” 2021, vol. 10 (2), s. 43, https://www.bibliotekacyfrowa.pl/Content/132241/PDF/Folia_Iuridica_Universitatis_Wratislaviensis_2021_vol_10_no_2.pdf#page=42 [dostęp 9.09.2023]. Cyt. za: P. Ślęzak, *Umowy w zakresie współczesnych sztuk wizualnych*, Warszawa 2012.

³⁶ J. Szyjewska-Bagińska, [w:] E. Ferenc-Szydełko (red.), *op. cit.*, wyd. 4, Warszawa 2021, Legalis, art. 53.

Prawo autorskie a technologia NFT

Duża część użytkowników pozostaje w błędnym przekonaniu, że wraz z zakupem NFT nabywają całą gamę praw własności intelektualnej do pierwotnych aktywów. Jednak w większości przypadków prawa przekazywane przy zakupie NFT są zwykłymi prawami własności do metadanych blockchain³⁷. Omawiając zagadnienie praw autorskich w kontekście technologii NFT, należy przede wszystkim mieć na uwadze fakt, że NFT są certyfikatami autentyczności, co oznacza, że kupujący nabywa dokładnie to, co zostało określone w smart kontrakcie powiązonym z NFT. Na kształt smart kontraktu wpływ ma sprzedawca oraz platforma, która określa regulamin sprzedaży. Zazwyczaj kupujący nabywa jedynie niewyłączną licencję na wyświetlanie lub odtwarzanie powiązanych mediów w portfelu do celów osobistych, chyba że stosowne postanowienia umowne lub regulamin platformy stanowią inaczej³⁸. Bardzo często zakup NFT przenosi na nabywcę jedynie prawa, podobne do tych, które przysługują nabywcy obrazu³⁹. Jednak na przykładzie przedstawionego projektu NEWM można dostrzec, że implementowane są także rozwiązania pozwalające na przenoszenie innych materialnych praw, np. prawa do reprodukcji.

W chwili obecnej istnieje wiele istotnych pytań o charakter i naturę NFT, na które nie można udzielić jednoznacznych odpowiedzi. Przede wszystkim należy ustalić, czy nabywca NFT faktycznie nabywa jedynie cyfrową kopię utworu, czy też sam NFT może być postrzegany jako utwór pierwotny⁴⁰ lub chociaż jako utwór zależny, który w myśl art. 5 ust. 1 pr. aut. jest przedmiotem prawa autorskiego bez uszczerbku dla prawa do utworu pierwotnego. Zdaje się, że przy tych rozważaniach istotne jest rozróżnienie pomiędzy sytuacją, w której istniejące faktycznie dzieło ma swoją reprezentację w formie NFT, a procesem tworzenia grafiki lub innego dzieła o walorach artystycznych w formie NFT⁴¹. Przepuszczalnie w pierwszym przypadku, który w dużej

³⁷ B. Kazenoff, *op. cit.*, s. 17. Cyt. za: L. Shin *et al.*, *op. cit.*; A. Solomon, *op. cit.*

³⁸ A. Bober-Kotarbińska, *Zarys zagadnień i wyzwań prawnych związanych z zastosowaniem technologii niewymienialnych tokenów w obszarze prawa własności intelektualnej*, „Palestra” 2023, nr 1-2, s. 109, <https://palestra.pl/pl/czasopismo/wydanie/1-2-2023/artukul/zarys-zagadnien-i-wyzwan-prawnych-zwiazanych-z-zastosowaniem-technologie-niewymienialnych-tokenow-w-obszarze-prawa-wlasnosci-intelektualnej> [dostęp 10.09.2023]. Cyt. za: Goforth, *What You Should Know before Buying or Selling an NFT in the US*, <https://cointelegraph.com/news/what-you-should-know-beforebuying-or-selling-an-nft-in-the-us> [dostęp 20.06.2022].

³⁹ B. Kazenoff, *op. cit.*, s. 17.

⁴⁰ *Ibidem*.

⁴¹ M. Misztela, A. Dobrzeniecka, *Obrót NFT – tworzenie praw własności intelektualnej przez tokeny niezbywalne*, „Rzeczpospolita” 23.05.2022, <https://www.rp.pl/finanse/art36348551-obrot-nft-tworzenie-praw-wlasnosci-intelektualnej-przez-tokeny-niezbywalne> [dostęp 11.09.2023].

mierze występuje w branży muzycznej, NFT postrzegać można jako swoistą kopię, reprodukcję, utwór pochodny lub nośnik. Z kolei w drugim przypadku można najprawdopodobniej mówić o utworze oryginalnym spełniającym kryteria art. 1 pr. aut.

Można wysunąć tezę, że wytworzenie NFT dla utworu muzycznego nie podlega zakresowi objętemu przez art. 2 ust. 1 pr. aut. Brak definicji opracowania cudzego utworu nie ułatwia sprawy i sam Sąd Najwyższy⁴² wskazuje, że oceny należy dokonywać w indywidualnym trybie. Być może NFT najbliższej jest do wymienionej przez ustawodawcę przeróbki, którą rozumie się jako „transpozycję, wyrażenie w inny sposób cudzego już istniejącego utworu”⁴³. Doktryna argumentuje, że NFT nie stanowi utworu, lecz jest sekwencją liczb wygenerowaną w odniesieniu do utworu. Wynikowego pliku nie można traktować jako reprodukcji ani adaptacji utworu⁴⁴. W obliczu takiej klasyfikacji w przypadku wygenerowania i publikacji NFT reprezentujących utwory muzyczne należy mówić raczej o rozpowszechnianiu czy publicznym udostępnianiu dzieła pierwotnego⁴⁵. Taka klasyfikacja prowadzi do konkluzji, w ramach której należy przyjąć, że tylko autor lub osoba, która uzyskała zgodę autora, jest uprawniona do stworzenia muzycznego NFT.

