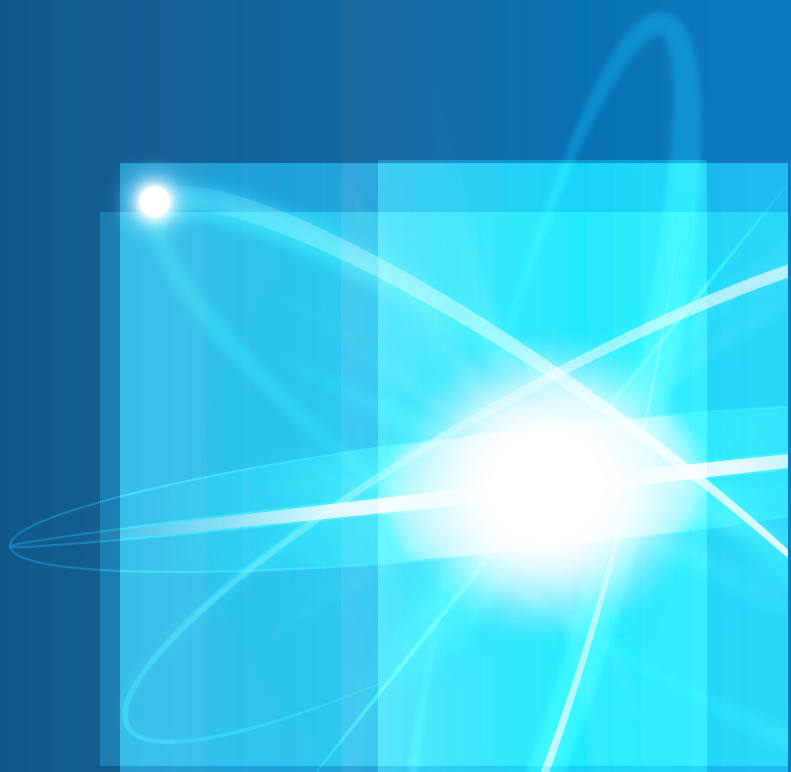
PME
3/2024

Prawo Mediów Elektronicznych

Kwartalnik Naukowy



CBKE

Dostęp online:
https://www.bibliotekacyfrowa.pl/dlibra/publication/158461
https://www.repozytorium.uni.wroc.pl/dlibra/publication/151198
https://www.pme.uni.wroc.pl
DOI: 10.34616/151198

Prawo Mediów Elektronicznych

Kwartalnik Naukowy

pod redakcją prof. Jacka Gołaczyńskiego

Uniwersytet Wrocławski
https://orcid.org/0000-0002-3295-7099

i pod redakcją dr. Rafała T. Prabuckiego
(redaktor numeru 3)

Uniwersytet Śląski
https://orcid.org/0000-0003-2397-1283

3/2024

Wrocław 2024

Czasopismo dofinansowane ze środków Ministerstwa Edukacji i Nauki
w ramach programu „Rozwój Czasopism Naukowych" (projekt nr RCN/SP/0553/2021/1).

Korekta (język polski): Sebastian Surrendra
Projekt i wykonanie okładki: Agata Jałowiecka
Skład i opracowanie techniczne: Munda Maciej Torz

Wydawca
E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa.
Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego

ISSN 2082-100X

Adres redakcji
Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii,
Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej
ul. Uniwersytecka 22/26, 51-145 Wrocław
e-mail: jacek.golaczynski@uwr.edu.pl

Wersją pierwotną (referencyjną) czasopisma jest wydanie elektroniczne.

Spis treści

DOI: 10.34616/151199

Prawo Mediów Elektronicznych. Kwartalnik Naukowy
2024, nr 3, 7–23

Justyna Doniec-Niezgoda
Uniwersytet Jagielloński
ORCID: 0000-0003-0817-3945

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

Streszczenie

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

Słowa kluczowe

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

1. Usługa hostingu, która przechowuje i rozpowszechnia publicznie informacje

Platforma internetowa to usługa hostingu, która na żądanie odbiorcy usługi przechowuje i rozpowszechnia publicznie informacje. Tych kilka słów zawiera w sobie szereg znaczeń mających wpływ na zakres zastosowania DSA. Najbardziej znaczącym elementem tej definicji wydaje się być konieczność rozpowszechniania treści, a zatem publicznego rozpowszechniania na żądanie odbiorcy, które to sfor-

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

mułowanie będzie wyłączać wiele podmiotów spod przepisów dotyczących platform internetowych. Element rozpowszechniania będzie miał w szczególności znaczenie z punktu widzenia celu samego DSA, wydaje się bowiem, że ta czynność stanowi fundament działalności użytkowników w internecie polegający na wymianie informacji pomiędzy użytkownikami. Do momentu bowiem, gdy dana treść nie zostanie publicznie rozpowszechniona na platformie na żądanie użytkownika, nie będzie ona dostępna dla innych odbiorców. Efektem tego będzie brak możliwości spowodowania zagrożeń, przed jakimi chce chronić DSA, w tym w szczególności związanych z rozpowszechnianiem nielegalnych treści lub dezinformacji.

a) Publiczne rozpowszechnianie informacji na gruncie DSA

Pojęcie publicznego rozpowszechniania informacji zostało zdefiniowane w pkt 14 preambuły DSA, w którym określono, że pojęcie „publicznego rozpowszechniania" powinno obejmować udostępnianie informacji potencjalnie nieograniczonej liczbie osób. Wykładnia tego pojęcia na podstawie preambuły DSA prowadzi do wniosku, że dostęp do informacji nie powinien być obiektywnie utrudniony. DSA wskazuje, że sytuacje, w których do usługi należy się zarejestrować lub zażądać dostępu do grupy, powinny podlegać ocenie na podstawie tego, czy rejestracja lub dostęp odbywa się automatycznie, bez konieczności potwierdzania rejestracji czy dostępu przez człowieka. Zatem wszędzie tam, gdzie dostęp do platformy będzie uzależniony od weryfikacji dostępności przez człowieka, nawet gdy na platformie będzie rozpowszechniana znaczna ilość informacji, dana platforma lub konkretna grupa wymiany informacji dostępna na platformie nie będzie musiała dostosować się pod regulacje wynikające z DSA wskazane dla platform internetowych[2]. Ten element „publiczności" został zatem niejako oderwany od celu wprowadzanej regulacji, bowiem niezależnie od zakresu publikowanych na platformie informacji oraz ich skali sam element łatwego dostępu do takiej platformy ma wpływ na rozumienie pojęcia „publiczności" i może powodować całkowite wyłączenie platform weryfikujących tożsamość użytkownika z udziałem człowieka spod reżimu platform internetowych. Z drugiej jednak strony, nie będzie miał znaczenia fakt, czy konkretny użytkownik posiadający łatwy dostęp do informacji faktycznie z niego skorzysta, istotna będzie wyłącznie możliwość takiego skorzystania.

[2] S. Gerdemann, G. Spindler, *Das Gesetz über digitale Dienste (Digital Services Act) (Teil 2)*, Gewerblicher Rechtsschutz und Urheberrecht 2023, vol. 115, s. 116.

Drugi element publicznego rozpowszechniania wymieniany w pkt 14 preambuły DSA dotyczy zakresu odbiorców informacji, która powinna być potencjalnie nieograniczoną liczbą odbiorców, nieokreśloną przez nadawcę komunikatu. Oznacza to, że na spełnienie tej przesłanki będzie miał wpływ sam usługodawca, jak i użytkownik, który będzie mógł ograniczyć zakres odbiorców usługi. Wydaje się jednak, że na właściwą kwalifikację będzie miał pośredni wpływ także sam charakter usługi i opcje dostępne na danej platformie związane z udostępnianiem treści, tj. np. czy dostawca platformy umożliwia w ogóle zawężenie kręgu odbiorców i jak będzie się kształtował dostęp do owej grupy. Co ciekawe, wydaje się, że ustawodawca europejski nie uzależnił dokonania czynności publicznego rozpowszechniania od liczby potencjalnych odbiorców, a położył nacisk wyłącznie na możliwość zapoznania się z informacją, a nie na faktyczne dostarczenie informacji do konkretnego odbiorcy czy grupy odbiorców platformy.

Mając na uwadze wskazane rozumienie „publicznego rozpowszechniania", DSA wprost wyłącza niektóre usługi jako niespełniające tej przesłanki. Usługi takie jak poczta elektroniczna lub usługi przesyłania wiadomości prywatnych (np. Messenger, Whatsapp, Telegram) nie będą podlegać pod regulacje dotyczące platform internetowych z uwagi na ograniczony przez odbiorcę usługi krąg adresatów informacji[3]. Z kolei rozpowszechnianie poprzez publiczne grupy lub otwarte kanały będzie spełniać przesłankę „publiczności". Pomiędzy tymi jasnymi przykładami wymienionymi w DSA powstaje wiele pytań w zakresie przykładów granicznych.

Wydaje się, że mając na uwadze przesłankę „publiczności", można wymienić wiele przypadków, w których dana usługa rozpowszechniania informacji dostępna na platformie nie będzie miała takiego waloru. W dodatku taka usługa może być dostępna na platformie, na której dostawca oferuje usługi zarówno uwzględniające przesłankę „publicznego rozpowszechniania", jak i jej nieuwzględniające. Jako przykład można podać platformę Facebook, która bez wątpienia podlegać będzie pod DSA, co potwierdziła także Komisja Europejska, wyznaczając Facebooka jako bardzo dużą platformę internetową na podstawie liczby użytkowników dostarczonych przez platformę[4]. Należy jednak zauważyć, że niektóre z funkcji Facebooka mogą nie być objęte zakresem zastosowania przepisów dotyczących platform internetowych z uwagi na brak spełnienia przesłanki „publiczności". Funkcje Facebooka takie jak publikowanie postów w zamkniętych grupach, tzw. prywatnych, nie

[3] *Ibidem*, s. 116.

[4] Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413 [dostęp: 25.02.2024].

będą spełniać przesłanki „publiczności", a to z uwagi na ograniczony przez odbiorcę usługi zakres osób, które będą mogły zapoznać się z treścią. Podobnie w przypadku grup, do których dostęp jest ograniczony poprzez konieczność rejestracji do nich, w szczególności, gdy dostęp jest udzielany przez zatwierdzenie dokonywane przez administratora, co w przypadku grup tworzonych na Facebooku jest możliwe. Także grupy, do których dostęp jest ograniczony poprzez konieczność odpowiedzi na określone pytania czy zadeklarowanie swojej przynależności do konkretnej grupy, np. zawodowej, będzie wyłączało możliwość zastosowania przepisów dot. platform internetowych do informacji rozpowszechnianych w takich grupach.

Jako przykład wymieniany jest także portal TikTok, w którego przypadku regulamin przewiduje możliwość tworzenia grup do 200 000 osób, zatem mając na uwadze przesłankę rozpowszechniania informacji „potencjalnie nieograniczonej liczbie osób", która zawarta jest w definicji „publicznego rozpowszechniania", takie grupy powinny w zgodzie z definicją prezentowaną w DSA być wyłączone spod regulacji rozporządzenia w zakresie dotyczącym platform internetowych[5]. Taki wniosek wydaje się całkowicie sprzeczny z celem Rozporządzenia i może być łatwo wykorzystywany przez platformy internetowe w celu omijania przepisów mających zastosowanie do platform internetowych. Z tego powodu należy się zastanowić nad możliwością wykładni omawianego pojęcia w sposób bardziej liberalny i możliwością uznania, że ograniczenie grupy do 200 000 osób przez dostawcę platformy będzie mogło spełniać definicję „potencjalnie nieograniczonej liczby osób". Wydaje się bowiem, że grupa ta jest na tyle duża, że rozpowszechnianie informacji będzie miało miejsce na bardzo szeroką skalę i liczba osób mogących zapoznać się z informacją oraz cel DSA będą uzasadniać taką wykładnię. W celu stworzenia wyraźnej wykładni tego pojęcia będzie konieczne skorzystanie z kompetencji TSUE. Należy bowiem pamiętać, że DSA wyraźnie wskazuje, że w sytuacji, gdy tylko niektóre z usług świadczonych przez dostawcę są objęte zakresem DSA, rozporządzenie będzie można stosować wyłącznie do usług, które będą wchodzić w zakres tej grupy. Jednak w pozostałym zakresie DSA nie powinno mieć zastosowania[6].

Powyższe rozumienie pojęcia publicznego rozpowszechniania jest częściowo zgodne z rozumieniem publicznego udostępniania utworów na gruncie art. 3 ust. 1 dyrektywy 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r.

---

[5] A. Peukert *et al.*, *European Copyright Society – comment on copyright and the Digital Services Act proposal*, „IIC – International Review of Intellectual Property and Competition Law" 2022, vol. 53(3), s. 5.

[6] Tak też: R. Janal, *Haftung und Verantwortung im Entwurf des Digital Services Acts*, „Zeitschrift für europäisches Privatrecht" 2021, s. 263–264.

w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz. Urz. UE L 167 z 2001 r., s. 10 z późn. zm.) i samo podobieństwo terminologiczne obu pojęć skłania do zastanowienia się nad możliwością zastosowania bogatej wykładni tego pojęcia dokonywanego przez TSUE.

Podobieństwo obu wyrażeń wydaje się istotne, mając na uwadze znaczenie pojęcia „rozpowszechniania" i „udostępniania" w języku polskim. Znamienny jest jednak fakt użycia w angielskiej wersji tekstu DSA sformułowania „dissemination information to the public" w porównaniu do „communication to the public" używanego w dyrektywie 2001/29/WE. Wydaje się, że te dwa odmienne wyrażenia oraz brak wyraźnego nawiązania w DSA, w tym w preambule, do utrwalonej interpretacji przesłanki „publiczności" oraz „udostępniania" na gruncie dyrektywy 2001/29/WE, powinien prowadzić do wniosku o konieczności traktowania obu pojęć w sposób oddzielny[7]. Co za tym idzie, nie byłoby właściwe przejmowanie przesłanek stworzonych czy utrwalonych przez TSUE w zakresie publicznego udostępniania utworów na gruncie dyrektywy 2001/29/WE.

W tym kontekście można znaleźć dalsze argumenty wskazujące na oddzielną interpretację obu pojęć. Można zauważyć brak wymienienia czy pośredniego odesłania w DSA do przesłanki „nowej publiczności", która jest obecna w orzeczeniach TSUE i w zasadzie można ją uznać za utrwaloną[8], a także podejścia do problemów związanych z interpretacją linkowania treści w internecie, częściowo rozwiązanego przez interpretacje TSUE[9]. Najistotniejszym argumentem, który uzasadniałby takie oddzielne rozumienie omawianych pojęć, jest inny cel obu aktów prawnych. Dyrektywa 2001/29/WE reguluje zasady dotyczące prawa autorskiego chroniącego utwory, a przede wszystkim ich twórców, próbując zachować właściwą równowagę pomiędzy wolnością i dostępem do informacji a należytym wynagradzaniem i ochroną praw twórców wynikających z istoty prawa autorskiego. Cel DSA jest odmienny[10].

