

Redakcja Kwartalnika Naukowego Prawo Mediów Elektronicznych**Redaktor naczelny:** prof. dr hab. *Jacek Gołaczyński*, UW**Sekretarz Redakcji:** dr *Aleksandra Klich*, USz**Członek Redakcji:** dr *Krzysztof Garstka*, Uniwersytet w Cambridge**Członkowie rady programowej:****Przewodniczący:** dr hab. *Wojciech Wiewiórowski* (UG, Europejski Inspektor Ochrony Danych)**Członkowie:**r.pr. *Włodzimierz Chróścik*adw. *Rafał Dębowski*dr hab. *Sviatlana Fursa*, prof. nauk prawnych Kijowskiego Narodowego Uniwersytetu im. Tarasa Szewczenkidr hab. prof. *Marlena Jankowska*, prof. nadzw. UŚadw. *Xawery Konarski*prof. Avv. *Michele Angelo Lupoi*, Uniwersytet Bolońskiprof. dr hab. *Jacek Mazurkiewicz*, UZprof. dr hab. *Radim Polcak*, Uniwersytet w Brniedr hab. *Grzegorz Sibiga*, INP PANdr hab. *Piotr Stec*, prof. nadzw. UOdr hab. *Dariusz Szostek*, prof. nadzw. UOprof. dr hab. *Grażyna Szpor*, UKSWprof. dr hab. *Andreas Wiebe*, Uniwersytet w Getyndze**Recenzenci:**dr hab. *Andrzej Adamski*, prof. nadzw. UMKprof. *Zsolt Balogh*, Uniwersytet Corvinus Budapesztprof. dr hab. *Sławomir Cieślak*, UŁdr hab. *Kinga Flaga-Gieruszyńska*, prof. nadzw. USzprof. dr hab. *Jacek Górecki*, UŚprof. em. dr *Wolfgang Kilian*, University of Hannoverprof. hab. dr *Vytautas Nekrošius*, Uniwersytet Wileńskidr hab. *Marek Świerczyński*, prof. nadzw. UKSWprof. *Richard Warner* Ph.D, Chicago – Kent College of Law**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: pme@beck.pl



C.H.BECK

Wydawca:Wydawnictwo C.H. Beck
ul. Bonifraterska 17
00-203 Warszawa

tel.: 22 33 77 600

fax: 22 33 77 602

www.czasopisma.beck.pl

Nakład: 250 egz.

Spis treści

Jak nie wpaść w Kanał (Sportowy), czyli o odpowiedzialności za bezpodstawne zgłoszenie internetowego naruszenia praw autorskich do dostawcy usług pośredniczących na tle sprawy Kanał Sportowy v. Polsat – cz. II <i>Martyna Mielniczuk-Skibicka, Rafał Skibicki</i>	4
Zlecenie płatnicze – jako rozliczenia pieniężne – zawierające polecenie wykonania transakcji płatniczej <i>dr Ewa Kowalewska</i>	14
Zdalne utworzenie spółki z o.o. przy użyciu środków komunikacji wideo na przykładzie implementacji dyrektywy 2019/1151 do prawa niemieckiego <i>Maja Mandrykowska</i>	21
Prawa własności intelektualnej wobec rozwoju technologii sztucznej inteligencji <i>Jakub Wyczik</i>	26

Contents

Responsibility for unjustified reporting of copyright infringement to the service provider based on the case Kanał Sportowy v. Polsat – part II <i>Martyna Mielniczuk-Skibicka, Rafał Skibicki</i>	4
Payment order – as cash settlements – containing an order to execute a payment transaction <i>dr Ewa Kowalewska</i>	14
Setting up a limited liability company online while using means of video communication based on implementation of Directive 2019/1151 to German law <i>Maja Mandrykowska</i>	21
Intellectual property rights v. the development of artificial intelligence <i>Jakub Wyczik</i>	26

Szanowni Państwo,

z przyjemnością przedstawiam drugi w 2021 r. numer kwartalnika naukowego Prawo Mediów Elektronicznych. Podobnie jak poprzednie numery, również ten został poświęcony zagadnieniom prawnym mającym związek z nowymi technologiami. Niezmiennie proponujemy współpracę i publikację artykułów, glos czy recenzji wszystkim tym autorom, którzy podejmują tematykę wpływu nowych technologii na prawo prywatne lub publiczne. Czasopismo ma charakter interdyscyplinarny i nie ogranicza się do jednej gałęzi prawa.

W bieżącym numerze znajdziecie Państwo opracowania poświęcone informatyzacji sektora bankowego. Zagadnienia te są niezwykle aktualne, a w bieżącym numerze szczegółowo omówione zostały kwestie dotyczące zlecenia płatniczego zawierającego polecenie wykonania transakcji płatniczej. W dalszym ciągu niezwykle interesujące zarówno z praktycznego, jak i teoretycznego punktu widzenia pozostają zagadnienia dotyczące sztucznej inteligencji. Z tego też względu proponujemy Państwu lekturę opracowania poświęconego prawu własności intelektualnej wobec rozwoju technologii sztucznej inteligencji. Celem kwartalnika jest również prezentowanie zagadnień prawnoporównawczych, dlatego w bieżącym numerze znajdziecie Państwo opracowanie poświęcone zasadom zdalnego utworzenia spółki z o.o. przy użyciu środków komunikacji wideo na przykładzie implementacji dyrektywy 2019/1151 do prawa niemieckiego. Zapraszamy także do zapoznania się z drugą częścią publikacji, w której autorzy podejmują próbę odpowiedzi na pytanie o to, jak nie wpaść w Kanał (Sportowy), analizując w tym zakresie odpowiedzialność za bezpodstawne zgłoszenie internetowego naruszenia praw autorskich do dostawcy usług pośredniczących na tle sprawy Kanał Sportowy v. Polsat.

Zapraszamy do publikacji na łamach Prawa Mediów Elektronicznych, a także do kontaktu z nami pod adresem: pme@beck.pl.

Zachęcam do lektury,
prof. dr hab. *Jacek Gołaczyński*

Jak nie wpaść w Kanał (Sportowy), czyli o odpowiedzialności za bezpodstawne zgłoszenie internetowego naruszenia praw autorskich do dostawcy usług pośredniczących na tle sprawy Kanał Sportowy v. Polsat – cz. II

Martyna Mielniczuk-Skibicka¹

Rafał Skibicki²

Artykuł został podzielony na dwie części. W pierwszej z nich³ autorzy omówili podstawy odpowiedzialności bezpodstawnie zgłaszającego internetowe naruszenie praw autorskich na gruncie prawa polskiego. Zagadnienie to rozważane było na podstawie przepisów ustawy z 12.7.2002 r. o świadczeniu usług drogą elektroniczną⁴, ogólnych zasad odpowiedzialności deliktowej z art. 415 i n. KC oraz ustawy z 16.4.1993 r. o zwalczaniu nieuczciwej konkurencji⁵. Opracowanie wieńczy rozważania o odpowiedzialności za naruszenie dóbr osobistych.

Część druga została natomiast poświęcona analizie odpowiedzialności bezpodstawnie zgłaszającego internetowe naruszenie praw autorskich na poziomie prawa unijnego. Pod uwagę zostały wzięte rozwiązania przyjęte w Finlandii, która jako jedyne państwo w UE bezpośrednio uregulowała odpowiedzialność za bezpodstawne zgłoszenie naruszenia praw podmiotom pośredniczącym. W dalszej kolejności rozważania prawnoporównawcze dotyczą prawa USA stanowiącego pierwowzór dla unijnych przepisów regulujących odpowiedzialność za naruszenie praw autorskich w Internecie i które także uregulowało bezpośrednio odpowiedzialność bezpodstawnie zgłaszającego. Ponadto omówiono implikacje dla analizowanego zagadnienia wynikające z nowych projektów prawodawczych – projektu ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych⁶ oraz unijnego rozporządzenia o usługach cyfrowych⁷. Na koniec autorzy formułują postulaty zarówno *de lege lata*, jak i *de lege ferenda*.

Regulacje w prawie Unii oraz jej państwach członkowskich, czyli czego możemy nauczyć się od Finów?

Prawodawca unijny nie zdecydował się na uregulowanie zasad, na jakich miałyby odpowiadać podmiot składający fałszywe zawiadomienie o naruszeniu praw autorskich w ramach dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z 8.6.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego⁸. Co więcej, rzezona dyrektywa, a tym samym obecnie cały system prawa unijnego, nie zawiera przepisów, które wprowadzałyby jakiegokolwiek skuteczne mechanizmy chroniące przed nieprawidłowym usuwaniem treści⁹. Sama zaś kwestia uregulowania procedury usuwania i blokowania dostępu do *contentu* także została pozostawiona państwom członkowskim do regulacji¹⁰, z czego skorzystało jedynie sześć państw członkowskich¹¹. Zważając zatem na powyższe oraz na motyw 10 ECD, zgodnie z którym środki nią przewidziane „ograniczają się ściśle do minimum niezbędnego do osiągnięcia celu, jakim jest sprawne funkcjonowanie rynku wewnętrznego”, należy uznać, że możliwość uregulowania odpowiedzialności za składanie fałszywych zawiadomień pozostała w gestii państw członkowskich.

¹ Uniwersytet Wrocławski, Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej – doktorantka. Kancelaria Prawna VenaGroup Gryc-Zerych i Kruk – prawnik. ORCID: 0000-0002-4998-1028.

² Uniwersytet Wrocławski, Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej – doktorant. Szostek Bar i Partnerzy Kancelaria Prawna – prawnik. ORCID: 0000-0003-1194-4173.

³ M. Mielniczuk-Skibicka, R. Skibicki, Jak nie wpaść w Kanał (Sportowy), czyli o odpowiedzialności za bezpodstawne zgłoszenie internetowego naruszenia praw autorskich do dostawcy usług pośredniczących na tle sprawy Kanał Sportowy v. Polsat – cz. I, PME 2021, Nr 1, s. 4–13.

⁴ T.j. Dz.U. z 2020 r. poz. 344 ze zm.

⁵ T.j. Dz.U. z 2020 r. poz. 1913 ze zm.

⁶ Analiza została dokonana na podstawie projektu z 15.1.2021 r. ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych opublikowanego 1.2.2021 r., <https://www.gov.pl/web/sprawiedliwosc/zachecamy-do-zapoznania-sie-z-projektem-ustawy-o-ochronie-wolnosci-uzytkownikow-serwisow-spolesnosciowych> (dostęp z 5.2.2021 r.).

⁷ Rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) i zmieniające dyrektywę 2000/31/WE, COM(2020) 825 final, 2020/0361(COD).

⁸ Dz.Urz. UE L Nr 178, s. 1; dalej jako: ECD.

⁹ A. de Streel, M. Husovec, Study for the committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, Luksemburg 2020, s. 41.

¹⁰ Art. 14 ust. 3 ECD. Zob. również M. Piech, Pośrednicy internetowi w prawie Unii Europejskiej. Rola i obowiązki wobec treści użytkowników, Lex/el. 2019, s. 207–209.

¹¹ Były to Francja, Finlandia, Węgry, Litwa, Szwecja oraz częściowo Wielka Brytania. Zob. A. Kuczerawy, From „Notice and Take Down” to „Notice and Stay Down”: Risks and Safeguards for Freedom of Expression, [w:] G. Froisio (red.), The Oxford Handbook of Intermediary Liability Online, Oxford 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3305153 (dostęp z 31.1.2021 r.).

Co ciekawe, tylko jedno z państw członkowskich zdecydowało się uregulować wspomniane zagadnienie i jest to Finlandia¹². Zgodnie z § 194 fińskiego kodeksu społeczeństwa informacyjnego¹³ każdy, kto poda nieprawdziwe informacje w zawiadomieniach o naruszeniu praw autorskich, o którym mowa w § 191 oraz 192 FinKSI¹⁴, jest obowiązany naprawić wyrządzoną szkodę. Obowiązek naprawienia szkody nie będzie ciążył na sprawcy lub będzie on mógł zostać skorygowany, jeżeli strona ta miała uzasadnione podstawy, aby przypuszczać, że informacje są prawdziwe lub jeśli fałszywe informacje mają niewielkie znaczenie, biorąc pod uwagę całą treść powiadomienia lub zarzutu¹⁵. Dokonując wykładni językowej wspomnianego przepisu, zwrócić należy uwagę, że nie wymaga on od poszkodowanego w celu dochodzenia naprawienia szkody udowodnienia winy lub złej wiary takiego zawiadamiającego. Musi on jedynie udowodnić nieprawdziwość informacji, co z perspektywy prawa autorskiego jest obiektywnie możliwe do udowodnienia. Z kolei zawiadamiający, który podał fałszywą informację w zawiadomieniu, jeśli chce uniknąć odpowiedzialności bądź ją zmniejszyć, musi powołać się na przesłanki egzoneracyjne, jakimi w tym wypadku są jego uzasadnione podstawy do uznawania prawdziwości informacji lub niewielkie znaczenie samej fałszywej informacji.

Na koniec niniejszej części warto wskazać, że istotnych zmian w tym zakresie do prawa unijnego nie wprowadza dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z 17.4.2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE¹⁶. Pośrednio polepsza ona sytuację użytkowników, nakazując w art. 17 ust. 9 państwom członkowskim wprowadzenie przepisów o „skutecznym i sprawnym mechanizmie składania skarg i dochodzenia roszczeń, dostępnym dla użytkowników” w przypadku sporów dotyczących zamieszczonych przez nich utworów. Przede wszystkim jednak dalsza część tego przepisu nakłada na podmioty uprawnione żądające zablokowania lub usunięcia treści naruszających ich prawa przedstawienia „należytego uzasadnienia”. Jest to zatem próba zbalansowania przez prawodawcę unijnego wzajemnej relacji użytkowników oraz podmiotów uprawnionych. Choć wspomniany przepis DSM sprzyja większej ochronie użytkownika, nie kreuje on podstawy roszczenia, jakie użytkownik może wysunąć przeciwko autorowi zawiadomienia opartego na fałszywych informacjach.

Prawo amerykańskie jako pierwowzór, ale nie wzór, regulacji

Rozwiązania przyjęte w ECD w zakresie odpowiedzialności, a w zasadzie wyłączenia odpowiedzialności pośredników internetowych były wzorowane na rozwiązaniach

stworzonych w prawie amerykańskim¹⁷, w szczególności zaś na przepisach *Digital Millenium Copyright Act*¹⁸. Pomimo dużych zbieżności pomiędzy tymi dwoma aktami prawnymi występują poważne różnice, wśród których najczęściej wymienia się rozszerzenie przez europejskiego prawodawcę w stosunku do DMCA wyłączenia odpowiedzialności pośredników o wszystkie treści bezprawne, a nie jedynie o treści naruszające prawa autorskie¹⁹, nieuregulowanie w unijnej dyrektywie narzędzi służących do lokalizacji informacji²⁰, wyróżnienia i ograniczenia odpowiedzialności organizacji oświatowych non profit²¹ czy pominięcie regulacji dotyczącej słynnej procedury *notice and takedown*²².

Różnicą najistotniejszą z punktu widzenia niniejszego artykułu jest kwestia uregulowania przez amerykańskiego prawodawcę odpowiedzialności za zgłoszenie nieprawdziwego (fałszywego) zawiadomienia o naruszeniu praw autorskich i tym samym za wprowadzenie w błąd. Zgodnie bowiem z 17 tytułem § 512(f) Kodeksu Stanów Zjednoczonych²³ każda osoba, która świadomie wprowadza w błąd istotny na podstawie tego paragrafu, że:

- 1) zgłoszony materiał lub działanie narusza prawo, lub
 - 2) materiał lub działanie zostały usunięte lub wyłączone przez pomyłkę lub błędną identyfikację
- ponosi odpowiedzialność za wszelkie szkody, w tym koszty sądowe i honoraria prawników, poniesione przez domniemanego naruszającego, przez jakiegokolwiek uprawnionego z tytułu praw autorskich lub upoważnionego licencjodawcę lub usługodawcę, poszkodowanych w wyniku takiego wpro-

¹² *Ibidem*.

¹³ Fiński Kodeks Społeczeństwa Informacyjnego (Information Society Code) 917/2014 z 7.11.2014 r., www.legislationline.org/download/id/6257/file/Finland%20Information%20Society%20Code%202014%20ENG.pdf (dostęp z 31.1.2021 r.), dalej jako: FinKSI.

¹⁴ Odpowiedzialność na podstawie § 194 FinKSI może ponieść zarówno zawiadamiający, jak i dostawca usług społeczeństwa informacyjnego – pośrednik, za podanie nieprawdy w zawiadomieniu do dostawcy treści o naruszeniu prawa lub podstawy jej naruszenia.

¹⁵ Z oficjalnej wersji anglojęzycznej: *A person who gives false information in the notification referred to in section 191 or in the plea referred to in section 192 shall be liable to compensate for the damage caused. However, there is no liability to compensate or it may be adjusted if the notifying party had reasonable grounds to assume that the information is correct or if the false information is only of minor significance, when taking into account the entire content of the notification or the plea.*

¹⁶ Dz.Urz. UE L 130, s. 92; dalej jako: DSM.

¹⁷ D. Gęsicka, Wyłączenie odpowiedzialności cywilnoprawnej dostawców usług sieciowych za treści użytkowników, *Lex/el.* 2014; V. McEvedy, *The DMCA and the eCommerce Directive*, *E.I.P.R.* 2002, 24(2), s. 65.

¹⁸ *Digital Millennium Copyright Act* z 28.10.1998 r. (Pub. L. No. 105–304, 112 Stat. 2860); dalej jako: DMCA.

¹⁹ G. Sartor, *Provider Liability: From the eCommerce Directive to the Future*, *Październik* 2017 r., s. 16, [https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA\(2017\)614179_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf) (dostęp z 19.2.2021 r.).

²⁰ Z ang. *Information location tools* – zob. 17 U.S. Code § 512(d).

²¹ Z ang. *Limitation on Liability of Nonprofit Educational Institution* – zob. 17 U.S. Code § 512(e).

²² Zob. 17 U.S. Code § 512(g).

²³ Dalej jako: U.S. Code lub U.S.C.

wadzenia błąd przez usługodawcę, który oparł się na takim wprowadzeniu w błąd, usuwając lub blokując dostęp do takich treści lub działań, które rzekomo naruszają prawo, lub na zastępowaniu usuniętych materiałów bądź ich odblokowywaniu²⁴.

Celem wprowadzenia tego przepisu, w ocenie Kongresu, było zachowanie równowagi pomiędzy podmiotami uprawnionymi z tytułu praw autorskich, dostawcami usług oraz użytkownikami Internetu poprzez powstrzymywanie świadomości fałszywych zawiadomień kierowanych pod adresem pośredników internetowych, by chronić ich przed stratami, jakie mogą być spowodowane poleganiem na fałszywych informacjach²⁵. Podkreślić jednak należy, że przepis ten nie obejmuje swoim zakresem kwestii niedokładnych, niepełnych, nieprecyzyjnych czy po prostu niestaranie przygotowanych zgłoszeń, a jedynie tych, poprzez które zostały przedstawione świadomie nieprawdziwe informacje o tym, że dana treść naruszała prawo.

Cenną wartość poznawczą w zakresie powyższego przepisu daje dotyczący go raport *United States Copyright Office* (USCO)²⁶. W toku tworzenia raportu jego autorzy próbowali uzyskać informacje na temat rozumienia i stosowania omawianego przepisu przez wszystkie zainteresowane nim strony – podmioty uprawnione z tytułu praw autorskich oraz dostawców usług on-line. Okazało się, że rozumienie rzeczonego przepisu przez obydwie te grupy jest całkowicie odmienne. Zdaniem podmiotów uprawnionych z tytułu praw autorskich przepis ten generalnie spełnia swoją rolę i skutecznie zniechęca do wysyłania fałszywych zawiadomień, a równocześnie nie obciąża nadmiernie ani posiadaczy praw autorskich, ani użytkowników²⁷. Zdaniem usługodawców prawda jest całkowicie odmienna. Przepis ten jest wręcz „bezzębny” i nie zapewnia odpowiedniego zabezpieczenia przed nadużyciem fałszywych zawiadomień²⁸. Jak wskazuje dalej USCO w swoim raporcie, niektórzy usługodawcy przedstawiali nawet dane pokazujące znaczną ilość fałszywych lub w inny sposób wadliwych zawiadomień²⁹. Natomiast *Authors Guild*, największa amerykańska organizacja zrzeszająca pisarzy, kontruje, wskazując, że fałszywe zawiadomienia zdarzają się niesłychanie rzadko³⁰.

Kluczowe znaczenie dla zastosowania 17 U.S.C. § 512(f) ma zwłaszcza ustalenie, czy, aby nadawca fałszywego zawiadomienia, o którym mowa w tym przepisie, poniósł odpowiedzialność za wyrządzoną jego złożeniem szkodę, wymagane jest, by subiektywnie wiedział on o fałszywości zawiadomienia, czy też kwestia ta powinna być oceniana obiektywnie, z punktu widzenia osoby rozsądnej i starannej. Ustaleniem tego zagadnienia zajęła się władza sądownicza w pierw w wyroku w sprawie *Diebold*³¹, następnie, co warto podkreślić, odmiennie w sprawie *Rossi*³², by w sprawie *Lenz* rozwinąć i utrzymać pogląd przedstawiony w tym drugim rozstrzygnięciu³³.

Powyższe zagadnienie subiektywności wiąże się bezpośrednio ze składaniem przy złożeniu zawiadomienia o naruszeniu praw autorskich, pod rygorem uznania za krzywoprzysięstwo (z ang. *under penalty of perjury*), pisemnym oświadczeniem. Zgodnie z jego treścią strona, która składa zawiadomienie, oświadcza, że działając w dobrej wierze, ma przekonanie, że na wykorzystanie utworu w treści zamieszczonej przez użytkownika zgody nie wyraził ani właściciel praw autorskich, ani jego przedstawiciel, ani też wykorzystanie tego utworu nie jest uprawnione na gruncie przepisów prawa³⁴. Jak wskazuje USCO, sens dodania tego oświadczenia przez Kongres pozostaje tajemnicą, tak samo jak jego powiązania z 17 U.S.C. § 512(f) – nie zachowały się bowiem żadne materiały dotyczące tych zagadnień z procesu legislacyjnego³⁵.

W chronologicznie pierwszej ze wspomnianych spraw tłem procesu była kwestia fałszywego zawiadomienia złożo-

²⁴ Z oryg. *Section 512(f) Misrepresentations*. – Any person who knowingly materially misrepresents under this section:

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification,

shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

²⁵ House Report. 105–551 – WIPO Copyright Treaties Implementation And On-Line Copyright Infringement Liability Limitation, Część 1, 22.5.1998 r., s. 27.

²⁶ United States Copyright Office, *Section 512 of title 17*, A report of the register of copyrights, maj 2020 r.

²⁷ *Ibidem*, s. 146.

²⁸ *Ibidem*.

²⁹ *Ibidem*, s. 147. Bezpośrednio warto jednak zapoznać się z przypisami na stronie tej publikacji, ponieważ zawierają one bezpośrednie wypowiedzi przedstawicieli ankietowanych stron, mogących zapewnić ciekawe i unikalne informacje, potwierdzające powyższe twierdzenia. Przykładowo przedstawiciele Amazona wskazali, że Amazon Kindle Worlds, strona zajmująca się publikowaniem utworów fan fiction, a więc gatunku opartego na inspiracji cudzymi utworami, większą część otrzymywanych zawiadomień dostaje od rywalizujących ze sobą pisarzy próbujących wbrew prawu usunąć z portalu swoich konkurentów.

³⁰ *Ibidem*, s. 148.

³¹ Zob. wyrok *US District Court for Northern District of California* z 30.9.2004 r. w sprawie *Online Policy Group (OPG), Nelson Chu Pavlosky, oraz Luke Thomas Smith v. Diebold, Incorporated* oraz *Diebold Election Systems, Incorporated*, 337 F. Supp. 2d 1195, <https://www.leagle.com/decision/20041532337fsupp2d119511436> (dostęp z 27.1.2021 r.).

³² Zob. wyrok *US Court of Appeals for the Ninth Circuit* z 1.12.2004 r. w sprawie *Michael J. Rossi, dba Internet Movies.Com, Plaintiff-Appellant, v. Motion Picture Association of America Inc.* i inni, No. 03-16034, <https://caselaw.findlaw.com/us-9th-circuit/1308565.html> (dostęp z 27.1.2021 r.).

³³ Zob. wyrok *Court of Appeals for the Ninth Circuit* z 14.9.2015 r. w sprawie *Lenz v. Universal Music Corp.*, 801 F.3d 1126 (2015), https://scholar.google.com/scholar_case?case=12567649168680108221&hl=en&as_sdt=6&as_vis=1&oi=scholar (dostęp z 5.7.2021 r.).

³⁴ 512(c)(3)(A)(v). W oryginale: „A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.”

³⁵ United States Copyright Office, *Section 512 of title 17*, s. 151.

nego przez *Diebold, Inc* oraz *Diebold Election Systems, Inc.*³⁶ będących producentami elektrycznych maszyn do głosowania. Dość wadliwych maszyn, trzeba dodać. Ta niezbyt przychylna informacja dostała się do wiadomości publicznej dzięki wysiłkowi dwóch studentów, którzy opublikowali na swoich stronach internetowych zarchiwizowane wiadomości e-mail pracowników firmy *Diebold* dotyczące wadliwości wspomnianych maszyn do głosowania. Następnie temat rozpowszechniła internetowa gazeta *IndyMedia*. W celu zablokowania tych negatywnych informacji przedstawiciele firmy *Diebold* zdecydowali się złożyć zawiadomienie do dostawców usług internetowych (ISP) całej wspomnianej trójki z tytułu naruszenia ich praw autorskich. W konsekwencji firma ta została pozwana przez domniemanych naruszcycieli właśnie za świadome wprowadzenie w błąd co do naruszenia praw autorskich do ujawnionej korespondencji. Sąd przyznał rację powodom, wskazując, że nikt racjonalny nie mógłby twierdzić, że e-maile zawierające głównie treści techniczne dotyczące maszyn do głosowania mogłyby podlegać ochronie prawnoautorskiej, a nawet jeśli, to takie działanie byłoby chronione przez *fair use*³⁷. Co najistotniejsze, sąd w swoim orzeczeniu odniósł się także do wymaganej do pociągnięcia zawiadamiającego do odpowiedzialności na gruncie 17 U.S.C. § 512(f) jego świadomości o wprowadzaniu w błąd w zawiadomieniu o naruszeniu. Odnosząc się do tej kwestii sąd uznał, że: „świadomie» oznacza sytuację, w której strona rzeczywiście wiedziała, powinna była wiedzieć, gdyby działała z należytą starannością, lub nie miałyby istotnych wątpliwości, działając w dobrej wierze, że przedstawia fałszywe informacje”³⁸. W ten sposób sąd zastosował do zawiadamiającego w ramach procedury *notice and takedown* miernik osoby rozsądnej³⁹. Było to zatem rozwiązanie korzystne zwłaszcza dla użytkowników Internetu, zarówno z punktu widzenia wolności słowa, jak i wolności artystycznej.