Ciekawą tezę na temat NFT jako nieautoryzowanych kopii lub pochodnych utworu bazowego wysunęła prof. Emily Behzadi, stwierdzając, że mintowanie⁴⁶ NFT nie może naruszać praw autorskich. Punktem wyjściowym tego stanowiska jest postrzeganie NFT jedynie jako swoistego linku do cyfrowej kopii utworu, a nie jako samej kopii czy pochodnego utworu⁴⁷. Autorka podkreśla, że NFT nie można uznawać za reprodukcję, jako że NFT tworzą metadane opisujące pewne zasoby, które są następnie wyświetlane, przesyłane i przechowywane cyfrowo. Wartość NFT nie wynika z samego utworu, lecz z unikalnego dowodu własności i autentyczności⁴⁸. NFT jest tu przyrównywany do hiperłącza⁴⁹. Jednak zgodnie z linią orzecniczą

⁴² Wyrok SN z dnia 14 listopada 2014 r, I CNP 10/14, Legalis.

⁴³ E. Ferenc-Szydelko (red.), *op. cit.*, wyd. 4, Warszawa 2021, Legalis, art. 2.

⁴⁴ A. Bober-Kotarbińska, *op. cit.*, s. 116. Cyt za: A. Guadamuz, *Non-fungible tokens (NFTs) and copyright*, https://www.wipo.int/wipo_magazine/en/2021/04/article_0007.html [dostęp 20.06.2023].

⁴⁵ Jakie prawa może naruszać nieuprawniona osoba, mintując NFT – zob. E. Bonadio, R. Mohnot, *NFTs and Copyright: Some Burning Issues*, „Kluwer Copyright Blog” 2022, <https://copyrightblog.kluweriplaw.com/2022/07/21/nfts-and-copyright-some-burning-issues> [dostęp 15.09.2023].

⁴⁶ Zob. definicję mintowania – *Mint NFT – co to znaczy?*, „Blog Binance” 2022, <https://www.binance.com/pl/blog/all/mint-nft--co-to-znaczy-421499824684903997> [dostęp 20.09.2023].

⁴⁷ E. Behzadi, *The Fiction of NFTs and Copyright Infringement*, „University of Pennsylvania Law Review Online’s” 2022, t. 170, s. 3, <https://www.pennlawreview.com/2022/04/12/the-fiction-of-nfts-and-copyright-infringement> [dostęp 15.09.2023].

⁴⁸ *Ibidem*, s. 4.

⁴⁹ *Ibidem*, s. 8.

Trybunału Sprawiedliwości Unii Europejskiej⁵⁰ przesądzenie o tym, czy hiperlink narusza prawa autorskie, wymaga indywidualnej oceny. Hiperlink może zostać uznany za publiczne udostępnianie w myśl dyrektywy 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r.⁵¹ nowelizowanej dyrektywą 2019/790 z dnia 17 kwietnia 2019 r.⁵², co zapewnia właścicielowi praw autorskich wyłączone prawo do zezwalania lub zakazywania na publiczne udostępnianie utworów⁵³. Trybunał w wyroku z 2016 r. w sprawie *GS Media BV przeciwko Sanoma Media Netherlands BV i in.*⁵⁴ wskazał, że indywidualna ocena ma na celu określenie, (1) czy treść jest ogólnodostępna i została zamieszczona za zgodą autora – jeśli tak, to nie ma naruszenia praw, (2) czy treść trafia do nowej publiczności takiej jak płatni subskrybenci – jeśli tak, to może dojść do naruszenia, (3) czy zamieszczenie hiperłącza wiąże się z działalnością zarobkową – jeśli tak, to może dojść do naruszenia, jeśli zamieszczający wiedział lub powinien był wiedzieć, że treść, do której prowadzi link, została opublikowana nielegalnie⁵⁵. Pojmując NFT jako hiperlink według powyższych kryteriów, zmintowanie i sprzedaż NFT bez zgody autora utworu muzycznego naruszałoby najprawdopodobniej prawa autorskie, w związku z czym z perspektywy prawa europejskiego nie można przyznać racji teorii prof. Behzadi.

Kwestia tego, czy NFT można rozumieć jako kopię, jest również nieodzowna w rozważaniach nad tym, czy wyrażona w art. 51 ust. 3 pr. aut. zasada wyczerpania prawa ma zastosowanie do omawianej technologii. Zgodnie z przepisem wprowadzenie do obrotu oryginału albo egzemplarza utworu na terytorium Europejskiego Obszaru Gospodarczego wyczerpuje prawo do zezwalania na dalszy obrót takim egzemplarzem na terytorium Rzeczypospolitej Polskiej, z wyjątkiem jego najmu lub użyczenia. W literaturze i orzecznictwie jest akcentowane, że możliwość wprowadzenia do obrotu obejmuje jedynie oryginał lub fizyczne kopie utworu utrwalone na materialnych nośnikach⁵⁶. Argumentując teorię wyczerpania, wskazuje się, że autor uzyskał wynagrodzenie, wprowadzając pewny egzemplarz utworu do obrotu, więc

⁵⁰ Wyrok TSUE z dnia 8.09.2016 r., C-160/15, *GS Media BV przeciwko Sanoma Media Netherlands BV*, EU:C:2016:644; wyrok TSUE z dnia 26.04.2017 r., C-527/15, *Stichting Brein przeciwko Jackowi Frederikowi Willemsowi*, ECLI:EU:C:2016:938.