---

[7] Tak też, jednak bez szerszego wyjaśnienia: F. Hofman, B. Raue, *Digital Services Act: Gesetz über digitale Dienste*, Baden-Baden 2023, s. 100.

[8] Np. wyrok TS z dnia 7 grudnia 2006 r. w sprawie C-306/05, *Sociedad General de Autores y Editores de España (SGAE) przeciwko Rafael Hoteles SA*, EU:C:2006:764; wyrok TS z dnia 7 marca 2013 r. w sprawie C-607/11, *ITV Broadcasting Ltd i inni przeciwko TV Catch Up Ltd*, EU:C:2013:147 i inne.

[9] Np. wyrok TS z dnia 13 lutego 2014 r., C-466/12, *Nils Svensson i inni przeciwko Retriever Sverige AG*, EU:C:2014:76 – dalej: „Wyrok Svensson"; postanowienie TS z dnia 21 października 2014 r., C-348/13, *BestWater International GmbH przeciwko Michael Mebes i Stefan Potsch*, EU:C:2014:2315; wyrok TS z dnia 8 września 2016 r., C-160/15, *GS Media przeciwko Sanoma Media Netherlands BV, Playboy Enterprises International Inc., Britt Geertruidzie Dekker*, ECLI:EU:C:2016:644, dalej: „Wyrok GS Media".

[10] Cel DSA został szeroko opisany w dokumencie Commission Staff Working Document Impact Assessment Accompanying The Document Proposal For A Regulation Of The European Parliament And Of The Council on a Single Market For Digital Services (Digital Services Act) and amending Di-

Z jednej strony jest nim także ochrona dostępu do informacji w internecie, podobnie jak w zakresie dyrektywy 2001/29/WE, jednak z drugiej strony nie ma faktycznej konieczności uwzględniania interesów twórców, którzy często są określani jako strona słabsza stosunku prawnego. DSA stoi na straży dobra wspólnego, jakim jest środowisko internetowe, oraz ochrony użytkowników internetu, a za przeciwstawną stronę, przed którą DSA niejako chroni użytkowników internetu, można uznać same platformy internetowe. W tym kontekście zatem to użytkownicy internetu stają się „słabszą stroną stosunku prawnego" i stroną, której należałoby przyznać szczególną ochronę przed praktykami stosowanymi przez dużych dostawców platform internetowych, dla których prawa jednostek nie zawsze muszą wyprzedzać ich interesy finansowe. Wydaje się zatem, że w przypadku dyrektywy 2001/29/WE konieczność ochrony praw i interesów dotyczy twórców jako strony słabszej. Wówczas, w zakresie DSA, po tej samej stronie „barykady" musieliby się znaleźć dostawcy platform internetowych, co uzasadnia zupełnie inną interpretację przesłanki „publicznego udostępniania" w porównaniu do rozumienia pojęcia „publicznego rozpowszechniania" na gruncie obu aktów, które z pozoru pozostają do siebie zbliżone. Waga interesów i podmiotów podlegających ochronie jest zupełnie inna, bowiem nie ma grupy interesariuszy, która „przeważałaby" interesami nad wartościami chronionymi w DSA takimi jak właściwie działające środowisko internetowe i uczestniczący w nim użytkownicy Internetu.

Wydaje się zatem, że z tego względu pojęcie publicznego rozpowszechniania informacji na gruncie DSA powinno być interpretowane szerzej niż pojęcie publicznego udostępniania utworów na gruncie dyrektywy 2001/29/WE. Dla przykładu, nieuprawnione byłoby dodawanie przesłanki „nowej publiczności" do wykładni publicznego rozpowszechniania na gruncie DSA. Należy bowiem zauważyć, że prawo autorskie zawiera liczne szczegółowe przepisy, co do których utrwaliła się wykładnia odnosząca się do zagadnień takich jak np. wyczerpanie prawa autorskiego. Kwestie te nie będą miały przełożenia na uregulowania zawarte w DSA, które, jak to zostało wyraźnie stwierdzone w kilku miejscach rozporządzenia, pozostawiają ochronę praw autorskich nienaruszoną[11].

W kontekście utrwalonego orzecznictwa w zakresie linkowania, który to problem można przenieść także na grunt rozpowszechniania informacji uregulowany

---

rective 2000/31/EC, Brussels, 15.12.2020 SWD(2020) 348 final, s. 36–37, wymienia się m.in. konieczność umieszczania obywateli w centrum uwagi i zapewnienie promowania ich praw podstawowych i praw konsumenta (pkt 4.2.3).

[11] Art. 2 ust. 4 lit. b) DSA.

w DSA, wydaje się, że wnioski z początkowych wyroków TSUE w tym zakresie mogłyby mieć odpowiednie zastosowanie. Podobnie jak w Wyroku Svensson należałoby dojść do wniosku, że aby doszło do publicznego rozpowszechnienia, wystarczy, aby informacja „była dostępna publiczności w sposób umożliwiający do niej dostęp, niezależnie czy z tej możliwości skorzystają”[12]. Rozumienie to jest zbieżne z tym opisywanym w pkt 14 preambuły DSA. Czytając jednak kolejne orzeczenia w sprawie linkowania, należałoby dojść do wniosku, że przesłanka umieszczania linków w celach zarobkowych bądź nie, lub wiedza o bezprawnym opublikowaniu informacji czy, jak można wyobrazić to sobie, o publikowaniu informacji stanowiących dezinformację, nie miałaby znaczenia w kontekście DSA[13]. Należy zauważyć, że wykładnia ta była dokonywana przez TSUE na podstawie głęboko zakorzenionych zasad prawa autorskiego, które nie będą mają przełożenia na grunt DSA.

Uzasadniony byłby jedynie jeden „wyłom” z powyższego wniosku, który naraża się na zarzut braku konsekwencji w zakresie prezentowanego stanowiska, ale wydaje się możliwy do obrony w kontekście celu DSA. Wskazywane już problemy dotyczące pojęcia „publiczności” byłyby możliwe do rozwiązania, gdyby można było rozumieć je podobnie jak w wyroku w sprawach połączonych C-682/18 i C-683/18, *Frank Peterson przeciwko Google LLC i inni*, tj. „pojęcie «publiczności» odnosi się do nieokreślonej liczby potencjalnych odbiorców i zakłada ponadto dość znaczną liczbę osób [wyrok z dnia 28 października 2020 r., BY (dowód z fotografii), C-637/19”[14]. Wydaje się, że w przypadku TikToka i grupy, która może posiadać do 200 000 osób, należałoby się zastanowić przy jej ocenie, nie tylko czy istnieje limit osób, ale także czy ów limit zakłada „dość znaczną liczbę osób”, która w przypadku 200 000 uczestników z pewnością musiałaby zostać uznana za „znaczną”. Wydaje się, że takie rozszerzenie interpretacji przesłanki „publiczności” byłoby zasadne także na gruncie DSA i nie stałoby w sprzeczności z jej celem.

Dla porządku należy także zaznaczyć, że pojęcie publicznego rozpowszechniania obecne w art. 4 ust. 1 dyrektywy 2001/29/WE także nie powinno mieć wpływu na rozumienie tego samego pojęcia (w polskim tłumaczeniu[15]) w zakresie DSA, bowiem reguluje ono zupełnie inne prawa.

---

[12] Wyrok Svensson, pkt 19.

[13] Przesłanki te są obecne w wyroku GS Media, pkt 30–31.

[14] Wyrok TSUE z dnia 22 czerwca 2022 r., C-682/18 i C-683/18, *Frank Peterson przeciwko Google LLC, YouTube Inc., YouTube LLC, Google Germany GmbH*, pkt 69, tak też: A. Peukert *et al.*, *op. cit.*, s. 6.

[15] W angielskim tłumaczeniu pojęcie to jest określone jako *distribution right*, co tym bardziej uzasadnia wniosek przedstawiony w tekście.

Należy jednak w tym zakresie zauważyć, że w przypadku, gdy rozpowszechniana informacja jest jednocześnie utworem, DSA pozostaje bez uszczerbku dla prawa Unii w zakresie prawa autorskiego i praw pokrewnych, w tym dyrektyw Parlamentu Europejskiego i Rady 2001/29/WE (21), 2004/48/WE (22) i (UE) 2019/790 (23), które są uznawane za akty prawa bardziej szczegółowego w zakresie ochrony praw autorskich i które powinny posiadać pierwszeństwo w ich zastosowaniu w zakresie ochrony prawnoautorskiej[16].

Konkludując, przesłanka publicznego rozpowszechniania powinna być interpretowana szeroko, zgodnie z celem DSA, którym jest stworzenie bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego. Zdaniem autorki zastosowanie wykładni obecnej na gruncie dyrektywy 2001/29/WE prowadziłoby do nieuprawnionego zawężenia pojęcia publicznego rozpowszechniania na gruncie DSA, poprzez dodanie przesłanek ugruntowanych w licznych orzeczeniach TSUE, które nie powinny być stosowane poza zakresem prawa autorskiego.

b) Wpływ użytkownika na czynność rozpowszechniania

Jako pozornie mało istotną przesłankę, ale faktycznie mającą znaczący wpływ na interpretację pojęcia platformy internetowej, należy uznać świadczenie usługi na „indywidualne żądanie odbiorcy" tej usługi. Wynika ona także ze znaczenia pojęcia usługi społeczeństwa informacyjnego, jednak została dodatkowo powtórzona przez ustawodawcę europejskiego w samej definicji platformy internetowej. Przywołując definicję zawartą w dyrektywie 2015/1535, „na indywidualne żądanie odbiorcy usług" oznacza, że usługa świadczona jest poprzez przesyłanie danych na indywidualne żądanie[17]. W dyrektywie wymienia się, że usługami nieświadczonymi na indywidualne żądanie będą np. usługi rozpowszechniania telewizyjnego czy usługi przesyłania sygnału radiowego[18]. W kontekście definicji platformy internetowej ma to o tyle znaczenie, że zakresem zastosowania DSA zostaną objęte wyłącznie te platformy, na których informacje będą publikowane i rozpowszechniane poprzez przesłanie ich do dostawcy platformy i zamieszczenie ich na platformie na żądanie konkretnego użytkownika platformy. W przypadku takich dostawców jak YouTube nie ma wątpliwości, że film umieszczany na platformie przez konkretnego użytkownika będzie świadczeniem usługi na indywidualne żądanie korzystającego z plat-

[16] Art. 1(5)(c) DSA, pkt 9 I 11 preambuły.

[17] Art. 1 lit b. pkt (iii) dyrektywy 2015/1535.

[18] Załącznik I do dyrektywy 2015/1535: „Przykładowy wykaz usług nieobjętych zakresem art. 1 ust. 1 lit. b) akapit drugi".

formy – dochodzi wówczas do czynności, podczas których użytkownik platformy wysyła żądanie zamieszczenia filmiku na platformie do dostawcy, a dostawca go zamieszcza na żądanie konkretnego, zindywidualizowanego użytkownika.

Termin „indywidualnego żądania" był przedmiotem wykładni TSUE, w szczególności w kontekście usług audiowizualnych[19]. TSUE zaznaczył, że jest istotne, czy lista filmów oferowanych w ramach usługi jest ustalana przez dostawcę usługi, czy filmy są dostępne w godzinach nadawania ustalonych przez dostawcę usługi oraz czy użytkownik ma wolny wybór programów w drodze interaktywnej. Z drugiej strony, nie ma znaczenia, czy użytkownik uzyskuje dostęp do platformy na podstawie indywidualnego kodu. W wyroku w sprawie platformy Airbnb TSUE wskazuje, że usługa ta jest świadczona na indywidualne żądanie jej odbiorców, ponieważ zakłada ona zarówno umieszczenie ogłoszenia w internecie przez wynajmującego, jak i indywidualne zapytanie najemcy zainteresowanego tym ogłoszeniem[20]. Podobnie TSUE wskazuje, że złożenie zamówienia poprzez użytkownika aplikacji informatycznej Star Taxi przez osobę, która zamierza przebyć trasę miejską, i połączenie się z tą aplikacją przez kierowcę taksówki posiadającego zezwolenie mają charakter „indywidualnego żądania" odbiorcy takiej aplikacji – usługi[21].

Mając na uwadze powyższe, należy podkreślić, że wszelkie podmioty, które nie będą świadczyły usługi na indywidualne żądanie, nie będą objęte regulacją DSA. Przykładem takich platform będzie Uber[22], ale też wszelkie platformy VoD, np. Netflix, HBO MAX, Disney Plus, Amazon Prime Video, Player, jak i wszelkie platformy, za treść których odpowiedzialność ponosi ich dostawca, który decyduje o ich zawartości[23]. Z tego powodu wyłączenie obejmie wszelkie strony internetowe, które będą stanowić gazety online, blogi, poradniki, a także wszelkie sklepy internetowe, które same publikują oferty sprzedaży na swoich stronach internetowych będących platformami do sprzedaży, a nie oferują usługi pośrednictwa w sprzedaży

---

[19] Wyrok TS z dnia 2 czerwca 2005 r., C-89/04, *Mediakabel Bv V. Commissariaat Voor De Media*, ZOTSiS 2005, nr 6A, poz. I-4891, pkt 37–39.

[20] Wyrok TS z dnia 19 grudnia 2019 r., C-390/18, *Postępowanie Karne Przeciwko X, przy udziale YA, Airbnb Ireland UC, Hôtelière Turenne SAS, Association pour un hébergement et un tourisme professionnels (AHTOP)*, Valhotel, pkt 48.

[21] Wyrok TS z dnia 3 grudnia 2020 r., C-62/19, *Star Taxi App Srl Przeciwko Unitatea Administrativ Teritorială Municipiul Bucureşti Prin Primar General I Consiliul General Al Municipiului Bucureşti*, pkt 47.

[22] Wyrok TSUE z dnia 20 grudnia 2017 r., C-434/15.

[23] F. Hofman, B. Raue, *op. cit.*, s. 82; X. Konarski, *Unijny Akt o Usługach Cyfrowych – cele uchwalenia, zakres stosowania oraz najważniejsze obowiązki dostawców usług pośrednich*, „Prawo Nowych Technologii" 2022, nr 3, s. 34.

produktów podmiotów trzecich[24]. Stąd takie platformy, jak Allegro, Amazon, OLX itd. będą podlegać pod definicję platformy internetowej zgodnie z DSA, ale już wszelkiego rodzaju sklepy internetowe, które oferują sprzedaż swoich produktów lub usług, nie będą objęte definicją platformy internetowej, a w związku z tym obowiązkami wynikającymi z DSA przypisywanymi platformom internetowym.

c) Istotność czynności rozpowszechniania informacji w odniesieniu do całości usługi

Znaczącym wyjątkiem w zakresie rozumienia pojęcia „platformy internetowej" jest wyłączenie wynikające z samej definicji z art. 3 lit. i) DSA, które zostało sformułowane w następujący sposób: jeśli działalność dostawcy usługi hostingu polegająca na przechowywaniu i rozpowszechnianiu publicznie informacji na żądanie odbiorcy jest jedynie „nieznaczną lub wyłącznie poboczną cechą innej usługi lub nieznaczną funkcją głównej usługi, i ze względów obiektywnych i technicznych nie można z niej skorzystać bez takiej innej usługi, a włączenie takiej cechy lub funkcji w taką inną usługę nie jest sposobem na obejście stosowania niniejszego rozporządzenia", wówczas dana usługa nie będzie klasyfikowana jako usługa „platformy internetowej" podlegająca pod DSA.