Jednak niedługo później, bo zaledwie po trzech miesiącach, amerykański Sąd Apelacyjny dla Dziewiątego Okręgu wydał przełomowe orzeczenie w sprawie *Rossi*, gdzie odrzucił wypracowany w sprawie *Diebold* w odniesieniu do zgłaszającego naruszenie miernik osoby rozsądnej. W sprawie *Rossi* sąd bowiem wskazał, że do jego zwolnienia z odpowiedzialności wystarczy, by zawiadamiający posiadał jedynie subiektywne przekonanie o tym, że dana treść narusza prawa autorskie⁴⁰. Sąd oparł swoje rozumowanie w szczególności na argumentach o racjonalności amerykańskiego prawodawcy i wymogu składania oświadczenia o zachowaniu dobrej wiary przez zawiadamiającego. Byłby to martwy przepis przy stosowaniu miernika obiektywnego⁴¹. Powyższa zmiana interpretacji wprowadziła zatem istotnie karkołomne zadanie dla powodów w sprawach odbywających się na kanwie 17 U.S.C. § 512(f), ponieważ wymagała od nich udowodnienia, że pozwany subiektywnie wiedział o fałszywych podstawach swojego zawiadomienia, co było w zasadzie nieweryfikowalne⁴².

Najciekawiej prezentuje się jednak ostatnia ze wspomnianych spraw, która stanowiła blisko dziesięcioletni bój między *S. Lenz* a *Universal Music Corp.*, zasłużonym amerykańskim krzyżowcem w walce z piractwem internetowym⁴³. Walka ta dotyczyła opublikowanego przez nią na YouTube 29-sekundowego filmiku, o bardzo niskiej jakości wideo i dźwięku, przedstawiającego jej dziecko tańczące do ledwie słyszalnej piosenki Prince’a „*Let’s Go Crazy*”⁴⁴. Po wrzuceniu tego filmiku *Universal* zgłosił zawiadomienie i zażądał jego usunięcia, co też YouTube uczynił niezwłocznie⁴⁵. *S. Lenz* odwołała się od tej decyzji serwisu pośredniczącego, co przyniosło skutek w postaci przywrócenia dostępu do filmiku sześć tygodni później, oraz pozwała *Universal Music* na podstawie 17 U.S.C. § 512(f)⁴⁶. Choć racje *S. Lenz* były oczywiste, wytwórnia *Universal Music* wcale nie zamierzała wycofać się z oskarżeń o naruszenie posiadanych przez nią praw autorskich do utworu *Prince’a*⁴⁷. Słusznie i trafnie całą sytuację komentuje *B. Wilson*, pisząc, że jeżeli „dział prawny dużej firmy muzycznej szczerze uważa, że domowy film przedstawiający tańczącego malucha naruszył jej prawa autorskie, to dozwolony użytek ma znikome znaczenie”⁴⁸.

Długoletni proces nie doprowadził do obalenia koncepcji subiektywnej wprowadzonej w sprawie *Rossi*. *Universal Music* nie została pociągnięta do odpowiedzialności na podstawie

³⁶ Dalej jako: *Diebold*.

³⁷ Zob. ww. wyrok US District Court for Northern District of California z 30.9.2004 r. w sprawie *Diebold*.

³⁸ W orygl. „*Knowingly*» means that a party actually knew, should have known if it acted with reasonable care or diligence, or would have had no substantial doubt had it been acting in good faith, that it was making misrepresentations”. Tworząc wspomnianą definicję sąd oparł się na definicjach „*knowledge*” pochodzących z *Black’s Law Dictionary*.

³⁹ *B. Wilson*, Notice, Takedown, and the Good-Faith Standard: How to Protect Internet Users From Bad-Faith Removal of Web Content, *St. Louis University Public Law Review*, Vol. 29, No. 613, 2010, s. 620, SSRN, <https://ssrn.com/abstract=3323485> (dostęp z 19.2.2021 r.).

⁴⁰ Zob. wyrok Sądu Apelacyjnego USA dla dziewiątego Okręgu z 1.12.2004 r. w sprawie *Michael J. Rossi*. Podobnie również wyrok Sądu Okręgowego USA dla Dystryktu Coloradu z 17.8.2005 r. w sprawie *Dudnikov v. MGA Entertainment, Inc.*, 410 F. Supp. 2d 1010, <https://casetext.com/case/dudnikov-v-mga-entertainment> (dostęp z 19.2.2021 r.).

⁴¹ *Ibidem*. Por. również *B. Wilson*, Notice, Takedown..., s. 621–622.

⁴² *B. Wilson*, Notice, Takedown..., s. 631 oraz 637.

⁴³ *L. Lessig*, *Remix. Making Art and Commerce Thrive in the Hybrid Economy*, Londyn 2008, s. 2.

⁴⁴ Zob. <https://www.youtube.com/watch?v=N1KfjHFWlhQ> (dostęp z 19.2.2021 r.). Po jego obejrzeniu sprawa wydaje się oparta o absurd. Zyskuje ona jednak dodatkowej głębi, kiedy zapozna się z wypowiedziami samego Prince’a w zakresie wykorzystania jego utworów muzycznych w Internecie, szczególnie w ramach user generated content. Wspomniany artysta pragnął bowiem „odzyskać swoją sztukę w Internecie”, domagając się blokowania lub usuwania wszystkich treści wykorzystujących jego utwory, na które sam nie zezwolił. Zob. https://www.reuters.com/article/internetNew/idUSL1364328420070914?feedtype=RSS&feedName_InternetNews&rpc=22&sp=true (dostęp z 31.1.2021 r.).

⁴⁵ Zob. wyrok Sądu Apelacyjnego USA dla dziewiątego Okręgu z 14.9.2015 r. w sprawie *Lenz v. Universal Music Corp.*

⁴⁶ *Ibidem*.

⁴⁷ *L. Lessig*, *Remix. Making Art...*, s. 3.

⁴⁸ *B. Wilson*, Notice, Takedown..., s. 631. Por. Dokładny opis takiego spotkania wraz krytyką takiego podejścia: *L. Lessig*, *Remix. Making Art...*, s. 2.

17 U.S.C. § 512(f). Sąd ograniczył jednak możliwość nadużywania składania zawiadomień, orzekając, że właściciele praw autorskich muszą przed złożeniem zawiadomienia dokonać analizy, czy materiał stanowi dozwolony użytek, a tym samym, czy dana treść nie będzie jednak naruszać ich praw autorskich⁴⁹. Było to zatem jedynie częściowe zwycięstwo na rzecz użytkowników Internetu, przez co istnieje obawa, że wspomniane uprzednie badania dozwolonego użytku wymagane od zgłaszających będą jedynie badaniami fasadowymi, wykonanymi przy jak najmniejszym wysiłku. Istnieje więc ryzyko, że będą one prawie bezcelowe⁵⁰ w świetle obowiązującej zasady u większości właścicieli praw autorskich w zakresie zawiadomień o naruszeniu praw autorskich „najpierw strzelaj, potem myśl”⁵¹.

Wyrok *Lenz* postawił w zasadzie więcej pytań niż odpowiedzi. Przykładowo, opierając się na jego literalnej treści, można zakwestionować korzystanie przez uprawnionych z praw autorskich z automatycznie generowanych zawiadomień o naruszeniu praw, na co wskazał jeden z pośredników internetowych biorących udział w ankiecie powiązanej z 17 U.S.C. § 512 przeprowadzonej przy okazji Raportu przez USCO. Pogląd ten uzasadnił on, wskazując, że algorytmy generujące automatyczne powiadomienia nie są w stanie w ogóle ocenić w większości przypadków, czy określone użycie narusza prawa autorskie, czy też nie, w szczególności w zakresie dozwolonego użytku⁵². Tym samym zgłoszenie naruszenia wyłącznie przez algorytmy uniemożliwia dokonanie obligatoryjnego badania dozwolonego użytku, o którym mowa w orzeczeniu w sprawie *Lenz*. Powyższy pogląd nie został jednak jeszcze zweryfikowany przez sądownictwo, a automatyczne systemy generujące zawiadomienia używane są po dziś dzień⁵³.

Być może należy spodziewać się nowelizacji wspomnianego przepisu. Jak bowiem puentuje USCO w swoim raporcie, w przyszłości Kongres mógłby rozważyć zmianę 17 U.S.C. § 512(f) w ten sposób, że wprowadziłby odpowiedzialność za rażące zaniedbania (ang. *reckless disregard*) w zakresie dokładności czy też prawdziwości zawiadomienia⁵⁴. Jakkolwiek w tym przypadku wiązałoby się to najpewniej z koniecznością rozróżnienia odpowiedzialności zgłaszającego w sytuacji jego świadomości o braku naruszenia praw autorskich oraz w przypadku jedynie jego rażącego niedbalstwa w tym zakresie⁵⁵.

„Dobra, zmiana!” czy „Dobra zmiana”? Czyli co przed świętami prawodawcy, polski i unijny, przynieśli w workach z prezentami?

Omawiane przez nas zagadnienie odpowiedzialności za bezpodstawne zgłoszenia naruszenia praw własności inte-

lektualnej przez użytkowników kierowane do podmiotów pośredniczących należy także zweryfikować w świetle najnowszych propozycji legislacyjnych dotyczących zgłaszania i usuwania treści bezprawnych w Internecie. W szczególności mamy tutaj na myśli projekt ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych⁵⁶ oraz projekt unijnego rozporządzenia o usługach cyfrowych⁵⁷.

Analizę zaczniemy od projektu krajowego, mającego mieć zastosowanie do *social media*, z których korzysta w Polsce co najmniej milion użytkowników. Ustawa o ochronie wolności słowa w internetowych serwisach społecznościowych przygotowana przez Ministerstwo Sprawiedliwości ma na celu walkę z usuwaniem przez serwisy społecznościowe wpisów oraz blokowaniem kont polskich użytkowników, jeśli zamieszczone w nich treści nie łamią polskiego prawa⁵⁸. Należy jednak

⁴⁹ *Ibidem*. Por. krytykę tego wyroku jako przeważającego idealny balans pomiędzy prawami użytkowników i właścicielami praw autorskich na rzecz tych pierwszy w: M.M. Fortunato, Let's Not Go Crazy: Why *Lenz v. Universal Music Corp.* Undermines the Notice and Takedown Process of the Digital Millennium Copyright Act, <https://digitalcommons.law.uga.edu/jipl/vol17/iss1/10>, s. 166–172 (dostęp z 19.2.2021 r.).

⁵⁰ Copyright Law — Digital Millennium Copyright Act — Ninth Circuit Requires Analysis of Fair Use Before Issuing of Takedown Notices. — *Lenz v. Universal Music Corp.*, No. 13-16106, 2016 WL 1056082 (9th Cir. Mar. 17, 2016), *Rehg En Banc Denied*, Id., *Harvard Law Review*, 129(8), 2016, s. 2289, www.jstor.org/stable/44072370 (dostęp z 31.1.2021 r.). Por. również syntezę krytyki oraz propozycji zastosowania tego wyroku w ramach amerykańskiej doktryny prawa w: A. Velay, Using the first fair use factor to screen dmca takedowns, *Virginia Sports and Entertainment Law Journal* 17(1), s. 64–69.

⁵¹ *Ibidem*, s. 2293.

⁵² A. Bridy, D. Keller, Additional Comments Submitted in Response to U.S. Copyright Office's, 8.11.2016, s. 2 oraz Verizon Communications, Comments Submitted in Response to U.S. Copyright Office's, 31.12.2015 r., Notice of Inquiry, s. 16 cyt. za: United States Copyright Office, Section 512 of title 17, s. 151.

⁵³ D. Seng, Copyrighting Copywrongs: An Empirical Analysis of Errors with Automated DMCA Takedown Notices (wrzesień 2019 r.), <https://ssrn.com/abstract=2563202> (dostęp z 31.1.2021 r.), s. 22, 61–63.

⁵⁴ United States Copyright Office, Section 512 of title 17..., s. 150. Podobnie również w zakresie wprowadzenia Copyright Law – Digital Millennium Copyright Act — Ninth Circuit Requires Analysis of Fair Use Before Issuing of Takedown Notices..., s. 2290, 2295–2296. Warto także odnieść się tutaj do propozycji M.J. Randazza, który proponuje wprowadzenie w takich sprawach przepisów przewidujących odszkodowanie ustawowe na wzór odszkodowania ustawowego za naruszenie praw autorskich z 17 tytułu Kodeksu USA § 504(c), co miałyby zrównoważyć prawa autorskie z wolnością wypowiedzi. Zob. M.J. Randazza, *Lenz v. Universal: A Call to Reform Section 512(f) of the DMCA and to Strengthen Fair Use*, *Vanderbilt Journal of Entertainment & Technology Law*, Vol. 18, No. 3, 2016, <https://ssrn.com/abstract=2773137> (dostęp z 31.1.2021 r.), s. 132–133, 135–138.

⁵⁵ United States Copyright Office, Section 512 of title 17, s. 150.

⁵⁶ Analiza została dokonana na podstawie projektu z 15.1.2021 r. ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych opublikowany 1.2.2021 r., <https://www.gov.pl/web/sprawiedliwosc/zachecamy-do-zapoznania-sie-z-projektem-ustawy-o-ochronie-wolnosci-uzytkownikow-serwisow-spolesnoscowych> (dostęp z 5.2.2021 r.).

⁵⁷ Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) i zmieniającej dyrektywę 2000/31/WE, COM(2020) 825 final, 2020/0361(COD), dalej jako: DSA lub rozporządzenie o usługach cyfrowych.

⁵⁸ Zob. <https://www.gov.pl/web/sprawiedliwosc/zachecamy-do-zapoznania-sie-z-projektem-ustawy-o-ochronie-wolnosci-uzytkownikow-serwisow-spolesnoscowych> (dostęp z 24.2.2021 r.).

zauważyć, że w rzeczonyj ustawie całkowicie pominięto treści naruszające prawa własności intelektualnej w definicji „treści bezprawnych”, którą ma zawierać ustawa⁵⁹. Co więcej, abstrahując od zakresu tego pojęcia, projektodawca zignorował także kwestię relacji pomiędzy zgłaszającym publikację bezprawnych treści a użytkownikiem, którego takie zgłoszenie dotyczy. Nawet w przypadku postępowania przed Radą Wolności Słowa, mającej być swoistym organem odwoławczym od decyzji o blokadzie dostępu do treści wydanej przez dany portal społecznościowy, zgłaszający nie mógłby być stroną takiego postępowania. Zaplanowano bowiem, że stroną będzie jedynie użytkownik, którego treści lub profil zostały zablokowane, oraz portal społecznościowy (usługodawca)⁶⁰. Jest to nawet szerszy problem całego projektu – w zasadzie nie dostrzega on w ogóle osoby zgłaszającej daną treść jako bezprawną, skupiając się jedynie na serwisach społecznościowych przyjmujących zgłoszenia naruszenia prawa oraz blokujących wskutek tych zgłoszeń dostęp do treści lub całych profili.

W przeciwieństwie do projektu polskiej ustawy, DSA w ramach pojęcia „nielegalnych treści” zawiera także naruszenia praw autorskich⁶¹. Prawodawca unijny zdecydował się uregulować także mechanizm usuwania tychże nielegalnych treści w sposób jednolity, a nie pozostawiać tego państwom członkowskim do decyzji, jak było to do tej pory w art. 14 ust. 3 ECD. Nie jest to jednak mechanizm *notice and takedown*, a bardziej rozwinięty i przystający do współczesnej techniki system *notice and action*⁶². Wzorem rozwiązania zastosowanego w prawie amerykańskim, w art. 14 ust. 2 DSA ustalono, że wymaganymi elementami zawiadomienia o nielegalnych treściach będą m.in.:

- a) wyjaśnienie powodów, dla których dana osoba lub dany podmiot uważają odnośne informacje za nielegalne treści⁶³, oraz
- b) oświadczenie potwierdzające powzięte w dobrej wierze przekonanie osoby lub podmiotu przekazującego zgłoszenie, że informacje i zarzuty w nim zawarte są prawidłowe i kompletne⁶⁴.

Takie kompletne zawiadomienie będzie uznawane za wiarygodną wiadomość o nielegalnych treściach, powodującą konieczność podjęcia przez *hostingprovidera* bezzwłocznie odpowiednich działań w celu usunięcia lub uniemożliwienia dostępu do nielegalnych treści w celu wyłączenia jego odpowiedzialności za publikowane treści⁶⁵. Prawodawca unijny także postanowił zająć się kwestią nadużyć ze strony podmiotów zawiadamiających, których zawiadomienia są często ewidentnie bezzasadne, pozwalając platformom internetowym na zawieszenie na rozsądny okres, po wydaniu uprzedniego ostrzeżenia, przetwarzania zgłoszeń i skarg składanych przez takie podmioty⁶⁶. Zgodnie z motywem 47 preambuły DSA, zgłoszenie trzeba będzie uznać za ewidentnie bezzasadne, jeśli dla osoby nieposiadającej wiedzy fachowej jest oczy-

wiste, bez przeprowadzenia jakiejkolwiek merytorycznej analizy, że są one bezzasadne. Co więcej, kluczowe dla zagadnienia rozważanego w niniejszym artykule jest zwłaszcza ostatnie zdanie wspomnianego motywu, zgodnie z którym przepisy projektowanego rozporządzenia mają pozostać bez uszczerbku dla jakiejkolwiek możliwości pociągnięcia do odpowiedzialności osób dopuszczających się niewłaściwego korzystania, w tym za szkody, którą przewidziano w prawie Unii lub prawie krajowym⁶⁷. To zatem przede wszystkim na prawodawcach krajowych będzie ciążyła konieczność uregulowania zasad takiej odpowiedzialności, na obecnym zaś etapie prac prawodawca unijny nie zamierza się pochylić nad tą kwestią.

Omawiając kwestię odpowiedzialności zgłaszającego za bezprawne zawiadomienie, nie można też pominąć instytucji zaufanych podmiotów sygnalizujących (z ang. *trusted flaggers*), która ma zostać uregulowana w ramach art. 19 DSA. Wiąże się ona z wprowadzeniem priorytetowej ścieżki usuwania treści bezprawnych, w tym także treści naruszających prawa własności intelektualnej wskutek zgłoszeń takich podmiotów ze względu na wysoki poziom zaufania do nich oraz ich obiektywizm. Zgodnie z motywem 46 DSM takimi zaufanymi podmiotami będą mogły zostać także podmioty uprawnione z tytułu tych praw. W wypadku powtarzającej niedokładności lub wadliwości w zgłoszeniach zaufanego podmiotu zgłaszającego taki podmiot będzie mógł utracić wspomniany status.

Równolegle jednak nie będzie wykluczone poniesienie odpowiedzialności odszkodowawczej za wadliwe działanie *trusted flagger* zgodnie z odpowiednimi krajowymi zasadami. Bezpodstawne zgłoszenie danej treści przez zaufany podmiot sygnalizujący byłoby wręcz swoistym sprzeniewierzeniem się

⁵⁹ Art. 3 pkt 8 projektu z 15.1.2021 r. ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych.

⁶⁰ Art. 23 projektu z 15.1.2021 r. ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych.

⁶¹ Art. 2 lit. g DSA, zgodnie z którym nielegalne treści oznaczają „wszelkie informacje, które same w sobie lub w odniesieniu do konkretnej aktywności, w tym sprzedaży produktu lub świadczenia usług, są niezgodne z prawem Unii lub prawem państwa członkowskiego, niezależnie od dokładnego przedmiaru lub natury takiego prawa” (tłum. własne).

⁶² Różnica pomiędzy tymi mechanizmami polega na umożliwieniu zastosowania w procedurze *notice and action* całego wachlarza różnych działań, jakie pośrednik może wykonać po otrzymaniu zawiadomienia, a nie tylko na zablokowaniu lub usunięciu danej treści, jak ma to miejsce w przypadku *notice and takedown*. Zob. A. Kuczerawy, *Intermediary Liability & Freedom of Expression: Recent Developments in the EU Notice & Action initiative*, *Computer Law and Security Review*, Vol 31. Issue 1 2015, CiTiP Working Paper 21/2015, <https://ssrn.com/abstract=2560257>, s. 46 (dostęp z 24.2.2021 r.).

⁶³ Art. 14 ust. 2 lit. a DSA.

⁶⁴ Art. 14 ust. 2 lit. d DSA.

⁶⁵ Zob. art. 14 ust. 3 oraz art. 5 DSA. Artykuł 5 stanowi w zasadzie rozwinięcie dotychczasowego art. 14 ECD.

⁶⁶ Art. 20 ust. 2 i 3 DSA.

⁶⁷ W org. „Those rules are without prejudice to any possibility to hold the persons engaged in misuse liable, including for damages, provided for in Union or national law”.

roli, jaką odgrywałby on w nowoczesnej gospodarce cyfrowej. Tym samym w wypadku odpowiedzialności deliktowej *de lege lata* obowiązek dochowania należytej staranności przez taki podmiot byłby na tyle wyśrubowany, by wręcz zbliżyć zasady jego odpowiedzialności do odpowiedzialności na zasadzie ryzyka. Być może warto byłoby uregulować wspomnianą kwestię jednolicie w całej UE w ramach DSA. Zagadnienie to jest o tyle istotne, że kiedy weźmie się pod uwagę badania empiryczne omówione na początku pierwszej części niniejszego artykułu, z których jasno wynika brak jakiegokolwiek refleksji po stronie pośredników w wypadku standardowych zgłoszeń, nie ma żadnych wątpliwości, że w przypadku zgłoszeń wysyłanych przez *trusted flaggers* tej refleksji u pośredników będzie jeszcze mniej.

Na koniec warto także wspomnieć, że kwestia odpowiedzialności za bezpodstawne zgłoszenia naruszeń praw może zostać także uregulowana częściowo w niedalekiej przyszłości w projektach prawodawczych dotyczących sztucznej inteligencji. Coraz więcej bowiem zawiadomień, czego niestety nie dostrzega polski prawodawca, składane jest przez zautomatyzowane systemy, które, jeżeli jeszcze nie są, to z pewnością w dużej mierze będą już w niedalekiej przyszłości oparte na szeroko pojętej sztucznej inteligencji⁶⁸. Powyższy problem dostrzega Parlament Europejski, podkreślając, że „AI lub powiązane z nią technologie (...) ustalania odpowiedzialności za naruszenia praw własności intelektualnej nie mogą zastąpić przeglądów dokonywanych przez człowieka w poszczególnych przypadkach w celu zapewnienia jakości i uczciwości decyzji”⁶⁹. Tym samym odpowiedzialność w tym zakresie może zostać określona w ewentualnym rozporządzeniu w sprawie odpowiedzialności za działanie systemów sztucznej inteligencji, którego przyjęcie proponuje Parlament Europejski w swojej rezolucji z 20.10.2020 r.⁷⁰. Byłaby to zatem odpowiedzialność przyjęta w sposób ujednolicony na terenie całej UE bądź na zasadzie ryzyka z pułapem kwotowym odpowiedzialności⁷¹, bądź na zasadzie winy, ale już bez pułapu kwotowego⁷². Proponowana kwestia jest jednak obecnie na bardzo wczesnym etapie rozwoju, dlatego dalsza analiza będzie możliwa dopiero po rozpoczęciu procesu legislacyjnego.

Podsumowanie, czyli jak wyważyć prawa w Internecie, by zachować doskonały balans?

Uzyskanie równowagi pomiędzy prawami a interesami użytkowników Internetu, podmiotów uprawnionych oraz serwisów pośredniczących w zasadzie od zawsze było jednym z podstawowych celów reformowania prawa autorskiego⁷³. Istotnym elementem wspomnianej równowagi jest także odpowiednie uregulowanie zasad odpowiedzialności za wa-

dlive lub fałszywe zawiadomienie o naruszeniu praw autorskich. Patrząc przez pryzmat polskiego prawa regulującego odpowiedzialność w Internecie, włączając w to także odpowiedzialność za naruszenie praw autorskich, znajdujemy się w najlepszym możliwym momencie legislacyjnym na wprowadzenie ewentualnych zmian lub uzupełnień w tym zakresie przynajmniej od 20 lat, kiedy wdrażano ECD, uchwalając ustawę o świadczeniu usług drogą elektroniczną. Równocześnie bowiem na szczeblu krajowym, jak też unijnym toczą się prace nad regulacjami od siebie odmiennymi, choć mającymi w gruncie rzeczy wspólny cel – przywrócenia równowagi pomiędzy użytkownikami, serwisami pośredniczącymi, a podmiotami uprawnionymi z tytułu praw autorskich.