⁵¹ Dz. Urz. UE L 167/10 z 22.06.2001 r.

⁵² Dz. Urz. UE L 130/92 z 17.05.2019 r.

⁵³ E. O'Hare, *Hyperlinking in the EU: balancing freedom of expression with protection of copyright and reputation without breaking the internet*, 2019, <https://www.stevens-bolton.com/site/insights/articles/hyperlinking-in-the-eu> [dostęp 20.09.2023].

⁵⁴ *GS Media BV przeciwko Sanoma Media Netherlands BV*.

⁵⁵ E. O'Hare, *op. cit.*

⁵⁶ J. Szyjewska-Bagińska, [w:] E. Ferenc-Szydelko (red.), *op. cit.* Art. 51. Cyt. za: Wyrok SA w Warszawie z dnia 30 czerwca 2011 r., VI ACa 1160/10, niepubl.

z wyjątkami ujętymi w art. 19, 19¹ i 19⁵ pr. aut. autor nie może ponownie żądać zapłaty przy przeniesieniu własności egzemplarza na kolejny podmiot⁵⁷. Teorii wyczerpania w zasadzie nie stosuje się w odniesieniu do egzemplarzy cyfrowych, jako że przy niematerialnym odtwarzaniu utworu zazwyczaj mamy do czynienia z wielokrotnością eksploatacji⁵⁸ jak w przypadku e-booków. Jednak, jak już wskazano, NFT to unikatowe tokeny, a przy ich sprzedaży czy odsprzedaży nie ma mowy o powstawaniu kopii samych NFT. Być może NFT powinny być traktowane podobnie do programu komputerowego z wyroku TSUE z 3.07.2012 r. w sprawie *UsedSoft przeciwko Oracle*⁵⁹. Przełomowe orzeczenie umożliwiło zastosowanie zasady wyczerpania praw majątkowych autora w odniesieniu do cyfrowych „egzemplarzy” utworu – programów komputerowych, co oznacza odstępianie od wymogu fizycznego nośnika utworu. Akcent postawiono tu na ocenie czynności prawnej „sprzedaży” dostępu do utworu. W sprawie kupujący po zapłacie uzyskiwał dostęp online do oprogramowania, które można było pobrać i załadować na dysku twardym komputera klienta. Dostęp do programu bez ograniczeń czasowych był dla Trybunału czynnikiem zaważającym o tym, że transakcję należy rozumieć jako sprzedaż. W końcu charakterystycznym elementem umowy sprzedaży jest oddanie przedmiotu umowy do dyspozycji kupującego na czas nieoznaczony w zamian za zapłatę z góry określonej ceny⁶⁰. W zasadzie NFT powinno traktować się tożsamo, jako że kupujący również uzyskuje nieograniczony czasowo dostęp do tokena. Mimo to zdaje się, że i w tym przypadku NFT wychodzi poza ustalone kategorie i kwestia ta najprawdopodobniej również będzie wymagała konkretnej regulacji. W kolejnych bowiem wyrokach TSUE wykluczono możliwość rozciągania interpretacji zawartej w sprawie *UsedSoft przeciwko Oracle* na kopie cyfrowe innych utworów niż programy komputerowe, np. na e-booki⁶¹. I w tym przypadku, jako że NFT ma zarówno unikalny komponent cyfrowy, jak i jest powiązany z aktywem, materialnym bądź niematerialnym, analiza jest skomplikowana⁶². Jednak obecnie twórca NFT za pomocą odpowiednio skonstruowanego smart kontraktu może śledzić dalszą sprzedaż aktywu oraz może zaimplementować automatyczny system pobierania tantiem lub

⁵⁷ J. Szyjewska-Bagińska, [w:] E. Ferenc-Szydełko (red.), *op. cit.*, art. 51.

⁵⁸ *Ibidem*. Cyt za: E. Traple, *Ustawowe konstrukcje*, s. 93.

⁵⁹ Wyrok TSUE z 3.07.2012 r., C-128/11, *UsedSoft GmbH przeciwko Oracle International Corp.*, ECLI:EU:C:2012:407.

⁶⁰ J. Szyjewska-Bagińska, *op. cit.*, art. 51.

⁶¹ *Ibidem*. Zob. też wyrok TSUE z dnia 19.12.2019 r., C-263/18, *Nederlands Uitgeversverbond i Groep Algemene Uitgevers*, ECLI:EU:C:2019:1111.

⁶² B. Kazenoff, *op. cit.*, s. 18.

pro wizji za każdym razem, gdy jego NFT jest odsprzedawany⁶³, co można byłoby pojmować jako ucieleśnienie wyjątku zawartego choćby w art. 19 pr. aut.

Wyzwania i perspektywy

Technologia NFT na gruncie prawa własności intelektualnej niesie ze sobą wyzwania dla władzy legislacyjnej z uwagi na trudności w umieszczeniu jej w konkretnych ramach pojęciowych. Oprócz tego występuje także szereg innych wyzwań technologicznych, o których należy tu wspomnieć.

Sprzedaż NFT odbywa się obecnie w głównej mierze na platformach, które są rzeczywistymi powiernikami NFT. Kupujący najczęściej nabywa unikalny podpis kryptograficzny, który po zdekodowaniu odnosi się do nośnika – utworu znajdującego się w innym miejscu w internecie. Często ten nośnik pozostaje pod kontrolą platformy na jej wewnętrznym serwerze i nabywca musi polegać na platformie, aby mieć wgląd w swoje aktywa, co naraża go na potencjalną utratę dostępu w przypadku nieprawidłowego funkcjonowania platformy⁶⁴. Jednym ze sposobów na ochronę swoich NFT przed hakerami czyhającymi na liczne platformy jest przechowywanie ich w trybie offline w portfelu sprzętowym typu *cold storage*⁶⁵.