W pkt 15 preambuły DSA ustawodawca europejski wymienia przykłady takich usług podlegających wyłączeniu: sekcja gazety internetowej przeznaczona na komentarze, w przypadku której jest oczywiste, że ma ona charakter poboczny w stosunku do głównej usługi, jaką jest publikowanie wiadomości, za które odpowiedzialność redakcyjną ponosi wydawca. Inny przykład stanowią usługi przetwarzania w chmurze lub usługi hostingu internetowego, jeżeli publiczne rozpowszechnianie określonych informacji stanowi nieznaczną i poboczną cechę lub nieznaczną funkcję takich usług. Oba przykłady wskazują jasno, że nawet w przypadku, gdy ta poboczna usługa dostępna u danego dostawcy spełniałaby przesłanki platformy internetowej, będzie miało zastosowanie wyłączenie dotyczące charakteru tej usługi.

Opisywany wyjątek nasuwa na myśl analizowaną już wyżej sprawę rozpatrywaną przez TSUE pod sygnaturą C-434/15 i rozważania dotyczące stosowania przepisów dot. usług społeczeństwa informacyjnego, w przypadku powiązania ich z inną, złożoną usługą niemającą takiego charakteru[25]. W orzecznictwu TSUE zostało utrwalone, że w przypadku dylematu co do zastosowania właściwego prawa decydujący

[24] Tak też: F. Hofman, B. Raue, *op. cit.*, s. 65.

[25] Wyrok TS z dnia 20 grudnia 2017 r., C-434/15, *Asociación Profesional Elite Taxi V. Uber Systems Spain Sl*, ZOTSiS 2017, nr 12, poz. I-981, pkt 40.

powinien być główny element usługi, tj. nadający jej znaczenie gospodarcze, który pociąga za sobą zastosowanie przepisów odpowiednich dla tej głównej usługi[26]. Za punkt graniczny zastosowania tej interpretacji uznaje się samodzielność gospodarczą tej usługi, tj. odpowiedź na pytanie, czy usługa „poboczna" mogłaby działać samodzielnie i być przedmiotem działalności gospodarczej odrębnego przedsiębiorcy[27].

Interpretowany wyjątek znajdujący się w definicji platformy internetowej w DSA wydaje się oparty na obecnych już w orzecznictwie TSUE, wyżej opisanych rozważaniach, co może stanowić ułatwienie dla interpretacji nowych przepisów. Sformułowaniem: „i ze względów obiektywnych i technicznych nie można z niej skorzystać bez takiej innej usługi", zdaniem autorki, DSA nawiązuje do pytania o samodzielność gospodarczą pobocznej usługi, która spełnia przesłanki DSA. Podobnie zatem jak w opinii M. Szpunara do wyroku C-434/15 należy przyjrzeć się kwestii, czy dana usługa posiada samodzielność gospodarczą. Powtórzony tutaj może być przykład platformy sprzedaży biletów lotniczych i rezerwacji hotelowych, które zgodnie z interpretacją M. Szpunara mają rzeczywistą wartość dodaną zarówno dla użytkownika, jak i dla danego przedsiębiorcy oraz pozostają „samodzielne pod względem gospodarczym, gdyż przedsiębiorca prowadzi swoją działalność w sposób niezależny"[28]. Jeśli zatem przedsiębiorca oferuje usługę, którą pod względem prawnym można rozłożyć na części – wiązkę pojedynczych usług, które są wzajemnie powiązane, z tym że niektóre z nich są poboczne w porównaniu do innej głównej części, to w przypadku, gdy taka nieznaczna usługa spełnia przesłanki „platformy internetowej", należałoby dokonać dalszej analizy. Powinna ona prowadzić do odpowiedzi na pytanie o samodzielność gospodarczą takiej usługi i istnienie jej wartości gospodarczej w oderwaniu od innych usług pozostających w ramach działalności danego dostawcy. Na sam koniec należałoby odpowiedzieć dodatkowo na pytanie, czy taki sposób udostępnienia tej usługi nie miał na celu obejście przepisów.

Ustawodawca europejski uzasadnia wprowadzenie opisywanego wyjątku chęcią uniknięcia nakładania zbyt szerokiego zakresu obowiązków na platformy internetowe. O ile ten argument może być uznany za uzasadniony, to znów: wyjątek ten będzie znacząco oddziaływał na zakres zastosowania przepisów dotyczących platform internetowych obecnych w DSA, mimo że cała argumentacja dotycząca konieczności wprowadzenia ochrony użytkowników internetu w tym zakresie będzie

[26] Opinia rzecznika generalnego TSUE M. Szpunara przedstawiona 11 maja 2017 r., sprawa C-434/15, *Asociación Profesional Elite Taxi przeciwko Uber Systems Spain SL*, pkt 35.

[27] *Ibidem*, pkt 34.

[28] *Ibidem*, pkt 34.

mogła znaleźć zastosowanie. Oznacza to zatem, że wszelkiego rodzaju miejsca na komentarze pod tekstem bloga, gazety internetowej, oceny danego wydarzenia czy usługi nie będą podlegać pod DSA, mimo że są to miejsca, w których powstają zagrożenia, przed którymi DSA powinno chronić zgodnie z jego celem. Szczególne znaczenie będzie mieć to także w zakresie reklamy internetowej, co zostanie niżej rozwinięte.

Wydaje się, że na omawiany przepis można patrzeć również z drugiej strony – jeśli platforma jest objęta zastosowaniem DSA, a niektóre z jej części podpadają pod wyjątek z opisywanej definicji, należałoby traktować je odrębnie. Przykładem może być platforma do sprzedaży online, na której znajduje się sekcja komentarzy dotyczących oceny produktu czy ich zastosowania. Wydaje się, że w takim przypadku można argumentować, że ta część platformy, stanowiąca odrębną usługę w stosunku do samej sprzedaży produktów za pomocą platformy, spełniałaby przesłanki omawianego wyjątku i przepisy DSA dotyczące platform internetowych nie miałyby zastosowania.

Na powyższe ustalenia należy także spojrzeć szerzej. DSA bowiem wskazuje wprost, że w przypadku, gdy usługa ma złożony charakter, a wyłącznie niektóre z usług będących wiązką złożonej usługi będą stanowić platformę internetową, przepisy DSA będą oddziaływać wyłącznie w tym wąskim zakresie, a nie będą mieć znaczenia dla całej usługi. Mimo że powyższe stwierdzenie dotyczy sytuacji, w której jest rozważane zastosowanie DSA lub brak jego zastosowania, a nie zastosowanie przepisów w ramach określonych grup dostawców usług pośrednich wyznaczonych w DSA, oznaczać to powinno, że na dostawcę platformy nie należy patrzeć w sposób jednolity, a interpretacja usług, które on dostarcza, powinna być dokonywana w zakresie każdej z nich z osobna.

Powyższe stwierdzenie potwierdza po pierwsze tekst pkt 15 preambuły DSA, który stanowi, że przepisy DSA powinny mieć zastosowanie wyłącznie w zakresie tych usług, które są objęte DSA, co *a contrario* oznacza, że zastosowanie DSA nie powinno być rozciągane na inne usługi. Stwierdzenie rozumiane szerzej w odniesieniu do konkretnych grup podmiotów wyznaczonych w DSA potwierdza poczynione rozważania – gdy tylko niektóre z usług dostawcy będą stanowić platformę internetową, np. służącą do sprzedaży produktów podmiotów trzecich (m.in. Allegro), tylko ona powinna być objęta zakresem zastosowania DSA, jednak sekcja komentarzy pod produktami, mając na uwadze konieczność zastosowania wyjątku dot. braku samodzielności gospodarczej takiej sekcji, nie będzie podlegać pod przepisy rozporządzenia.

Po drugie, powyższy wniosek wywodzić można ze zmiany pierwotnego tekstu Rozporządzenia, w którym „platforma internetowa" była zdefiniowana jako „dostawca usługi hostingu", co mogłoby sugerować położenie nacisku na sam podmiot jako dostawcę usługi, a nie samą usługę hostingu. W końcowym tekście Rozporządzenia w definicji platformy internetowej nie ma słowa „dostawca", pozostał jedynie fragment: „platforma internetowa oznacza usługę hostingu". W kontekście celu DSA oraz pkt 15 preambuły Rozporządzenia wskazana zmiana wydaje się dalece uzasadniona i prowadzi do możliwości przeprowadzenia spójnej wykładni, a także potwierdza wniosek, zgodnie z którym możliwość zastosowania DSA należy rozpatrywać nie z perspektywy samego dostawcy i globalnej usługi, jaką on świadczy, lecz należy dokonać analizy poszczególnych usług, które są świadczone przez dostawcę, i próbować zakwalifikować je do zakresu definicji platformy internetowej. Jednocześnie należy także poszukiwać możliwości wyłączenia zastosowania DSA w przypadku, gdy poboczna i nieznaczna usługa pozostająca w wiązce usług danego dostawcy nie ma samodzielnego charakteru.

Dla porządku należy ponadto zaznaczyć, że rozporządzenie nie pozostawia wątpliwości w zakresie interpretacji usług stanowiących wyłącznie podstawę techniczną działalności danego dostawcy, stanowiąc, że takie usługi nie powinny być uznawane za platformę internetową w rozumieniu DSA[29]. Zostało to również wyraźnie zaznaczone w art. 2 ust. 2 DSA w szerszym zakresie – rozporządzenie nie ma zastosowania do innych usług niż usługi pośrednie, nawet gdy usługa pośrednia stanowi infrastrukturę świadczenia usług danego dostawcy usług. Taki wniosek wydaje się logiczny i uzasadniony w kontekście celu rozporządzenia, którym jest m.in. ochrona konsumentów, niepozostających w relacji między dostawcą infrastruktury do usługi a samym dostawcą usługi.

2. Zakończenie

Definicja platformy internetowej została przez ustawodawcę europejskiego znacząco zawężona poprzez takie ukształtowanie przesłanek składających się na rozumienie platformy oraz zastosowanie wyjątków, które w praktyce istotnie wpływają na krąg adresatów przepisów. Z jednej strony zabieg ten można uznać za zrozumiały w kontekście konieczności zachowania zasad proporcjonalności i chęci braku ograniczania rynku. Z drugiej jednak strony wiele obszarów, które potrzebują regulacji,

[29] Pkt 13 preambuły DSA.

patrząc z perspektywy użytkowników internetu, nie zostało wziętych pod uwagę[30]. Zawód może być tym większy, że DSA stanowiło właściwe narzędzie do regulacji tych kwestii jako ustanowione w formie rozporządzenia, a czas na wprowadzenie takich regulacji wydaje się właściwy. W konsekwencji, gdy dana usługa będąca usługą pośrednią nie zostanie zakwalifikowana w zakres pojęcia usługi platformy internetowej lub będzie miał do niej zastosowanie wyjątek opisany w definicji platformy internetowej (art. 3 lit. i) DSA), jej dostawca nie będzie mieć obowiązku prowadzania wewnętrznego systemu rozpatrywania skarg (art. 20 DSA), pozasądowego systemu rozstrzygania sporów (art. 21 DSA), wprowadzenia zaufanych podmiotów sygnalizujących (art. 22 DSA), zawieszenia świadczenia usług w stosunku do osób, które często przekazują nielegalne treści (art. 23 DSA), obowiązków sprawozdawczych (art. 24 DSA), właściwej organizacji interfejsów internetowych (art. 25 DSA), reklam i systemów rekomendacji (art. 26 i 27 DSA) oraz ochrony małoletnich (art. 28 DSA).

DSA będzie miało niewątpliwie wpływ na działanie internetu i będzie prowadziło do konieczności wprowadzenia wielu zmian technicznych w systemach dostawców usług internetowych. Zmiany te będą pozytywnie wpływać na ochronę użytkowników internetu, w tym na konsumentów, którzy podlegają szczególnej ochronie. Zasadne jest jednak stwierdzenie, że DSA nie zmieni całego internetu, a to już z tego powodu, że nie obejmie ono swoim zastosowaniem wszystkich podmiotów, które znajdują się w środowisku wirtualnym. Co do takiego stanu prawnego można wyrazić jedynie zawód wobec możliwości faktycznego wpłynięcia na funkcjonowanie i bezpieczeństwo w internecie i zwiększenie ochrony użytkowników.

Wybiórcze wprowadzenie przepisów wyłącznie wobec platform internetowych, które to przepisy byłyby uzasadnione dla całego środowiska internetowego, może mieć także negatywny wpływ na odbiór zmian przez użytkowników końcowych. Dla przeciętnego konsumenta nie będzie klarowne, dlaczego na niektórych stronach wyświetlane mu są dodatkowe informacje oraz może on korzystać z dodatkowych funkcji, a na innych już nie. Sytuacja ta może rozwijać się w dwóch kierunkach. Pierwszą opcją będzie zaimplementowanie przez rynek przepisów w szerszym zakresie, niż wymagane jest to przez DSA w celu dostosowania się do wspólnego poziomu usług. Druga opcja może być jednak nieco bardziej pesymistyczna i prowadzić do konfuzji użytkowników końcowych, którzy będą się czuć jeszcze bardziej zagubieni wobec wybiórczych standardów poszczególnych stron internetowych.

[30] Taki wniosek prezentuje także: R. Janal, *op. cit.*, s. 273, pkt 11. Autorka kwestionuje także wyznaczoną w art. 33 ust. 1 DSA granicę 45 mln średnio miesięcznie aktywnych odbiorców usługi w Unii dla spełnienia przesłanki definicji bardzo dużej platformy internetowej.

Wydaje się, że ustawodawca europejski mógłby pójść o krok dalej i choćby w ograniczonym zakresie objąć regulacjami wszystkich dostawców usług społeczeństwa informacyjnego. Obecne już w przepisach ograniczenie zastosowania DSA do dostawców innych niż mikro i średnie przedsiębiorstwa minimalizuje ryzyko trudności i kosztów dostosowania się mniejszych organizacji do nowych regulacji. Z tej perspektywy wydaje się, że możliwości tego aktu prawnego nie zostały wystarczająco wykorzystane mimo szerokiej perspektywy, do której nawiązywano w preambule Rozporządzenia, określając jego cel jako stworzenie „bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego". Realizacja tego celu z pewnością może, a wręcz powinna nastąpić poprzez wydanie aktu prawnego w postaci rozporządzenia na gruncie Unii Europejskiej z uwagi na ponadterytorialny zakres wymiany informacji w Internecie. Wydaje się jednak, że tym aktem, który stwarzałby dla użytkowników końcowych realną „bezpieczną przestrzeń", nie jest jeszcze omawiane w tym artykule Rozporządzenie.