W pierwszej kolejności należałoby zweryfikować, czy prawo polskie reguluje wspomnianą relację w sposób odpowiedni. Pomimo że nie wyraża się ono w tej kwestii bezpośrednio, nie pozostawia wszak poszkodowanego przez takie bezpodstawne zgłoszenie bez jakiegokolwiek możliwości dochodzenia odszkodowania. Co więcej, jak przedstawiono w pierwszej części niniejszego artykułu, przewiduje aż trzy odmienne regulacje, na które taki poszkodowany może się powołać, dochodząc odpowiedzialności od podmiotu bezpodstawnie zgłaszającego naruszenie. Każda z tych podstaw prawnych ma jednak swoje wady, co więcej – żadna z nich nie jest oczywista. Pierwsza z nich, czyli odpowiedzialność deliktowa na podstawie art. 415 KC może powodować trudności w zakresie udowodnienia winy podmiotu zgłaszającego. Rozwiązania wprowadzone w ustawie o zwalczaniu nieuczciwej konkurencji dotyczą natomiast tylko stosunków obustronnie profesjonalnych. Natomiast w wypadku ochrony dóbr osobistych wydaje się, że nie zawsze w wyniku takiego fałszywego zgłoszenia dojdzie do zagrożenia lub naruszenia konkretnego dobra osobistego. Pomimo że ostatnia ze wspo-

⁶⁸ J. Penney, Privacy and Legal Automation: The DMCA as a Case Study, Stanford Technology Law Review, Vol. 22, No. 1, 412, <https://ssrn.com/abstract=3504247> (dostęp z 31.1.2021 r.), s. 414–442.

⁶⁹ Rezolucja Parlamentu Europejskiego z 20.10.2020 r. w sprawie praw własności intelektualnej w dziedzinie rozwoju technologii sztucznej inteligencji (2020/2015(INI)), pkt 16, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_PL.pdf (dostęp z 5.2.2021 r.).

⁷⁰ Rezolucja Parlamentu Europejskiego z 20.10.2020 r. z zaleceniami dla Komisji w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję (2020/2014(INL), dalej jako: Rezolucja. Zob. w szczególności załącznik do Rezolucji zawierającego szczegółowe zalecenia dla przygotowujących projekt rozporządzenia Parlamentu Europejskiego i Rady ws. odpowiedzialności za działanie systemów sztucznej inteligencji.

⁷¹ Zob. art. 4 oraz art. 5 projektu rozporządzenia zawartego w szczegółowych zaleceniach dla przygotowujących projekt rozporządzenia Parlamentu Europejskiego i Rady ws. odpowiedzialności za działanie systemów sztucznej inteligencji załączonych do Rezolucji.

⁷² Zob. art. 8 i n. projektu rozporządzenia zawartego w szczegółowych zaleceniach dla przygotowujących projekt rozporządzenia Parlamentu Europejskiego i Rady ws. odpowiedzialności za działanie systemów sztucznej inteligencji załączonych do Rezolucji.

⁷³ Por. motyw 31 dyrektywy 2001/29/WE Parlamentu Europejskiego i Rady z 22.5.2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym Dz.Urz. UE L Nr 167, s. 10–19, motyw 41 ECD oraz motyw 6 DSM.

mnianych podstaw wydaje się *de lege lata* podstawą najbardziej sprzyjającą dochodzeniu odpowiedzialności od sprawcy przez użytkownika, zwłaszcza pod kątem ciężaru dowodu, naszym zdaniem może być ona w pewien sposób podstawą powoływaną na wyrost. Ma ona bowiem do spełnienia inne cele prawne niż ograniczenia składania fałszywych czy wadliwych zawiadomień z tytułu naruszenia praw autorskich. Wydaje się zatem, że wprowadzenie do polskiego porządku prawnego bezpośredniej regulacji odpowiedzialności fałszywie zgłaszającego naruszenie byłoby uzasadnione.

Niewątpliwie najlepiej zbadanym na świecie przepisem regulującym odpowiedzialność za składanie fałszywych zawiadomień jest 17 U.S.C. § 512(f). Obraz, jaki płynie z jego analizy na poziomie akademickim, jak również tych przeprowadzanych praktyków prawa, przede wszystkim urzędników USCO, nie jest pozytywny. Wspomniany system, wbrew zdaniu posiadaczy praw autorskich, nie chroni skutecznie użytkowników Internetu przed bezzasadnymi zgłoszeniami naruszenia praw autorskich ze względu na rozłożoną w procesie kwestię ciężaru dowodu co do świadomości teże bezzasadności.

W regulacji amerykańskiej problemem jest przede wszystkim kwestia rozumianej subiektywności wprowadzonej w sprawie *Rossi*, co zdecydowanie utrudnia, nawet w sprawach oczywistych takich jak sprawa *Lenz*, poniesienie odpowiedzialności przez właściciela praw autorskich nadużywającego system *notice and take down* fałszywymi zawiadomieniami. Sytuacja, w której to użytkownik musi udowodnić okoliczność tak bardzo nie do udowodnienia jak subiektywne przekonania właściciela praw autorskich, najczęściej będących dużą korporacją, jest niczym innym jak sprawą z góry skazaną na procesową porażkę. Kluczowa jest bowiem kwestia, kto ma wiedzę o dobrej lub złej wierze zgłaszającego. Nie ma raczej wątpliwości, że użytkownik jej nie ma, i co więcej – mieć nie może. Natomiast właściciel praw autorskich z reguły ją ma. Rozwiązanie stosowane w systemie amerykańskim jest bowiem nietypowym przykładem wyjątku od zasady *ignorantia iuris nocet*, co powinno budzić zaskoczenie u polskiego prawnika, zwłaszcza jeżeli mowa jest o odpowiedzialności deliktowej. Podsumowując i oceniając rozwiązania wprowadzone w amerykańskim systemie prawnym w ramach 17 U.S.C. § 512(f), samą regulację należy ocenić jako niewystarczającą do spełnienia zadań, jakie przed nią stoją. Jakkolwiek jest to także system, na podstawie którego doświadczeń możemy się również uczyć.

Z doświadczeń systemu amerykańskiego możemy wyciągnąć wnioski zarówno dla tworzenia prawa w UE, jak i w Polsce. Przede wszystkim warto zwrócić uwagę, że w art. 14 ust. 2 lit. d DSA, wprowadzając mechanizm *notice and action*, prawodawca unijny zamierza uregulować kształt zawiadomień o bezprawnych treściach i jednym z jego czterech elementów uczynić oświadczenie o posiadaniu dobrej wiary zgłaszającego, że informacje i twierdzenia zawarte w nim są dokładne

i kompletne. Niebezpiecznie zaczyna przypominać to rozwiązanie systemu amerykańskiego. Dlatego rolą legislatorów, w pierw unijnego, a następnie, jeżeli przepis wejdzie w życie w takiej formie, krajowego, jest zabezpieczenie możliwości dochodzenia odszkodowania przez użytkowników od fałszywie zawiadamiającego, bez konieczności wykazywania przez takiego użytkownika złej wiary zawiadamiającego. Podstawę dla takiego działania widzimy szczególnie w motywie 47 DSA. W przeciwnym razie, jeżeli przeszczepimy rozwiązania amerykańskie do systemu europejskiego, podstawowe prawa użytkowników Internetu staną się fikcją.

Drugi wniosek moglibyśmy wyciągnąć ze sprawy *Lenz*, nakazującej przed złożeniem zawiadomienia sprawdzenie przez podmioty uprawnione, czy dana treść nie jest chroniona dozwolonym użytkowaniem. Przynajmniej częściowo wymóg ten powinien odciążyć serwisy pośredniczące przed dokonywaniem takiej oceny samodzielnie. Także tutaj można uczynić sugestię dla prawodawcy europejskiego, by wprost wskazać, że zgłaszający w wypadku zgłaszania naruszenia praw autorskich ma obowiązek przed jego złożeniem przeanalizować, czy w danej sytuacji nie są spełnione przesłanki dozwolonego użytku, oraz złożyć w tej kwestii stosowne oświadczenie. Brak przeprowadzenia takiej analizy przez zgłaszającego wskazywałby w większości przypadków, spoza sytuacji nagłych jak w wypadku konieczności blokady streamingu transmisji *live* wydarzeń sportowych, na niedołożenie należytej staranności przez zawiadamiającego, uzasadniając tym samym poniesienie przezeń odpowiedzialności odszkodowawczej. Wspomniany postulat nie tylko przerzuciłby też obowiązki w tym zakresie na zawiadamiających, ale przyczyniłby się również do podniesienia jakości samych zawiadomień, co byłoby pożądanym kierunkiem.

W USA wprowadzenie takiego rozwiązania spotkało się z oskarżeniem o wprowadzanie „nieproporcjonalnych” obowiązków dla podmiotów uprawnionych. Naszym zdaniem taką argumentację należałoby odrzucić. Wspomniany obowiązek możemy porównać do wprowadzenia w europejskim porządku prawnym zasady rozliczalności w art. 5 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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)⁷⁴ przydający administratorom danych osobowych obowiązek wykazania przestrzegania wszystkich przepisów dotyczących ochrony danych osobowych. Czy zatem obowiązek przestrzegania zasad dozwolonego użytku w zakresie *user generated content* byłby aż tak ogromnym ciężarem dla podmiotów uprawnionych z tytułu praw autorskich w porównaniu do

⁷⁴ Dz.Urz. UE. L Nr 119, s. 1.

potencjalnych konsekwencji, jakie może za sobą nieść dla użytkowników blokada dostępu do tworzonych przez nich treści lub całych ich profili na platformach internetowych?

W naszej ocenie w zakresie regulacji odpowiedzialności fałszywie zawiadamiającego należałoby szczególnie wzorować się na rozwiązaniach stosowanych w § 194 FinKSI, gdzie na użytkownika ciążyłoby jedynie wykazanie fałszywości zawiadomienia. Wobec tego to właściciel praw autorskich w celu uniknięcia odpowiedzialności musiałby udowodnić, że bądź miał uzasadnione podstawy, by uważać informację o naruszeniu za prawdziwą, bądź że była ona nieistotna z punktu widzenia decyzji o usunięciu zgłoszonej treści. Taki podmiot posiada bowiem najlepsze informacje o tym, jak wyglądał u niego proces zgłoszenia danej treści, dlatego też procesowe udowodnienie przez niego zaistnienia wspomnianych przesłanek egzoneracyjnych wydaje się rozsądniejszym rozwiązaniem niż nakazywanie udowodnienia jego złej wiary poszkodowanemu użytkownikowi, tak jak jest to przyjęte w 17 tytułem 17 U.S.C. § 512(f). Wprowadzenie takiej regulacji byłoby także korzystne w ramach DSA, co ujednoliciłoby w tym zakresie unijny rynek cyfrowy.

Zwróćmy uwagę, że wdrożenie proponowanego przez nas rozwiązania w zakresie odnoszącym się do nałożenia obowiązku uprzedniej weryfikacji dozwolonego użytku na podmioty uprawnione w wypadku składania przez nie zawiadomienia o naruszeniu praw autorskich przez użytkowników platform internetowych byłoby także korzystne z punktu widzenia ochrony instytucji dozwolonego użytku w UE. Pomogłoby także rozwiązać, przynajmniej częściowo, problem ochrony dozwolonego użytku w ramach art. 17 DSM. Ważkość i trudność rozwiązania tej kwestii podkreśla zwłaszcza postępowanie przed TSUE w sprawie skargi polskiego rządu na wspomniany artykuł⁷⁵. Proponowane przez nas rozwiązanie mogłoby także znaleźć zastosowanie i zmniejszyć tym samym ryzyko naruszenia dozwolonego użytku na platformach internetowych w myśl postulatów

zgłoszonych niedawno przez prof. dr hab. Ryszarda Markiewicza⁷⁶. Nie rozwiąże to naturalnie całego problemu dozwolonego użytku w art. 17 DSM, ale powinno się przyczynić do jego poprawnego i zrównoważonego zastosowania.

Czy zatem możliwe jest osiągnięcie równowagi w zakresie ochrony praw autorskich w Internecie? Tak, ale należy wziąć pod uwagę każdą zainteresowaną stronę – serwisy pośredniczące, użytkowników i właścicieli praw autorskich, a także ich wzajemne relacje. System prawa autorskiego powinien być odporny na jego naruszenie przez każdy ze wspomnianych podmiotów, równocześnie jednak nie ograniczając kreatywności i postępu artystycznego i technologicznego. Nadużycia ze strony pośredników internetowych, jakie ci mogą popełnić wobec właścicieli praw autorskich i użytkowników, są przedmiotem największego zainteresowania legislatorów. Zagadnienia tego dotyczy w zasadzie każdy projekt legislacyjny (DSM, DSA, czy ustawa o wolności słowa) omawiany w niniejszym artykule. Nadużycia ze strony użytkowników są natomiast uregulowane bezpośrednio przez przepisy prawa autorskiego, zarówno cywilnoprawne, jak i karnoprawne, oraz regulaminu danych serwisów pośredniczących. Najmniej zaś uregulowana jest kwestia nadużyć ze strony podmiotów praw autorskich. Skutki braku stosownej regulacji w tym zakresie uwidaczniają także wyniki badań empirycznych w zakresie wadliwości zgłoszeń naruszeń przywoływanych w pierwszej części niniejszego artykułu. Stąd też konieczne staje się uregulowanie tego zagadnienia. W innym przypadku osiągnięcie równowagi będzie jedynie mrzonką.

⁷⁵ P. Keller, CJEU hearing in the Polish challenge to Article 17: Not even the supporters of the provision agree on how it should work, 11.11.2020 r., <http://copyrightblog.kluweriplaw.com/2020/11/11/cjeu-hearing-in-the-polish-challenge-to-article-17-not-even-the-supporters-of-the-provision-agree-on-how-it-should-work/?print=print> (dostęp z 20.2.2021 r.).

⁷⁶ R. Markiewicz, Prawo autorskie na jednolitym rynku cyfrowym. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790, Warszawa 2021, s. 272–278.

Słowa kluczowe: prawo własności intelektualnej, zgłoszenia naruszeń praw, hostingodawcy, odpowiedzialność za bezzasadne zgłoszenie naruszenia.

Responsibility for unjustified reporting of copyright infringement to the service provider based on the case *Kanał Sportowy v. Polsat* – part II

The article is divided into two parts. In the first one, the authors discuss the basis of responsibility for unjustified reporting of copyright infringement on the grounds of Polish law. The issue is considered based on the Act of 12 July 2002 on supply of e-services, the principle of delictual liability of article 415 of civil code and the Act of 16 April 1993 on preventing unfair competition. The paper is concluded with deliberations on responsibility for infringement of personal interests.

The second part is devoted to the analysis of responsibility of a person who unjustifiably reports copyright infringement on the level of EU law. The authors took into account solutions implemented in Finland, which is the only country in the EU that regulated the issue of unjustified reporting of copyright infringement to intermediary entities. Later on in the article, legal and comparative deliberations regard the U.S. law, which represents the archetype for EU regulations regarding responsibility for online copyright infringement, and regulated responsibility of a person who unjustifiably reports it. Moreover, the authors discuss implications of the changing issue resulting from new legislative projects – a draft law on protection of freedom of speech in social media and the EU regulation on digital services. Finally, there are postulates both *de lege lata* and *de lege ferenda*.

Keywords: intellectual property law, reporting law violation, hosting providers, responsibility for unjustified reporting of violation.

Nowe technologie w pracy prawnika



ksiegarnia.beck.pl

Zadzwon: 81 46 13 300

E-mail: kontakt@beck.pl



Zlecenie płatnicze – jako rozliczenia pieniężne – zawierające polecenie wykonania transakcji płatniczej

dr Ewa Kowalewska¹

Problematyka rozliczeń pieniężnych należy obecnie to zagadnień o doniosłym znaczeniu w kontekście funkcjonowania banków, przede wszystkim z uwagi na rozwój bankowości internetowej. Ponadto obejmuje swym zakresem zagadnienia o charakterze szerszym, odnoszącym się do funkcjonowania rynku usług płatniczych, a nawet całego rynku finansowego. Podstawowym celem badań i analiz przeprowadzonych na potrzeby niniejszego opracowania było nie tyle kompleksowe ujęcie problematyki rozliczeń pieniężnych, ile przede wszystkim próba usystematyzowania rozwiązań prawnych w zakresie zleceń płatniczych, które służą wykonywaniu transakcji płatniczych. W związku z tym zwrócono uwagę na zasady, które obowiązujące ustawodawstwo przypisało realizacji zleceń płatniczych, zwracając jednocześnie uwagę na podstawowe w tym obszarze (i jednocześnie szczególne) definicje. Zasadniczą tezą badawczą było założenie, że zlecenia płatnicze nie mogą stanowić autonomicznego obszaru działalności (bankowej czy też innej), która będzie podlegała regulacji jedynie jednego aktu prawnego. Podstawową metodą badawczą wykorzystaną na potrzeby niniejszego opracowania była metoda dogmatyczno-prawna, a analizie poddano obowiązujące ustawodawstwo oraz literaturę przedmiotu.

Uwagi wstępne

Zlecenie płatnicze, uregulowane na gruncie ustawy z 19.8.2011 r. o usługach płatniczych², obok polecenia przelewu i polecenia zapłaty, podlegających reżimowi ustawy z 29.8.1997 r. – Prawo bankowe³, jest formą rozliczenia pieniężnego opartego na oświadczeniu określonej kategorii podmiotów (płatnika lub odbiorcy), które zawiera polecenie wykonania transakcji płatniczej.

Odnosząc się do szeroko pojętego zagadnienia rozliczeń pieniężnych, należy wskazać, że analiza podstawowych w tym zakresie regulacji prawnych, tj. przepisów Kodeksu cywilnego oraz Prawa bankowego, wskazuje, że nie można uznać ich za regulację kompleksową. Poszerzenie tej analizy o ustawę o usługach płatniczych jest niezbędne.

Jednocześnie przeprowadzone badania wykazały, że dokonanie analizy regulacji prawnej, odnoszącej się do zleceń płatniczych tylko na podstawie ustawy o usługach płatniczych jest niewystarczające. W związku z tym charakterystyka regulacji rozliczeń pieniężnych, a w szczególności zlecenia płatniczego, wymaga szerokiego spojrzenia, przez pryzmat wymienionych wyżej aktów prawnych.

Mając na względzie tytułowy przedmiot rozważań, należy w pierwszej kolejności zwrócić uwagę na zakres transakcji płatniczych oraz umowę rachunku płatniczego, która służy wykonaniu takich transakcji. Ponadto wyodrębnić trzeba charakterystyczne elementy tzw. umowy ramowej, o której mowa w ustawie o usługach płatniczych. Takie usystematyzowanie pozwoli wyłonić cechy charakterystyczne dla rozliczeń pieniężnych, a w szczególności zleceń płatniczych, przy jednoczesnym wskazaniu problemów interpretacyjnych.

Zakres podmiotowy i przedmiotowy transakcji płatniczych – podstawowe definicje

W myśl postanowień ustawy o usługach płatniczych transakcją płatniczą to zainicjowana przez płatnika lub odbiorcę wpłata, transfer lub wypłata środków pieniężnych. Do wykonywania transakcji płatniczych służy rachunek płatniczy. Zakres podmiotowy transakcji płatniczych wskazuje na płatnika i odbiorcę. Zgodnie z przedmiotową ustawą przez płatnika należy rozumieć osobę fizyczną, osobę prawną oraz jednostkę organizacyjną niebędącą osobą prawną, której ustawa przyznaje zdolność prawną (czyli: spółka jawna, spółka komandytowa), składającą zlecenie płatnicze. Podobnie zdefiniowano odbiorcę, którą jest osoba fizyczna, osoba prawna oraz jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, będąca odbiorcą środków pieniężnych stanowiących przedmiot transakcji płatniczej. Odbiorca to podmiot, który uczestniczy w transakcji płatniczej. Ponadto podkreślić należy, że zgodnie z treścią art. 2 pkt 34 UslPłatU, płatnik i odbiorca stanowią grupę tzw. użytkowników.

Mając na uwadze powyższe, wskazać należy także, że ustawodawca w ustawie o usługach płatniczych określił, iż inicjatorem transakcji płatniczej może być płatnik – składający zlecenie płatnicze lub odbiorca – środków pieniężnych stanowiących przedmiot tej transakcji. Jednak należy zwrócić uwagę, że odbiorca jako beneficjent transakcji może być jej inicjatorem w ograniczonym zakresie, np. w przypadku polecenia zapłaty.

¹ Wydział Prawa i Administracji, Uniwersytet Szczeciński.

² T.j.: Dz.U. z 2020 r. poz. 794 ze zm.; dalej jako: UslPłatU.

³ T.j.: Dz.U. z 2020 r. poz. 1896 ze zm.; dalej jako: PrBankU.

Jak wskazano wyżej, przedmiotem transakcji płatniczej może być: wpłata, transfer lub wypłata środków pieniężnych. Istotą transakcji płatniczej jest zatem zainicjowanie:

- a) wpłaty środków pieniężnych na rachunek płatniczy,
- b) transferu środków między rachunkami płatniczymi,
- c) wypłaty środków pieniężnych z rachunku płatniczego.

Wykonywanie transakcji płatniczych odbywa się poprzez wykorzystanie rachunku płatniczego, który może być prowadzony dla jednej lub większej liczby użytkowników. Przez rachunek płatniczy rozumieć można także rachunek bankowy oraz rachunek członka spółdzielczej kasy oszczędnościowo-kredytowej, pod warunkiem że rachunki te służą do wykonywania transakcji płatniczych. Ponieważ ustawodawca określa, że rachunek płatniczy prowadzony jest dla użytkowników i przez nich wykorzystywany, to wywnioskować można, że rachunek taki może być prowadzony dla płatnika lub dla odbiorcy. Podkreślić należy, że rachunek płatniczy prowadzony jest przez tzw. dostawcę usług płatniczych. Jednocześnie warto zauważyć, że w myśl postanowień ustawy o usługach płatniczych dostawca usług płatniczych prowadzi rachunek płatniczy tylko dla płatnika. Ustawodawca nie wymienił w tym przypadku odbiorcy, który przecież jest wskazany w definicji użytkownika i w konsekwencji zaliczony do podmiotów, dla których prowadzi się rachunek płatniczy. Takie przeoczenie ustawodawcy należy ocenić krytycznie, wywołuje bowiem niepotrzebne wątpliwości natury praktycznej.

Odwołując się do treści art. 4 ust. 2 UsłPłatU, wskazać trzeba, że ustawodawca określił zakres podmiotowy dostawcy, mając na uwadze obowiązujące regulacje prawne, w szczególności Prawo bankowe. W związku z tym dostawcą może być wyłącznie:

- a) bank krajowy,
- b) oddział banku zagranicznego,
- c) instytucja kredytowa i oddział instytucji kredytowej,
- d) instytucja pieniądza elektronicznego i oddział instytucji pieniądza elektronicznego,
- e) oddział podmiotu świadczącego w innym niż Rzeczpospolita Polska (dalej: RP) państwie członkowskim, zgodnie z prawem tego państwa, pocztowe usługi płatnicze,
- f) instytucja płatnicza,
- g) Europejski Bank Centralny, Narodowy Bank Polski, bank centralny państwa członkowskiego innego niż RP,
- h) organ administracji publicznej,
- i) spółdzielcza kasa oszczędnościowo-kredytowa lub Krajowa Kasa Oszczędnościowo-Kredytowa,
- j) biuro usług płatniczych,
- k) mała instytucja płatnicza,
- l) dostawca świadczący wyłącznie usługę dostępu do informacji o rachunku.

W kontekście wskazanego katalogu odnotować należy, że implementując dyrektywę 2007/64/WE Parlamentu Europejskiego i Rady z 13.11.2007 r. w sprawie usług płatniczych

w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE⁴, każde z państw zostało zobligowane do wyróżnienia sześciu kategorii dostawców usług płatniczych: instytucje kredytowe (w tym także oddziały instytucji kredytowych), instytucje pieniądza elektronicznego, instytucje świadczące żyro pocztowe uprawnione do świadczenia usług płatniczych zgodnie z prawem krajowym, instytucje płatnicze, Europejski Bank Centralny i krajowe banki centralne oraz państwa członkowskie UE bądź ich władze regionalne lub lokalne. Katalog dostawców wskazany w ustawie o usługach płatniczych uwzględnia zatem nie tylko wymogi unijne, ale także w ramach tzw. opcji narodowych specyfikę podmiotów tworzących rynek bankowy w Polsce. Taka konstrukcja katalogu dostawców wskazuje na konsekwencję ustawodawcy polskiego i podział zastosowany w ustawie Prawo bankowe na banki krajowe i zagraniczne oraz wyodrębnienie instytucji kredytowej jako „innego” podmiotu, co stanowi wyraz kompromisu między prawem unijnym a prawem polskim⁵.

Charakter prawny umowy ramowej

Wykonywanie transakcji płatniczych odbywa się na podstawie umowy ramowej jako umowy o usługę płatniczą, która reguluje wykonywanie „indywidualnych transakcji płatniczych”, może także zawierać postanowienia w zakresie prowadzenia rachunku płatniczego (co oznacza, że umowa ramowa może być umową rachunku płatniczego). Podkreślić należy, że rodzaje usług płatniczych wymienił ustawodawca w art. 3 UsłPłatU, co należy ocenić jako istotny walor tej ustawy. W tym katalogu znalazły się m.in. czynności określone jako transakcje płatnicze: „wpłata gotówki na rachunek płatniczy”, „wypłata gotówki z rachunku płatniczego” oraz „transfer środków pieniężnych na rachunek płatniczy”. Świadczy to zatem o zaliczeniu transakcji płatniczych do katalogu usług płatniczych. Wydaje się jednak, że właściwsze byłoby określenie, że usługi płatnicze polegają m.in. na wykonywaniu transakcji płatniczych. Takie założenie pozostaje w zgodzie z przyjętą regulacją (wyrażoną w rozdziale 3 UsłPłatU), w myśl której umowa o usługę płatniczą reguluje wykonywanie transakcji płatniczych.

Należy zwrócić uwagę, że formułując definicję umowy ramowej, ustawodawca odniósł ją nie do „transakcji płatniczych”, ale do „indywidualnych transakcji płatniczych”, co stanowi istotną różnicą. Podkreślić należy także, że ustawodawca nie definiuje wymienionej „indywidualnej transakcji płatniczej”, a jedynie, co wskazano wyżej, „transakcję płatniczą”.

⁴ Dz.Urz. UE L Nr 319, s. 1.

⁵ A. Zalcewicz, [w:] A. Zalcewicz, B. Bajor (red.), Ustawa o usługach płatniczych. Komentarz, Warszawa 2016, s. 99.