Inwestorzy powinni być również świadomi ryzyka zakupu NFT, który może naruszać prawa autorskie autora, w związku z czym kupujący może stracić dostęp do aktywów⁶⁶. Obecnie brak odpowiedniej regulacji prawnej w tej kwestii, dlatego to, czy nabywca utraci dostęp do naruszającego prawa autorskie NFT, zależy od regulaminu platformy. Niektóre obligują sprzedawcę do zwrotu pieniędzy za sprzedaż NFT, jeśli później okaże się, że token naruszył prawa własności intelektualnej podmiotu uprawnionego. Inne ograniczają swoją odpowiedzialność, uchylając się od sprawdzania transakcji czy egzekwowania zobowiązań wobec anonimowych kupujących i sprzedających, stanowiąc jednocześnie, że to użytkownik ponosi pełne ryzyko swoich zakupów⁶⁷. Do

⁶³ F. Teomete Yalabik, *op. cit.*, s. 10.

⁶⁴ B. Kazenoff, *op. cit.*, s. 18. Cyt. za: *Not Your Keys, Not Your Coins: Why It Matters*, <https://www.ledger.com/academy/not-your-keys-not-your-coins-why-it-matters>.

⁶⁵ G. Kaur, K. Lucrezia Cornèr, *How to store NFT assets – A beginner's guide*, „Cointelegraph” 2023, <https://cointelegraph.com/learn/how-to-store-nft-assets-a-beginners-guide> [dostęp 24.09.2023].

⁶⁶ B. Kazenoff, *op. cit.* s. 18. Cyt. za: B. Munster, *People Are Stealing Art and Turning It Into NFTs*, „VICE Media” 2021, <https://www.vice.com/en/article/n7vxe7/people-are-stealing-art-and-turning-it-into-nfts>.

⁶⁷ *Ibidem*, s. 19. Cyt. za: Terms of Service, *Superrare.co*, <https://help.superrare.co/en/articles/4792372-2-4-copyright-on-superrare>; M. Gitlitz, D. Ervin, C. Wilson, *What Cos. Need To Know Before Entering Nascent NFT Market*, „Law360” 2021, <https://www.law360.com/articles/1370358/what-cos-need-to-know-before-entering-nascent-nft-market>.

rozstrzygnięcia pozostaje również kwestia, czy ta ostatnia praktyka platform może być w ogóle wiążąca. W końcu w większości jurysdykcji odpowiedzialność podmiotów pośredniczących zależy od: (a) występowania lub braku świadomości lub rzeczywistej wiedzy platformy o naruszeniu, (b) procedury *notice & takedown* oraz (c) aktywnej roli platformy w organizowaniu bądź jedynie biernego dostarczania treści. Platforma poniesie najprawdopodobniej odpowiedzialność, jeśli posiadała wiedzę o naruszeniu, nadal udostępnia treść naruszającą prawa własności intelektualnej mimo otrzymania powiadomienia o konieczności jej usunięcia oraz aktywnie uczestniczy w organizowaniu treści⁶⁸.

Blockchain oferuje szereg rozwiązań technologicznych, które mają potencjał na zrewolucjonizowanie branży muzycznej. Najczęściej wymienianymi zaletami wykorzystania blockchainu w branży muzycznej są: wprowadzenie powszechnej przejrzystości w obrocie, automatyzacja realizacji płatności, eliminacja wpływu pośredników zewnętrznych czy większe tantiemy dla muzyków⁶⁹. Rewolucja Web3 oznacza też demokratyzację dostępu do czerpania zysków z muzycznej ekspresji, dając szansę artystom bez kapitału⁷⁰. Zautomatyzowana dystrybucja tantiem wydaje się szczególnie atrakcyjna w zestawieniu z obecnym fragmentarycznym polskim modelem, w którym funkcjonują cztery organizacje zbiorowego zarządzania odpowiedzialne za pobór i podział tantiem należnych za wykorzystywanie chronionych utworów muzycznych i słowno-muzycznych⁷¹.

Technologia blockchain może być też ciekawą alternatywą dla ambitnego, choć nieudanego projektu stworzenia globalnej bazy zbiorowego zarządzania – the Global Repertoire Database (GRD), która miała zawierać bazę wszystkich utworów muzycznych, jakie kiedykolwiek powstały wraz z bazą wszystkich właścicieli praw autorskich. W 2014 r. ogłoszono niepowodzenie i zaprzestano prac nad projektem⁷². Zdecentralizowana baza zarządzania prawami autorskimi mogłaby działać

⁶⁸ E. Bonadio, R. Mohnot, *op. cit.*

⁶⁹ A. Taghdiri, *op. cit.*, s.174.

⁷⁰ B. Rauman, *The Budding Disruption of Blockchain Technology Upon the Current Structure of the Music Industry*, 2021, s. 2-3, https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=1468&context=senior_theses [dostęp 28.09.2023]. Cyt. za: C. L. Bergendorff, *From the Attention Economy to the Creator Economy: A Paradigm Shift*, <https://www.forbes.com/sites/claralindhbergen-dorff/2021/03/12/from-the-attention-economy-to-the-creator-economy-a-paradigm-shift>.