Bibliografia

Akty prawne

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

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

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

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

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

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

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

Orzeczenia sądów i trybunałów oraz opinie i inne dokumenty wydawane przez organy Unii Europejskiej

Wyrok TS z dnia 2 czerwca 2005 r., C-89/04, *Mediakabel Bv V. Commissariaat Voor De Media*, ZOTSiS 2005, nr 6A, poz. I-4891.

Wyrok TS z dnia 7 grudnia 2006 r., C-306/05, *Sociedad General de Autores y Editores de España (SGAE) przeciwko Rafael Hoteles SA*.

Wyrok TS z dnia 7 marca 2013 r., C-607/11, ITV *Broadcasting Ltd i inni przeciwko TV Catch Up Ltd*.

Wyrok TS z dnia 13 lutego 2014 r., C-466/12, *Nils Svensson i inni przeciwko Retriever Sverige AG*.

Postanowienie TS z dnia 21 października 2014 r., C-348/13, *BestWater International GmbH przeciwko Michael Mebes i Stefan Potsch*.

Wyrok TS z dnia 8 września 2016 r., C-160/15, *GS Media przeciwko Sanoma Media Netherlands BV, Playboy Enterprises International Inc., Britt Geertruidzie Dekker*.

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

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

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

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

Wyrok TS z dnia 3 grudnia 2020 r., C-62/19, *Star Taxi App Srl Przeciwko Unitatea Administrativ Teritorială Municipiul Bucureşti Prin Primar General I Consiliul General Al Municipiului Bucureşti*.

Wyrok TSUE z dnia 22 czerwca 2022 r., C-682/18 i C-683/18, *Frank Peterson przeciwko Google LLC, YouTube Inc., YouTube LLC, Google Germany GmbH*.

Commission Staff Working Document Impact Assessment Accompanying The Document Proposal For A Regulation of the European Parliament And Of The Council On a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, Brussels, 15.12.2020 SWD(2020) 348 final.

Literatura (opracowania o charakterze naukowym)

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

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

Gerdemann S., Spindler G., *Das Gesetz über digitale Dienste (Digital Services Act) (Teil 2)*, „Gewerblicher Rechtsschutz und Urheberrecht" 2023, vol. 115.

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

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

Janal R., *Haftung und Verantwortung im Entwurf des Digital Services Acts*, „Zeitschrift für europäisches Privatrecht" 2021.

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

Konarski X., *Unijny Akt o Usługach Cyfrowych – cele uchwalenia, zakres stosowania oraz najważniejsze obowiązki dostawców usług pośrednich*, „Prawo Nowych Technologii" 2022, nr 3.

Peukert A., Husovec M., Kretschmer M., Mezei P., Quintais J.P., *European Copyright Society – comment on copyright and the Digital Services Act proposal*, „IIC – International Review of Intellectual Property and Competition Law" 2022, vol. 53(3).

Źródła internetowe

Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413 [dostęp: 25.02.2024].

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

Abstract

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

Keywords

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

DOI: 10.34616/151200

Prawo Mediów Elektronicznych. Kwartalnik Naukowy
2024, nr 3, 24–44

Elżbieta Dziuba
absolwentka Wydziału Prawa i Administracji Uniwersytetu Śląskiego,
aplikantka rzecznikowska
ORCID: 0009-0002-3063-2204

Konstytucja internetu a własność intelektualna – jak Akt o usługach cyfrowych chroni dobra niematerialne?

Streszczenie

Akt o usługach cyfrowych ma stworzyć bezpieczne, godne zaufania i przejrzyste środowisko internetowe dla konsumentów oraz konkurujących przedsiębiorców. Zadanie to ma również przekładać się na zwiększenie ochrony oraz poziomu egzekwowania praw własności intelektualnej na platformach internetowych. Rozporządzenie to ma za zadanie zniechęcić przedsiębiorców do sprzedawania towarów lub usług naruszających prawa posiadaczy praw własności intelektualnej, takich jak choćby znaki towarowe, wzory przemysłowe czy patenty. Celem artykułu jest ukazanie wpływu Aktu o usługach cyfrowych na prawo własności intelektualnej, z uwzględnieniem odniesienia do dyrektywy w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz rozporządzenia w sprawie ogólnego bezpieczeństwa produktów.

Słowa kluczowe

Akt o usługach cyfrowych, treści nielegalne, towary podrobione, towary pirackie, produkty niebezpieczne

Wstęp

Moderowanie treści, przedstawiciele prawni, obowiązki sprawozdawcze w zakresie przejrzystości, mechanizmy zgłaszania i działania, zaufane podmioty sygnalizujące, VLOP i VLOSE, system rekomendacji, koordynatorzy ds. usług cyfrowych – wszystkie te zagadnienia odnoszą się do najważniejszego obecnie na poziomie Unii Europejskiej, obok Aktu o rynkach cyfrowych, rozporządzenia regulującego funkcjonowanie przestrzeni cyfrowej – Aktu o usługach cyfrowych, zwanego również „konstytucją internetu". Kwestie te tworzą swoistą mozaikę zagadnień ujętych w rozporządzeniu, także w kontekście własności intelektualnej.

Celem przepisów Aktu o usługach cyfrowych jest stworzenie bezpiecznego, godnego zaufania i przejrzystego środowiska internetowego dla dwóch zasadniczych grup

podmiotów: konsumentów oraz konkurujących przedsiębiorców. Zadanie to ma również przekładać się, co nie jest oczywiste, na zwiększenie ochrony oraz poziomu egzekwowania praw własności intelektualnej na platformach internetowych. Choć fraza „własność intelektualna", z pominięciem przypisów, pojawia się w Akcie jedynie cztery razy, wpływ tego dokumentu na prawo własności intelektualnej jest kluczowy. Akt o usługach cyfrowych ma bowiem zniechęcić przedsiębiorców do sprzedawania towarów lub usług naruszających prawa posiadaczy praw własności intelektualnej, takich jak choćby znaki towarowe, wzory przemysłowe czy patenty, a także prawa autorskie.

Artykuł ukazuje wpływ Aktu o usługach cyfrowych na prawo własności intelektualnej, z uwzględnieniem odniesienia do dyrektywy w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym (dalej: dyrektywa DSM) oraz rozporządzenia w sprawie ogólnego bezpieczeństwa produktów. Przybliża również, czym są towary podrobione i pirackie oraz towary niebezpieczne. Ponadto przedstawia relację między wymienionymi towarami a pojęciem treści nielegalnych, uregulowanych w Akcie o usługach cyfrowych.

1. Główne założenia Aktu o usługach cyfrowych w kontekście prawa własności intelektualnej

Rozporządzenie (UE) 2022/2065 w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (Akt o usługach cyfrowych)[1] zmienia dyrektywę 2000/31/WE w sprawie handlu elektronicznego[2], która przez ponad 20 lat była główną regulacją w zakresie kształtowania się przestrzeni cyfrowej. Ze względu jednak na dynamiczny rozwój środowiska cyfrowego zauważalny stał się jej niewystarczający zakres. Z pomocą przyjść miał właśnie Akt o usługach cyfrowych. Treść Aktu uwzględnia obowiązujące przepisy dyrektywy o handlu elektronicznym dotyczące wyłączeń odpowiedzialności, gwarantujących, że usługi pośrednie mogą być nadal rozwijane na jednolitym rynku[3].

---

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

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

[3] Komisja Europejska, *Akt o usługach cyfrowych: Pytania i odpowiedzi*, https://digital-strategy.ec.europa.eu/pl/faqs/digital-services-act-questions-and-answers [dostęp: 17.06.2024].

Akt o usługach cyfrowych wprowadza zestaw przepisów, których zadaniem jest:

– skuteczniejsza ochrona konsumentów i ich praw podstawowych;

– określenie jasnych obowiązków dla platform internetowych i mediów społecznościowych;

– zwalczanie nielegalnych treści lub produktów;

– osiągnięcie większej przejrzystości poprzez lepszą sprawozdawczość i nadzór;

– wspieranie innowacji, wzrostu i konkurencyjności na rynku wewnętrznym UE[4].

Rozporządzenie wprowadza jasne i proporcjonalne przepisy, uwzgledniające ochronę konsumentów oraz ich praw podstawowych i tworzące sprawiedliwe środowisko platform internetowych. Ustanawia również długo oczekiwaną równowagę w zakresie roli poszczególnych uczestników rynku cyfrowego: użytkowników, platform internetowych oraz organów publicznych[5]. Odnosi się ono do świadczenia usług pośrednich. Usługi te, choć w definicji odwołują się do usług społeczeństwa informacyjnego, podobnie jak w dyrektywie 2000/31/WE[6], obejmują jedynie usługę zwykłego przekazu, usługę cachingu oraz usługę hostingu, regulując obowiązki oraz system przejrzystości i rozliczalności dla dostawców usług pośrednich, takich jak:

– usługi dostępu do internetu;

– usługi hostingowe, np. usługi przetwarzania w chmurze i usługi hostingu internetowego;

– rejestry nazw domen;

– internetowe platformy handlowe;

– sklepy z aplikacjami;

– platformy wspierające gospodarkę współpracy;

– sieci społecznościowe;

– platformy wymiany treści;

– internetowe platformy dotyczące podróży i zakwaterowania[7].

Obowiązki poszczególnych uczestników rynku cyfrowego zostały określone, uwzględniając ich rolę, udział w rynku, a także siłę oddziaływania na środowisko

[4] EUR-lex, *Akt o usługach cyfrowych*, https://eur-lex.europa.eu/PL/legal-content/summary/digital-services-act.html [dostęp: 17.06.2024].

[5] M. Gumularz, [w:] M. Gumularz (red.), *Akt o usługach cyfrowych. Komentarz*, Warszawa 2024.

[6] M. Namysłowska, D. Lubasz, [w:] R. Shulze, D. Staudmayer (red.), *EU Digital Law. Article-by-Article Commentary*, Oxford 2020, s. 419.

[7] EUR-lex, *Akt o usługach cyfrowych*, https://eur-lex.europa.eu/PL/legal-content/summary/digital-services-act.html [dostęp: 17.06.2024].

internetowe. Przepisów rozporządzenia muszą przestrzegać wszyscy usługodawcy internetowi, którzy działają na rynku Unii Europejskiej, bez względu na to, czy ich siedziba mieści się na terenie Unii Europejskiej, czy też poza nią. Co ważne, małe i średnie przedsiębiorstwa zostały zwolnione z części odpowiedzialności, stosownie do ich udziału w rynku oraz wyników[8].

Kluczowe daty odnoszące się do zbioru nowych przepisów to 25 kwietnia 2023 r. oraz 17 lutego 2024 r. 25 kwietnia 2023 r. Komisja Europejska ogłosiła listę 19 wielkich platform internetowych (*Very Large Online Platforms* – VLOPs) i wielkich wyszukiwarek internetowych (*Very Large Online Search Engines* – VLOSEs), czyli największych podmiotów działających w przestrzeni internetowej. W ciągu czterech miesięcy firmy musiały wprowadzić szereg zmian, doprowadzając do tego, że ich usługi stały się bezpieczniejsze dla użytkowników.

Bardzo duże platformy internetowe i wyszukiwarki to te, które mają ponad 45 mln użytkowników w Unii Europejskiej, a więc są wykorzystywane przez ponad 10% z 450 mln konsumentów w UE[9]. Muszą one być zgodne z najbardziej rygorystycznymi przepisami Aktu. Od końca sierpnia 2023 r. przepisy Aktu obowiązywały już te podmioty.

Tabela 1. Lista VLOPs[10]

Alibaba	Google Maps	Temu
AliExpress	Google Shopping	TikTok
Amazon Store	Instagram	Twitter
Apple AppStore	LinkedIn	Wikipedia
Booking.com	Pinterest	YouTube
Facebook	Shein	Zalando
Google Play	Snapchat	

Tabela 2. Lista VLOSEs[11]

Bing
Google Search

[8] Komisja Europejska, *Unijny akt o usługach cyfrowych*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_pl [dostęp: 17.06.2024].

[9] Komisja Europejska, *DSA: duże platformy internetowe i wyszukiwarki*, https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops [dostęp: 17.06.2024].

[10] Komisja Europejska, *Wykaz wyznaczonych VLOP i VLOSE*, https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses [dostęp: 13.12.2024].

[11] *Ibidem*.

Bardzo duże platformy i wyszukiwarki muszą obecnie zezwalać na otworzenie czarnych skrzynek swoich algorytmów i udostępnianie ich niezależnym audytorom oraz badaczom. Podmioty te nie mogą już dłużej wprowadzać na rynek nowych usług opartych na systemach sztucznej inteligencji bez obligatoryjnych ocen ryzyka. Jeżeli Komisja Europejska uzna, że środki zapobiegające, które wprowadziły bardzo duże platformy i wyszukiwarki, są nieadekwatne, może nałożyć na nie kary, a nawet wykluczyć z funkcjonowania na europejskim rynku.

Z kolei od 17 lutego 2024 r. rozporządzenie ma zastosowanie do wszystkich dostawców usług cyfrowych. Począwszy od tej daty, co najmniej raz w roku wszyscy dostawcy usług pośrednich są zobligowani do publikowania sprawozdań dotyczących moderowania treści. Sprawozdania mają zawierać informacje na temat stosowanych przez nie praktyk moderowania treści, a także liczbę nakazów otrzymanych od wszystkich właściwych krajowych organów sądowych bądź administracyjnych, liczbę usuniętych treści oraz dokładność i poziom błędów w ich automatycznych systemach moderowania treści[12].

Komisja Europejska będzie sprawować nadzór przede wszystkim nad VLOPs i VLOSEs, podczas gdy państwa członkowskie będą odpowiedzialne za inne platformy oraz wyszukiwarki, w zależności od miejsca ich siedziby. Uprawnienia nadzorcze Komisji Europejskiej wynikające z Aktu o usługach cyfrowych są tożsame z tymi, jakie przysługują jej na mocy obowiązujących przepisów antymonopolowych, włączając w to uprawnienia dochodzeniowe oraz możliwość nakładania grzywien w wysokości do 6% globalnych dochodów[13].

W kontekście własności intelektualnej za najważniejsze można uznać funkcje Aktu w zakresie zwalczania nielegalnych treści online, w tym towarów i usług, przede wszystkim poprzez:

– oferowanie większej kontroli nad tym, co użytkownicy widzą w internecie, oraz zapewnienie im dokładniejszych informacji o wyświetlanych reklamach;

– oferowanie możliwości łatwego znakowania nielegalnych treści lub produktów;

– zapewnienie platformom środków do współpracy z zaufanymi podmiotami sygnalizującymi (ang. *trusted flaggers*);

– nałożenie obowiązków w zakresie identyfikowalności przedsiębiorców na internetowych platformach handlowych (*Know Your Business Customer* – KYBC);

---

[12] D. Lubasz, [w:] D. Lubasz, M. Namysłowska (red.), *Akt o usługach cyfrowych. Komentarz*, Warszawa 2024, s. 104.