Zauważyć warto również, że „indywidualna transakcja płatnicza” nie może być utożsamiana z „pojedynczą transakcją płatniczą”, ponieważ, jak wskazano w definicji w art. 2 pkt 23 UstPłatU, jest to transakcja nieobjęta umową ramową. W literaturze przedmiotu przyjmuje się, że indywidualna transakcja płatnicza to każda transakcja płatnicza wykonywana na podstawie umowy o usługę płatniczą⁶. Pomimo takiego wniosku należy jednak krytycznie ocenić postawę ustawodawcy, który wykazuje się niedbałością legislacyjną, pomijając zdefiniowanie stosowanych w ustawie pojęć⁷.

Rachunek płatniczy służy do wykonywania transakcji płatniczych. Przyjmując zatem, że transakcja płatnicza jest jednym z kilku rodzajów usług płatniczych, to umowa ramowa jako umowa o usługę płatniczą będzie nie tylko umową rachunku płatniczego, ale także jej zakres może być szerszy, podyktowany pełnym katalogiem usług płatniczych, wymienionych w art. 3 UstPłatU.

Jak wyżej wskazano, rachunek płatniczy może być prowadzony przez banki (rachunek bankowy) i spółdzielcze kasy oszczędnościowo-kredytowe (rachunek członka spółdzielczej kasy oszczędnościowo-kredytowej), pod warunkiem że rachunki te służą do wykonywania transakcji płatniczych. Odwołując się do rodzajów rachunku bankowego, wymienionych w art. 49 PrBankU, należy zastanowić się, jakie rachunki bankowe w powyższym kontekście miał na myśli ustawodawca w ustawie o usługach płatniczych. Ponieważ na gruncie ustawy o usługach płatniczych mowa o rachunkach bankowych tylko w odniesieniu do usług płatniczych, to konsekwencją tego będzie wyłączenie niektórych rodzajów rachunków bankowych wymienionych w Prawie bankowym. W tym zakresie zastosowanie znajduje także art. 6 UstPłatU, gdzie określone zostały wyłączenia przedmiotowe, w tym m.in. usługi wykonywane wyłącznie z wykorzystaniem papierowych książeczek oszczędnościowych, w przypadku gdy wszelkie transakcje są rejestrowane wyłącznie w tych książeczkach. Oznacza to, że poza pojęciem rachunku płatniczego pozostaną rachunki oszczędnościowe związane z książeczkami oszczędnościowymi. Wątpliwości pojawiają się także z uznaniem jako rachunku płatniczego rachunku lokaty terminowej czy rachunku terminowej lokaty oszczędnościowej, które powiązane są z instytucją tzw. lokat sztywnych, niepozwalających na dokonywanie wpłat i wypłat środków pieniężnych (czyli na dokonywanie transakcji płatniczych). Wyłączeniem w tym zakresie objęte będą także rachunki bankowe prowadzone w walutach innych niż waluty państw członkowskich⁸.

Mając powyższe na uwadze, należy uznać, że umowa rachunku bankowego może stanowić umowę ramową, jednakże pod warunkiem spełnienia łącznie dwóch następujących warunków:

1) rachunek bankowy będzie rachunkiem płatniczym,

2) usługi, świadczone w ramach tego rachunku bankowego, mogą być objęte zakresem zastosowania ustawy o usługach płatniczych (tj. usługi płatnicze).

Podstawy prawne przeprowadzania rozliczeń pieniężnych

Przepisy prawne odnoszące się do rozliczeń pieniężnych, zawarte w Kodeksie cywilnym (przepisy o umowie rachunku bankowego) i w ustawie Prawo bankowe, należą do dziedziny prawa prywatnego. Chociaż obecnie brak definicji legalnej rozliczeń pieniężnych⁹, to nie ma wątpliwości, że należą one do kategorii czynności bankowych *sensu stricto*¹⁰. W myśl postanowień art. 63 PrBankU rozliczenia takie mogą być przeprowadzane, jeżeli przynajmniej jedna ze stron rozliczenia ma rachunek bankowy. Doktryna zalicza bankowe rozliczenia pieniężne do operacji pośredniczących¹¹. Odnotować należy, że rozliczenia pieniężne powinny prowadzić do zmiany stanu środków pieniężnych na rachunku bankowym, należącym do posiadacza. W związku z tym rozliczeniem pieniężnym nie będzie dokonanie przez bank operacji, w wyniku których następuje zmiana zapisu w księgach rachunkowych, która jednocześnie nie wywołuje skutków o charakterze cywilnoprawnym¹². Ponadto warto podkreślić, że zdarzeniem, które inicjuje rozliczenie pieniężne, jest będące oświadczeniem woli, tzw. polecenie rozliczeniowe, które pochodzi od posiadacza rachunku bankowego. W literaturze przedmiotu podkreślono, że na gruncie Kodeksu cywilnego zwane jest ono zleceniem, ale nie może być ono utożsamiane ze zleceniem, o którym mowa w art. 734 i n. KC¹³.

Przepisy Prawa bankowego wskazują sposoby dokonywania rozliczeń pieniężnych¹⁴, wymieniając dwie formy: gotówkowe i bezgotówkowe oraz dwa sposoby ich przeprowadzania: tradycyjny i nowoczesny. Pierwszy sposób polega na wykorzystaniu papierowych nośników danych, drugi na

⁶ W. Iwański, Umowa rachunku bankowego objętego bankowością internetową z punktu widzenia nowej regulacji usług płatniczych, Warszawa 2014, s. 42.

⁷ Należy także zwrócić uwagę, że ustawodawca w ustawie o usługach płatniczych posługuje się pojęciem „środki pieniężne” lecz nie definiuje tego pojęcia, co wydaje się być istotnym mankamentem przy interpretacji przepisów dotyczących pieniądza elektronicznego.

⁸ W. Iwański, Umowa rachunku..., s. 95.

⁹ W wyniku nowelizacji PrBankU z 7.1.002 r. zrezygnowano z tej definicji, którą wyrażał art. 63 PrBankU.

¹⁰ Z. Ofiarski, Prawo bankowe, Warszawa 2017, s. 238.

¹¹ W.L. Jaworski, Z. Krzyżkiewicz, B. Kosiński, Banki – rynki, operacje, polityka, Warszawa 1999, s. 106 i n.

¹² A. Socha, Bankowe rozliczenia pieniężne a świadczenia pieniężne, Radca Prawny 2000, Nr 2, s. 65.

¹³ W. Iwański, Umowa rachunku..., s. 116 oraz przywołany tam: S. Grzybowski, System Prawa Cywilnego, Wrocław 1976, T. 3, cz. 1, s. 771 i n.

¹⁴ Szerzej: Z. Ofiarski, Prawo..., s. 239; M. Chudzik, Obowiązkowe pośrednictwo uprawnionych banków w świetle znówelizowanego prawa bankowego, Prawo Bankowe 2008, Nr 4, s. 49.

tomiast oznacza wykorzystanie nośników elektronicznych¹⁵. Rodzaje rozliczeń gotówkowych nie budzą wątpliwości, zalicza się do nich чеки gotówkowe oraz wpłatę gotówki na rachunek bankowy wierzyciela. Natomiast bezgotówkowe rozliczenia pieniężne to w szczególności polecenie przelewu, polecenie zapłaty, czek rozrachunkowy i karta płatnicza. Nie jest to jednak katalog zamknięty¹⁶. Banki mogą oferować także inne formy rozliczeń. Przepisy Prawa bankowego nie definiują, czym jest „rozliczenie” czy „bankowe rozliczenie pieniężne”.

Mając na uwadze nie tylko regulacje ustawy Prawo bankowe, ale także definicje, o których mowa wyżej, tj. „usługa płatnicza” i „transakcja płatnicza”, podkreślić należy, że każde rozliczenie pieniężne będzie zawierało się w pojęciach usługi płatniczej oraz transakcji płatniczej¹⁷. Jednocześnie zaważyć trzeba, że do transakcji płatniczych będą należały wpłaty i wypłaty dokonywane na rzecz posiadacza rachunku, które nie mieszczą się w pojęciu rozliczeń pieniężnych. Uznanie rozliczeń pieniężnych za takie, które mieszczą się w definicji usług płatniczych, nie przesądza ostatecznie o objęciu ich regulacją ustawy o usługach płatniczych¹⁸. Należy mieć na uwadze, że w ustawie o usługach płatniczych zawarte zostały definicje jedynie wybranych usług płatniczych (polecenia zapłaty i usługi przekazu pieniężnego).

W literaturze przedmiotu pojęcie to definiowane jest jako działania prawne i faktyczne, które prowadzą do¹⁹:

- 1) zmiany stanu środków pieniężnych na dwóch rachunkach (na rachunku, który ma być obciążony daną sumą pieniężną i na rachunku, który tą sumą pieniężną ma być uznany);
- 2) zmiany stanu środków pieniężnych na określonym rachunku bankowym, będącej następstwem wpłaty środków pieniężnych na ten rachunek bądź wypłaty z tego rachunku na rzecz osoby trzeciej.

Istota umowy rachunku bankowego, określona w art. 725 KC, wskazuje, że prowadzenie rozliczeń pieniężnych przez banki jest z nią ściśle powiązane. Przez umowę rachunku bankowego bank zobowiązuje się względem posiadacza rachunku, na czas oznaczony lub nieoznaczony, do przechowywania jego środków pieniężnych oraz jeśli umowa tak stanowi, do przeprowadzania na jego zlecenie rozliczeń pieniężnych. Z powyższego wynika jednoznacznie, że bank zobowiązany jest w ramach prowadzonego rachunku bankowego do przeprowadzania rozliczeń pieniężnych na zlecenie posiadacza rachunku. W tym zakresie niemożliwe są także postanowienia umowne wyłączające taki obowiązek.

Mając na uwadze przepisy Kodeksu cywilnego i Prawa bankowego, odnoszące się do przeprowadzania rozliczeń pieniężnych (w literaturze przedmiotu określane także jako polecenie rozliczeniowe²⁰), stwierdzić należy, że regulacja ta jest ograniczona. W dalszej części opracowania omówione zostaną regulacje ustawy o usługach płatniczych, które mają

kluczowe znaczenie dla przeprowadzania zleceń płatniczych, a jednocześnie obarczone zostały pewnymi brakami legislacyjnymi, w związku z czym odwołanie do Kodeksu cywilnego czy prawa bankowego wydaje się niezbędne.

Cechy i zasady realizacji zlecenia płatniczego na gruncie ustawy o usługach płatniczych

Jak już wyżej wskazano, transakcja płatnicza inicjowana przez płatnika oznacza wykonanie zlecenia płatniczego. Natomiast zlecenie płatnicze, zdefiniowane w ustawie o usługach płatniczych, to oświadczenie płatnika lub odbiorcy skierowane do jego dostawcy zawierające polecenie wykonywania transakcji płatniczej. W doktrynie podkreślono, że taka definicja oznacza, że każde polecenie rozliczeniowe będzie poleceniem płatniczym. Jednocześnie na uwagę zasługuje fakt, że pojęcie zlecenia płatniczego jest pojęciem szerszym²¹. Obejmuje również inne polecenia posiadacza rachunku bankowego związane z wpłatami i wypłatami z rachunku na jego rzecz²².

Ustawa o usługach płatniczych wyróżnia trzy różne rodzaje transakcji płatniczych, w zależności od sposobu zainicjowania:

- a) zainicjowane przez płatnika (np. polecenie przelewu);
- b) zainicjowane przez płatnika za pośrednictwem odbiorcy (np. zapłata kartą płatniczą);
- c) zainicjowane przez odbiorcę (np. polecenie zapłaty).

Należy zwrócić uwagę, że ustawa o usługach płatniczych, regulując zagadnienie zlecenia płatniczego, odniosła się do niego w szerokim zakresie. W związku z tym niezbędne jest ustalenie, czy w ogóle, a jeśli tak, to w odniesieniu do jakich zagadnień, stosowane będą przepisy Prawa bankowego czy Kodeksu cywilnego²³. Mając powyższe na uwadze, podkreślenia wymaga, po pierwsze, fakt, że w ustawie o usługach płatniczych nie uregulowano treści zlecenia płatniczego. Oznacza to, że w tym zakresie zastosowanie powinny mieć regulacje zawarte w Kodeksie cywilnym czy Prawie bankowym, jednakże przepisy wymienionych aktów prawnych nie odnoszą się do treści rozliczeń pieniężnych. W związku z czym uznać należy, że zagadnienie „treści zlecenia płatniczego” jest przed-

¹⁵ Z. Ofiarski, Prawo..., s. 239.

¹⁶ W. Iwański, Umowa rachunku..., s. 114.

¹⁷ W. Pyziół, A. Walaszek-Pyziół, Ustawa z 2011 roku o usługach płatniczych a umowa rachunku bankowego, Przegląd Ustawodawstwa Gospodarczego 2012, s. 3.

¹⁸ W. Iwański, Umowa rachunku..., s. 115.

¹⁹ Ibidem, s. 116 i podane tam: W. Pyziół, Umowa rachunku bankowego, [w:] J. Panowicz-Lipska (red.), SPP, t. 8, Prawo zobowiązań – część szczegółowa, Warszawa 2011, s. 521 i n.

²⁰ W. Iwański, Umowa rachunku..., s. 116.

²¹ Ibidem, s. 118.

²² W. Pyziół, A. Walaszek-Pyziół, Ustawa z 2011 roku..., s. 4 i 6.

²³ Por. W. Iwański, Umowa rachunku..., s. 118.

miotem umów. Po drugie, w ustawie o usługach płatniczych nie zostały wprowadzone wymogi odnoszące się do formy zlecenia płatniczego. W tym zakresie można stwierdzić, że w przypadku braku odmiennych regulacji umownych zastosowanie znajdują zasady ogólne, czyli przewidujące każdą formę (art. 60 KC). Trzeba także pamiętać, że możliwa jest forma elektroniczna, którą dopuszcza Prawo bankowe²⁴. Po trzecie, ustawodawca wskazał w definicji zlecenia płatniczego, że opiera się ono na oświadczeniu płatnika lub odbiorcy, jednakże nie wskazał szczegółowo, jak takie oświadczenie powinno być wyrażone. Z ustawy o usługach płatniczych wynika jedynie, od jakich podmiotów zlecenie płatnicze powinno pochodzić. Odwołując się do przepisów Kodeksu cywilnego, tj. treści art. 61 § 1, oświadczenie woli uznaje się za złożone z chwilą, gdy doszło do drugiej strony, w taki sposób, że mogła ona zapoznać się z jego treścią. Natomiast, w myśl art. 61 § 2 KC, jeśli chodzi o oświadczenie woli wyrażone w postaci elektronicznej, jest ono złożone z chwilą, gdy wprowadzono je do środka komunikacji elektronicznej, w taki sposób, że można było zapoznać się z jego treścią. W bankowości elektronicznej (internetowej) najczęściej będzie to moment wprowadzenia polecenia do systemu bankowości internetowej. Po czwarte, należy zwrócić uwagę na regulację art. 49 ust. 1 UsłPłatU, gdzie określony został moment otrzymania zlecenia płatniczego jako moment, w którym zlecenie zostało otrzymane przez dostawcę płatnika. Podkreślić jednak należy, że zlecenie może być przekazane bezpośrednio przez płatnika oraz przez odbiorcę albo za pośrednictwem odbiorcy²⁵. Ustalenie tego momentu ma fundamentalne znaczenie dla wskazania chwili zrealizowania transakcji, a w efekcie dla ustalenia terminu spełnienia świadczenia. Ponadto, z treści art. 49 ust. 1 UsłPłatU wynika, że jeśli dzień otrzymania zlecenia nie jest dniem roboczym w świetle obowiązujących przepisów, wtedy przyjmuje się, że zlecenie zostało otrzymane pierwszego dnia roboczego po tym dniu. Zasada powyższa nie odbiega od zasad określonych na gruncie Kodeksu cywilnego, w związku z czym należy przyjąć, że ma charakter informacyjny i nie stanowi rozwiązania szczególnego.

Na tle przyjętego w art. 49 UsłPłatU rozwiązania istotne jest przede wszystkim wskazanie, kiedy i po spełnieniu jakich wymogów można uznać, że dostawca otrzymał zlecenie. Należy zatem ustalić, jakie warunki muszą być spełnione, żeby można było stwierdzić, że zlecenie zostało otrzymane przez dostawcę. W tym zakresie ważną rolę spełniać będzie umowa, która powinna określać, w jaki sposób następuje przekazanie zlecenia, czyli jakie informacje powinien przekazać płatnik czy odbiorca, oraz jakie procedury i instrumenty powinny być w tym zakresie wykorzystane²⁶. Szczegółne rozwiązanie zaproponował ustawodawca w art. 49 ust. 2 i 3 UsłPłatU. W myśl tych postanowień dostawca może ustalić nieprzekraczalny, przypadający pod koniec dnia roboczego moment, w którym otrzymane zle-

cenie płatnicze uznaje się za otrzymane pierwszego dnia roboczego po tym dniu. Takie zlecenie płatnicze będzie więc traktowane jako otrzymane w kolejnym dniu roboczym. Dodatkowo należy zauważyć, że jeśli następny dzień będzie dniem ustawowo wolnym, to w takiej sytuacji, dniem otrzymania zlecenia będzie pierwszy dzień roboczy po dniu wolnym. Ustawodawca określił tu szczególną zasadę, stosując zwrot nieostry „po koniec dnia”. Taka regulacja ustawowa pozwoliła wypracować bankom praktykę nazwaną *cut-off times*. Oznacza ona, że banki wprowadzają w swoich regulaminach (ogólnych warunkach) zasady odnoszące się do realizacji pojedynczych transakcji płatniczych tzw. *data spot*, określając, że standardowy termin rozliczenia transakcji przypada na drugi dzień roboczy po dniu złożenia zlecenia, pod warunkiem iż zostało ono złożone zgodnie z obowiązującym w banku *cut-off time*²⁷. W ten sposób, w zakresie funkcjonowania bankowości internetowej, banki wprowadzają umowne ograniczenia godzinowe dla składania poleceń rozliczeniowych, co oznacza, że polecenia, które dotarły do banku po tej godzinie, są uznawane za złożone następnego dnia roboczego²⁸.

Na uwagę zasługuje także regulacja art. 49 ust. 3 UsłPłatU, gdzie określone zostały zasady odnoszące się do ustalenia chwili otrzymania zlecenia w przypadku zleceń, których realizacja jest odroczone w czasie (z odroczonym terminem płatności). Jeżeli użytkownik inicjujący zlecenie płatnicze i jego dostawca uzgodnią, że wykonanie zlecenia płatniczego rozpoczyna się:

- 1) określonego dnia,
- 2) pod koniec wskazanego okresu,
- 3) w dniu, w którym płatnik przekazuje do dyspozycji swojemu dostawcy środki pieniężne na wykonanie zlecenia płatniczego,

wówczas za moment otrzymania zlecenia dla celów obliczenia maksymalnego terminu realizacji uznaje się początek dnia, o którym mowa w pkt 1, albo dnia będącego ostatnim dniem okresu, o którym mowa w pkt 2, albo dnia, o którym mowa w pkt 3. Jeżeli realizacja zlecenia płatniczego ma nastąpić w dniu określonym w umowie, wówczas przyjąć należy, że momentem otrzymania zlecenia jest początek

²⁴ Oświadczenie woli posiadacza rachunku bankowego może być złożone poprzez bankowość internetową, która jest uzgodnioną pomiędzy bankiem a posiadaczem rachunku, uzgodnionym sposobem komunikacji.

²⁵ B. Bajor, [w:] A. Zalcewicz, B. Bajor (red.), Ustawa o usługach płatniczych. Komentarz, Warszawa 2016, s. 217.

²⁶ *Ibidem*, s. 217.

²⁷ Przykładowo: Zasady realizacji pojedynczych transakcji płatniczych w podkarpackim banku spółdzielczym, materiał źródłowy: <https://www.banknowybfq.pl/docman-wszystko/regulaminy/103-zasady-realizacji-pojedynczych-transakcji-płatniczych/file>; Ogólne warunki realizacji zleceń płatniczych w ipko biznes w systemie informatycznym banku, https://www.pkobp.pl/media_files/e0dde6d3-8e76-4485-9c2b-61899031fd5f.pdf (dostęp z 22.3.2021 r.).

²⁸ Patrz także: W. Iwański, Umowa rachunku..., s. 117.

tego dnia. Jeśli z umowy wynika, że wykonanie zlecenia płatniczego nastąpi pod koniec wskazanego w umowie okresu, wówczas ostatni dzień tego okresu jest traktowany jako dzień otrzymania zlecenia. W ostatnim przypadku, gdy dniem tym jest dzień, w którym płatnik przekazuje do dyspozycji środki pieniężne dostawcy, to momentem otrzymania zlecenia jest początek dnia, w którym środki te zostaną przekazane.

W przedmiocie analizowanych zagadnień należy także zwrócić uwagę na zakres regulacji ustawy o usługach płatniczych, który wprowadza zasadę dotyczącą odmowy wykonania zlecenia. W myśl regulacji art. 50 UstPłatU dostawca nie może odmówić wykonania autoryzowanego zlecenia płatniczego, zainicjowanego przez płatnika albo odbiorcę lub za jego pośrednictwem, jeżeli zostały spełnione postanowienia wskazane w umowie łączącej dostawcę i użytkownika. Oznacza to zatem, że odmowa możliwa jest tylko wówczas, gdy nie zostały spełnione przez płatnika postanowienia umowy lub możliwość albo obowiązek odmowy wynika z odrębnych przepisów (np. z ustawy z 11.3.2018 r. o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu²⁹). Dostawca, odmawiając wykonania zlecenia płatniczego, jest zobowiązany powiadomić o tym fakcie płatnika wraz z podaniem przyczyn tej odmowy (pod warunkiem że przepisy odrębne nie ograniczają lub nie wyłączają takiej możliwości). Natomiast w sytuacji odmowy wykonania zlecenia płatniczego, spowodowanej wystąpieniem w zleceniu błędu, dostawca jest zawiadamiany o procedurze sprostowania błędów, które taką odmowę spowodowały. Z powyższego wynika, że na banku, który występuje jako dostawca usług płatniczych, spoczywają obowiązki informacyjne, ale wynikają one także z Prawa bankowego. W tym zakresie ustawa o usługach płatniczych jedynie je ugruntowała.

Na zakończenie powyższych rozważań, dotyczących regulacji zlecenia płatniczego w ustawie o usługach płatniczych, należy odnotować, że ustawa ta zawiera także regulację, w której określono zasady „odwołania zlecenia płatniczego”, wskazując także, do którego momentu możliwe jest owo odwołanie. W myśl postanowień art. 51 UstPłatU użytkownik nie może odwołać zlecenia płatniczego od chwili jego otrzymania przez dostawcę płatnika. Jest to zgodne z zasadą wyrażoną w art. 61 § 1 KC. Oświadczenie woli o odwołaniu zlecenia płatniczego musi dotrzeć najpóźniej wraz z oświadczeniem zlecenia transakcji płatniczej. Taka zasada nie jest możliwa do spełnienia w przypadku transakcji dokonywanych przy wykorzystaniu instrumentów płatniczych (np. kart płatniczych)³⁰. Te szczególne reguły odwołania zlecenia płatniczego dotyczą sytuacji, gdy inicjatorem transakcji jest odbiorca lub gdy transakcja jest inicjowana za jego pośrednictwem. Płatnik nie może wtedy odwołać zlecenia płatniczego po przekazaniu zlecenia odbiorcy lub po udzieleniu przez płatnika zgody odbiorcy na

wykonanie transakcji. W doktrynie podkreśla się, że jedynie umowa może przewidywać inne rozwiązanie³¹.

Nieco odmienne zasady wprowadził ustawodawca w ustawie o usługach płatniczych, w stosunku do odwołania polecenia zapłaty. Płatnik może odwołać transakcję, przy zachowaniu prawa do zwrotu kwoty tej transakcji, nie później jednak niż do końca dnia roboczego poprzedzającego uzgodniony dzień obciążenia rachunku płatniczego. Oznacza to, że złożenie oświadczenia musi nastąpić przed końcem dnia oraz musi być to dzień uznawany za dzień roboczy. Na podobnych zasadach użytkownik może odwołać zlecenie płatnicze w przypadku odroczenia transakcji płatniczej. Po upływie terminu do odwołania zlecenia płatniczego można je odwołać, wyłącznie po uzgodnieniu między sobą przez użytkownika i jego dostawcę. W niektórych przypadkach wymagana jest zgoda dostawcy (art. 51 ust. 2 i 3). Ponadto dostawca może pobierać opłaty za odwołanie zlecenia, jeżeli tak uzgodniono w umowie.

Podsumowanie

Podjętą się badań, które z jednej strony obejmują specyficzne dla rynku usług płatniczych instytucje (zlecenie płatnicze, transakcje płatnicze, umowa ramowa), a z drugiej strony dotyczą podmiotów, które równolegle funkcjonują na rynku usług bankowych (banki), trzeba przede wszystkim zwrócić uwagę na regulacje prawne rozproszone w różnych aktach prawnych, mając świadomość, że każde z nich, interpretowane osobno nie spełnia kryterium kompleksowości. Ponadto należy pamiętać, że z jednej strony są to regulacje ogólne i mające powszechne zastosowanie (jak te o oświadczeniu woli, wynikające z Kodeksu cywilnego), jak również szczególne, odnoszące się tylko do określonego podmiotowo lub przedmiotowo zakresu czynności (np. dostawca usług płatniczych).

Przeprowadzona na potrzeby niniejszego opracowania analiza ustawodawstwa wykazała, że tradycyjne podejście do funkcjonowania banków, a przede wszystkim zawieranych przez nie umów rachunku bankowego jest niewystarczające, aby dokonać interpretacji i wykazać znaczenie umów rachunku płatniczego, które służą wykonywaniu transakcji płatniczych. Współcześnie, prowadzenie rachunków płatniczych przez banki czy spółdzielcze kasy oszczędnościowo-kredytowe jest jednym z ważniejszych obszarów działalności tych podmiotów. Należy mieć na uwadze, że rynek usług płatniczych opiera się wprawdzie na podmiotach funkcjonujących na rynku bankowym, ale

²⁹ T.j.: Dz. U. z 2020 r. poz. 971 ze zm.