⁷¹ Obwieszczenie Ministra Kultury i Dziedzictwa Narodowego z 26.03.2009 r. w sprawie ogłoszenia decyzji Ministra Kultury i Dziedzictwa Narodowego o udzieleniu i o cofnięciu zezwolenia na podjęcie działalności organizacji zbiorowego zarządzania prawami autorskimi lub prawami pokrewnymi (M.P. z 2009 r. Nr 21, poz. 270).

⁷² A. Taghdiri, *op. cit.* s. 184. Cyt. za: *Blockchain: Recording the Music Industry: How Blockchain Technology Could Save the Music Industry Billions*, „PricewaterhouseCoopers LLP”, <https://www.pwc.fr/>

na zasadzie globalnej, zsynchronizowanej platformy do rejestracji i handlu prawami autorskimi bez korzystania z chmury. Kraje partycypujące w projekcie otrzymałyby członkostwo w federacji praw autorskich i uczestniczyłyby w tworzeniu bloków przy wykorzystaniu algorytmu konsensusu *proof-of-authority*. W proponowanym modelu każdy miałby wgląd do bazy i mógłby sprawdzić utwór chroniony prawem autorskim, ale tylko zarejestrowani użytkownicy mogliby dokonywać transakcji⁷³.

Eksperci szacują, że jedna trzecia słuchaczy nadal korzysta z pirackiej muzyki poprzez streaming i nielegalne pobieranie⁷⁴. Blockchain może pomóc w zwalczaniu tego zjawiska, choć eksperci twierdzą, że nie jest wystarczającym rozwiązaniem do całkowitej eliminacji bezprawnego kopiowania. Blockchain umożliwia np. opatrywanie utworu znakiem wodnym w sposób niezmienny i odporny na manipulacje sposobem, tym samym uniemożliwiając plagiowanie wcześniej chronionych prawem autorskim materiałów⁷⁵.

Technologię NFT można zastosować również w sprzedaży biletów koncertowych, co rozwiązałoby problem nielegalnej odsprzedaży biletów, „branzę”, której wartość jest szacowana na 2,6 mld USD w 2022 r., a w 2031 r. ma osiągnąć 5,9 mld USD⁷⁶. Wator tego rozwiązania dostrzegł zespół muzyczny Kings of Leon, który nawiązał współpracę z firmą Yellowheart przy tworzeniu biletów koncertowych w postaci NFT. Smart kontrakt powiązany z biletami określał m.in., ile razy bilet mógł zostać odsprzedany, wymagany wiek nabywcy oraz sposób podziału przychodów z odsprzedaży⁷⁷.

Wnioski

Technologia blockchain i NFT niosą ze sobą wiele korzyści dla branży muzycznej, lecz do wykorzystania ich pełnej operatywności należy najpierw przezwyciężyć szereg przeszkód technologicznych, jak i regulacyjnych. Wśród zalet tej technologii

[fr/as sets/files/pdf/2018/07/pwc-blockchain-recording-music-industry.pdf](#) [dostęp 17.11.2018]; *Statement on the GRD*, „PRS for Music” 2014, <https://www.prsformusic.com/press/2014/statement-on-the-grd>.

⁷³ M.M. Islam, H.P. In, *Decentralized Global Copyright System Based on Consortium Blockchain with Proof-of-Authority*, 2023, s. 1, https://www.techrxiv.org/articles/preprint/Decentralized_Global_Copyright_System_Based_on_Consortium_Blockchain_with_Proof-of-Authority/16564218/1 [dostęp 28.09.2023].

⁷⁴ D. Jugovic Spajic, *Piracy Is Back: Piracy Statistics for 2023*, <https://dataprot.net/statistics/piracy-statistics> [dostęp 28.09.2023].

⁷⁵ A. Tuck, *How blockchain can tackle piracy in entertainment*, „Technology Magazine” 2022, <https://technologymagazine.com/articles/how-blockchain-can-tackle-piracy> [dostęp 28.09.2023].

⁷⁶ *Secondary Tickets Market*, „Straits Research”, <https://straitsresearch.com/report/secondary-tickets-market> [dostęp 28.09.2023].

⁷⁷ B. Kazenoff, *op. cit.*, s. 20. Cyt. za: S. Hissong, *A Field Guide to Music's Potential Crypto Boom*, „Rolling Stone Magazine” 2021, <https://www.rollingstone.com/pro/features/music-crypto-blockchain-nfts-guide-1116327>.

na pierwszy plan wysuwa się od dawna już postulowane wzmocnienie pozycji artystów poprzez wprowadzenie mechanizmów umożliwiających przejrzysty i sprawiedliwy, a przy tym zautomatyzowany podział zysków. Ponadto blockchain może ułatwić śledzenie i zarządzanie prawami autorskimi, a także stać się nowoczesnym narzędziem do walki z fonograficznym piractwem czy nielegalną odsprzedażą biletów koncertowych. Jednakże wdrażanie tych technologii wiąże się z wyzwaniem. Jednym z nich jest rosnąca pozycja platform, na których w głównej mierze odbywa się sprzedaż NFT i które stają się rzeczywistymi powiernikami cyfrowych aktywów. Wzmacniający się wpływ platform może wspierać proces centralizacji. Osoby rozważające zakup muzycznego NFT powinny mieć pełną świadomość tego, co nabywają oraz jakie prawa wynikają z tego zakupu. Ponadto ważne jest, by byli oni świadomi ogólnego ryzyka inwestycyjnego, a także specyficznego ryzyka zakupu NFT, który może naruszać prawa autorskie twórcy oraz niepewności prawnych związanych z taką transakcją.