[13] Komisja Europejska, *Akt o usługach cyfrowych: Pytania…*

– wzmocnienie pozycji użytkowników i społeczeństwa obywatelskiego, w tym możliwość kwestionowania decyzji w sprawie moderowania treści i korzystania ze środków odwoławczych, takich jak mechanizm rozstrzygania sporów lub sądowe środki odwoławcze oraz przejrzystość w zakresie szeregu kwestii, w tym algorytmów stosowanych przy rekomendowaniu treści lub produktów[14].

Z perspektywy ochrony praw własności intelektualnej za istotne należy uznać treści nielegalne, dokładnie określone w dokumencie. W Akcie o usługach cyfrowych pojawiają się również treści szkodliwe, choć tym razem bez konkretnej definicji legalnej. Zgodnie z motywem 12 rozporządzenia treści nielegalne należy zdefiniować szeroko, tak aby obejmowały także informacje dotyczące nielegalnych treści, produktów, usług oraz działań, niezależnie od ich formy. Jako przykłady nielegalnych działań dotyczących nielegalnych treści wskazano bezprawne udostępnianie prywatnych obrazów bez zgody, sprzedaż produktów niespełniających wymogów lub podrobionych, sprzedaż towarów lub świadczenie usług z naruszeniem prawa ochrony konsumentów czy też nieuprawnione wykorzystanie materiałów chronionych prawem autorskim. Założenia szerokiego zdefiniowania treści nielegalnych, przyjęte w motywie 12, uległy udanej materializacji w art. 3 Aktu, zgodnie z którym treści nielegalne: „oznaczają informacje, które same w sobie lub przez odniesienie do działania, w tym sprzedaży produktów lub świadczenia usług, nie są zgodne z prawem Unii lub z prawem jakiegokolwiek państwa członkowskiego, które jest zgodne z prawem Unii, niezależnie od konkretnego przedmiotu lub charakteru tego prawa".

Nielegalne treści są to zatem informacje, których istota bądź też odniesienie do konkretnych działań, takich jak świadczenie usług lub sprzedaż towarów, nie są zgodne ani z prawem Unii Europejskiej, ani z prawem określonego państwa członkowskiego. Treści te obejmują zatem informacje, których rozprzestrzenianie jest sprzeczne z prawem, co czyni je jednoznacznie treściami nielegalnymi. Pojawiają się jednak głosy mówiące o tym, że definicja ta nie spełnia podstawowych wymogów stawianych poprawnie skonstruowanym definicjom, co wynika z faktu, iż zarówno pojęcie definiowane, jak i sama definicja nie są znane (łac. *ignotum per ignotum*). Dokonanie uszczegółowienia w definicji, że mowa tu o treściach niezgodnych z krajowym lub europejskim porządkiem prawnym, jest przez niektórych uznawane za niewystarczające[15]. Z pewnością definicja pojęcia „nielegalne treści" jest ujęta

[14] EUR-lex, *Akt o usługach cyfrowych*, https://eur-lex.europa.eu/PL/legal-content/summary/digital-services-act.html [dostęp: 17.06.2024].

[15] P. Polański, *Model odpowiedzialności za nielegalne treści na gruncie Aktu o Usługach Cyfrowych*, „Monitor Prawniczy" 2022, nr 20, s. 998.

szeroko i opiera się na założeniu, że wszystko co jest nielegalne *offline*, powinno być również nielegalne *online*[16]. Pojęcie to w kontekście całości przepisów Aktu o usługach cyfrowych uznać można za kluczowe, gdyż do niego odnosi się szereg szczegółowych postanowień rozporządzenia, przykładowo dobrowolne czynności sprawdzające podejmowane przez dostawców platform internetowych w celu identyfikacji i usuwania nielegalnych treści, nakaz podjęcia działań przeciwko nielegalnym treściom, mechanizm zgłaszania i działania wraz z uzasadnieniem takich działań czy też rozpoznawanie skarg i sporów w zakresie usunięcia treści[17]. Odpowiedzialność usługodawcy pośredniego za nielegalne treści wynika ostatecznie z przepisów materialnoprawnych będących podstawą dla takiej odpowiedzialności, a więc z przepisów prawa cywilnego, prawa karnego, prawa autorskiego czy prawa konsumenckiego[18]. W tym miejscu warto również pochylić się nad zjawiskiem moderowania treści. Proces ten obejmuje wykrywanie, identyfikowanie oraz usuwanie treści nielegalnych, które naruszają warunki korzystania z określonej usługi[19]. W przypadku VLOPs oraz VLOSEs Akt zakłada dalsze obowiązki związane z moderowaniem treści[20].

Akt o usługach cyfrowych wprowadza środki służące zwalczaniu nielegalnych towarów, usług i treści w internecie, takie jak choćby mechanizm sygnalizowania tych treści przez użytkowników, a w przypadku platform wprowadza mechanizm współpracy z zaufanymi podmiotami sygnalizującymi. Zgodnie z art. 22 ust. 2 Aktu status zaufanego podmiotu sygnalizującego powinien być przyznawany przez koordynatora ds. usług cyfrowych państwa członkowskiego, w którym osoba ubiegająca się o ten status ma siedzibę. Dodatkowo, status ten powinien być uznawany przez wszystkich dostawców platform internetowych. Wewnętrzna procedura służąca przyznaniu statusu zaufanego podmiotu sygnalizującego powinna cechować się bezstronnością i transparentnością, a także posiadać jasne kryteria oceny podmiotów. Status zaufanego podmiotu sygnalizującego przyznaje się jedynie podmiotom, nie indywidualnym osobom, które to podmioty wykażą, że mają

---

[16] M. Berberich, *Sorgfaltspflichten, Moderationsverfahren und prozedurale Fairness*, [w:] B. Steinrotter (red.), *Europaische Platformregulierung: DSA, DMA , P2B-VO, DGA, DA, AI Act, DSM-RL. Rechtshandbuch*, Baden-Baden 2023, s. 137.

[17] M. Grochowski *et al.*, [w:] M. Grochowski (red.), *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, Warszawa 2024, s. 103–104.

[18] F. Hofmann, [w:] F. Hofmann, B. Raue (red.), *Digital Services Act: Article-by-Article Commentary*, C.H. Beck 2024, s. 94.

[19] *Ibidem*, s. 108.

[20] M. Barudi, E. Wagner, [w:] R. Muller-Terpitz, M. Kohler (red.), *Digital Services Act: DSA*, C.H. Beck 2024, s. 50.

szczególną wiedzę ekspercką i kompetencje w zakresie zwalczania nielegalnych treści oraz że działają w sposób dokładny, obiektywny i z zachowaniem należytej staranności. Wiedza zaufanych podmiotów sygnalizujących może odnosić się do konkretnej dziedziny. Powinni oni przy wykorzystaniu odpowiednich narzędzi, technologii i metodologii być w stanie wykrywać i identyfikować treści nielegalne. Zaufany podmiot sygnalizujący musi być niezależny od dostawców platform internetowych. Nie może być powiązany kapitałowo ani kontrolowany przez żadnego z dostawców. Ma to służyć eliminacji potencjalnych konfliktów interesów i zapewnieniu obiektywnego działania w zakresie zwalczania nielegalnych treści. Platformy internetowe mają za zadanie zapewnienie priorytetowego traktowania zgłoszeń składanych przez zaufane podmioty sygnalizujące, a także ich terminowe przetwarzanie.

Z kolei koordynator ds. usług cyfrowych to organ odpowiedzialny za stosowanie i egzekwowanie Aktu w każdym państwie członkowskim. Jego rolą, poza przyznawaniem statusu zaufanego podmiotu sygnalizującego, jest również monitorowanie, wraz z Komisją Europejską i Radą Usług Cyfrowych, egzekwowania Aktu o usługach cyfrowych. Może on także żądać dostępu do danych VLOPs oraz VLOSEs czy też nakładać kary w przypadku naruszeń treści rozporządzenia.

2. Mechanizmy zgłaszania i działania skierowane do dostawców usług hostingu (*notice and action mechanisms*)

Dostawcy usług hostingu, zgodnie z art. 16 Aktu, wdrażają mechanizmy umożliwiające dowolnej osobie lub dowolnemu podmiotowi zgłoszenie im obecności w ich usłudze określonych informacji, które dana osoba lub dany podmiot uważają za nielegalne treści. Mechanizmy te muszą być łatwo dostępne i przyjazne dla użytkownika oraz muszą pozwalać na dokonywanie zgłoszeń wyłącznie drogą elektroniczną. Obowiązek wdrożenia mechanizmów jest adresowany do wszystkich dostawców usług hostingu, bez względu na ich wielkość.

Mechanizmy, o których mowa w art. 16 ust. 1, muszą być mechanizmami ułatwiającymi dokonywanie wystarczająco precyzyjnych i odpowiednio uzasadnionych zgłoszeń. Muszą być dostępne dla dowolnej osoby bądź podmiotu, którzy zamierzają zgłosić dane treści za nielegalne. Dostęp do tych mechanizmów nie może być jednak ograniczony jedynie do odbiorców usług. Z mechanizmów powinny mieć możliwość swobodnego korzystania zaufane podmioty sygnalizujące, których zgłoszenia powin-

ny być traktowane jako priorytetowe[21]. Mechanizm zgłoszeniowy musi umożliwiać zgłaszanie wielu określonych informacji o nielegalnych treściach jednocześnie[22]. W tym celu dostawcy usług hostingu przyjmują niezbędne środki umożliwiające im i ułatwiające dokonywanie zgłoszeń zawierających wszystkie poniższe elementy:

a) wystarczająco uzasadnione wyjaśnienie powodów, dla których dana osoba lub dany podmiot uważają, że odpowiednie informacje stanowią nielegalne treści;

b) jasne wskazanie dokładnej elektronicznej lokalizacji informacji, takiej jak dokładny adres URL lub dokładne adresy URL, oraz, w stosownych przypadkach, dodatkowe informacje umożliwiające identyfikację nielegalnych treści, stosownie do rodzaju treści i konkretnego rodzaju usługi hostingu;

c) imię i nazwisko lub nazwę oraz adres e-mail osoby lub podmiotu dokonujących zgłoszenia, z wyjątkiem zgłoszenia dotyczącego informacji uznawanych za związane z jednym z przestępstw, o których mowa w art. 3–7 dyrektywy 2011/93/UE;

d) oświadczenie potwierdzające powzięte w dobrej wierze przekonanie osoby lub podmiotu dokonujących zgłoszenia, że informacje i zarzuty w nim zawarte są prawidłowe i kompletne.

Nie oznacza to jednak, że dostawcy usług hostingu nie mogą się zwrócić do danego podmiotu w celu żądania dodatkowych informacji bądź dowodów. W kwestii wyjaśnienia nie wystarcza samo stwierdzenie, że konkretne treści są nielegalne. Konieczne jest poparcie tego stwierdzenia faktami, okolicznościami i argumentami przemawiającymi za jego poprawnością. Treść postanowienia musi być wystarczająca, aby dostawca usług hostingu mógł podjąć świadomą decyzję, że dane treści są nielegalne, a w rezultacie czy należy ograniczyć do nich dostęp bądź też je usunąć. Odnosząc się do wskazania dokładnej elektronicznej lokalizacji, może się zdarzyć, że podanie adresu lub adresów URL nie będzie wystarczające. Wtedy też konieczne będzie podanie przez podmiot zgłaszający dodatkowych informacji. Identyfikacja zgłaszającego może okazać się niezbędna do ustalenia, czy dane treści stanowią treści nielegalne. Może to dotyczyć choćby praw autorskich, w przypadku których to od decyzji dysponenta tych praw będzie zależało, czy dane treści są nielegalne. Z kolei złożenie oświadczenia o prawidłowości oraz kompletności informacji i zarzutu może zostać potraktowane jako swego rodzaju przypomnienie o konieczności rzetelnego wypełnienia zgłoszenia, z uwzględnieniem wszystkich istotnych okoliczności sprawy[23].

---

[21] P. Drobek, [w:] M. Grochowski (red.), *op. cit.*, s. 214.

[22] G. Spindler, *Der Vorschlag fur ein neues Haftungsregime fur Internetprovider – der EU-Digital Services Act (Teil 1)*, GRUR 2021/545, s. 552.

[23] *Ibidem*, s. 217.

Art. 16 Aktu o usługach cyfrowych nakłada na dostawców usług hostingu obowiązek rozpatrywania wszystkich zgłoszeń złożonych w ramach mechanizmu zgłaszania i działania. Są oni zobligowani do podjęcia decyzji w kwestii otrzymanych informacji w sposób terminowy, niearbitralny, obiektywny oraz z zachowaniem należytej staranności. Działania podejmowane przez dostawców usług hostingu powinny zmierzać do uniemożliwienia dostępu do treści uznanych za nielegalne bądź też do ich usunięcia, przy zachowaniu wolności wypowiedzi i informacji użytkowników. Konkretne terminy rozpatrzenia zgłoszenia i podjęcia decyzji nie zostały wprowadzone. Zastosowana elastyczność umożliwia dostawcom dostosowanie terminu do złożoności sprawy i rodzaju zgłaszanych treści. Jedynie zgłoszenia otrzymane przez zaufane podmioty sygnalizujące powinny zostać rozpatrzone bez zbędnej zwłoki.

W celu zapewnienia przejrzystości decyzji w art. 17 Aktu wskazano na elementy uzasadnienia wydanego użytkownikom przez dostawców usług hostingu. Uzasadnienie to powinno być postrzegane jako element gwarancji proceduralnych, mających na celu ochronę odbiorców usługi, którzy zostali dotknięci nałożonymi ograniczeniami. Dostawcy usług hostingu przedstawiają wszystkim zainteresowanym odbiorcom usługi jasne i konkretne uzasadnienie w odniesieniu do następujących ograniczeń nałożonych ze względu na fakt, iż informacje przekazane przez odbiorcę usługi stanowią nielegalne treści lub są niezgodne z warunkami korzystania z usług dostawcy:

a) ograniczenia w zakresie widoczności określonych informacji przekazywanych przez dostawcę usługi, w tym usuwanie treści, uniemożliwianie dostępu do treści lub depozycjonowanie treści;

b) zawieszenie, zakończenie lub inne ograniczenie płatności pieniężnych;

c) zawieszenie lub zakończenie świadczenia usługi w całości lub w części;

d) zawieszenie lub zamknięcie konta odbiorcy usługi.

Minimalny zakres treści uzasadnienia nałożonych ograniczeń obejmuje co najmniej informacje o zastosowanych ograniczeniach, podstawie faktycznej i prawnej, a także wykorzystaniu zautomatyzowanych środków. Dodatkowo, powinny zostać wskazane: ograniczenie terytorialne podjętej decyzji oraz okres jej obowiązywania.

Obowiązek uzasadnienia wprowadzonych ograniczeń nie ma zastosowania w przypadku informacji będących wprowadzającymi w błąd treściami handlowymi o dużej objętości. Mowa o rozpowszechnianiu wprowadzających w błąd treści handlowych w celu manipulowania usługą. Należy przez to rozumieć nieautentycz-

ne korzystanie z usługi, a więc korzystanie niezgodnie z jej celem, włączając w to używanie botów, fałszywych kont czy też innych nieuczciwych metod korzystania z danej usługi[24].