³⁰ B. Bajor, [w:] A. Zalcewicz, B. Bajor (red.), Ustawa..., s. 221.

³¹ *Ibidem*, s. 221.

charakteryzuje się swoistością wykonywanych na tym rynku usług (usługi płatnicze), uregulowanych w znacznej mierze odrębną regulacją. Rynek ten tworzą podmioty, które są ukierunkowane na świadczenie określonych usług, przy jednoczesnym ograniczeniu możliwości ich świadczenia przez inne podmioty. Wyodrębnienie rynku usług płatniczych w ujęciu funkcjonalnym nie może oznaczać zawężenia re-

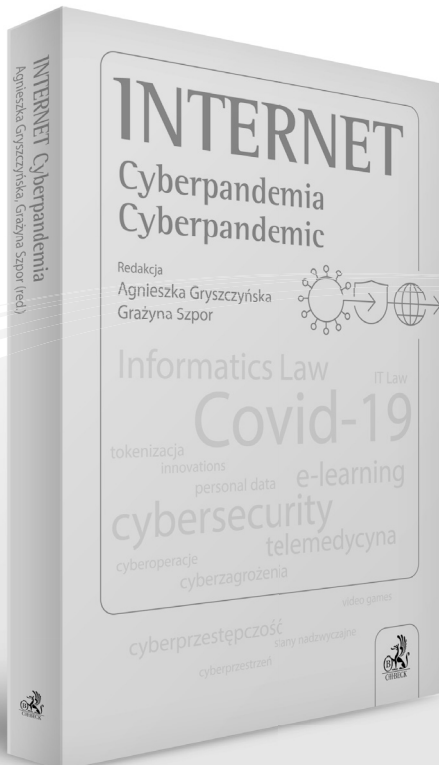
gulacyjnego tylko do tego obszaru funkcjonowania. Stąd też przyjętą tezę badawczą należy potwierdzić. Realizowanie zleceń płatniczych, służących wykonywaniu transakcji płatniczych, nie stanowi autonomicznego pod względem regulacyjnym, obszaru działalności. Nie jest to możliwe przede wszystkim z uwagi na działalność w tym obszarze banków podlegających reżimowi Prawa bankowego.

Słowa kluczowe: zlecenie płatnicze, rozliczenie pieniężne, usługa płatnicza, transakcja płatnicza.

Payment order – as cash settlements – containing an order to execute a payment transaction

Currently, the issues of monetary settlements are matters of great importance in the context of the functioning of banks, primarily due to the development of online banking. Moreover, it covers issues of a broader nature, relating to the functioning of the payment services market, and even the entire financial market. The main goal of the research and analyses carried out for the needs of this study was not so much a comprehensive approach to the issue of monetary settlements, but above all an attempt to systematize legal solutions in the field of payment orders that are used to perform payment transactions. Therefore, attention was drawn to the principles that the applicable legislation attribute to payment orders, at the same time paying attention to basic (and also specific) definitions in this area. The main thesis statement was the assumption that payment orders cannot constitute an independent area of activity (banking or other), which will be regulated by only one legal act. The basic research method used for the needs of this study was a dogmatic and legal method, and the applicable legislation and literature on the subject were analyzed.

Keywords: payment order, payment transaction, cash settlement, payment service.



Cyberpandemia

Redakcja
Agnieszka Gryszczyńska
Grażyna Szpor

Informatics Law IT Law
Covid-19
tokenizacja innovations personal data e-learning
cybersecurity cyberoperacje cyberzagrożenia
cyberprzestępczość siany nadwycieczne cyberprzestrzeń

ksiegarnia.beck.pl
Zadzwoń: 81 46 13 300
E-mail: kontakt@beck.pl



C.H.BECK

Zdalne utworzenie spółki z o.o. przy użyciu środków komunikacji wideo na przykładzie implementacji dyrektywy 2019/1151 do prawa niemieckiego

Maja Mandrykowska¹

Celem niniejszego opracowania jest próba przedstawienia rozwiązań proponowanych przez Federalne Ministerstwo Sprawiedliwości i Ochrony Konsumentów w Niemczech, które są odpowiedzią na wymogi wprowadzone przez dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1151 z 20.6.2019 r. zmieniającą dyrektywę (UE) 2017/1132 w odniesieniu do stosowania narzędzi i procesów cyfrowych w prawie spółek². Zmiany wprowadzone przez dyrektywę 2019/1151 zakładają m.in. procedurę zakładania spółki z o.o. w pełni online, w której komunikacja z notariuszem odbywa się za pośrednictwem systemu teleinformatycznego. Stąd też głównym tłem rozważań będą przepisy ustanawiające zasady składania oświadczeń woli za pomocą środków komunikacji wideo bez fizycznej obecności stron umowy w kancelarii notarialnej.

Uwagi wstępne

Obecnie, w czasach zdalnej rzeczywistości, posługiwanie się narzędziami cyfrowymi przy dokonywaniu czynności prawnych, w tym również w zakresie prawa spółek handlowych, wydaje się nie tylko wygodnym rozwiązaniem, ale także koniecznością. Nieuchronne jest zatem ciągłe unowocześnianie i dostosowanie przepisów prawnych, tak aby umożliwiały wykorzystywanie narzędzi i procesów cyfrowych w celu założenia spółki całkowicie za pośrednictwem Internetu, co „stanowi jeden z warunków wstępnych skutecznego funkcjonowania, unowocześnienia i administracyjnego usprawnienia konkurencyjnego rynku wewnętrznego oraz zapewnienia konkurencyjności i wiarygodności spółek”³. Parlament Europejski i Rada, chcąc sprostać wyzwaniom gospodarczym i społecznym związanym z globalizacją i cyfryzacją, przyjęły dyrektywę 2019/1151, której celem jest „zapewnienie większej liczby rozwiązań cyfrowych dla spółek na rynku wewnętrznym”⁴. Dyrektywa 2019/1151 wyznacza nowe zasady i standardy w zakresie dostępu do narzędzi internetowych umożliwiających przedsiębiorcom i spółkom kontakt z organami w kwestiach dotyczących prawa spółek, co ma zniwelować różnice między regulacjami państw członkowskich. Przedmiotem regulacji powołanej dyrektywy są między innymi przepisy umożliwiające zakładanie spółki z o.o. całkowicie online, a także normy dotyczące ujawniania informacji rejestrowych, usprawnienia transgranicznej wymiany informacji o oddziałach spółek oraz o osobach objętych zakazem pełnienia funkcji kierowniczych.

Zgodnie z treścią dyrektywy 2019/1151 państwa członkowskie powinny wprowadzić w życie przepisy niezbędne do jej wykonania do 1.8.2021 r.⁵. Zaawansowane prace nad implementacją przepisów dyrektywy 2019/1151 trwają

w Niemczech – 10.2.2021 r. Rząd Federalny przyjął Projekt ustawy o wdrożeniu dyrektywy 2019/1151, zawierający przepisy wprowadzające między innymi procedurę zakładania spółki GmbH⁶ z wykorzystaniem środków komunikacji wideo z notariuszem. Ustawa ma wejść w życie do 1.8.2022 r., a w stosunku do spółek GmbH ma obowiązywać od 1.1.2023 r.

Wprowadzenie możliwości założenia niemieckiej spółki z o.o. w pełni zdalnie

Zgodnie z dodanym przez dyrektywę 2019/1151 art. 13g ust. 1 „państwa członkowskie zapewniają, aby tworzenie spółek przez Internet mogło odbywać się w pełni przez Internet, bez konieczności osobistego stawiennictwa wnioskodawców przed organem lub osobą lub podmiotem, upoważnionym na mocy prawa krajowego do zajmowania się którymkolwiek z aspektów tworzenia spółek przez Internet, w tym sporządzaniem aktu założycielskiego spółki”⁷. W prawie niemieckim w tym zakresie decydujące znaczenie ma zmia-

¹ Autorka jest absolwentką stacjonarnych studiów prawa na Uniwersytecie Wrocławskim oraz Szkoły Prawa Niemieckiego działającej na Wydziale Prawa Administracji i Ekonomii Uniwersytetu Wrocławskiego we współpracy z Wydziałem Prawa Uniwersytetu Humboldtów w Berlinie oraz Niemiecko-Polskim Stowarzyszeniem Prawników w Berlinie.

² Dz.Urz. UE L Nr 186, s. 1; dalej jako: dyrektywa 2019/1151.

³ Motyw 2 dyrektywy 2019/1151.

⁴ Motyw 40 dyrektywy 2019/1151.

⁵ Art. 2 ust. 1 dyrektywy 2019/1151.

⁶ *Gesellschaft mit beschränkter Haftung* – niemiecka spółka z o.o., dalej jako: GmbH.

⁷ Art. 1 ust. 5 dyrektywy 2019/1151.

na § 2 GmbHG⁸, polegająca na dodaniu ust. 3, który po raz pierwszy będzie umożliwiał utworzenie spółki GmbH całkowicie online, również w wariantcie formy prawnej UG (*haftungsbeschränkt*)⁹. Środkiem, który umożliwić ma założenie spółki GmbH całkowicie online, jest notarialne uwierzytelnienie oświadczeń woli za pośrednictwem środków komunikacji wideo, opisane w dalszej części artykułu. Co ważne, do założenia spółki GmbH online nadal wymagany będzie udział notariusza. Nowy ust. 3 tego przepisu pozwala na notarialne poświadczenie aktu założycielskiego i umowy spółki oraz uchwał wspólników podjętych w trakcie tworzenia spółki, w przypadku tworzenia spółki bez wkładów niepieniężnych, zgodnie z zasadami wyznaczonymi przez dodane przepisy § 16a–16e *Beurkundungsgesetz*¹⁰. Do „podpisania” cyfrowej umowy spółki wystarczą kwalifikowane podpisy elektroniczne wszystkich wspólników – w Niemczech może to się odbyć w szczególności za pomocą e-dowodu osobistego z odpowiednim certyfikatem podpisu. Użycia e-dowodu tożsamości będzie można dokonać za pomocą specjalnego czytnika kart bądź telefonu komórkowego z funkcją NFC¹¹. Nowy, w pełni cyfrowy sposób zakładania spółki z o.o. umożliwiają szeroko zakrojone zmiany w *Beurkundungsgesetz*. Nowa regulacja koncentruje się na procedurze, w której notariusz jest upoważniony do uwierzytelniania oświadczeń woli bez fizycznej obecności w jego kancelarii zainteresowanych stron, za pośrednictwem systemu komunikacji wideo, prowadzonego przez Federalną Izbę Notarialną (*Bundesnotarkammer*). Co ważne, utworzenie i obsługa systemu komunikacji wideo zostanie powierzona wyłącznie Federalnej Izbie Notarialnej – nie będzie więc możliwe dokonanie czynności prawnej za pomocą systemu udostępnionego przez inny podmiot. To ograniczenie ma gwarantować bezpieczeństwo – prywatne osoby trzecie spoza administracji państwowej nie uzyskają dostępu do wrażliwych treści aktów notarialnych. Szczegółowe przepisy dotyczące technicznego działania systemu komunikacji wideo, jak również bezpieczeństwa danych, są zastrzeżone do uregulowania w drodze rozporządzenia. Warto również zwrócić uwagę na przepisy wprowadzające zasady finansowania systemu komunikacji wideo dla czynności notarialnych. Budowa i eksploatacja systemu ma być finansowana z opłat pobieranych przez notariuszy za czynności, których dokonują przy użyciu systemu teleinformatycznego. Notariusze mają być zobowiązani do utworzenia i utrzymywania w gotowości systemu komunikacji wideo, niezależnie od rzeczywistego wykorzystania systemu¹².

Zasady zdalnego zakładania spółki z o.o.

Wprowadzenie nowych przepisów będzie dawało zainteresowanym stronom możliwość wyboru rodzaju procedu-

ry – tradycyjnej albo zdalnej – w zależności od tego, która odpowiada ich potrzebom. Natomiast notariusze nie będą mogli swobodnie decydować o tym, czy oprócz procedury tradycyjnej będą oferowali dokonanie czynności notarialnej w formie przekazu wideo. Regulacje ustawowe nie będą w tym zakresie dawały notariuszom żadnej swobody decyzyjnej, w związku z tym będą oni musieli proponować obie procedury¹³. Jedynie w przypadku gdy notariusz nie jest w stanie w danej sytuacji zagwarantować wypełnienia swoich obowiązków służbowych w ramach procedury online, jest on uprawniony i zobowiązany do odmowy przeprowadzenia czynności notarialnej za pomocą środków komunikacji wideo¹⁴. Jako przykładowe sytuacje, w których notariusz może odmówić dokonania czynności, w Projekcie ustawy w sprawie wdrożenia dyrektywy 2019/1151, wskazano wątpliwości co do tożsamości osoby lub zdolności prawnej, lub zdolności do czynności prawnych strony, przy czym katalog ten nie jest zamknięty. W sytuacji odmowy dokonania czynności notarialnej z wykorzystaniem środków wideo notariusz odsyła zainteresowane strony do tradycyjnej procedury, co ma na celu przede wszystkim wyeliminowanie wątpliwości, które powstały w trakcie zdalnej komunikacji. Istnieje również inne rozwiązanie – notariusz zamiast odmawiać dokonania czynności za pomocą środków komunikacji wideo, może kontynuować czynność i udokumentować powzięte przez niego wątpliwości w protokole. Metoda ta może być rozwa-

⁸ Pełna nazwa aktu: *Gesetz betreffend die Gesellschaften mit beschränkter Haftung* – Ustawa o spółkach z o.o., dalej jako: GmbHG; dodany ust. 3 w § 2 GmbHG będzie brzmiał: „Notarialne poświadczenie aktu założycielskiego i umowy spółki oraz uchwał wspólników podjętych w trakcie tworzenia spółki może, w przypadku tworzenia spółki bez wkładów niepieniężnych, być również dokonane za pomocą środków komunikacji wideo zgodnie z § 16a–16e Ustawy o notariacie. W tym przypadku, niezależnie od ust. 1 zd. 2, kwalifikowany podpis elektroniczny wszystkich wspólników jest wystarczający do złożenia podpisu. Utworzenie za pomocą środków komunikacji wideo może również odbywać się w drodze procedury uproszczonej zgodnie z ust. 1a z wykorzystaniem wzorców protokołów określonych w załączniku Nr 2. W przypadku korzystania ze wzorców protokołów określonych w załączniku Nr 2 stosuje się odpowiednio ust. 1a zd. 3–5”.

⁹ Zgodnie z § 5a GmbHG jest to spółka, która została założona z kapitałem zakładowym mniejszym niż 25 000 euro i jednocześnie w nazwie firmy musi używać oznaczenia „*Unternehmergesellschaft (haftungsbeschränkt)*” lub „UG (*haftungsbeschränkt*)”.

¹⁰ *Beurkundungsgesetz* – ustawa o dokonywaniu poświadczeń urzędowych; dalej jako: *Beurkundungsgesetz*.

¹¹ Pojęcie to oznacza komunikację bliskiego zasięgu (*Near Field Communication*) wykorzystywaną między innymi do realizacji płatności za pomocą telefonu komórkowego lub zapewnienia dostępu do pomieszczeń – zob. S. Piątek, Prawo telekomunikacyjne. Komentarz, Legalis/el. 2019.

¹² Bundesministerium der Justiz und für Verbraucherschutz, Entwurf eines Gesetzes zur Umsetzung der Digitalisierungsrichtlinie (dokument elektroniczny), s. 107, https://www.bmjd.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_DiRUG.pdf;jsessionid=-4CACB819C5C2CF3478159094624D1B66_1_cid324?__blob=publication-File&v=1 (dostęp z 2.3.2021 r.); dalej jako: Projekt ustawy w sprawie wdrożenia dyrektywy 2019/1151.

¹³ Projekt ustawy w sprawie wdrożenia dyrektywy 2019/1151, s. 110.

¹⁴ *Ibidem*.

żana w wyjątkowych przypadkach, jeżeli notariusz dojdzie do wniosku, że istniejące wątpliwości nie mogą zostać rozwiązane również w ramach procedury tradycyjnej¹⁵.

W uzasadnieniu do Projektu ustawy w sprawie wdrożenia dyrektywy 2019/1151 wskazano, iż wykorzystanie środków komunikacji wideo jest najbardziej odpowiednie z dostępnych cyfrowych narzędzi, ponieważ jako jedyne umożliwia wiarygodne ustalenie przez notariusza w czasie rzeczywistym zdolności stron do zawarcia umowy i swobodnego kształtowania ich woli¹⁶. Inne formy komunikacji na odległość nie nadają się w równym stopniu do odczytywania treści aktów notarialnych i osobistego zbadania przez notariusza woli stron i wyczerpującego ustalenia faktów, na których opiera się umowa.

Dokonana czynność prawna zostaje udokumentowana przez notariusza w formie elektronicznej, zamiast dokumentu papierowego, jak przy dokonywaniu czynności notarialnych w tradycyjny sposób¹⁷. Utworzony dokument elektroniczny jest traktowany jako oryginał, co umożliwia zastąpienie podpisu tradycyjnego składanego na dokumencie papierowym przez podpisanie dokumentu elektronicznego za pomocą elektronicznych podpisów kwalifikowanych¹⁸. Proponowane regulacje odnoszą się również do określenia miejsca dokonywania czynności notarialnej, z racji tego, że uczestnicy nie spotykają się fizycznie w tym samym miejscu, lecz w różnych miejscach i są połączeni ze sobą jedynie za pomocą środków komunikacji wideo. W tym względzie decydujące o miejscu czynności notarialnej jest miejsce sporządzania dokumentu elektronicznego przez notariusza¹⁹.

Z uwagi na to, że w procedurze zdalnej nie jest możliwe podpisanie dokumentów własnoręcznie przez strony, konieczne jest opatrzenie ich podpisami elektronicznymi. Dotyczy to wszystkich osób uczestniczących w dokonywanej czynności notarialnej – stron i notariusza – a ponadto także tłumaczy, mediatorów, świadków lub drugiego notariusza²⁰. Ze względu na to, że podpisy elektroniczne zastępują podpisy tradycyjne, przejmują one funkcję autoryzacji oraz wywołują ten sam skutek prawny²¹. Notariusz oraz strony muszą samodzielnie złożyć podpis elektroniczny. W przypadku naruszenia tego wymogu elektroniczna czynność notarialna nie zostanie sporządzona w sposób ważny²².

Identyfikacja za pomocą środków komunikacji wideo

Identyfikacja elektroniczna to „proces używania zestawu danych umożliwiających ustalenie tożsamości osoby, unikalnie związanych z tą osobą”²³. Unikalność danych w tym kontekście należy rozumieć jako niepowtarzalność, która pozwala na jednoznaczne ustalenie tożsamości określonej osoby²⁴. Notariusz jest zobowiązany do poprawnego ustale-

nia tożsamości stron czynności notarialnej przy zachowaniu szczególnej ostrożności²⁵. Związane jest to przede wszystkim z faktem, że ustalenia dotyczące tożsamości stron w rejestrach państwowych, do których składane są dokumenty sporządzone przez notariusza, przyjmowane są bez dalszego badania²⁶. Po wpisaniu ich do rejestru handlowego objęte są rękojmią wiary publicznej i są ogólnie uznane za prawidłowe. Notariusz w trakcie dokonywania czynności notarialnej powinien „zbadać wolę stron uczestniczących w czynności, wyjaśnić stan faktyczny sprawy, pouczyć strony uczestniczące o skutkach prawnych transakcji oraz zamieścić ich oświadczenia w sposób jasny i jednoznaczny w protokole. Czyniąc to, zapewnia on unikanie błędów i wątpliwości oraz dba o to, aby niedoświadczeni i niewykwalifikowani uczestnicy nie byli poszkodowani”²⁷. Ponadto właściwa identyfikacja stron przez notariusza jest również ważnym elementem skutecznego zapobiegania przestępstwom, w szczególności w zakresie prania pieniędzy, finansowania terroryzmu, uchylania się od płacenia podatków, niewypłacalności i innych przestępstw gospodarczych. Wiarygodna identyfikacja stron ma zatem dwójakie znaczenie – z jednej strony chroni interesy stron umowy, z drugiej zaś zapobiega wyrządzeniu szkody ogółowi społeczeństwa²⁸.

Proponowana w Projekcie ustawy w sprawie wdrożenia dyrektywy 2019/1151 zmiana przepisów dotyczących identyfikacji stanowi uzupełnienie istniejących ogólnych wymogów w zakresie identyfikacji stron w procedurze online. Za proces identyfikacji odpowiedzialny jest notariusz, który ocenia wiarygodność podawanych przez strony informacji w sposób swobodny i sumienny. Jednocześnie Projekt ustawy w sprawie wdrożenia dyrektywy 2019/1151 przewiduje

¹⁵ Projekt ustawy..., s. 112.

¹⁶ Projekt ustawy..., s. 110.

¹⁷ Projekt ustawy..., s. 112.

¹⁸ Projekt ustawy..., s. 113.

¹⁹ *Ibidem*.

²⁰ *Ibidem*.

²¹ Projekt ustawy..., s. 114.

²² *Ibidem*.

²³ Ł. Goździaszek, Identyfikacja elektroniczna i usługi zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym Unii Europejskiej. Komentarz, Legalis/el. 2019. Potocznie identyfikację elektroniczną określa się mianem eID.

²⁴ *Ibidem*.

²⁵ Zob. *Urteil des Bundesgerichtshofs vom 20. März 1956 – III ZR 11/55* – wyrok Trybunału Federalnego z 20.3.1956 r., III ZR 11/55 (dokument elektroniczny), https://www.prinz.law/urteile/bgh/III_ZR_11-55 (dostęp z 2.3.2021 r.).

²⁶ Projekt ustawy..., s. 115; zgodnie z § 415 *Zivilprozessordnung* (Ustawa o postępowaniu cywilnym) „Dokumenty sporządzone w przepisanej formie przez organ władzy publicznej w granicach jego urzędowych kompetencji lub przez osobę posiadającą władzę publiczną w zakresie powierzonej jej działalności (dokumenty urzędowe), jeżeli zostały sporządzone w związku z oświadczeniem złożonym przed tym organem lub osobą uwiarytelniającą, stanowią pełnoprawny dowód czynności stwierdzonej przez ten organ lub osobę uwiarytelniającą”.

²⁷ § 17 *Beurkundungsgesetz*.

²⁸ *Ibidem*.

dwa rodzaje możliwych środków identyfikacji elektronicznej. Z jednej strony jest to elektroniczny dowód tożsamości²⁹. Z drugiej strony w procedurze online dopuszcza się elektroniczne środki identyfikacji wydane przez inne państwo członkowskie UE i przeznaczone do celów uwierzytelniania transgranicznego, zgodnie z art. 6 rozporządzenia Parlamentu Europejskiego i Rady (UE) 910/2014 z 23.7.2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE³⁰, które są zgodne z wysokim wymogiem bezpieczeństwa w rozumieniu art. 8 ust. 2 lit. c wspomnianego rozporządzenia eIDAS i które umożliwiają elektroniczny odczyt przechowywanych danych osobowych, w tym oficjalnego cyfrowego zdjęcia posiadacza, w celu umożliwienia notariuszowi porównanie zdjęcia. Projekt ustawy w sprawie wdrożenia dyrektywy 2019/1151 korzysta z możliwości przewidzianej w art. 13b ust. 2 dyrektywy 2019/1151, zgodnie z którą państwa członkowskie mogą odmówić uznania elektronicznych środków identyfikacji, jeżeli nie spełniają one wymogów określonych w art. 6 ust. 1 rozporządzenia eIDAS. Jednocześnie w uzasadnieniu do Projektu ustawy w sprawie wdrożenia dyrektywy 2019/1151 wskazano na fakt, że w procedurze online stosowane są tylko takie środki identyfikacji, które umożliwiają notariuszowi elektroniczny odczyt przechowywanych danych osobowych, w tym oficjalnego zdjęcia cyfrowego, w celu umożliwienia notariuszowi porównania zdjęcia. W ten sposób notariusz może porównać wizerunek osoby, z którą porozumiewa się za pomocą środka komunikacji wideo z odczytanym zdjęciem posiadacza użytego środka identyfikacji, a tym samym upewnić się co do jego tożsamości. Zatem zasadniczym elementem nowej procedury identyfikacji online jest odczytanie zdjęcia i innych danych z chipu znajdującego się w elektronicznym dowodzie osobistym, należącym do strony umowy, a następnie porównanie obrazu odczytanego zdjęcia z wyglądem osoby biorącej udział w czynności notarialnej. Ten sposób ustalenia tożsamości osób z wykorzystaniem środków komunikacji wideo mają umożliwiać proponowane przepisy § 16c *Beurkundungsgesetz* oraz § 20 ust. 6 *Personalausweisgesetz*³¹. Tak określona identyfikacja pozwala na bezpieczny dostęp do danych osobowych i fotografii, podobnie jak w przypadku procedury bezpośredniej, a notariusz może w ten sposób wypełnić w wymaganym zakresie swoje prawne obowiązki identyfikacyjne³².

Jeżeli strona nie działa sama przy dokonywaniu czynności prawnej, ale jest reprezentowana przez pełnomocnika, notariusz musi zweryfikować pełnomocnictwo. Z racji tego, że załączenie w oryginale lub uwierzytelnionej kopii pełnomocnictwa jest niemożliwe, gdyż zapis elektroniczny z czynności notarialnej jest sporządzany w formie dokumentu elektronicznego, konieczne jest przedłożenie oryginału lub uwierzytelnionej elektronicznie kopii dowodu reprezentacji³³.

Jeśli nie jest możliwe techniczne uzyskanie elektronicznych kopii dokumentów zgodnych z wymogami państw członkowskich, dokumenty mogą być w drodze wyjątku dostarczane do notariusza w formie papierowej, co nie narusza wymogu określonego w art. 13g ust. 1 dyrektywy 2019/1151³⁴.