Z perspektywy prawa własności intelektualnej największy problem stanowi precyzyjne zdefiniowanie i klasyfikacja niewymienialnych tokenów. To, czy NFT powiązany z utworem muzycznym będziemy traktować jako certyfikat autentyczności składający się z ciągu liczb, kopię, reprodukcję, nośnik, utwór pochodny czy też utwór oryginalny, jest kluczowe dla określenia możliwych konsekwencji prawnych ewentualnych naruszeń. Uzasadniona wydaje się teza, że muzyczny NFT oscyluje w ramach pojęciowych takich jak cyfrowa kopia utworu, swoiste hiperłącze do utworu, jego certyfikat autentyczności, reprodukcja czy cyfrowy nośnik. Mintowanie muzycznego NFT można pojmować także jako innowacyjny sposób na rozpowszechnianie czy publiczne udostępnianie dzieła pierwotnego, lecz zdecydowanie ciężko będzie dowieść, że muzyczny NFT wypełnia przesłanki definicji utworu pierwotnego.

W Polsce i Europie kwestia NFT nie była dotychczas przedmiotem licznych spraw sądowych, a liczba wyroków dotyczących tej tematyki pozostaje ograniczona. Należy zatem zastanowić się, czy ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych jest na tyle nowoczesna i uniwersalna, aby można było stosować jej przepisy w kontekście muzycznych NFT. Zdaje się, że zastosowanie istniejących instytucji prawnych, takich jak prawo do odsprzedaży (art. 19 pr. aut.), wyczerpanie praw autorskich (art. 51 pr. aut.), czy pola eksploatacji (art. 50 pr. aut.)⁷⁸

⁷⁸ M. Kubiak, E. Karwowska, *Obrót NFT jako nowa forma dystrybucji przedmiotów własności intelektualnej*, „Prawo Nowych Technologii” 2022, nr 1, s. 28, Legalis.

w sferze technologii NFT jest możliwe, choć niedoskonałe. Zwłaszcza na kanwie art. 51 ust. 3 pr. aut., regulującego wyczerpanie prawa do zezwalania na dalszy obrot egzemplarza wprowadzonego do obrotu, można dostrzec jak NFT wymykają się spoza utartych struktur koncepcyjnych. Tradycyjnie ta instytucja prawna znajduje zastosowanie do oryginału lub fizycznych kopii utworów utwalonych na materialnych nośnikach. Zdaje się, że należy odstąpić od tej reguły w przypadku NFT, podobnie jak uczyniono to w stosunku do programów komputerowych.

Jako przełomowy krok regulacyjny dla branży blockchain można postrzegać opublikowany przez Komisję Europejską 24 września 2020 r. projekt⁷⁹ rozporządzenia w sprawie rynków kryptoaktywów, zmieniającego dyrektywę 2019/1937, znanego jako MiCA (ang. *Markets in crypto-assets regulation*)⁸⁰, które zacznie obowiązywać w 2024 r. Ogólnie rzecz biorąc, NFT rozumiane jako reprezentacja unikatowych, niepodzielnych i niezamiennych aktywów, takich jak usługi, dobra cyfrowe lub fizyczne, nie będą podlegać MiCA. Wyjątkiem będą NFT, które przyznają posiadaczowi lub emitentowi określone prawa związane z instrumentami finansowymi, takie jak prawa do zysku lub inne uprawnienia⁸¹. To, jak postrzegane będą muzyczne NFT i czy zostaną objęte zakresem regulacyjnym MiCA, nie jest pewne.

Na drodze masowej adopcji technologii blockchain i NFT w branży muzycznej stoją liczne wyzwania. Chociaż wiele dyskusji skupia się na problemach technologicznych i regulacyjnych, nie można pomijać ważnej kwestii dotyczącej gotowości społeczeństwa na wysoki poziom przejrzystości, jaki gwarantuje księga blockchain⁸².

Bibliografia

Akty prawne

Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz. Urz. UE L 167/10 z 22.06.2001 r.)

⁷⁹ Wniosek – Rozporządzenie Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów i zmieniające dyrektywę (UE) 2019/1937, COM(2020) 593 final, 2020/0265(COD).

⁸⁰ A. Behan, *Waluty wirtualne jako przedmiot przestępstwa, MiCA – Rozporządzenie w sprawie rynków kryptoaktywów i zmieniające dyrektywę (UE) 2019/1937*, 2022 wyd. 1, s. 54, Legalis.

⁸¹ J. Ibáñez Jiménez, E.M. Ibáñez Jiménez, *NFT Legal and Market Challenges in Permissioned Blockchain Networks*, „Blockchain Applications – Transforming Industries, Enhancing Security, and Addressing Ethical Considerations” 2023, <https://www.intechopen.com/chapters/84502> [dostęp 1.10.2023].

⁸² A. Taghdiri, *op. cit.*, s. 193. Cyt. za: *Music on the Blockchain, Blockchain For Creative Industries Research Cluster*, Middlesex University 2016, https://www.mdx.ac.uk/__data/assets/pdf_file/0026/230696/Music-On-The-Blockchain.pdf.

Dyrektywa 2019/790 Parlamentu Europejskiego i Rady z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz. Urz. UE L 130/92 z 17.05.2019 r.).

Wniosek – Rozporządzenie Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów i zmieniające dyrektywę (UE) 2019/1937, COM(2020) 593 final, 2020/0265(COD).

Obwieszczenie Ministra Kultury i Dziedzictwa Narodowego z 26.03.2009 r. w sprawie ogłoszenia decyzji Ministra Kultury i Dziedzictwa Narodowego o udzieleniu i o cofnięciu zezwolenia na podjęcie działalności organizacji zbiorowego zarządzania prawami autorskimi lub prawami pokrewnymi (M.P. z 2009 r. Nr 21, poz. 270).