W przypadku gdy dostawca usług hostingu poweźmie jakiekolwiek informacje dające podstawę do podejrzenia, że popełniono przestępstwo zagrażające życiu lub bezpieczeństwu osób, natychmiast informuje o swoim podejrzeniu organy ścigania lub organy sądowe zainteresowanego państwa członkowskiego i przekazuje wszystkie dostępne informacje na ten temat.

Dostawcy platform internetowych zawieszają na rozsądny okres i po wydaniu uprzedniego ostrzeżenia świadczenie usług na rzecz odbiorców usługi często przekazujących nielegalne treści.

3. Identyfikowalność użytkowników biznesowych – *Know Your Business Customer*

Akt ustanawia nowe obowiązki dotyczące identyfikowalności użytkowników biznesowych na internetowych platformach handlowych, których celem jest pomoc w wykrywaniu sprzedawców nielegalnych towarów. Art. 30 Aktu o usługach cyfrowych nakłada na dostawców internetowych platform handlowych obowiązek umożliwienia konsumentom zawierania umów na odległość z przedsiębiorcami, włączając w to możliwość otrzymania przez konsumentów określonych informacji od przedsiębiorców.

W szczególności tacy dostawcy muszą teraz zapewnić, aby sprzedawcy przekazywali zweryfikowane informacje na temat ich tożsamości, zanim będą mogli rozpocząć sprzedaż towarów na internetowych platformach handlowych. Niepodanie bądź też podanie nieprawdziwych, nieaktualnych lub niekompletnych informacji przez przedsiębiorcę ma skutkować odmową zezwolenia na korzystanie z usługi przez przedsiębiorcę lub zawieszeniem tej usługi. Z przepisu tego wyłączeni zostali mali oraz średni przedsiębiorcy. Dostawcy ci muszą również zagwarantować, że użytkownicy będą mogli łatwo zidentyfikować osobę odpowiedzialną za sprzedaż. Następnie muszą zapewnić bezpieczne przechowywanie tych informacji przez określony czas[25]. Ponadto, jeżeli dostawca internetowej platformy handlowej dowiaduje

[24] *Ibidem*, s. 231.

[25] X. Konarski, *Unijny Akt o Usługach Cyfrowych – cele uchwalenia, zakres stosowania oraz najważniejsze obowiązki dostawców usług pośrednich*, „Prawo Nowych Technologii" 2022, nr 3.

się o sprzedaży nielegalnego produktu lub usługi przez sprzedawcę, musi poinformować o tym użytkowników, którzy zakupili nielegalny towar lub usługę, a także jest zobligowany do podania informacji o tożsamości sprzedawcy i możliwościach dochodzenia roszczeń.

Dostawcy platform internetowych umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość zapewniają, aby przedsiębiorcy mogli korzystać z tych platform internetowych jedynie w celu propagowania wiadomości o produktach lub usługach bądź też oferowania towarów lub usług konsumentom znajdującym się w Unii, jeżeli przed takim skorzystaniem z ich usług do tych celów uzyskali – o ile dotyczy to danego przedsiębiorcy – następujące informacje:

a) imię i nazwisko lub nazwę, adres, numer telefonu i adres poczty elektronicznej przedsiębiorcy;

b) kopię dokumentu tożsamości przedsiębiorcy lub jakąkolwiek inną identyfikację elektroniczną zgodnie z definicją w art. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014[26];

c) dane rachunku płatniczego przedsiębiorcy;

d) w przypadku gdy przedsiębiorca jest wpisany do rejestru handlowego lub podobnego rejestru publicznego – rejestr handlowy, do którego przedsiębiorca jest wpisany, oraz jego numer rejestracyjny lub równoważne środki pozwalające na ustalenie tożsamości znajdujące się w rejestrze;

e) własne poświadczenie przedsiębiorcy, w którym zobowiązuje się do oferowania wyłącznie produktów lub usług zgodnych z mającymi zastosowanie przepisami prawa Unii.

Do czasu podania wymaganych informacji i ich dokładnej weryfikacji przez dostawcę platformy pod względem wiarygodności oraz pełności, dostawca nie może umożliwić przedsiębiorcy korzystania ze swoich usług. Jeśli wymagane informacje nie zostaną przekazane przez przedsiębiorcę, przedsiębiorca nie może korzystać z platformy[27]. Dostawca platformy może zażądać od przedsiębiorcy zaświadczeń potwierdzających prawdziwość przedstawionych informacji w postaci odpowiednich dokumentów[28].

---

[26] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. L 257 z 28.08.2014 r.).

[27] K. Menszig-Wiese, P. Podrecki, [w:] M. Grochowski (red.), *op. cit.*, s. 319.

[28] K. v. Lewinski, *Compliance-Pflichten nach dem DSA – ein umfassender Uberblick*, „Recht Digital" 2023/4, s. 189.

Jeśli z kolei przedsiębiorca podał niepełne lub nieprawdziwe dane i mimo żądania dostawcy nie uzupełnił ich bądź nie sprostował, dostawca platformy internetowej umożliwiającej konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość ma obowiązek szybko zawiesić świadczenie usług na rzecz tego przedsiębiorcy w zakresie oferowania produktów lub usług konsumentom znajdującym się w Unii do czasu spełnienia żądania w całości.

W przypadku odmowy świadczenia usługi przez dostawcę platformy ze względu na nieprzekazanie wymaganych danych bądź ich negatywną weryfikację, a także w przypadku zawieszenia świadczenia usługi, przedsiębiorcy przysługuje prawo do skargi. Dzięki temu ma zapewniony dostęp do wewnętrznego systemu rozpatrywania skarg oraz do konkretnych pozasądowych mechanizmów rozwiązywania sporów.

Obowiązek identyfikowalności ma pozwolić konsumentom efektywniej dochodzić swoich praw. Dodatkowo pozwala on na informowanie konsumentów od samego początku korzystania z platformy, że poprzez nabycie towarów czy usług zawierają oni umowę z przedsiębiorcą, a nie z dostawcą usługi platformy.

4. Towary podrobione i pirackie

Szacuje się, że ok. 6% towarów importowanych do Unii Europejskiej to towary podrobione, których wartość wynosi ok. 119 bln euro. Ponad połowa towarów podrobionych trafia na rynek UE za pośrednictwem właśnie platform internetowych[29].

Kwestię towarów podrobionych oraz towarów pirackich reguluje szczegółowo, w art. 2 ust. 1 pkt 5 oraz 6, rozporządzenie[30] w sprawie egzekwowania praw własności intelektualnej przez organy celne. Zgodnie z treścią rozporządzenia za towary podrobione uznaje się te produkty, które są przedmiotem działania naruszającego znak towarowy lub oznaczenie geograficzne. Najczęściej zarówno towary te, jak i opakowanie, etykieta, naklejka, broszura, instrukcja obsługi, dokument gwarancji lub inny podobny artykuł są opatrzone znakiem lub oznaczeniem geograficznym bez zgody ich właściciela bądź też oznaczeniem podobnym do oryginalnego. Poprzez termin towary pirackie rozumie się z kolei towary będące przedmiotem działania

[29] EUIPO, *Counterfeit goods cost EU industries billions of euros and thousands of jobs annually*, https://www.euipo.europa.eu/en/news/counterfeit-goods-cost-eu-industries-billions-of-euros-and-thousands-of-jobs-annually [dostęp: 17.06.2024].

[30] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 608/2013 z dnia 12 czerwca 2013 r. w sprawie egzekwowania praw własności intelektualnej przez organy celne oraz uchylające rozporządzenie Rady (WE) nr 1383/2003 (Dz. Urz. L 181 z 29.06.2013 r.).

naruszającego prawo autorskie lub prawo pokrewne lub wzór w państwie członkowskim, w którym zostały ujawnione. Muszą one być kopią oryginalnych towarów, wykonaną bez zgody posiadacza prawa autorskiego, prawa pokrewnego lub wzoru.

Unia Europejska jest drugim na świecie importerem towarów i usług, co daje ogromne możliwości, ale niesie również ryzyko pojawienia się na dużą skalę towarów podrobionych. Gospodarka Unii Europejskiej specjalizuje się głównie w produktach o znacznej wartości i najczęściej wysokiej jakości, które często są chronione znakami towarowymi, wzorami przemysłowymi, patentami czy też oznaczeniami geograficznymi. Biorąc pod uwagę ich charakter, zwiększa to prawdopodobieństwo ich podrobienia. Problemem fałszerstw najbardziej są dotknięte branża kosmetyczna, farmaceutyczna, alkoholowa, zabawek oraz gier[31].

Głównym krajem pochodzenia towarów naruszających prawa własności intelektualnej nadal są Chiny. Tuż za nimi wymienić można Hongkong czy Bangladesz. Z Turcji najczęściej są sprowadzane inne podrobione napoje, perfumy i kosmetyki. Z Rosji i Ukrainy z kolei często docierają do UE podrobione środki ochrony roślin[32].

Konkurencyjność europejska powiązana jest z badaniami i rozwojem, innowacjami oraz prawami własności intelektualnej. Zjawisko podrabiania towarów, naruszające prawa własności intelektualnej, przynosi poważne negatywne konsekwencje dla gospodarki Unii Europejskiej, gdyż ogranicza motywację do innowacji i hamuje bezpośrednie inwestycje zagraniczne. Co więcej, niejednokrotnie przyczynia się do likwidacji miejsc pracy i umożliwia tworzenie nielegalnego systemu gospodarczego, który jest kontrolowany przez grupy przestępcze[33].

Podrabianie towarów, przede wszystkim proceder podrabiania środków ochrony roślin, powoduje również poważne szkody dla środowiska. Towary podrobione nie mają odpowiednich norm jakości. Ponadto wyeliminowanie ich z obiegu handlowego i zniszczenie wiąże się z wysokimi kosztami. Naprzeciw tym niebezpieczeństwom ma wyjść właśnie Akt o usługach cyfrowych, który, co do zasady, powinien gwarantować konsumentom możliwość wolnego, przejrzystego i bezpiecznego wyboru towarów w środowisku cyfrowym.

Niezwykle ważną rolę w walce z towarami podrobionymi i pirackimi odgrywają organy celne, które nie dopuszczają do ich przywozu z państw trzecich i skrupulatnie

---

[31] Dangerous Fakes: Trade in counterfeit goods that pose health, safety and environmental risks, OECD/EUIPO (2022), s. 30–31.

[32] Illicit Trade. Global Trade in Fakes. A Worrying Threat, OECD/EUIPO 2021, s. 21–22.

[33] Commission Recommendation (EU) 2024/915 of 19 March 2024 on measures to combat counterfeiting and enhance the enforcement of intellectual property rights, C/2024/1739, s. 1–3.

sprawdzają spełnienie przewidzianych prawnie wymagań co do ich jakości, oznakowania, koniecznych dokumentów czy przeprowadzonych badań. Tym samym służba celna może doprowadzić do skutecznego zatrzymywania towarów niepożądanych lub stwarzających ryzyko dla zdrowia i życia konsumentów, zanim zostaną one wprowadzone do obrotu w Unii Europejskiej. W walkę z naruszeniami praw własności intelektualnej, w tym w zwalczanie procederu podrabiania towarów, zaangażowane są również najważniejsze międzynarodowe instytucje, takie jak Światowa Organizacja Własności Intelektualnej (WIPO), Europejski Urząd ds. Ochrony Własności Intelektualnej (EUIPO), Organizacja Współpracy Gospodarczej i Rozwoju (OECD) czy Agencja Unii Europejskiej ds. Współpracy Organów Ścigania (EUROPOL).

5. Akt o usługach cyfrowych a dyrektywa w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym

Zgodnie z art. 2 rozporządzenia Akt o usługach cyfrowych nie wpływa ono na funkcjonowanie innych aktów prawnych regulujących inne aspekty świadczenia usług pośrednich na rynku wewnętrznym lub określających i uzupełniających rozporządzenie. Na tej podstawie można stwierdzić, że Akt o usługach cyfrowych powinien być traktowany jako *lex generalis* w odniesieniu do regulowania rynku usług cyfrowych, podczas gdy inne przepisy, odnoszące się do środowiska cyfrowego, będą stanowić *lex specialis*.

Tak jest w przypadku choćby dyrektywy w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym[34]. W kontekście usług cyfrowych jako kluczowy jawi się art. 17, który nakłada na dostawców usług online obowiązek weryfikacji treści przed ich publicznym rozpowszechnieniem[35]. Dotyczy on treści, które użytkownicy chcą zamieścić na platformach dostawców. Przepis ten przewiduje, że dostawca usług udostępniania treści online musi uzyskać zezwolenie od podmiotów uprawnionych, np. poprzez zawarcie umowy licencyjnej. W przypadku udostępnienia treści chronionej prawem autorskim to na dostawcy usług online spoczywa obowiązek wykazania, że dołożył wszelkich starań, aby uzyskać zezwolenie oraz aby zapewnić brak dostępu do poszczególnych utworów i innych przedmiotów objętych

[34] Dyrektywa 2019/790 w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz. Urz. L 130 z 17.05.2019 r.).

[35] R. Markiewicz, *Prawo autorskie na jednolitym rynku cyfrowym. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790*, Warszawa 2021, s. 201.

ochroną, w odniesieniu do których podmioty uprawnione przekazały dostawcom usług odpowiednie i niezbędne informacje. Dodatkowo, dostawca usług online musi wykazać, że działał niezwłocznie po otrzymaniu odpowiednio uzasadnionego zastrzeżenia od podmiotów uprawnionych w celu zablokowania dostępu do utworów lub innych przedmiotów objętych ochroną, których dotyczy zastrzeżenie lub też, że usunął te treści ze swoich stron internetowych. Ponadto konieczne jest wykazanie, że dołożono wszelkich starań, aby zapobiec przyszłemu zamieszczaniu treści objętych prawami autorskimi.

Zgodnie z art. 8 Aktu o usługach cyfrowych na dostawców usług pośrednich nie nakłada się ogólnego obowiązku monitorowania informacji, które dostawcy ci przekazują lub przechowują, ani aktywnego ustalania faktów lub okoliczności wskazujących na nielegalną działalność. Za ogólny obowiązek monitorowania należy uznać proces, poprzez który pośrednik jest zobowiązany do wprowadzenia środków technologicznych, mających na celu monitorowanie aktywności użytkowników w konkretnym serwisie pośrednika. Zakaz ogólnych obowiązków w zakresie monitorowania ma zapobiec nadmiernie nieproporcjonalnemu oraz szerokiemu nadzorowi pośredników nad treściami pochodzącymi od użytkowników. Jednocześnie umożliwia korzystanie z konkretnych środków, aby eliminować nielegalną działalność w środowisku cyfrowym, opierając się na uzasadnionych podstawach[36]. Celem regulacji jest zapewnienie równowagi między ochroną praw użytkowników oraz praw własności intelektualnej a ochroną prywatności i wyrażania opinii, a także zapewnienia pewności prawnej dla dostawców usług pośrednich. Wyłączenie ogólnego obowiązku monitorowania ma zabezpieczać pośredników przed nadmiernymi obciążeniami. Zakaz ogólnego monitorowania współgra z art. 17 dyrektywy DSM, który stanowi, że usługodawcy będący pośrednikami nie mogą prowadzić ogólnego monitorowania treści, które podlega ochronie prawnoautorskiej. Nie oznacza to jednak, że pośrednicy są całkowicie zwolnieni z odpowiedzialności za to, jakie treści umieszczają w ich serwisach użytkownicy.