Procedura mieszana

Paragraf 16e *Beurkundungsgesetz* otwiera możliwość dokonania czynności notarialnej w sposób mieszany, w którym jedna ze stron dokonuje czynności w obecności notariusza, a druga za pomocą środków komunikacji wideo³⁵. W takim przypadku należy sporządzić dwa dokumenty o identycznej treści. Jeden dokument zostaje podpisany przez fizycznie obecne strony, natomiast drugi jest sporządzony w formie elektronicznej oraz podpisany – przez strony połączone za pomocą środków komunikacji wideo – kwalifikowanymi podpisami elektronicznymi. Fakt, że dana czynność notarialna została dokonana w drodze procedury mieszanej, należy odnotować w protokołach do obu czynności notarialnych. Jednocześnie oba protokoły uzyskują ten sam numer w rejestrze dokumentów, co ma gwarantować dostępność do pełnej dokumentacji w jednym miejscu. Szczegóły dotyczące przechowywania protokołów są zastrzeżone do uregulowania w drodze rozporządzenia.

Podsumowanie

Niewątpliwie problematyka dokonywania czynności prawnych online, bez fizycznego udziału stron nabiera coraz większego znaczenia, co widać również w kierunku obranym przez organy unijne, które chcąc sprostać współczesnym wyzwaniom, wyznaczają nowe standardy działania jednostek, przedsiębiorstw, jak też organów państwowych, oparte na nowoczesnych rozwiązaniach technologicznych. Wprowadzenie procedury założenia spółki z o.o. w sposób w pełni zdalny stanowi krok ku szerokiej cyfryzacji czynności prawnych dokonywanych przez przedsiębiorców i wydaje się naturalną konsekwencją współczesnego sposobu funkcjonowania społeczeństwa. Rozwiązanie proponowane przez niemieckie Ministerstwo Sprawiedliwości i Ochrony Konsumentów będące

²⁹ Projekt ustawy..., s. 116.

³⁰ Dz.Urz. UE L Nr 257, s. 14; dalej jako: rozporządzenie eIDAS.

³¹ Pełna nazwa ustawy: *Gesetz über Personalausweise und den elektronischen Identitätsnachweis* – Ustawa o dowodach osobistych i elektronicznym dowodzie tożsamości.

³² Deutscher Notarverein, Referentenentwurf eines Gesetzes zur Umsetzung der Digitalisierungsrichtlinie (DiRUG) Ihr Schreiben vom 17. Dezember 2020 (Az. III A 5 -9520/3822-1-31 551/2020) (dokument elektroniczny), s. 2, https://www.dnotv.de/wp-content/uploads/StN-DNotV_V_RefE-DiRUG_final_20210115.pdf (dostęp z 2.3.2021 r.).

³³ Projekt ustawy..., s. 117.

³⁴ Projekt ustawy..., s. 118.

³⁵ *Ibidem*.

implementacją dyrektywy 2019/1151 jest odpowiedzią na rosnące potrzeby i oczekiwania niemieckich obywateli, a przede wszystkim daje im wybór między tradycyjną procedurą założenia spółki a procedurą przy użyciu wideokonferencji. Powszechny dostęp do nowoczesnych technologii, a także wielość metod umożliwiających komunikację na odległość z niemalże każdego miejsca powoduje, że nie jest konieczne tworzenie zupełnie nowych rozwiązań i procedur od podstaw, lecz można wykorzystać dostępne narzędzia, odpowiednio dopasowując je i modyfikując, tak aby odpowiadały celom i wymogom prawa. W rozwiązaniu niemieckim na pierwszy plan wysuwa się bezpieczeństwo. Przebieg utworzenia spółki kontroluje notariusz, który uczestniczy w procedurze (tak jak

w formie tradycyjnej) i ma możliwość odmowy dokonania czynności notarialnej w razie powzięcia wątpliwości, przykładowo co do tożsamości stron. Ponadto procedura online może odbywać się tylko za pośrednictwem systemu udostępnionego i zarządzanego przez organ państwowy – Federalną Izbę Notarialną, przez co osoby trzecie nie mają dostępu do informacji i danych zawartych w aktach notarialnych. Jednocześnie, co podkreśla się w uzasadnieniu do Projektu ustawy w sprawie wdrożenia dyrektywy 2019/1151, sądy rejestrowe nadal będą odgrywały decydującą rolę w procedurze tworzenia spółek handlowych³⁶.

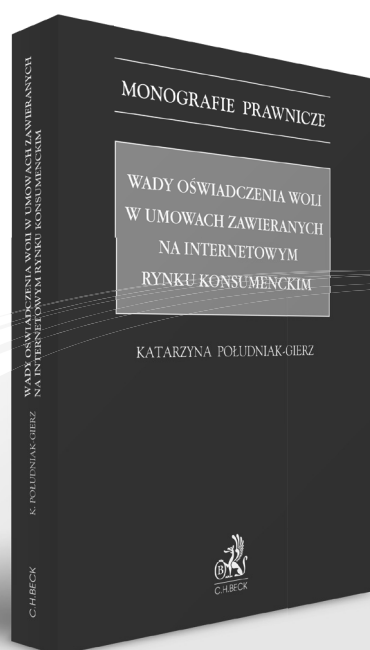
³⁶ Projekt ustawy..., s. 71.

Słowa kluczowe: dyrektywa 2019/1151, spółka z o.o., elektroniczna identyfikacja, komunikacja wideo.

Setting up a limited liability company online while using means of video communication based on implementation of Directive 2019/1151 to German law

The purpose of this article is an attempt to present the solutions proposed by the Federal Ministry of Justice and Consumer Protection in Germany that respond to the requirements introduced by Directive (EU) 2019/1151 of the European Parliament and of the Council of 20 June 2019 amending Directive (EU) 2017/1132 regarding the use of digital tools and processes in company law. The changes introduced by Directive 2019/1151 assume, among other things, a procedure for setting up a limited liability company fully online, in which communication with a notary takes place via electronic system. Consequently, the main background for consideration will be the regulations establishing rules for making declarations of will via means of video communication without the physical attendance of the parties to the contract in the notary's office.

Keywords: Directive 2019/1151, limited liability company, electronic identification, video communication.



Internetowy rynek konsumencki

ksiegarnia.beck.pl

Zadzwoni: 81 46 13 300

E-mail: kontakt@beck.pl



C.H. BECK

Prawa własności intelektualnej wobec rozwoju technologii sztucznej inteligencji

Jakub Wyczik¹

Artykuł przedstawia najistotniejsze zagadnienia dotyczące praw własności intelektualnej w dziedzinie sztucznej inteligencji (AI). Celem jest wyjaśnienie pojęcia AI z zachowaniem spójności terminologicznej z naukami informatycznymi, a następnie analiza ram prawnych regulujących zasady wykorzystywania danych do budowy AI, ochronę systemów AI jako takich (ze szczególnym uwzględnieniem ochrony programów komputerowych oraz możliwości patentowania wynalazków w tym zakresie), jak również wyników generowanych przez tego rodzaju rozwiązania. Na końcu artykułu autor przedstawia do ogólnego rozważenia propozycję uregulowania „własności” danych w erze gospodarki cyfrowej.

Uwagi wstępne

Rozwój technologii AI² stanowi współcześnie prawdopodobnie najbardziej burzliwy temat debaty naukowej. Wiele dziedzin nauki pozostaje zainteresowanych rozwojem AI, poczynając od pierwotnych nauk związanych z tym zagadnieniem dotyczących technologii informatycznych poprzez nauki prawne oraz wiele innych. Wyzwania związane z postępem technologicznym w tym zakresie zostały dostrzeżone na arenie międzynarodowej. Pośród tych podmiotów znalazła się także UE, która za cel postawiła sobie wyprzedzenie rozwoju technologicznego i uczynienie Unii światowym liderem w dziedzinie technologii AI³. Aktualny etap prac dobrze obrazują trzy sprawozdania Parlamentu Europejskiego przyjęte 20.10.2020 r. w sprawie aspektów etycznych AI⁴, odpowiedzialności cywilnej za AI⁵ oraz praw własności intelektualnej w dziedzinie rozwoju technologii AI⁶. Szczegółowe omówienie każdego z nich zasługuje na osobne opracowanie. Niemniej celem niniejszego artykułu jest przedstawienie wybranych aspektów ostatniego z wymienionych dokumentów i poddanie go pod dalsze rozważania. Jednocześnie na etapie pisania niniejszego artykułu oczekiwano, że Komisja Europejska opublikuje projekt wniosku legislacyjnego w sprawie AI w pierwszym kwartale 2021 r., co ostatecznie nastąpiło 21.4.2021 r.⁷ Jakkolwiek regulacje praw własności intelektualnej nie znalazły swojego miejsca w tym projekcie, zatem bez wątpienia zasługują na poddanie ich gruntownej rewizji, a przynajmniej weryfikacji, z uwagi na ciągły postęp technologiczny. Prace w tym zakresie zostały zapowiedziane przez Komisję Europejską, która pod koniec listopada 2020 r. opublikowała Plan działania w zakresie własności intelektualnej wspierający odbudowę i odporność UE⁸, wskazując za cel m.in. zagwarantowanie, by system ochrony własności intelektualnej był dostosowany do ery gospodarki cyfrowej. Równolegle zdają się trwać prace w WIPO, które 29.5.2020 r. opublikowało zmieniony dokument tematyczny dotyczący polityki w dziedzinie własności intelektualnej i AI⁹.

Analizując zawarte w powyższych dokumentach propozycje oraz obecne ramy prawne, możemy uznać, że o prawach własności intelektualnej wobec AI będziemy mówić przede wszystkim w kontekście:

- ochrony „klasycznych” utworów,
- ochrony programów komputerowych¹⁰,

¹ Autor jest doktorantem na Uniwersytecie Śląskim w Katowicach w obszarze badawczym nauk prawnych.

² Na potrzeby treści niniejszego artykułu, odnosząc się do sztucznej inteligencji, autor posługuje się zasadniczo bardziej precyzyjnym, angielskim akronimem AI (*Artificial Intelligence*).

³ Zob. <https://ec.europa.eu/digital-single-market/en/artificial-intelligence> (dostęp z 16.2.2021 r.).

⁴ Rezolucja Parlamentu Europejskiego z 20.10.2020 r. zawierająca zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii [2020/2012(INL)], https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_PL.html (dostęp z 16.2.2021 r.).

⁵ Rezolucja Parlamentu Europejskiego z 20.10.2020 r. z zaleceniami dla Komisji w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję [2020/2014(INL)], https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_PL.html (dostęp z 16.2.2021 r.).

⁶ Rezolucja Parlamentu Europejskiego z 20.10.2020 r. w sprawie praw własności intelektualnej w dziedzinie rozwoju technologii sztucznej inteligencji [2020/2015(INI)], https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_PL.html (dostęp z 16.2.2021 r.).

⁷ Wniosek Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii, COM(2021) 206 final, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206> (dostęp 5.7.2021 r.).

⁸ Bruksela, 25.11.2020 r., COM(2020) 760 final; <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020DC0760> (dostęp z 16.2.2021 r.).

⁹ Revised Issues Paper on Intellectual Property Policy and Artificial Intelligence, WIPO/IP/AI/2/GE/20/1 REV., https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=499504 (dostęp z 16.2.2021 r.).

¹⁰ Zgodnie z art. 1 ust. 1 dyrektywy Parlamentu Europejskiego i Rady 2009/24/WE z 23.4.2009 r. w sprawie ochrony prawnej programów komputerowych (Dz.Urz. UE L Nr 111, s. 16; dalej jako: dyrektywa 2009/24/WE), programy komputerowe chronione są jak utwory literackie, jednak ze swojej natury ich regulacja podyktowana jest szeregiem odmienności. Warto zauważyć, że zgodnie z utrwalonym orzecznictwem TS pojęcie utworu w ogólności jest autonomicznym pojęciem prawa Unii, które należy interpretować w sposób jednolity – zob. wyrok z 12.9.2019 r., C-683/17, w sprawie Cofemel – Sociedade de Vestuário SA przeciwko G-Star Raw CV, ECLI:EU:C:2019:721. W tym kontekście należy pamiętać, że zgodnie z art. 1 ust. 3 dyrektywy 2009/24/WE program komputerowy podlega ochronie, jeżeli jest oryginalny w takim rozumieniu, że jest własną intelektualną twórczością jego autora. Żadnych innych kryteriów nie stosuje się przy dokonywaniu jego kwalifikacji do ochrony.

- ochrony baz danych¹¹,
- ochrony tajemnicy przedsiębiorstwa¹²,
- praw własności przemysłowej, w szczególności patentów.

W celu odpowiedniego przedstawienia jednak zakresu ich oddziaływania należy w pierwszej kolejności wyjaśnić istotę AI, zważywszy na fakt, że współcześnie przedstawiciele nauki odnoszą się do tego pojęcia w sposób niejednolity, używając często powiązanej z nim terminologii jako synonimów¹³.

Pojęcie AI

Prawom własności intelektualnej przeciwstawia się pojęcie AI. Celem niniejszego fragmentu nie jest kompleksowe przytoczenie literatury prawniczej, lecz wskazanie przedmiotu regulacji od strony pragmatycznej, z punktu widzenia dziedziny techniki, która zajmuje się tworzeniem tego rodzaju rozwiązań. Jedynie na potrzeby dyskursu naukowego należałoby wskazać, że współcześnie podejmowane są liczne próby klasyfikacji AI, przy jednocześnie zbiorczym podejściu do szerszego pojęcia technik algorytmicznych¹⁴. Na etapie prac legislacyjnych bardzo często jednak przedstawia się szerokie rozumienie pojęcia AI. Przykładowo na potrzeby zaleceń dla przygotowujących projekt rozporządzenia w sprawie zasad etycznych AI uznano, że „sztuczna inteligencja” oznacza system, który opiera się na oprogramowaniu albo na wbudowanym urządzeniu i wykazuje się inteligentnym zachowaniem poprzez między innymi gromadzenie, przetwarzanie, analizowanie i wyciąganie wniosków dotyczących otoczenia oraz podejmowanie działań, w pewnym stopniu autonomicznie, aby osiągnąć konkretne cele¹⁵. Nie ulega wątpliwości, że takie podejście prowadzi do objęcia pojęciem AI wielu różnych wariantów tego rodzaju technologii. Wydaje się jednak, że uniwersalne podejście do regulowania AI jest w praktyce niemożliwe, wobec czego należałoby skupić się na rozwiązaniach sektorowych¹⁶.

Tymczasem AI powszechnie uważane jest za rodzaj nauki i inżynierii polegający na tym, by komputery zachowywały się w sposób, który do niedawna wymagał ludzkiej inteligencji (prof. A. Moore)¹⁷. AI obejmuje wiele różnych rozwiązań, do których zaliczyć należy zarówno wykrywanie obrazów np. w autonomicznych samochodach, jak i zautomatyzowane tworzenie nowych dzieł artystycznych na bazie dostarczonych informacji¹⁸ czy inne skomplikowane rozwiązania, w szczególności w obszarze *Business Intelligence*¹⁹. Systemy technologii AI zaimplementowane są jednak także w mniej futurystycznych rozwiązaniach. Działające w ten sposób kody towarzyszą społeczeństwu od dłuższego czasu, z uwagi na ich implementację przykładowo w oprogramowaniu tłumaczącym, takim jak np. Google Translator, systemach nawigacji, tzw. autokorekcie w telefonach, czy również algorytmach w mediach społecznościowych sugerujących użytkownikom następne treści na bazie ich dotychczasowych aktywności²⁰.

Wobec powyższych, z punktu widzenia techniki, komentujący, odnosząc się do AI, może mieć zasadniczo na myśli zarówno:

- a) cały system AI, oparty na oprogramowaniu (*software*) wraz z niezbędną infrastrukturą techniczną (*hardware*);
- b) wyłącznie część programistyczną AI (*software*), czyli kod źródłowy programu komputerowego wraz z zaimplementowanymi algorytmami; jak i
- c) tylko algorytmy oparte na modelach matematycznych, czasem także wraz z danymi lub bez nich oraz innymi elementami systemu.

Należy zatem postulować, by każdorazowo autor wyraźnie zaznaczył, o jakim rozumieniu AI się wypowiada. Niniejsza praca stanowi przekrojowe omówienie problematyki AI, odnosząc się w poszczególnych fragmentach do każdego ze wskazanych powyżej elementów.

¹¹ Skupiającej się na ochronie istotnej inwestycji jakościowej i/lub ilościowej dla uzyskania, weryfikacji lub prezentacji jej zawartości (art. 7 ust. 1 dyrektywy 96/9/WE Parlamentu Europejskiego i Rady z 11.3.1996 r. w sprawie ochrony prawnej baz danych, Dz.Urz. UE L Nr 77, s. 20; dalej jako: dyrektywa 96/9/WE). „Baza danych” oznacza zbiór niezależnych utworów, danych lub innych materiałów uporządkowanych w sposób systematyczny lub metodyczny, indywidualnie dostępnych środkami elektronicznymi lub innymi sposobami (art. 1 ust. 2 dyrektywy 96/9/WE).

¹² Poufnych informacji, mających wartość handlową, które zostały podane rozsądnym działaniom do utrzymania ich w tajemnicy [art. 2 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/943 z 8.6.2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem, Dz.Urz. UE L Nr 157, s. 1; dalej jako: dyrektywa 2016/943].

¹³ Szczegółowe rozważenie wszystkich kategorii praw mogłoby z powodzeniem stać się przedmiotem rozbudowanej monografii naukowej. Charakter niniejszego artykułu naukowego i ograniczenia techniczne pozwalają skupić się wyłącznie na wybranych zagadnieniach. Autor szerzej podejmuje problematykę danych w ramach prac badawczych prowadzonych nad przygotowywaną rozprawą doktorską.

¹⁴ Zob. M. Cantero Gamito, M. Ebers, *Algorithmic Governance and Governance of Algorithms: An Introduction*, [w:] M. Ebers, M. Cantero Gamito (red.), *Algorithmic Governance and Governance of Algorithms*, 2021.

¹⁵ Por. art. 4 lit. a załącznika Nr 1 do Rezolucji Parlamentu Europejskiego z 20.10.2020 r. zawierający zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii (2020/12(INL)).

¹⁶ Zob. M. Ebers, *Regulating AI and Robotics: Ethical and Legal Challenges*, [w:] M. Ebers, S. Navas (red.), *Algorithms and Law*, Cambridge University Press 2020, s. 40 i n.

¹⁷ P. High, Carnegie Mellon Dean Of Computer Science On The Future Of AI, <https://www.forbes.com/sites/peterhigh/2017/10/30/carnegie-mellon-dean-of-computer-science-on-the-future-of-ai/?sh=c00475321979> (dostęp z 16.2.2021 r.).

¹⁸ Jak przykładowo słynny już The Next Rembrandt, <https://www.nextrembrandt.com/> (dostęp z 16.2.2021 r.).

¹⁹ Zob. https://en.wikipedia.org/wiki/Business_intelligence (dostęp z 16.2.2021 r.).

²⁰ Problematyka algorytmów wykorzystywanych w mediach społecznościowych znacząco wykracza poza ramy niniejszego opracowania, niemniej warto zauważyć, że podjęto już pierwsze kroki w celu regulacji tego problemu w ramach projektowanego rozporządzenia Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) i zmieniającego dyrektywę 2000/31/WE, Bruksela, 15.12.2020 r., (COM(2020) 825 final). Zob. również Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych), Bruksela, 15.12.2020 r., COM(2020) 842 final.

Zasadniczym podziałem przyjmowanym w dziedzinie IT jest klasyfikowanie AI w zależności od poziomu jej zaawansowania, wobec czego wyróżnia się:

- 1) *Artificial Narrow Intelligence* (ANI) – w literaturze prawniczej nazywana także „słabą AI”; skupia się wyłącznie na jednym, wąskim zadaniu do wykonania. Jest to jedyny rodzaj AI obecnie dostępny. Obejmuje różnego rodzaju „inteligentne” rozwiązania takie jak np. asystenci głosowi czy systemy wyszukiwarki Google;
- 2) *Artificial General Intelligence* (AGI) – to technologia, która działałaby na poziomie ludzkiego umysłu. Z tego powodu prawdopodobnie jej powstanie będzie wymagało trochę czasu, ponieważ do dziś nie wiadomo jeszcze wszystkiego o ludzkim mózgu, co stanowi główne wyzwanie w nauczaniu maszyny abstrakcyjnego myślenia.
- 3) *Artificial Super Intelligence* (ASI) – teoretyczna inteligencja, która dorówna, a następnie znacząco przewyższy ludzki umysł. Taka technologia musiałaby zostać uznana za bardziej zdolną niż człowiek w każdym możliwym aspekcie. AI takiego rodzaju posiadałaby nawet zdolność do odczuwania emocji i nawiązywania relacji²¹.

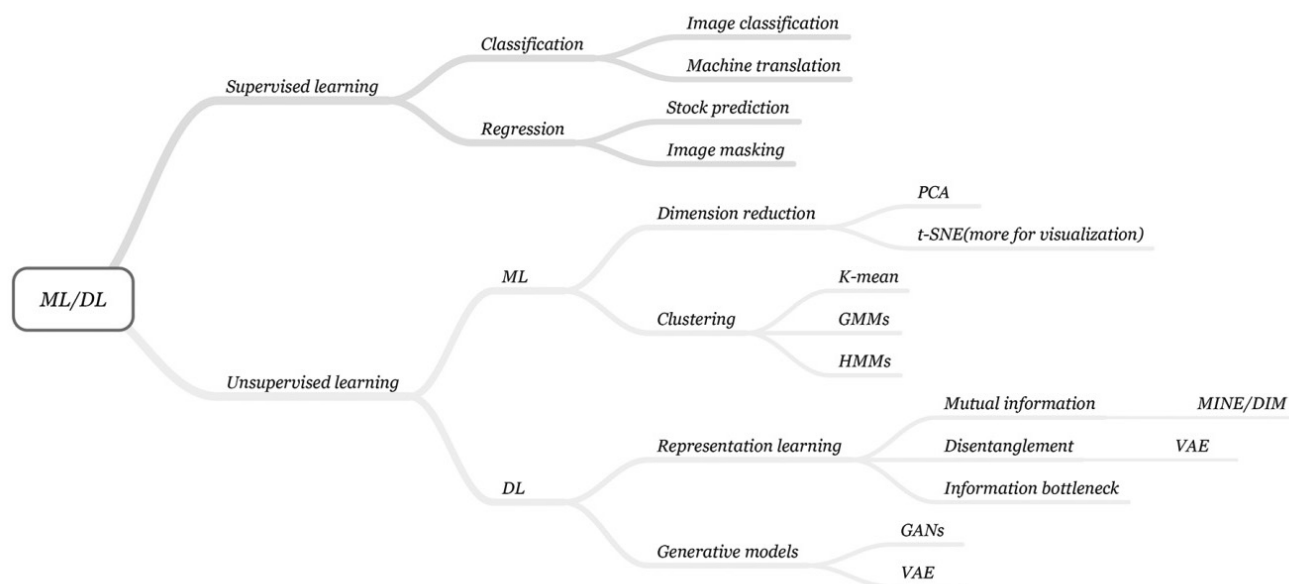
Podzbiorem AI jest tzw. *Machine Learning*. Uczenie maszynowe definiuje się jako gałąź AI, która koncentruje się na badaniu algorytmów komputerowych, które pozwalają programom komputerowym na automatyczne ulepszanie dzięki doświadczeniu²². ML jest jednym ze sposobów, których oczekujemy, aby osiągnąć AI. Nauka maszynowa polega na pracy z małymi i dużymi zbiorami danych poprzez badanie oraz porównywanie ich w celu znalezienia wspólnych wzorców i zbadania ich niuansów²³.

²¹ Zob. *Lawtomed*, AI for Legal: ANI, AGI and ASI, <https://lawtomed.medium.com/ai-for-legal-ani-agi-and-asi-cea6e7a4079e>; N. Joshi, 7 Types Of Artificial Intelligence, <https://www.forbes.com/sites/cognitive-world/2019/06/19/7-types-of-artificial-intelligence/> (dostęp z 16.2.2021 r.).

²² T. Mitchell, *Machine Learning*, McGraw Hill 1997, s. 2.

²³ Przykładowo, jeżeli modelowi uczenia maszynowego dostarczymy wiele piosenek, które odpowiadają naszym gustom wraz z ich opisem (takim jak np. tempo, gatunek muzyczny itp.), wówczas powinniśmy być w stanie stworzyć system rekomendacji, aby w przyszłości sugerować użytkownikowi nowe utwory, odpowiadające jego gustom muzycznym, tak jak robią to współcześnie platformy streamingowe, takie jak Netflix czy Spotify. Wszystko to z wykorzystaniem metod matematycznych. Warto zauważyć, że uczenie maszynowe jako gałąź AI zostało wprost wskazane w Załączniku 1 do projektu aktu w sprawie sztucznej inteligencji, COM(2021) 206 final.

Rys. 1. Drzewo algorytmów uczenia maszynowego



Źródło: Schemat S. Chen, Shukla, et al., *Machine Learning Algorithms For Beginners with Code Examples in Python, Towards AI*, 2020.

Bardziej zaawansowane algorytmy opierają się na tzw. *deep learning*, który przedstawia się zazwyczaj jako rodzaj uczenia maszynowego, polegający na tworzeniu warstwowych sieci neuronowych. Mówi się, że mają one imitować ludzki umysł, jednak te zasadniczo się od niego różnią²⁴. W praktyce mamy wówczas do czynienia z bardziej rozbudowanymi rozwiązaniami, które zawierają pewnego rodzaju ukryte powiązania mające imitować reakcje neuronowe zachodzące w ludzkim mózgu. Koncepcja „głębokiego uczenia” wykorzystuje wiele warstw do stopniowego wyodrębnienia cech wyższego poziomu z surowych danych. Przykładowo w przetwarzaniu obrazu niższe warstwy mogą identyfikować krawędzie, podczas gdy wyższe warstwy mogą identyfikować składające się z tych krawędzi cyfry, litery lub twarze²⁵.