Orzeczenia

Wyrok SN z dnia 14 listopada 2014 r., I CNP 10/14, Legalis.

Wyrok TSUE z dnia 3 lipca 2012 r., C-128/11, *UsedSoft GmbH przeciwko Oracle International Corp.*, ECLI:EU:C:2012:407.

Wyrok TSUE z dnia 8 września 2016 r., C-160/15, *GS Media BV przeciwko Sanoma Media Netherlands BV*, EU:C:2016:644

Wyrok TSUE z dnia 26 kwietnia 2017 r., C-527/15, *Stichting Brein przeciwko Jackowi Frederikowi Willemsowi*, ECLI:EU:C:2016:938.

Wyrok TSUE z dnia 19 grudnia 2019 r., C-263/18, *Nederlands Uitgeversverbond i Groep Algemene Uitgevers*, ECLI:EU:C:2019:1111.

Literatura

Behan A., *Waluty wirtualne jako przedmiot przestępstwa, MiCA – Rozporządzenie w sprawie rynków kryptoaktywów i zmieniające dyrektywę (UE) 2019/1937*, 2022 wyd. 1, Legalis.

Behzadi E., *The Fiction of NFTs and Copyright Infringement*, „University of Pennsylvania Law Review Online’s” 2022, t. 170, <https://www.pennlawreview.com/2022/04/12/the-fiction-of-nfts-and-copyright-infringement> [dostęp 15.09.2023].

Bober-Kotarbińska A., *Zarys zagadnień i wyzwań prawnych związanych z zastosowaniem technologii niewymienialnych tokenów w obszarze prawa własności intelektualnej*, „Palestra” 2023, nr 1-2, <https://palestra.pl/pl/czasopismo/wydanie/1-2-2023/artukul/zarys-zagadnien-i-wyzwan-prawnych-zwiazanych-z-zastosowaniem-technologii-niewymienialnych-tokenow-w-obszarze-prawa-wlasnosci-intelektualnej> [dostęp 10.09.2023].

Bonadio E., Mohnot R., *NFTs and Copyright: Some Burning Issues*, „Kluwer Copyright Blog” 2022, <https://copyrightblog.kluweriplaw.com/2022/07/21/nfts-and-copyright-some-burning-issues> [dostęp 15.09.2023].

Compare P., *The Merge NFT: Ethereum Collection That Raised \$90,000,000+*, „CoinCodex” 2023, <https://coincodex.com/article/24706/the-merge-nft> [dostęp 20.08.2023].

Ferenc-Szydełko E. (red.), *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, wyd. 4, Warszawa 2021, Legalis.

Flegel A., *Powstanie nowych pól eksploatacji utworów i ich wpływ na treść umów prawnoautorskich w perspektywie prawnoporównawczej*, „Folia Iuridica Universitatis Wratislaviensis” 2021,

- vol. 10 (2), https://www.bibliotekacyfrowa.pl/Content/132241/PDF/Folia_Iuridica_Universitatis_Wratislaviensis_2021_vol_10_no_2.pdf#page=42 [dostęp 9.09.2023].
- Gherghelas S., *Dapp Industry Report 2022*, <https://dappradar.com/blog/dapp-industry-report-2022-dapp-industry-proves-resilient-in-crypto-winter> [dostęp 20.08.2023].
- Gherghelas S., *State of the Dapp Industry in Q2 2023*, <https://dappradar.com/blog/state-of-the-dapp-industry-in-q2-2023> [dostęp 20.08.2023].
- Hayward A., *What Are CryptoPunks? The Ethereum NFT Sensation's Wild Ride*, „Decrypt” 2023, <https://decrypt.co/resources/what-are-cryptopunks-ethereum-nft-avatars> [dostęp 20.08.2023].
- Hissong S., *Kings of Leon Will Be the First Band to Release an Album as an NFT*, „Rolling Stone” 2021, <https://www.rollingstone.com/pro/news/kings-of-leon-when-you-see-yourself-album-nft-crypto-1135192> [dostęp 26.08.2023].
- Ibáñez Jiménez J., Ibáñez Jiménez E. M., *NFT Legal and Market Challenges in Permissioned Blockchain Networks*, „Blockchain Applications – Transforming Industries, Enhancing Security, and Addressing Ethical Considerations” 2023, <https://www.intechopen.com/chapters/84502> [dostęp 1.10.2023].
- Islam M.M., In H.P., *Decentralized Global Copyright System Based on Consortium Blockchain with Proof-of-Authority*, 2023, https://www.techrxiv.org/articles/preprint/Decentralized_Global_Copyright_System_Based_on_Consortium_Blockchain_with_Proof-of-Authority/16564218/1 [dostęp 28.09.2023].
- Jugovic Spajic D., *Piracy Is Back: Piracy Statistics for 2023*, <https://dataprot.net/statistics/piracy-statistics> [dostęp 28.09.2023].
- Kaur G., Lucrezia Cornè K., *How to store NFT assets — A beginner's guide*, „Cointelegraph” 2023, <https://cointelegraph.com/learn/how-to-store-nft-assets-a-beginners-guide> [dostęp 24.09.2023].
- Kazenoff B., *NFTs, Blockchain Technology, and Copyrights: How the Future of the Music Industry Will Be Decentralized*, „Entertainment, Arts and Sports Law Journal” 2021, t. 32, nr 3, https://nysba.org/app/uploads/2021/11/EASL-Journal-2021-Vol-32-No-3_8.5X11_WEB.pdf [dostęp 30.08.2023].
- Krzemińska M., Rzeszutek M., *Stosowanie smart kontraktów w obrocie konsumenckim – wybrane problemy*, „internetowy Kwartalnik Antymonopolowy i Regulacyjny” 2021, nr 6(10), https://ikar.wz.uw.edu.pl/images/numery/ikar_6_10/iKAR_610-21.pdf [dostęp z 2.09.2023].
- Kubiak M., Karwowska E., *Obrót NFT jako nowa forma dystrybucji przedmiotów własności intelektualnej*, „Prawo Nowych Technologii” 2022, nr 1, Legalis.
- LCX Team, *The History of NFTs*, 2023, <https://www.lcx.com/the-history-of-nfts> [dostęp 20.08.2023].
- Marszałek P., *Kryptowaluty – pojęcie, cechy, kontrowersje*, „Studia BAS” 2019, nr 1(57), [https://orka.sejm.gov.pl/WydBAS.nsf/0/F8F4218303461D74C12583E10037EC68/\\$file/5.Marszalek.pdf](https://orka.sejm.gov.pl/WydBAS.nsf/0/F8F4218303461D74C12583E10037EC68/$file/5.Marszalek.pdf) [dostęp 27.08.2023].
- Mint NFT – co to znaczy?*, „Blog Binance” 2022, <https://www.binance.com/pl/blog/all/mint-nft--co-to-znaczy-421499824684903997> [dostęp 20.09.2023].
- Misztela M., Dobrzeńska A., *Obrót NFT – tworzenie praw własności intelektualnej przez tokeny niezbywalne*, „Rzeczpospolita” 23.05.2022, <https://www.rp.pl/finanse/art36348551-obrot-nft--tworzenie-praw-wlasnosci-intelektualnej-przez-tokeny-niezbywalne> [dostęp 11.09.2023].
- NEWM Whitepaper (biała księga), s. 3, https://newm.io/wp-content/uploads/2022/06/projectNEWM_Whitepaper_V1.pdf [dostęp 2.09.2023].