W obu przypadkach wprowadzona została jednak tzw. klauzula dobrego Samarytanina (*Good Samaritan Protection*). Zakłada ona, że usługodawcy internetowi nie będą tracili wyłączeń odpowiedzialności jedynie z tego powodu, że prowadzą z własnej inicjatywy dochodzenia lub inne działania mające na celu wykrycie, identyfikację i usunięcie nielegalnych treści lub uniemożliwienia do nich dostępu. Poprzednio usługodawcy, którzy dobrowolnie wykrywali i usuwali, ich zdaniem, nielegalne tre-

[36] M. Wilczyńska, [w:] M. Grochowski (red.), *op. cit.*, s. 149.

ści, często musieli się liczyć z negatywnymi konsekwencjami, gdy okazało się, iż dana treść jednak nie jest nielegalna. Klauzula dobrego Samarytanina niweluje tego typu negatywne skutki.

6. Akt o usługach cyfrowych a rozporządzenie w sprawie ogólnego bezpieczeństwa produktów

Jak zostało wskazane, Akt o usługach cyfrowych definiuje treści nielegalne. Wśród treści nielegalnych wyróżnić można towary podrobione i towary pirackie. Pośród tych produktów z kolei często znajdują się towary, których występowanie reguluje obecnie dyrektywa w sprawie ogólnego bezpieczeństwa produktów[37], a od 13 grudnia 2024 r. będzie w zakresie rozporządzenia w sprawie ogólnego bezpieczeństwa produktów[38].

Dokument ten, w art. 3, definiuje, czym są produkt bezpieczny oraz produkt niebezpieczny. Za produkt bezpieczny uznaje się każdy produkt, który w zwykłych lub dających się racjonalnie przewidzieć warunkach używania, w tym w rzeczywistym czasie używania, nie stwarza jakiegokolwiek ryzyka lub jedynie minimalne ryzyko zgodne z jego używaniem, uważane za dopuszczalne i odpowiadające wysokiemu poziomowi ochrony zdrowia i bezpieczeństwa konsumentów. Produktem niebezpiecznym jest z kolei każdy produkt, którego nie można uznać za produkt bezpieczny.

Rozporządzenie odnosi się zarówno do nowych, jak i używanych, naprawionych lub odnowionych produktów. Reguluje towary oferowane konsumentom w Unii Europejskiej za pośrednictwem wszystkich kanałów sprzedaży, w tym za pośrednictwem internetowych platform handlowych.

Nie dotyczy jednak następujących kategorii produktów:

– produktów leczniczych do stosowania u ludzi ani do weterynaryjnych produktów leczniczych;

– żywności i pasz;

– żywych roślin i zwierząt, organizmów zmodyfikowanych genetycznie oraz mikroorganizmów zmodyfikowanych genetycznie stosowanych w sposób ograniczony;

---

[37] Dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady z dnia 3 grudnia 2001 r. w sprawie ogólnego bezpieczeństwa produktów (Dz. Urz. L 11 z 15.01.2002 r.).

[38] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/988 z dnia 10 maja 2023 r. w sprawie ogólnego bezpieczeństwa produktów, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 i dyrektywę Parlamentu Europejskiego i Rady (UE) 2020/1828 oraz uchylające dyrektywę 2001/95/WE Parlamentu Europejskiego i Rady i dyrektywę Rady 87/357/EWG (Dz. Urz. L 135 z 23.05.2023 r.).

– produktów ubocznych pochodzenia zwierzęcego i produktów pochodnych;

– produktów ochrony roślin;

– sprzętu wykorzystywanego do przemieszczania się lub podróży, gdy jest on obsługiwany bezpośrednio przez usługodawcę;

– statków powietrznych, których konstrukcja, wytwarzanie, obsługa techniczna i eksploatacja stwarzają niewielkie zagrożenie dla bezpieczeństwa;

– antyków;

– produktów wymagających naprawy lub odnowienia przed użyciem, w przypadku gdy noszą wyraźne oznaczenie, że wymagają naprawy lub odnowienia przed użyciem[39].

Rozporządzenie nakłada na operatorów internetowych platform handlowych obowiązek zapewnienia, że oferta nie będzie mogła zostać opublikowana bez minimalnych informacji dotyczących bezpieczeństwa i identyfikowalności produktów dostarczanych przez zainteresowanego przedsiębiorcę. Co więcej, operatorzy będą musieli za pomocą publicznych baz danych wyrywkowo weryfikować, czy oferowane produkty są bezpieczne. Dodatkowo wprowadza się obowiązek niezwłocznego reagowania na zarządzenia władz i powiadomienia podmiotów zewnętrznych. Operatorzy będą musieli również zapewnić, aby usunięte oferty nie pojawiły się ponownie. Poza tym konieczne stanie się dostarczanie konsumentom odpowiednich i aktualnych informacji w przypadku wycofania produktu z rynku poprzez bezpośredni kontakt ze wszystkimi osobami, które zakupiły dany produkt na platformie operatora i publikowanie szczegółowych informacji na stronie internetowej operatora. Ponadto nakłada się obowiązek informacyjny poinformowania właściwego podmiotu gospodarczego oraz organów nadzoru rynku w przypadku wycofania produktu z rynku.

Zgodnie z Aktem o usługach cyfrowych w sytuacji gdy dostawca usług hostingu poweźmie jakiekolwiek informacje dające podstawę do podejrzenia, że popełniono przestępstwo zagrażającego życiu lub bezpieczeństwu, natychmiast informuje o swoim podejrzeniu organy ścigania lub organy sądowe zainteresowanego państwa członkowskiego i przekazuje wszystkie dostępne informacje na ten temat. Przestępstwem zagrażającym życiu lub bezpieczeństwu jest z pewnością kontakt z produktami niebezpiecznymi bądź ich używanie. Widoczny jest zatem bezpośredni związek między Aktem o usługach cyfrowych, który nakłada ogólne obowiązki na

[39] EUR-lex, *Rozporządzenie w sprawie ogólnego rozporządzenia produktów (2023)*, https://eur-lex.europa.eu/PL/legal-content/summary/general-product-safety-regulation-2023.html [dostęp: 17.06.2024].

internetowe platformy handlowe, a rozporządzeniem w sprawie ogólnego bezpieczeństwa produktów, które uszczegóławia obowiązki operatorów platform w przypadku umieszczenia na internetowych platformach handlowych produktów niebezpiecznych, a tym samym dopuszczeniem do udostępnienia ich szerokiemu gronu odbiorców.

7. Podsumowanie

Jak zostało wyraźnie wskazane, choć Akt o usługach cyfrowych reguluje przede wszystkim funkcjonowanie środowiska cyfrowego i interakcje między konsumentami, dostawcami usług pośrednich a organami nadzoru, bezsprzecznie wpływa również na prawo własności intelektualnej. Wpływ ten i pewnego rodzaju zależność uznać należy za pozytywne. Względem innych aktów prawnych odnoszących się do przestrzeni cyfrowej Akt o usługach cyfrowych pełni funkcję *lex generalis*. Wyznacza zatem ogólne prawa i obowiązki uczestników rynku cyfrowego, podczas gdy inne regulacje będą stanowić względem niego *lex specialis*. Tak jest choćby w przypadku rozporządzenia w sprawie egzekwowania praw własności intelektualnej przez organy celne, dyrektywy w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym czy rozporządzenia w sprawie ogólnego bezpieczeństwa produktu. Za kluczowe w Akcie należy uznać szerokie uregulowanie kwestii treści nielegalnych, wraz z przytoczonymi przykładami. W zakresie treści nielegalnych mieszczą się bowiem towary podrobione i pirackie, a także produkty niebezpieczne, których występowanie wprost regulują przepisy w zakresie prawa własności intelektualnej. Dzięki mechanizmom zgłaszania i działania oraz identyfikowalności użytkowników biznesowych Akt o usługach cyfrowych wprowadza środki mające na celu zwiększenie ochrony i egzekwowalności praw własności intelektualnej, jednocześnie zapewniając uczestnikom rynku cyfrowego bezpieczne, transparentne i godne zaufania środowisko funkcjonowania w przestrzeni cyfrowej.

Bibliografia

Akty prawne

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

Dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady z dnia 3 grudnia 2001 r. w sprawie ogólnego bezpieczeństwa produktów (Dz. Urz. L 11 z 15.01.2002 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 608/2013 z dnia 12 czerwca 2013 r. w sprawie egzekwowania praw własności intelektualnej przez organy celne oraz uchylające rozporządzenie Rady (WE) nr 1383/2003 (Dz. Urz. L 181 z 29.06.2013 r.).

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

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

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/988 z dnia 10 maja 2023 r. w sprawie ogólnego bezpieczeństwa produktów, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 i dyrektywę Parlamentu Europejskiego i Rady (UE) 2020/1828 oraz uchylające dyrektywę 2001/95/WE Parlamentu Europejskiego i Rady i dyrektywę Rady 87/357/EWG (Dz. Urz. L 135 z 23.05.2023 r.).

Pozycje książkowe, zalecenia i raporty

Commission Recommendation (EU) 2024/915 of 19 March 2024 on measures to combat counterfeiting and enhance the enforcement of intellectual property rights, C/2024/1739.

Dangerous Fakes: Trade in counterfeit goods that pose health, safety and environmental risks, OECD/EUIPO (2022).

Grochowski M. (red.), *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, Warszawa 2024.

Hofmann F., B. Raue, (red.), *Digital Services Act: Article-by-Article Commentary*, C.H. Beck 2024.

Illicit Trade. Global Trade in Fakes. A Worrying Threat, OECD/EUIPO 2021.

Konarski X., *Unijny Akt o Usługach Cyfrowych – cele uchwalenia, zakres stosowania oraz najważniejsze obowiązki dostawców usług pośrednich*, „Prawo Nowych Technologii" 2022, nr 3.

Lewinski K. v., *Compliance-Pflichten nach dem DSA – ein umfassender Uberblick*, „Recht Digital" 2023/4.

Lubasz D., Namysłowska M. (red.), *Akt o usługach cyfrowych. Komentarz*, Warszawa 2024.

Markiewicz R., *Prawo autorskie na jednolitym rynku cyfrowym. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790*, Warszawa 2021.

Muller-Terpitz R., Kohler M. (red.), *Digital Services Act: DSA*, C.H. Beck 2024.

Polański P., *Model odpowiedzialności za nielegalne treści na gruncie Aktu o Usługach Cyfrowych*, „Monitor Prawniczy" 2022, nr 20.

Shulze R., Staudmayer D., *EU Digital Law. Article-by-Article Commentary*, Oxford 2020.

Spindler G., *Der Vorschlag fur ein neues Haftungsregime fur Internetprovider – der EU-Digital Services Act (Teil 1)*, GRUR 2021/545.

Steinrotter B. (red.), *Europaische Platformregulierung: DSA, DMA , P2B-VO, DGA, DA, AI Act, DSM-RL. Rechtshandbuch*, Baden-Baden 2023.

Źródła internetowe

EUIPO, *Counterfeit goods cost EU industries billions of euros and thousands of jobs annually*, https://www.euipo.europa.eu/en/news/counterfeit-goods-cost-eu-industries-billions-of-euros-and-thousands-of-jobs-annually

EUR-lex, *Akt o usługach cyfrowych*, https://eur-lex.europa.eu/PL/legal-content/summary/digital-services-act.html

EUR-lex, *Rozporządzenie w sprawie ogólnego rozporządzenia produktów (2023)*, https://eur-lex.europa.eu/PL/legal-content/summary/general-product-safety-regulation-2023.html

Komisja Europejska, *Akt o usługach cyfrowych: Pytania i odpowiedzi*, https://digital-strategy.ec.europa.eu/pl/faqs/digital-services-act-questions-and-answers

Komisja Europejska, *Unijny akt o usługach cyfrowych*, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_pl

Komisja Europejska, *DSA: duże platformy internetowe i wyszukiwarki*, https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops

Komisja Europejska, *Wykaz wyznaczonych VLOP i VLOSE*, https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses

The constitution of the internet and intellectual property law – how the Digital Services Act protects intangible assets?

Abstract

The Digital Services Act is expected to create a safe, trustworthy and transparent online environment for consumers and competing businesses. It encompasses as well an increased protection and enforcement of intellectual property rights on online platforms. The regulation is designed to discourage entrepreneurs from selling goods or services that infringe on intellectual property rights, such as trademarks, designs or patents. The purpose of this article is to show the impact of the Digital Services Act on intellectual property law, with reference to the Directive on copyright and related rights in the Digital Single Market and the General Product Safety Regulation.

Keywords

Digital Services Act, illegal content, counterfeit goods, pirated goods, dangerous products

DOI: 10.34616/151201

Prawo Mediów Elektronicznych. Kwartalnik Naukowy
2024, nr 3, 45–76

Adw. Oskar Grajewski
ORCID: 0009-0009-7968-5543

Mateusz Jakubik
Uniwersytet Jagielloński w Krakowie
Wydział Prawa i Administracji
ORCID: 0000-0002-8992-7309

Wybrane zagadnienia dotyczące roli sygnalistów[1] i kanałów zgłaszania w kontekście rozwoju technologii cyfrowych oraz zmian prawodawczych, a także związanych z tym wyzwań i perspektyw[2]

Streszczenie

Niniejsza praca skupia się na ewolucji roli sygnalistów w erze cyfrowej oraz na analizie wpływu nowoczesnych technologii, takich jak sztuczna inteligencja (AI), *blockchain*, *big data* oraz internet rzeczy (IoT), na skuteczność i bezpieczeństwo kanałów zgłaszania naruszeń. Celem pracy jest ocena, w jaki sposób technologie te mogą zrewolucjonizować proces zgłaszania nieprawidłowości, a także jakie wyzwania i możliwości wiążą się z ich integracją w kontekście współczesnych zmian prawodawczych, ze szczególnym uwzględnieniem dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 z 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii oraz Ustawy z dnia 14 czerwca 2024 r. o ochronie sygnalistów. Metodologia badawcza obejmuje przeglądy literatury oraz analizę regulacji prawnych. Kluczowe ustalenia wskazują, że technologie cyfrowe mogą znacznie podnieść poziom bezpieczeństwa, anonimowości oraz efektywności systemów zgłaszania, lecz jednocześnie stawiają przed prawodawcami i organizacjami poważne wyzwania, związane z zapewnieniem zgodności z przepisami, ochroną danych osobowych oraz transparentnością. Praca podkreśla, że istotnym aspektem w przyszłości ochrony sygnalistów będzie harmonizacja przepisów prawnych z dynamicznie rozwijającym się krajobrazem technologicznym oraz edukacja w zakresie nowych narzędzi zgłaszania. Implikacje badań sugerują konieczność elastycznego podejścia do regulacji prawnych w ten sposób, aby

[1] W treści artykułu autorzy posługują się przeważnie terminem „sygnalista", będącym tłumaczeniem angielskiego wyrazu *whistleblower* (a także jego innej formy *whistle-blower*), jednakże we fragmentach poświęconych etymologii przedmiotowego terminu w obu formach, a także we fragmentach poświęconych tematom, w których zachodzą różnice w obrębie tych pojęć, wyrazy te wykorzystywane są równolegle w celu uwypuklenia uwag.