Jak wynika z powyższych, wydaje się, że mimo wszystko mówimy nadal o systemach bazujących na programach komputerowych, przynajmniej w ujęciu informatycznym. Programowanie AI różni się od tworzenia normalnych programów tym, że w przypadku standardowego programu programista ma za zadanie stworzyć kod²⁶ rozumiany jako zestaw instrukcji i poleceń, prowadzący do uzyskania określonego rezultatu. W dużym skrócie, w przypadku natomiast AI konieczne jest przygotowanie danych wejściowych, na bazie których wyznacza się programowi pewne zadanie oraz katalog narzędzi. Następnie realizuje się proces uczenia modelu, który może polegać na tzw. uczeniu nadzorowanym i wprowadzeniu do niego danych o określonych parametrach wejściowych i wyjściowych. Zadaniem programu jest wypracowanie uniwersalnego rozwiązania, które z danych wejściowych stworzy dane wyjściowe (opracowanie algorytmu). Celem jest uzyskanie programu, który wykorzysta zdobyte doświadczenie, by automatycznie ustalać kolejne dane wyjściowe na podstawie nowych danych wejściowych. Ponadto tego typu programy mają w zamyśle autonomicznie dostosowywać się do zmian, modyfikując stworzone już algorytmy, by były adekwatne do dynamicznie zmieniającego się stanu rzeczy.

W rezultacie to, co uzyska się na skutek działania AI, w dużej mierze zależy od danych, jakie zostaną wykorzystane w trakcie uczenia programu. Dlatego też problematyka ich wykorzystania, jakości i gwarancji pozostaje w ścisłej korelacji z przedstawianym zagadnieniem, jednak jej szczegółowe omówienie zasługuje na szczegółowe opracowanie. Wyjaśniaszy jednak istotę AI, można skupić się na rozważaniach Parlamentu Europejskiego zawartych w przytoczonej we wstępie rezolucji. Na potrzeby usystematyzowania dalszych rozważań przyjęto podział oparty na cyklu produkcyjnym AI, skupiając się kolejno na:

- danych wykorzystywanych do trenowania modeli,
- systemach AI *per se* oraz
- wynikach generowanych przez tego rodzaju rozwiązania.

Ze względu na ograniczone ramy niniejszego opracowania pominięto w dalszych rozważaniach zawarte w rezolu-

lucji ogólne rozważania dotyczące AI ukierunkowanego na człowieka.

Dane wykorzystywane do trenowania modeli AI

Słusznie zauważono w rezolucji, że AI i powiązane technologie zależą w znacznym stopniu od wcześniej istniejących treści i dużej ilości danych. Bez wątpienia sformułowany postulat zapewnienia większej przejrzystości i otwartości w dostępie do niektórych danych nieosobowych i baz takich danych w Unii, zwłaszcza dla sektora MŚP i start-upów, należy uznać za słuszny. Także wskazywana w rezolucji interoperacyjność danych, która ogranicza efekt blokady technologicznej, odegra kluczową rolę w rozwoju europejskiej AI. Pierwszą inicjatywą w tym zakresie było przyjęcie instrumentów *soft law* opartych na art. 6 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z 14.11.2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej²⁷. SWIPO (ang. *Switching Cloud Providers and Porting Data*) jest wielostronnym stowarzyszeniem wspieranym przez Komisję Europejską, w celu opracowania dobrowolnych kodeksów postępowania dla właściwego stosowania powyższej regulacji²⁸. Członkami stowarzyszenia jest obecnie 26 podmiotów, pośród których znajdują się takie korporacje, jak AWS, Google, Microsoft czy SAP. Organizacja zapewnia możliwość przystąpienia przez podmioty oferujące usługi chmurowe do stosowania dotychczas opracowanych kodeksów postępowania²⁹, które dedykowane są m.in. dostawcom świadczącym usługi w modelu IaaS czy SaaS.

Na potrzeby rozwoju technologii AI konieczne jest także usunięcie „zbędnych barier prawnych” (pkt 5). Analiza danych niejednokrotnie będzie wymagała wykorzystania utworów chronionych prawem autorskim lub innych elementów ochrony praw własności intelektualnej. Probą usunięcia tych barier jest przede wszystkim wyjątek *Text & Data Mining* (TDM) zawarty w art. 3 i 4 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/790 z 17.4.2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE³⁰.

²⁴ Por. <https://bdtechtalks.com/2018/08/21/artificial-intelligence-vs-human-mind-brain/> (dostęp z 16.2.2021 r.).

²⁵ Zob. szerzej https://en.wikipedia.org/wiki/Deep_learning (dostęp z 16.2.2021 r.).

²⁶ Zob. także uwagi na temat problematyki kodów wyrażone w: D. Szostek, R. Prabucki, J. Wyczik, Kod jako prawo?, [w:] D. Szostek (red.), Legal-Tech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym, Warszawa 2021, s. 16–40.

²⁷ Dz.Urz.UE L Nr 303, s. 59.

²⁸ Zob. <https://swipo.eu/> (dostęp z 16.2.2021 r.).

²⁹ <https://swipo.eu/download-section/copyrighted-downloads/> (dostęp z 16.2.2021 r.).

³⁰ Dz.Urz.UE L Nr 130, s. 92; dalej jako: dyrektywa 2019/790. Zob. R. Markiewicz, Prawo autorskie na jednolitym rynku cyfrowym, Warszawa 2021, s. 40 i n.

Przepisy te wprowadzają wyjątki dla ochrony własności intelektualnej w zakresie praw:

- producenta bazy danych przewidzianych w art. 7 ust. 1 dyrektywy 96/9/WE;
- prawa do tymczasowego lub stałego zwielokrotniania utworu, o którym mowa w art. 2 dyrektywy 2001/29/WE oraz art. 5 lit. a dyrektywy 96/9/WE;
- praw wydawców publikacji prasowych w zakresie zwielokrotniania ich publikacji, wynikających z art. 15 ust. 1 dyrektywy 2019/790;
- prawa do trwałego lub czasowego powielania programu komputerowego oraz dokonywania jego modyfikacji [art. 4 ust. 1 lit. a) i b) dyrektywy 2009/24/WE].

Powyższe wyjątki dotyczą wyłącznie zwielokrotnień i poobrań dokonywanych w celu eksploracji tekstów i danych, za którą zgodnie z art. 2 pkt 2 dyrektywy uznaje się zautomatyzowaną technikę analityczną służącą do analizowania tekstów i danych w postaci cyfrowej w celu wygenerowania informacji obejmujących między innymi wzorce, tendencje i korelacje. W tym zakresie mogą powstać uzasadnione wątpliwości, jak należy traktować modyfikowanie pobranych danych i ich opracowywanie. Dla skutecznego wykorzystania danych w rozwoju AI zasadniczo wymagane jest najpierw ich stosowne przetworzenie, uporządkowanie czy też „oczyszczenie” (ang. *cleaning*). Dopiero później można przystąpić do trenowania na nich modeli analitycznych. Opierając się wyłącznie na wykładni literalnej, oznaczałoby to, że podmioty korzystające z rozwiązań TDM uprawnione zostaną wyłącznie do tego, aby zbierać dane, bez możliwości ich przetwarzania i dalszego wykorzystywania³¹.

Dyrektywa różnicuje zakres powyższego wyjątku w zależności od tego, czy wykorzystywane materiały chronione przeznaczone są na potrzeby badań naukowych czy do innych celów. Niemalże dowolne korzystanie z materiałów w powyższym zakresie może dotyczyć badań naukowych, jednak należy zwrócić uwagę na tę różnicę, że wyjątek dotyczący praw do programów komputerowych znajduje zastosowanie tylko na zasadach wyjątku na inne cele (art. 4 dyrektywy 2019/790)³². Jakkolwiek badania naukowe w rozumieniu dyrektywy wiążą się przede wszystkim z działalnością niekomercyjną³³, więc samo powoływanie się na prowadzenie prac badawczo-rozwojowych lub status centrum badawczo-rozwojowego, czyli bardzo popularne rozwiązania podatkowe stosowane wśród *software houses* nie przyniosą tutaj żadnych efektów.

Natomiast w przypadku wyjątku na inne cele, dedykowanego dla wszystkich zainteresowanych podmiotów, trzeba mieć na uwadze, że znajduje on zastosowanie, tylko pod warunkiem że podmioty uprawnione w odpowiedni sposób, na przykład za pomocą środków nadających się do odczytu maszynowego, nie zastrzegą wyraźnie inaczej. Tego rodzaju podejście sugeruje, że wprowadzane rozwiązanie oparto na tzw. modelu *opt-out*. Do decyzji dysponentów poszczegół-

nych treści oddano możliwość wyłączenia stosowania wyjątku TDM w tym zakresie. W rezultacie kilka słów tudzież linijek kodu pozwoli na skuteczne wyłączenie tego wyjątku w przypadku większości materiałów cyfrowych. Spoglądając na aktualne tendencje na rynku oprogramowania, wydaje się, że praktyka rynkowa będzie zmierzać właśnie w tym kierunku³⁴. Tym samym wyjątek TDM najprawdopodobniej będzie miał znikome znaczenie praktyczne w biznesie.

Przy omawianiu kwestii związanych z zasilaniem AI danymi należy także zwrócić uwagę na koncepcję otwartych danych i promowania ich dobrowolnej wymiany. Na uwagę zasługuje m.in. dyrektywa 2019/2014 o otwartych danych sektora publicznego³⁵. Podkreślono w niej, że będące w posiadaniu podmiotów tego sektora zbiory danych wysokiej wartości, obejmujące m.in. kody pocztowe, mapy krajowe i lokalne (dane geoprzestrzenne), zużycie energii i obrazy satelitarne (dane dotyczące obserwacji Ziemi i środowiska), dane *in situ* z instrumentów i prognozy pogody (dane meteorologiczne), wskaźniki demograficzne i gospodarcze (dane statystyczne), rejestry przedsiębiorstw i numery identyfikacyjne (dane dotyczące przedsiębiorstw i ich własności), znaki drogowe i śródlądowe drogi wodne (dane dotyczące mobilności) mają być udostępniane zasadniczo:

- bezpłatnie;
- w formacie nadającym się do odczytu maszynowego;
- za pośrednictwem interfejsów API oraz
- w odpowiednich przypadkach, w sposób umożliwiający zbiorcze pobieranie.

³¹ Na dodatkową uwagę zasługuje tu szczególna regulacja art. 2 ustawy 4.2.1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2021 r. poz. 1062 ze zm.), która w sposób odrębny reguluje autorskie prawa zależne do rozporządzania i korzystania z opracowań (utworów zależnych). Jak stanowi ust. 1, tego rodzaju utwory pozostają bez uszczerbku dla prawa do utworu pierwotnego.

³² Potencjalnie problematyczna jawi się w tym kontekście kwestia eksploatacji danych zawartych na stronach internetowych, którym nie sposób odmówić statusu programu komputerowego w powszechnym ujęciu. Zob. szerzej w części poświęconej ochronie samego AI.

³³ Definicja „organizacji badawczej”, do której odwołuje się art. 3, oznacza uczelnię, łącznie z należącymi do niej bibliotekami, instytut badawczy lub inny podmiot, których głównym celem jest prowadzenie badań naukowych lub działalności edukacyjnej obejmującej także prowadzenie badań naukowych: a) w sposób nienastawiony na zysk lub poprzez ponowne inwestowanie całości zysków w swoje badania naukowe; lub b) zgodnie z uznaną przez dane państwo członkowskie misją realizowania interesu publicznego; w taki sposób, że z dostępu do wyników takich badań naukowych nie może korzystać na preferencyjnych warunkach przedsiębiorstwo mające decydujący wpływ na taką organizację.

³⁴ Standardem rynkowym jest zarówno stosowanie klauzul umownych zabraniających dokonywania eksploracji danych generowanych przez oprogramowanie poza przypadkami dopuszczalnymi na podstawie bezwzględnie obowiązujących przepisów prawa, jak i korzystanie z plików typu robots.txt.

³⁵ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z 20.6.2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz.Ur. UE L Nr 172, s. 56).

Tym bardziej dziwi też tworzenie dodatkowej regulacji w tym zakresie w sprawie zarządzania danymi³⁶, podczas gdy istnieje już przyjęta dyrektywa dotycząca danych sektora publicznego. Należałoby postulować doprecyzowanie obecnych regulacji, zamiast prowadzić do dalszego rozdrobnienia i braku przejrzystości co do zakresu oddziaływania na siebie obu aktów.

Odnosząc się do koncepcji *open-source*, warto też zwrócić uwagę na *OPEN SOURCE SOFTWARE STRATEGY 2020–2023 Think Open* zawartą w komunikacie Komisji Europejskiej z 21.10.2020 r.³⁷, która zakłada propagowanie podejścia *open-source* w stosunku do rozwiązań AI. Zagadnienia związane z *open-source* budzą wiele wątpliwości prawnych, w szczególności w zakresie interpretacji poszczególnych postanowień licencyjnych³⁸. Zauważyć należy jednak, że mimo wspomnianych deklaracji, zdecydowana większość bibliotek wykorzystywanych w AI podlega właśnie licencjonowaniu w ramach idei *open-source*³⁹. Mimo że propagowanie takiego podejścia wydaje się uzasadnione, to jest ono wyraźnie spóźnione. Przedsiębiorcy działający w obszarze AI już od dawna wykorzystują rozwiązania *open-source* do dostarczania inteligentnych systemów. Jeżeli rozwiązania projektowane przez Komisję Europejską nie zaproponują w tym zakresie nic nowego, to prawdopodobnie pozostaną jedynie symbolem działania, który nie będzie w praktyce wykorzystywany. Zwłaszcza należy zwrócić uwagę, że nieuzasadnione dla projektów komercyjnych byłoby licencjonowanie oparte na modelu *copyright*⁴⁰.

Parlament podkreśla również, że należy ocenić, czy unijne przepisy dotyczące własności intelektualnej są odpowiednim narzędziem do ochrony danych, w tym danych sektorowych potrzebnych do rozwoju AI. Jednocześnie w tym samym miejscu „przypomina, że dane ustrukturyzowane, takie jak bazy danych, w przypadku gdy podlegają ochronie własności intelektualnej, zazwyczaj nie mogą być uznawane za dane”⁴¹. Trudno jest zrozumieć, co poślowie dokładnie mieli na myśli. Dane jako takie stanowią reinterpretowalne przedstawienie informacji dokonane w sposób na tyle sformalizowany, że nadaje się ono do komunikacji, interpretacji lub przetwarzania⁴². Nie ulega zatem wątpliwości, że z perspektywy prawnej dane mogą podlegać różnorodnej ochronie jako dobra niematerialne. Objęcie różnorodną ochroną nie wyklucza jednak uznania ich jako takich za dane, tym bardziej zatem budzi zdziwienie sformułowanie zawarte w rezolucji. Można się jedynie zastanawiać, czy powyższy fragment miał jednak dotyczyć innych kwestii. W szczególności wskazać można tu złożoną problematykę baz danych programów komputerowych, która to znacząco wykracza poza ramy niniejszego opracowania⁴³.

Parlament z zadowoleniem przyjmuje także zamiar Komisji dotyczący utworzenia jednolitej europejskiej przestrzeni danych. Mimo że ujednolicenie przykładowo ram prawnych

transferu danych w UE byłoby bardzo wartościowym rozwiązaniem, trzeba jednak pamiętać, że wszystkie regulacje muszą uwzględniać należyty poziom ochrony interesów podmiotów, które te dane będą udostępniać, co może być bardzo trudne w uwzględnieniu z uwagi na naciski międzynarodowych korporacji BigTech, takich jak Google czy Amazon. Niemniej Komisja Europejska zdaje się podejmować próbę walki z nadużyciami na rynku danych, czego ostatnim wyrazem jest wstępna opinia na temat praktyk ograniczających konkurencję podejmowanych przez ostatniego z powyżej wymienionych⁴⁴.

Prawa własności intelektualnej do AI

1. Osobowość prawna AI

Kolejnym istotnym zagadnieniem jest ochrona samego systemu AI. Początkowo pojawiało się wiele postulatów dotyczących przyznania AI osobowości prawnej⁴⁵. Jak wynika

³⁶ Zob. projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi), Bruksela, 25.11.2020 r., COM(2020) 767 final.

³⁷ C(2020) 7149 final.

³⁸ Tytułem przykładu można wskazać na wątpliwości związane z rozumieniem *derivative works* w stosunku do programów komputerowych korzystających z bibliotek udostępnionych na licencji GNU GPL. Mimo że konstrukcja licencji zdaje się sugerować, że słowa tego użyto zgodnie z rozumieniem „utworów zależnych”, tak jednak szczegółowa treść opracowań przygotowanych przez Free Software Foundation budzi w tym zakresie wątpliwości. W szczególności problematyczne jest ustalenie wpływu sposobu linkowania bibliotek programów na oddziaływanie licencji GNU GPL na komponenty powiązane.

³⁹ Przykładowo scikit-learn (BSD), H2O (Apache License, Version 2.0), Apache Hadoop (Apache License, Version 2.0) czy nawet środowisko programistyczne R (w zdecydowanej większości GPL-2 | GPL-3).

⁴⁰ Odpowiedni model licencjonowania *open-source* zdaje się podkreślać w rezolucji także Parlament Europejski, wskazując, że europejska strategia w zakresie danych musi zapewniać równowagę między promowaniem przepływu danych, szerokim dostępem do nich oraz ich wykorzystywaniem i udostępnianiem a ochroną praw własności intelektualnej i tajemnic przedsiębiorstwa, przy jednoczesnym poszanowaniu zasad ochrony danych i prywatności (pkt 18). Naturalnie udostępnienie wszystkich danych podmiotów prywatnych wiązałoby się z całkowitą katastrofą na europejskim rynku danych.

⁴¹ „Recalling that structured data, such as databases, when enjoying IP protection, may not usually be considered to be data”.

⁴² Zgodnie z terminologią ISO/IEC 2382-1:1993. Podobne rozumienie przedstawia się w projekcie aktu w sprawie zarządzania danymi, gdzie przez *data* rozumie się „any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording”.

⁴³ Zob. P. Polański, Some reflections on the duality of regime for software protection in the European Union, *Computer Law & Security Report* 29(3), June 2013.

⁴⁴ Amazon został oskarżony przez Komisję Europejską o tego typu praktyki z uwagi na wykorzystywanie danych dotyczących ofert niezależnych retailerów wystawiających produkty na jego platformie, w celu promowania własnych ofert, w których Amazon występuje jako bezpośredni konkurent-sprzedawca, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077 (dostęp z 16.2.2021 r.).

⁴⁵ P. Čerka, J. Grigienė, G. Sirbikytė, Is it possible to grant legal personality to artificial intelligence software systems?, *Computer Law & Security Review*, Volume 33, Issue 5, 2017, s. 685–699.

jednak z rezolucji, koncepcję tę jednoznacznie odrzucono, wskazując, że „autonomizacja w procesie tworzenia treści o charakterze artystycznym może rodzić pytania związane z tytułem do praw własności intelektualnej obejmujących te treści; [Parlament] uważa w związku z tym, że nie należy dążyć do nadania osobowości prawnej technologiom AI i wskazuje na negatywny wpływ takiej możliwości na bodźce motywacyjne dla twórców będących ludźmi” (pkt 13). Wydaje się, że jest to zabieg całkowicie słuszny, ponieważ problematycznym byłoby współcześnie uznanie, że treści generowane AI stanowią „własność” tego rodzaju algorytmu tudzież kodu programu komputerowego⁴⁶.

2. AI jako program komputerowy

Pozostawiając jednak dalsze rozważania o koncepcji osobowości AI i odnosząc się ściśle do obecnych ram prawnych własności intelektualnej, należy wskazać, że z punktu widzenia techniki mowa przede wszystkim o programach komputerowych (*software*). Wydaje się uzasadnione, by to właśnie tam poszukiwać podstawowej ochrony. Ochrona programów komputerowych w świetle prawa europejskiego wynika z regulacji dyrektywy 2009/24/WE. Jak jednak zaznaczono na samym początku aktu prawnego, ochronie podlega tylko forma wyrażenia programu komputerowego, a nie koncepcje, metody i zasady leżące u podstaw jakiegokolwiek jego elementu (art. 1 ust. 2). Prawodawca europejski nie sformułował jednak definicji legalnej przedmiotu ochrony w celu uelastycznienia tworzonych norm prawnych z uwagi na szybki rozwój technologii informatycznej⁴⁷. Pomocniczo w tym zakresie należałoby skorzystać z dokumentów sporządzonych podczas prac nad Traktatem WIPO o prawie autorskim (WCT), z których wynika, że na potrzeby projektowanego traktatu za program komputerowy uznano „zestaw instrukcji umożliwiających, po umieszczeniu na nośniku danych nadającym się do odczytu maszynowego, spowodowanie, że maszyna posiadająca możliwości przetwarzania informacji wskaże, wykona lub osiągnie szczególną funkcję, zadanie lub wynik”⁴⁸.

Realnie zasady ochrony programów komputerowych w UE ukształtowały się jednak dopiero za sprawą orzecznictwa TS. Jak wskazano wcześniej, kluczowe dla ustalenia zakresu ochrony jest udzielenie odpowiedzi na pytanie, co stanowi formę wyrażenia programu komputerowego zgodnie z art. 1 ust. 2 dyrektywy 2009/24/WE. W wyroku TS z 22.12.2010 r. w sprawie *Bezpečnostní softwarová asociace – Svaz softwarové ochrany przeciwko Ministerstvo Kultury*⁴⁹ wskazano, że z motywu siódmego dyrektywy Rady 91/250/EWG z 14.5.1991 r. w sprawie ochrony prawnej programów komputerowych⁵⁰ wynika, że „do celów tej dyrektywy pojęcie *program komputerowy* obejmuje programy w jakiegokolwiek formie, włącznie z programami zintegrowanymi ze sprzętem komputerowym”. Trybunał, odwołując się do

art. 10 ust. 1 porozumienia TRIPS⁵¹, wywnioskował, że to właśnie kod źródłowy i kod obiektowy programu komputerowego stanowią jego formy wyrażenia, które zasługują na ochronę zgodnie z rzeczoną dyrektywą⁵². Ponadto zdaniem Trybunału z powyższych wynika, że ochrona przyznana dyrektywą obejmuje program komputerowych tylko w takich wyrażeniach, które pozwalają na jego powielanie w różnych językach informatycznych (mając na uwadze wspomniany kod źródłowy i obiektowy)⁵³. Wydaje się, że takie określenie zakresu ochrony powinno być jasne, jednak w praktyce nasuwa dodatkowe wątpliwości.

W rezultacie bowiem Trybunał uznał, że formą wyrażenia programu komputerowego w rozumieniu dyrektywy nie będą takie rozwiązania, jak: interfejs graficzny⁵⁴, format plików, zbiór funkcji programu czy język programowania⁵⁵. Wątpliwe wydaje się w tym zakresie, czy obrazy generowane przez program komputerowy rzeczywiście nie stanowią jego formy wyrażenia. Dla przeciętnego użytkownika korzystanie z programu bez tego typu elementów jest bezwartościowe. Problematyka ta jest szczególnie istotna w odniesieniu do ochrony stron internetowych⁵⁶. Oczywiście należy pamiętać, że jeżeli taki interfejs nie jest chroniony jak program komputerowy, to nie oznacza, że nie może być chroniony jako inny utwór, jeżeli spełnia przesłanki do takiej ochrony⁵⁷. Powstaje jednak uzasadnione pytanie, co należy zrobić z resztą programu? Czy chronione są gotowe modele implementujące algorytmy wykorzystywane w AI, cała architektura czy też struktura logiczna programu? Analogicznie – co z danymi stanowiącymi część programu, na których wykonywane są polecenia? Zaznaczyć trzeba jednak, że nie będzie zasad-

⁴⁶ Szerzej o osobowości AI: S. Chesterman, *Artificial Intelligence and The Limits of Legal Personality*, International & Comparative Law Quarterly, Volume 69, Issue 4, 2020, s. 819–844.

⁴⁷ Definicję legalną programu komputerowego zawiera przykładowo prawo amerykańskie, w którym pod sformułowaniem *computer program* rozumie się „set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result” (17 U.S.C. § 101).

⁴⁸ Zgodnie z rozumieniem przyjętym na podstawie postanowień wzorcowych WIPO w sprawie ochrony programów komputerowych (*WIPO Model Provisions on the Protection of Computer Programs*); zob. http://www.wipo.int/edocs/mdocs/copyright/en/wipo_ip_cm_07/wipo_ip_cm_07_www_82573.doc (dostęp z 16.2.2021 r.).

⁴⁹ C-393/09, ECLI:EU:C:2010:816.

⁵⁰ Dz.Urz.UE L Nr 122, s. 42 – zastąpiona obecnie przez dyrektywę 2009/24/WE, która nie dokonała istotnych zmian w tym zakresie.

⁵¹ Zgodnie z którym programy komputerowe chronione są jak dzieła literackie na podstawie konwencji berneńskiej, zarówno w kodzie źródłowym, jak i obiektowym.

⁵² Pkt 32–34 wyroku C-393/09.

⁵³ Pkt 35 wyroku C-393/09.

⁵⁴ Pkt 39–42 wyroku C-393/09.

⁵⁵ Zob. wyrok TS z 2.5.2012 r. w sprawie *SAS Institute Inc. przeciwko World Programming Ltd*, C-406/10, ECLI:EU:C:2012:259, pkt 29–46.

⁵⁶ Zob. P. Polański, *Ochrona stron internetowych jako programów komputerowych*, [w:] K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Media elektroniczne. Współczesne problemy prawne*, Warszawa 2016, *passim*.

⁵⁷ Pkt 44–50 wyroku C-393/09.

niczo mowy o ochronie samych metod matematycznych, na których oparto modele AI⁵⁸, jednak czym innym będzie już gotowy program, który ma realizować określone funkcje, niż metoda matematyczna, która za nim stoi.

Skupiając swoją uwagę na tym, że w zasadzie dyrektywa 2009/24/WE chroni kod programistyczny, trzeba również podkreślić, że takie podejście prowadzi do błędu logicznego *ignotum per ignotum* w definiowaniu programów komputerowych. Ze swojej natury kod programu składa się zarówno z instrukcji, jak i danych, na których wykonywane są operacje⁵⁹. Niektóre instrukcje mogą zawierać dane zakodowane w strukturze programu bądź ulokowane w zewnętrznych bazach danych⁶⁰. Jeżeli polecenie odwołuje się do wyświetlenia na ekranie określonego obrazu (lub innej danej), to jego zastąpienie inną zmienną spowoduje utratę pożądanego rezultatu.