- O'Hare E., *Hyperlinking in the EU: balancing freedom of expression with protection of copyright and reputation without breaking the internet*, 2019, <https://www.stevens-bolton.com/site/insights/articles/hyperlinking-in-the-eu> [dostęp 20.09.2023].
- Piech K., *Leksykon pojęć na temat technologii blockchain oraz kryptowalut*, https://bitcoin.org.pl/wp-content/uploads/2023/06/leksykon_pojec_na_temat_tehnologii_blockchain_i_kryptowalut.pdf [dostęp 2.09.2023].
- Rauman B., *The Budding Disruption of Blockchain Technology Upon the Current Structure of the Music Industry*, 2021, https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=1468&context=senior_theses [dostęp 28.09.2023].
- Rot A., Zygala R., *Technologia blockchain jako rewolucja w transakcjach cyfrowych. Aspekty technologiczne i potencjalne zastosowania*, „Informatyka Ekonomiczna” 2018, nr 4 (50), https://dbc.wroc.pl/Content/72987/Rot_Zygala_Technologia_blockchain_jako_rewolucja.pdf [dostęp 27.08.2023].
- Ruby D., *39+ Detailed NFT Statistics In 2023*, <https://www.demandsage.com/nft-statistics> [dostęp 20.08.2023].
- Secondary Tickets Market*, „Straits Research”, <https://straitresearch.com/report/secondary-tickets-market> [dostęp 28.09.2023].
- Zymaniak M., *Zniszczyła go powódź tysiąclecia. Obraz polskiego artysty nie tylko ożył dzięki NFT. Dziś trafia też na aukcję*, „Spider's Web” 2021, <https://spidersweb.pl/plus/2021/12/nft-aukcja-sztuka-licytacja-kowalewski-libera> [dostęp 1.10.2023].
- Taghdiri A., *How Blockchain Technology Can Revolutionize the Music Industry*, „Harvard Journal of Sports & Entertainment Law” 2019, t. 10, <https://theblockchaintest.com/uploads/resources/Arya%20taghdiri%20-%20How%20blockchain%20Technology%20Can%20revolutionize%20the%20Music%20Industry%20-%20na.pdf> [dostęp 20.08.2023].
- Teomete Yalabik F., *Future of NFTs in the entertainment industry: No longer the 'Wild West' of intellectual property law?*, „European Journal of Law and Technology” 2023, t. 14, nr 1, <https://ejlt.org/index.php/ejlt/article/view/949/1066> [dostęp 31.08.2023].
- Tuck A., *How blockchain can tackle piracy in entertainment*, „Technology Magazine” 2022, <https://technologymagazine.com/articles/how-blockchain-can-tackle-piracy> [dostęp 28.09.2023].
- Utility Token*, „CoinMarketCap”, <https://coinmarketcap.com/alexandria/glossary/utility-token> [dostęp 2.09.2023].
- Wilser J., *15 NFT Use Cases That Could Go Mainstream*, „CoinDesk” 2021, <https://www.coindesk.com/business/2021/10/14/15-nft-use-cases-that-could-go-mainstream> [dostęp 20.08.2023].

Intellectual property law and NFT technology in the context of the music industry: challenges and perspectives

Abstract

The purpose of this paper is to provide a comprehensive analysis of intellectual property law issues involving the use of NFT technology in the music industry. NFT technology, which is developing at a rapid pace, opens up new opportunities for both creators and consumers of music.

At the same time, the new technology brings many challenges, particularly from a regulatory perspective. The study also addresses ethical and economic aspects, which allows us to better understand the problem and identify the appropriate path of regulatory development.

Keywords

intellectual property law, copyrights, NFT (Non-Fungible Token), music industry, blockchain technology, smart contract, digital transformation.