3. Ochrona patentowa AI

Wątpliwości wynikające z ochrony autorskiej prowadzą zatem do konkluzji, że w rezultacie lepszym rozwiązaniem byłoby stosowanie do AI ochrony patentowej. Problem w dochodzeniu skutecznej ochrony jest jednak analogiczny jak w prawie autorskim, konwencja o patencie europejskim wyłącza bowiem spod ochrony patentowej programy komputerowe i metody matematyczne jako takie⁶¹. Tego typu rozwiązania mogą jednak kwalifikować się do ochrony na podstawie art. 52 ust. 3 EPC, jeżeli są wykorzystywane jako część systemu AI, która przyczynia się do osiągnięcia dalszych skutków technicznych. Jak wskazuje się w podręczniku egzaminacyjnym EPO⁶², dalszy skutek techniczny musi wykraczać poza „normalne” interakcje zachodzące pomiędzy programem komputerowym a urządzeniem, na którym jest uruchamiany. W konsekwencji efekt działania programu komputerowego w postaci obiegu prądu elektrycznego w komputerze nie jest wystarczający, aby nadać programowi komputerowemu takiego dalszego efektu technicznego (G-II, 3.6)⁶³. Rozwiązania kwalifikujące się do takiej ochrony to przykładowo program komputerowy, który implementuje metodę sterowania układem ABS w samochodzie, program umożliwiający kompresję wideo⁶⁴ czy kod szyfrowania komunikacji elektronicznej (G-II, 3.6.1).

Podręcznik egzaminacyjny EPO zawiera także w części poświęconej metodom matematycznych fragment dotyczący AI i ML (G-II, 3.3.1). Wskazuje się w nim, że oba rozwiązania opierają się na modelach obliczeniowych i algorytmach na potrzeby klasyfikacji, grupowania, regresji i redukcji, do których zaliczyć należy w szczególności sieci neuronowe⁶⁵. Tego typu modele czy algorytmy mają jako takie abstrakcyjny charakter metod matematycznych, a zatem wytyczne w zakresie metod matematycznych (G-II, 3.3) znajdują do nich zastosowanie. Podkreśla się jednak, że AI i ML znajdują zastosowanie w róż-

nych dziedzinach techniki, wskazując za przykład urządzenie monitorujące pracę serca w celu identyfikacji nieregularnych uderzeń. Takie zastosowanie będzie miało charakter dalszego skutku technicznego, w rezultacie pozwalając na ochronę patentową. Analogicznie zdaniem autorów należy traktować klasyfikację obrazów cyfrowych, filmów, sygnałów dźwiękowych lub mowy w oparciu przykładowo o krawędzie lub atrybuty pikseli w odniesieniu do pierwszego z wymienionych w tym zdaniu rozwiązań. Jakkolwiek klasyfikacja plików tekstowych wyłącznie w odniesieniu do tekstu nie jest sama w sobie uważana za skutek techniczny⁶⁶.

Jednocześnie należy podkreślić, że ochrona patentowa może być przyznana wynalazkowi, jeśli jest on nowy, nieoczywisty i powstał w wyniku innowacyjnego działania. Przy czym istotną przeszkodą w zakresie uzyskania skutecznej ochrony patentowej jest wymóg kompleksowego opisu technologii, co może stanowić wyzwanie w przypadku niektórych technologii AI. Należy pamiętać, że to, co wyznacza zakres ochrony, to przede wszystkim zastrzeżenia patentowe, w myśl art. 69 EPC bowiem ochrona leży pomiędzy ścisłą interpretacją opisanych zastrzeżeń, a tym co znawcy dziedziny mogliby wywnioskować z opisu patentowego i rysunków, uwzględniając zastrzeżenia jako wskazówki.

Dodatkowe wątpliwości budzi postęp technologiczny i przesłanka nowości, która może sugerować, że stworzenie drugiego systemu AI opartego na tych samych funkcjach mogłoby napotykać problemy przy rejestracji. Implementacje AI mają tożsamy charakter z programami komputerowymi w szerokim ujęciu. Objęcie patentową ochroną szeroko rozumianej AI może negatywnie wpłynąć na rozwój rynku

⁵⁸ Jak stanowi art. 2 Traktatu WIPO: „Ochrona prawa autorskiego obejmuje formę wyrażenia, a nie idee, procedury, metody działania czy też pojęcia matematyczne jako takie”.

⁵⁹ Jak podaje Wikipedia: „In computer science and software engineering, computer software is all information processed by computer systems, including programs and data”, <https://en.wikipedia.org/wiki/Software> (dostęp z 16.2.2021 r.).

⁶⁰ Przykładowo łączonych z programem dynamicznie, https://en.wikipedia.org/wiki/Dynamic_loading (dostęp z 16.2.2021 r.).

⁶¹ Warto zauważyć, że w prawie amerykańskim nie istnieje przepis wyłączający spod takiej ochrony programy komputerowe. Wyjątki w tym zakresie wypracowało orzecznictwo, przy czym kluczowy dla ustalenia zakresu patentowalności zgłoszonych rozwiązań jest tzw. Alice/Mayo test wynikający z orzeczeń w sprawach Mayo v. Prometheus (2012) oraz Alice Corp. v. CLS Bank International (2014).

⁶² Podręcznik egzaminacyjny EPO nie jest naturalnie źródłem wiążącej organ wykładni, jednak z uwagi na swój charakter stanowi cenne źródło wiedzy dla rzeczników patentowych i osób szukających ochrony, ponieważ najlepiej obrazuje podejście organu w zakresie wydawanych decyzji.

⁶³ https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_6_1.htm (dostęp z 16.2.2021 r.).

⁶⁴ Wówczas efekt techniczny polega na zaoszczędzeniu miejsca na nośniku danych.

⁶⁵ „Artificial intelligence and machine learning are based on computational models and algorithms for classification, clustering, regression and dimensionality reduction, such as neural networks, genetic algorithms, support vector machines, k-means, kernel regression and discriminant analysis”.

⁶⁶ Podręcznik EPO wskazuje w tym zakresie decyzję w sprawie T 1358/09 (Classification/BDGB ENTERPRISE SOFTWARE) z 21.11.2014 r.

i monopolizację niektórych rozwiązań. Dopóki zatem mowa o patentach na tego typu rozwiązania, należy zachować zdrowy rozsądek przy wyznaczaniu dopuszczalności ochrony patentowej i jej zakresu⁶⁷.

4. Nadużycia w wykorzystaniu AI

Wydaje się, że rezolucja Parlamentu uzupełnia także braki w białej księdze⁶⁸ dotyczące takich wyzwań jak syntetyczne media⁶⁹. Tego typu rozwiązania wykorzystują AI do tworzenia sztucznych, fikcyjnych mediów i danych w sposób zautomatyzowany. Zjawisko to określane również mianem *deepfake*, choć oparte o powszechnie znane tworzenie nieprawdziwych informacji, polega jednak na wykorzystaniu zaawansowanych technologii opartych na *deep learningu*, obejmujących zasadniczo generatywne sieci przeciwstawne (ang. GANs)⁷⁰. W rezultacie efekty działania takich algorytmów pozwalają na zdecydowanie większą dostępność tego typu technologii, nie wymagając od korzystających rozbudowanej wiedzy i umiejętności, a nawet sprzętu⁷¹. Tym samym korzystając z dostępnych w Internecie narzędzi, można w kilka minut stworzyć krótkie nagranie, na którym zamiast twarzy celebryty znajdzie się realistycznie odwzorowana twarz innej osoby. Głównym zagrożeniem jest wykorzystanie tego narzędzia na potrzeby tworzenia pornografii bez zgody osób, których wizerunek utrwalono (*nonconsensual pornography*), jak również do manipulacji wypowiedzi osób publicznych, w szczególności w kontekście kampanii wyborczych. Omawiane zjawisko niewątpliwie zasługuje na podjęcie działań legislacyjnych, zwłaszcza że pewne państwa zdążyły już przyjąć rozwiązania w tym zakresie, które pojawiły się między innymi w Stanach Zjednoczonych czy Chinach⁷². Parlament zauważa możliwość nadużywania systemów AI w tym zakresie (pkt 17).

Wyniki działania AI

Ostatnim kluczowym elementem ochrony własności intelektualnej w kontekście AI są generowane przez tego typu rozwiązania wyniki. Problem ten wynika w szczególności z faktu, że niejednokrotnie trudno będzie dokonać prawidłowego rozróżnienia pomiędzy twórczością człowieka jedynie wspomaganą przez AI⁷³ a twórczością autonomicznie generowaną przez tego rodzaju systemy.

Kwestia treści generowanych przez AI jawi się jako niezwykle interesująca, biorąc pod uwagę, że już teraz słyszymy o ochronie twórców generowanych niemalże autonomicznie przez AI. Na uwagę zasługuje orzeczenie chińskiego Sądu w Shenzhen, w prowincji Guangdong, który orzekł, że dzieło stworzone ostatecznie przez AI kwalifikuje się do ochrony praw autorskich⁷⁴. W sierpniu 2018 r. Tencent Robot Dreamwriter napisał raport finansowy zawierający ówczesny

indeks szanghajski, kursy walutowe i przepływy kapitałowe. W artykule, opublikowanym na stronie Tencent Securities, zamieszczono klauzulę, że „artykuł został automatycznie napisany przez Tencent Robot Dreamwriter”. Pozwany skopiował powyższy artykuł na swoją własną stronę internetową, co spotkało się z reakcją w postaci rzeczzonego pozwu.

Sąd stwierdził, że forma wyrażenia artykułu jest zgodna z wymogami utworu pisemnego, a jego treść ukazuje wybór, analizę i ocenę odpowiednich informacji i danych giełdowych. W celu zapewnienia ochrony artykułu sąd uznał, że było to właśnie dzieło wspomagane przez AI. Wybór dokonany przez zespół Tencent Shenzhen w zakresie danych wejściowych, ustawień systemu, wybór szablonu i stylu są zdaniem sądu czynnościami, które zachowują bezpośredni związek ze sposobem wyrażenia artykułu. Działania te charakteryzowały się pewnym stopniem oryginalności, co pozwoliło na uznanie, że nie był to utwór autonomicznie generowany przez AI⁷⁵. Tego typu podejście budzi istotne wątpliwości w przypadku jego szerszego zastosowania. Zastanawiające jest w tym kontekście postrzeganie utworu poprzez charakter czynności podjętych celem jego stworzenia. Oparcie kryteriów ochrony wyłącznie na podstawie działań podjętych przed powstaniem utworu sugeruje, że tak wygenerowany artykuł sam w sobie nie musi być wyrażony w sposób oryginalny⁷⁶, a jedynie istotne jest, by działania,

⁶⁷ Z uwagi na ograniczone ramy niniejszego opracowania tytułem uzupełnienia warto jedynie wskazać, że amerykański organ patentowy USPTO wydał w październiku 2020 r. raport dedykowany patentowaniu AI, https://www.uspto.gov/sites/default/files/documents/USPTO_AI-Report_2020-10-07.pdf (dostęp z 16.2.2021 r.). Wnikliwa analiza raportu powinna przyświecać pracom nad ewentualną rewizją aktualnego systemu ochrony patentowej.

⁶⁸ Biała księga Komisji Europejskiej pt. „Sztuczna inteligencja – europejskie podejście do doskonałości i zaufania”, Bruksela, 19.2.2020 r., COM(2020) 65 final.

⁶⁹ Pojęcie to odnosi się do treści generowanych przez AI w celu wprowadzenia ich odbiorców w błąd. Zob. I. Dirik, Why it's time to change the conversation around synthetic media, <https://venturebeat.com/2020/08/12/why-its-time-to-change-the-conversation-around-synthetic-media/> (dostęp z 16.2.2021 r.).

⁷⁰ Zob. <https://en.wikipedia.org/wiki/Deepfake> (dostęp z 24.2.2021 r.).

⁷¹ Przykładowo tego typu możliwości daje aplikacja mobilna Reface, dostępna w Apple AppStore oraz Google Play.

⁷² Zob. M. Langer, J. Wycik, Legal aspects of deepfakes, *Annals of the Administration and Law* 2020, XX, v. 4, s. 205–212; K. Szpyt, Sztuczna inteligencja i nowe technologie (nie zawsze) w służbie ludzkości, czyli cywilnoprawna problematyka rozwoju i popularyzacji technologii deepfake, [w:] K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe*. Zagadnienia wybrane, Warszawa 2019, *passim*.

⁷³ Tak jak przykładowo grafik komputerowy korzysta z programu graficznego.

⁷⁴ *Shenzhen Tencent Computer System Co., Ltd. v. Shanghai Yingxun Technology Co., Ltd.* [(2019) Yue 0305 Min Chu 14010], 24.11.2019 r.

⁷⁵ Zob. B. Zhou, Artificial Intelligence and Copyright Protection-Judicial Practice in Chinese Courts, https://www.wipo.int/export/sites/www/about-ip/en/artificial_intelligence/conversation_ip_ai/pdf/ms_china_1_en.pdf (dostęp z 24.2.2021 r.).

⁷⁶ Co zdaje się pozostawać w świetle prawa europejskiego sprzeczne z wyrokiem TS z 11.6.2020 r. w sprawie SI i Brompton Bicycle Ltd przeciwko Chedech/Get2Get, C-833/18, ECLI:EU:C:2020:461, w tym pkt 34, który

które zostały podjęte w celu jego wygenerowania, miały taki charakter⁷⁷.

Parlament Europejski podkreśla szczególnie powyższą różnicę, zwracając uwagę, że twórczość generowana przez AI wiąże się z wieloma nowymi wyzwaniami regulacyjnymi w zakresie ochrony praw własności intelektualnej, w tym związanymi z takimi kwestiami, jak własność, wynalazczość, odpowiedniość wynagrodzenia czy potencjalna koncentracja na rynku (pkt 14). Niezależnie od tego Parlament Europejski jest zdania, że „twórczość technologiczna tworzona przez technologie AI musi być chroniona w ramach praw własności intelektualnej, aby zachęcić do inwestowania w tę formę twórczości i zwiększyć pewność prawa dla obywateli, przedsiębiorstw i wynalazców, którzy obecnie należą do najczęstszych użytkowników technologii AI” (pkt 15). Powyższe stwierdzenie, choć wydaje się oczywiste, jest kluczowe, ponieważ brak ochrony nie będzie zachęcał do inwestowania w te rozwiązania, których istotą jest przede wszystkim komercyjne wykorzystanie w sektorze biznesowym dla uzyskania przewagi konkurencyjnej. Jednocześnie w tym kontekście jeszcze raz neguje się koncepcję osobowości prawnej AI, która prowadziłaby do problemów z ustaleniem dysponentów praw własności intelektualnej⁷⁸.

Na drodze do skutecznego rozwiązania problemu ochrony treści generowanych przez AI w konsekwencji stoi przede wszystkim koncepcja autorstwa. Aktualnie niemalże powszechnie przyjmuje się, że twórcą może być tylko człowiek, co doprowadzi do uznania, że wytwory AI będą należały do domeny publicznej. Doktryna postuluje najczęściej dwa rozwiązania tego problemu: pierwsze, polegające na rozszerzeniu koncepcji autorstwa, tak by objęła ona wytwory AI, oraz drugie, zakładające objęcie tego rodzaju utworów ochroną *sui generis*⁷⁹. Pytanie, które rozwiązanie należy wybrać, pozostaje póki co bez odpowiedzi.

Szczegółowe ustalenie kompleksowego zakresu ochrony danych generowanych przez AI wymagałoby dalej idącego opracowania oraz studium indywidualnego przypadku. Uwzględnić należałoby w szczególności także ochronę tajemnicy przedsiębiorstwa, co do której można wysunąć ogólne wnioski, że tylko pewne rodzaje danych generowane przez specyficzne rozwiązania AI w sektorze biznesowym, będą mogły zostać uznane za poufne w tym sensie, że jako całość lub w szczególnym zestawie i zbiorze ich elementów nie są ogólnie znane lub łatwo dostępne dla osób z kręgów, które zwykle zajmują się tym rodzajem informacji⁸⁰.

Podsumowanie

Uważam, że w celu rozwiązania wielu przytoczonych problemów należy rozważyć zmianę podejścia do ochrony własności intelektualnej i uznać AI każdorazowo za narzędzie służące do wytwarzania treści, do których prawa przysłu-

gują osobie, w której posiadaniu znajduje się dany system. Nie jestem jednak pewien, czy powinniśmy mówić wówczas o twórczości – myślę, że ta koncepcja w dobie cyfryzacji i gospodarki opartej na danych stała się przestarzała i być może warto rozważyć inne podejście wzorowane na cywilnoprawnej „własności”.

W dzisiejszych czasach wszystko, co znajduje się w cyberświecie, ma charakter niematerialny, a jednak użytkownicy zamieszczają różne treści w Internecie, pobierają udostępnione pliki i wymieniają się nimi między sobą, jak również zdobywają wirtualne przedmioty w grach komputerowych, traktując wszystko tak, jakby stanowiło ich własność⁸¹. Należy zatem zadać pytanie, czy kluczem do rozwiązania wielu problemów nie jest dokonanie zmiany w postrzeganiu własności? Czy nie powinniśmy zatem uznać, że dane cyfrowe też mogą mieć swojego właściciela?

W tym aspekcie warto przytoczyć wyrok Trybunału z 3.7.2012 r. w sprawie *UsedSoft GmbH przeciwko Oracle International Corp.*, C-128/11⁸². Uznano w nim, że prawo do rozpowszechniania kopii programu komputerowego zostaje wyczerpane, jeśli podmiot praw autorskich, który zezwolił, choćby i nieodpłatnie, na pobranie tej kopii z Internetu na nośnik danych, również przyznał, w zamian za zapłatę ceny

stanowi, że „do celów ustalenia, czy dany produkt może być chroniony prawem autorskim, sąd odsyłający powinien zbadać, czy poprzez ten wybór formy produktu jego autor wyraził swoje możliwości twórcze w sposób oryginalny, dokonując swobodnych i twórczych wyborów, i zaprojektował ten produkt tak, by odzwierciedlał on jego osobowość”.

⁷⁷ Pytanie o minimalny wysiłek intelektualny, który gwarantuje ochronę prawa autorskiego, narasta w kontekście problematyki tzw. granicznych wytworów intelektu zob. K. Grzybczyk, *Graniczne wytwory intelektu* [w:] P. Słęzak (red.), *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, Warszawa 2017, s. 10–13. W tym zakresie należy jednak uwzględnić najnowsze orzecznictwo TS zawarte m.in. w przytoczonym już wcześniej wyroku C-683/17, pytanie o słusność dotychczasowej w sprawie *Cofemel – Sociedade de Vestuário SA przeciwko G-Star Raw CV* oraz wyroku C-833/18, w sprawie *SI i Brompton Bicycle Ltd przeciwko Chedech/Get2Get*, które rodzą koncepcji utworu prezentowanej w polskim orzecznictwie i doktrynie.

⁷⁸ „15. (...) zaleca, aby wszelkie prawa własności przysługiwały wyłącznie osobom fizycznym lub prawnym, które stworzyły utwór zgodnie z prawem, i wyłącznie za zgodą podmiotu praw autorskich, jeżeli wykorzystywane są materiały chronione prawem autorskim, chyba że mają zastosowanie wyjątki lub ograniczenia dotyczące praw autorskich (...)”.

⁷⁹ S. Navas, *Creativity of Algorithms and Copyright Law*, [w:] M. Ebers, S. Navas (red.), *Algorithms and Law*, Cambridge University Press 2020, s. 226–232. Zob. także K. Grzybczyk, *Wyzwania dla prawa własności intelektualnej w dobie cyfryzacji*, *Przegląd Prawa Konstytucyjnego* 2020, Nr 3 (55), s. 65–68.

⁸⁰ Zgodnie z definicją art. 2 pkt 1 dyrektywy 2016/943.

⁸¹ Prezentowane podejście przedstawiają także przedsiębiorcy, w tym korporacje BigTech, takie jak Microsoft, który w swoim Kodeksie postępowania Dostawcy firmy Microsoft nakazuje dostawcom „Traktować wszystkie dane przechowywane lub przesyłane przy użyciu urządzeń będących własnością firmy Microsoft lub dzierżawionych przez nią jako własność firmy Microsoft. Firma Microsoft może monitorować cały proces wykorzystywania sieci korporacyjnej i wszystkich systemów (w tym poczty elektronicznej) oraz może uzyskiwać dostęp do wszystkich danych przechowywanych lub przesyłanych za pośrednictwem sieci firmy Microsoft” (s. 12), <https://www.microsoft.com/en-us/procurement/supplier-conduct.aspx> (dostęp z 24.2.2021 r.).

⁸² ECLI:EU:C:2012:407.

mającej umożliwić mu uzyskanie wynagrodzenia odpowiadającego wartości gospodarczej kopii dzieła, którego jest on właścicielem, prawo do nieograniczonego w czasie korzystania z tej kopii⁸³. W polskiej doktrynie mówi się w tym kontekście o „koncepcji legalnego posiadacza”⁸⁴. Abstrahując od kompetencji Trybunału i jego prawotwórczego działania, trzeba jednoznacznie podkreślić, że Trybunał posługuje się wprost określeniem „własność kopii programu komputerowego”⁸⁵. Trybunał mówi wprawdzie dalej o „uprawnionym nabywcy”, jednak w kontekście argumentacji legalności działań polegających na pobraniu kopii używanego programu na swój komputer⁸⁶. Trybunał wielokrotnie powtarza przy tym, że pobranie kopii programu komputerowego i zawarcie związanej z nią umowy licencyjnej są ze sobą nierozdzielnie związane i należy je uznać za jedną całość stanowiącą transakcję sprzedaży⁸⁷. Odpowiedź na drugie i trzecie pytanie sądu odsyłającego jednoznacznie stwierdza ponadto, że „drugi nabywca tej licencji, podobnie jak każdy następny, mogą się powołać na przewidziane w art. 4 ust. 2 tej dyrektywy [2009/24/WE] wyczerpanie prawa do rozpowszechniania, i, co za tym idzie, mogą zostać uznani za uprawnionych nabywców kopii programu komputerowego w rozumieniu art. 5 ust. 1 tej dyrektywy i korzystać z przewidzianego w tym przepisie prawa do zwielokrotniania”⁸⁸. Sugeruje to wbrew przekonaniu niektórych autorów, że Trybunał wprost stwierdza, że wraz z przeniesieniem „własności kopii programu” dochodzi do przejścia na wtórny nabywcę także związanej z nią licencji, natomiast w zakresie, w jakim licencja ta nie pozwala na transfer kopii programu na rzecz kolejnego nabywcy (a tym samym na zwielokrotnienie go w takim zakresie), wówczas takie uprawnienie wynika z art. 5 ust. 1 dyrektywy 2009/24/WE.

Słowa kluczowe: sztuczna inteligencja (AI), prawa własności intelektualnej, algorytmy, dane, programy komputerowe.

Oczywiście mówiąc o samej koncepcji „własności kopii programu komputerowego”, być może Trybunał posłużył się w swoich rozważaniach nie do końca precyzyjną terminologią, jednak w moim przekonaniu, koncepcja własności danych jako dóbr niematerialnych jest co najmniej warta rozważenia. Należy jednak zwrócić uwagę, że choć w literaturze anglojęzycznej zyskuje ona coraz to więcej zwolenników⁸⁹, każdorazowo należy pamiętać, że przy tworzeniu nowych regulacji o charakterze *erga omnes* trzeba wyważyć zarówno interes publiczny polegający w tym przypadku na rozwoju technologicznym społeczeństwa, jak i prywatne interesy dysponentów praw wyłącznych, skupiające się na postrzeganiu zarówno AI, jak i danych w kategoriach majątkowych, które w szczególności budują wartość przedsiębiorstwa.

⁸³ Pkt 72 wyroku C-128/11.

⁸⁴ Zob. A. Nowicka, [w:] R. Markiewicz (red.), Komentarz do ustawy o prawie autorskim i prawach pokrewnych, [w:] Ustawy autorskie. Komentarze. Tom II, Warszawa 2021, art. 75, uw. 53–67; Z. Okoń, [w:] D. Flisak (red.), Prawo autorskie i prawa pokrewne. Komentarz, Warszawa 2015, art. 74, uw. 69–75.

⁸⁵ Zob. pkt 42–46 wyroku C-128/11. Jak stanowi pkt 46: „W tych okolicznościach transakcje, o których mowa w pkt 44 niniejszego wyroku, badane jako całość, wiążą się z przeniesieniem prawa własności kopii danego programu komputerowego” (ang. „In those circumstances, the operations mentioned in paragraph 44 above, examined as a whole, involve the transfer of the right of ownership of the copy of the computer program in question”).

⁸⁶ Pkt 73–88 wyroku C-128/11.

⁸⁷ Pkt 44, 48, 84 wyroku C-128/11.

⁸⁸ Ang. „(...) the second acquirer of the licence, as well as any subsequent acquirer of it, will be able to rely on the exhaustion of the distribution right under Article 4(2) of that directive, and hence be regarded as lawful acquirers of a copy of a computer program within the meaning of Article 5(1) of that directive and benefit from the right of reproduction provided for in that provision”.

⁸⁹ Zob. M. Ebers, Regulating AI and Robotics..., s. 68.

Intellectual property rights v. the development of artificial intelligence

This article presents the most relevant issues concerning intellectual property rights in the field of artificial intelligence (AI). The purpose of the article is to explain the concept of AI while maintaining terminological consistency with information sciences, and then to analyze the legal framework governing the principles of using data to build AI, the protection of AI systems as such (with particular emphasis on the protection of computer programs and the possibility of patenting inventions in this field), as well as results generated by such solutions. At the end of the article, for general consideration, the author presents a proposal for the regulation of data “ownership” in the era of the digital economy.

Keywords: artificial intelligence, intellectual property rights, algorithms, data, computer programs.



beckakademia
konferencje • szkolenia • webinaria