[2] Przedstawione w artykule opinie stanowią wyraz osobistych poglądów autorów i nie powinny być utożsamiane ze stanowiskiem żadnej organizacji lub instytucji, z którą autorzy byli albo są powiązani.

zapewnić skuteczną ochronę sygnalistów w erze cyfrowej, oraz wskazują na potrzebę ciągłego monitorowania i adaptacji przepisów do nowych wyzwań technologicznych.

Słowa kluczowe

sygnaliści, ochrona sygnalistów, kanały zgłaszania naruszeń, technologie cyfrowe, sztuczna inteligencja (AI), *big data*, internet rzeczy (IoT), RODO

Uwagi wstępne

Celem niniejszej pracy jest zbadanie znaczenia, wyzwań i perspektyw związanych z rolą sygnalistów w erze cyfrowej oraz analiza, w jaki sposób technologie, takie jak AI, *big data* czy *blockchain*, mogą wpłynąć na skuteczność i bezpieczeństwo kanałów zgłaszania nieprawidłowości. Praca ta ma na celu również ocenę, jak zmiany prawodawcze, zwłaszcza dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (UE)[3] i ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów[4], dostosowują się do dynamicznie rozwijającego się krajobrazu technologicznego oraz prawodawczego i jakie implikacje niosą one dla przyszłości ochrony sygnalistów.

Artykuł ten nie aspiruje jednak do miana pracy propedeutycznej ani tym bardziej wyczerpującej temat sygnalistów i kanałów zgłaszania, co usiłowano zaznaczyć już w samym tytule. Choć powodów tego działania jest wiele, to dla dochowania zasady oględności można poprzestać na stwierdzeniu, iż problematyka ta w samym jej bieżącym zakresie jawi się jako nie mniej obszerna niż dotychczasowe dzieje zjawiska „sygnalistów" i godna jest wnikliwszych oraz z pewnością bardziej obszernych badań i analiz. W ich efekcie prawdopodobne byłoby, iż przy nagromadzeniu tak wielu zagadnień doczesnych ich ekspozycja odbyłaby się kosztem właśnie tego aspektu, któremu w niniejszej pracy pragną przyjrzeć się autorzy. Mowa tu o samym znaczeniu, wyzwaniach i perspektywach omawianego zjawiska, których natura nakazuje nam odnosić się do przyszłości, na co w dobie cyfrowej, gdy „wartość czasu" wykracza poza jego „kantowskie"[5] rozumienie jako *a priori* formę naszej zmysłowości[6], prawdopodobnie mało kto może sobie pozwolić. To hipotetyczne za-

[3] Dz. Urz. UE L 305/17 z 2019 r. (dalej: „dyrektywa 2019/1937" oraz „dyrektywa").

[4] Dz. U. z 2024 r. poz. 928 (dalej: „Ustawa o ochronie sygnalistów" oraz „u.o.s.").

[5] Chodzi o I. Kanta (ur. 22 kwietnia 1724 r., zm. 12 lutego 1804 r.), niemieckiego filozofa, profesora logiki i metafizyki na Uniwersytecie Albrechta w Królewcu, jednego z najwybitniejszych reprezentantów oświecenia, zob. I. Kant, [w:] *Encyklopedia PWN*, https://encyklopedia.pwn.pl/haslo/Kant-Immanuel;3919929.html/ [dostęp: 30.08.2024].

[6] I. Kant, *Krytyka czystego rozumu*, tłum. R. Ingarden, Warszawa 1957, s. 79.

niechanie niosłoby za sobą niemałą szkodę, bowiem konsekwencją stale przez nas doświadczanego tempa rozwoju jest potrzeba podjęcia się zarówno indywidualnie, jak i zbiorowo wzmożonej pracy nad zrozumieniem możliwych przyszłych zmian w zakresie problematyki sygnalistów. Niezbędne w tym celu pozostaje także zrozumienie korelacji zjawiska sygnalistów z dalszym rozwojem rzutujących na ich aktywność technologii, a także wpływu sygnalistów na dotychczasowy sposób funkcjonowania społeczeństwa. Następstwem tych starań powinno być wypracowanie i wdrożenie odpowiednich mechanizmów oraz higieny korzystania z rozwijanych przez cywilizację technologii, a także zyskanie perspektywy i narzędzi do podejmowania działań prawodawczych, które zdołają dotrzymać kroku temu rozwojowi w wymiarze praktycznym, a nie jedynie postulatywnym, a to wszystko bynajmniej nie w celu zapewnienia sobie komfortu w miejscu, w którym aktualnie się znajdujemy, lecz w celu zachowania kontroli nad tym, dokąd zmierzamy.

Według poczynionych założeń nie można więc oczekiwać, aby w tak krótkiej formie publicystycznej przedstawić w sposób kompleksowy genezę bohaterów niniejszego tekstu, wszelkich możliwych kanałów zgłaszania, dorobku prawodawczego, doktrynalnego i jurydycznego, czemu z pewnością poświęcono już liczne publikacje oraz mnóstwo uwagi. Zamiast tego analizie poddane zostaną te zagadnienia, które zdają się obecnie dominować dyskurs nowych technologii w prawie. Dowodząc słuszności takiego działania, należy zwrócić uwagę na uzasadnione i nieodparte wrażenie autorów, iż w kontekście szybkiego rozwoju technologicznego i zmieniającego się otoczenia prawnego wzrasta także znaczenie problematyki sygnalistów, których rola ściśle wiąże się z tym dynamizmem i wpływa na nas jak jeszcze nigdy dotąd.

1. Ewolucja znaczenia „sygnalistów” i ich roli w kontekście technologii cyfrowych

Uprzedzając ewentualne uwagi, jakoby określanie sygnalistów mianem „bohaterów” stanowiło przejaw grandilokwencji, stwierdzić należy, iż zabieg ten, prócz waloru stylistycznego, umotywowany był także donioślejszą przyczyną. Zbyteczne byłoby pochylanie się nad kwestią ewentualnych osobistych korzyści, jakich mógłby potencjalnie doświadczyć sygnalista, lecz bez względu na to, chcąc wykazać, z jak istotną w tym przypadku mierzymy się materią, konieczne jest odnieść się do znaczenia roli sygnalistów i korzyści płynących z ich działalności w ujęciu powszechnym. Stając przed takim problemem, naturalne zdaje się postawienie najpierw pytania jeszcze bardziej ogólnego, a mianowicie: kim *de facto* są „sygnaliści”? Wiążąc

ładunek znaczeniowy omawianego pojęcia z samym terminem „sygnalista", można by poprzestać na przytoczeniu jedynie definicji tego pojęcia, jednakże w celu podkreślenia istoty zagadnienia konieczne zdaje się podjęcie próby dokonania jego egzegezy, co z kolei wymaga przytoczenia najpierw rysu historycznego.

W anglojęzycznych słownikach etymologicznych pochodzenie pojęcia *whistleblower* powiązano w sposób oczywisty z czynnością polegającą na dmuchaniu w gwizdek (ang. *blow the whistle*) i wskazano na jego występowanie w powszechnym obiegu co najmniej od XIX w., pierwotnie z łącznikiem jako *whistle-blower*, a następnie w zapisie łącznym *whistleblower*[7]. Jednakże jeszcze w XIX w. *whistleblower* nabrało bardziej specyficznego znaczenia, albowiem nie odnosiło się już tylko do osoby, która gwizdała w jakikolwiek sposób, lecz słowo to oznaczało również sędziego w zawodach sportowych[8]. Po tym jak pojęcia *whistleblower* zaczęto powszechnie stosować w odniesieniu do sędziego w zawodach sportowych, termin ten zaczął być także używany w znaczeniu zwrócenia uwagi publicznej na zdarzenie utrzymywane w tajemnicy[9]. Następnie zaś coraz częściej pojęcie *whistleblower* zaczęło być wiązane z ujawnianiem zdarzeń dotyczących naruszeń przepisów prawa, w tym także o charakterze przestępczym[10]. Z drugiej strony odnaleźć można także dowody wskazujące na to, iż metaforyczne znaczenie terminu *whistleblower* funkcjonowało już w drugiej połowie XIX w.[11]

W powszechnym obiegu ugruntował się także pogląd, iż pojęcie *whistleblower* w jego aktualnym znaczeniu zostało spopularyzowane w latach 60. i 70. XX w. przez dziennikarzy[12] i działaczy politycznych, takich jak R. Nader[13], amerykański

---

[7] *Whistleblower*, [w:] *Online Etymology Dictionary*, https://www.etymonline.com/search?q=whistleblower%20/ [dostęp: 30.08.2024].

[8] *Whistleblower*, [w:] *Merriam-Webster*, https://www.merriam-webster.com/wordplay/whistle-blower-blow-the-whistle-word-origins/ [dostęp: 30.08.2024], gdzie jako przykłady wskazano wybrane publikacje z czasopism: „The Huddersfield Chronicle and West Yorkshire Advertiser", Huddersfield 1890, „Jackson's Oxford Journal", Oxford 1894, „The Hampshire Advertiser", Southampton 1895.

[9] *Ibidem*, gdzie jako przykłady wskazano wybrane publikacje z czasopism: „San Francisco Chronicle", San Francisco 1929, „Richmond Times Dispatch", Richmond 1934.

[10] *Ibidem*, gdzie jako przykłady wskazano wybrane publikacje z czasopism: „Variety", City of New York 1963, „Asbury Park Press", Asbury Park 1966, „The Pittsburgh Press", Pittsburgh 1967.

[11] *Whistle-blower*, [w:] *Phrases Finder*, https://www.phrases.org.uk/meanings/whistle-blower.html/ [dostęp: 30.08.2024], gdzie jako przykład wskazano wybrany artykuł z czasopisma: „Wisconsin's Janesville Gazette", Wisconsin 1883, w którym słowem *whistleblower* nazwano policjanta, który użył gwizdka, aby powiadomić obywateli o zamieszkach.

[12] *Whistleblower*, [w:] Wayback Machine, https://web.archive.org/web/20120429004210/http://www.wordor igins.org/index.php/site/whistleblower/ [dostęp: 30.08.2024].

[13] J.K. Devitt, *Speaking Up Safely Civil Society Guide To Whistleblowing: Middle East And North Africa Region*, „Transparency International" 2015, s. 5–7, http://www.jstor.org/stable/resrep20533/ [dostęp: 30.08.2024].

prawnik, wykładowca, aktywista polityczny i wielokrotny kandydat na prezydenta Stanów Zjednoczonych Ameryki, założyciel Public Citizen[14], będącej organizacją non profit, zajmującą się obroną praw konsumentów[15]. Pogląd ten wymusza dookreślenie aktualnego znaczenia słowa *whistleblower*, które w słownikach języka angielskiego opisywane jest jako „osoba donosząca na inną osobę lub ujawniająca publicznie korupcję, nieprawidłowości, problemy lub tajne informacje, zwłaszcza wewnątrz organizacji" (ang. *a person who informs on another or makes public disclosure of corruption, wrongdoing, problems, or secret information, especially within an organization*)[16] albo ogólniej jako „osoba, która ujawnia coś tajnego lub donosi o kimś innym" (ang. *one who reveals something covert or who informs against another*)[17]. Podobnie omawiany termin pisany w formie *whistle-blower* definiowany jest jako „osoba próbująca podnieść alarm w sprawie jakiegoś problemu i nagłaśniać go wewnątrz lub na zewnątrz swojej organizacji" (ang. *a person who tries to raise the alarm about a problem and publicizes it inside and/or outside of his/her organization*)[18]. Co ciekawe, w chwili powstawania niniejszego artykułu *Słownik języka polskiego PWN* definiuje „sygnalistę" jedynie jako „osobę nadającą i odbierającą sygnały za pomocą odpowiednich urządzeń"[19], tym samym pomijając zupełnie tak powszechne i omawiane obecnie rozumienie tego słowa. Podobnie, co jednak zdaje się bardziej zrozumiałe, znaczenia tego nie zawiera *Słownik języka polskiego* pod red. W. Doroszewskiego, w którym „sygnalista", to „ten, kto nadaje i gra sygnały (np. na statku, w kopalni) za pomocą odpowiednich urządzeń, jak dzwonki, lampy, syreny alarmowe itp." Interesujące nas znaczenie „sygnalisty"[20], oprócz tożsamego do opisanych powyżej, znaleźć można dopiero w internetowym słowniku języka polskiego, znajdującym się na witrynie sieciowej SJP[21], który redagowany jest

---

[14] *Ralph Nader*, https://achievement.org/achiever/ralph-nader/ [dostęp: 30.08.2024].

[15] *Nader Riders*, https://pophistorydig.com/topics/naders-raiders-1968-1974/ [dostęp: 30.08.2024].

[16] *Whistleblower*, [w:] *Oxford English Dictionary*, https://www.dictionary.com/browse/whistleblower/ [dostęp: 30.08.2024], tłum. własne.

[17] *Whistleblower*, [w:] *Meriiam-Webster*, https://www.merriam-webster.com/dictionary/whistleblower/ [dostęp: 30.08.2024], tłum. własne.

[18] *Whistle-blower*, [w:] *Phrase Finder*, https://www.phrases.org.uk/meanings/whistle-blower.html/ [dostęp: 30.08.2024], tłum. własne.

[19] *Sygnalista*, [w:] *Słownik języka polskiego PWN*, https://sjp.pwn.pl/ [dostęp: 31.08.2024].

[20] *Sygnalista*, [w:] *Słownik języka polskiego*, red. W. Doroszewski, https://sjp.pwn.pl/doroszewski/sygnalista/ [dostęp: 31.08.2024].

[21] Zob. *SJP*, https://sjp.pl/, który to słownik powstał na bazie dawnego słownika do programu ispella, napisanego w 1971 r. przez R.E. Gorina i służącego do sprawdzania pisowni dla systemów uniksowych, a więc systemów operacyjnych rozwijanych od 1969 r. w Bell Labs przez UNIX System Laboratories.

obecnie przez hobbystów i udostępniany jest na otwartych licencjach[22], a w którym przyjęto, iż „sygnalista" to także „osoba zgłaszająca w dobrej wierze informacje o nieprawidłowościach w miejscu pracy"[23].

Odnosząc takie stwierdzenie do wspominanej wcześniej okoliczności wciąż ugruntowującego się znaczenia terminu „sygnalista", zrozumiała pozostaje aprobata doktryny wobec wprowadzenia na etapie prac nad projektem ustawy o ochronie sygnalistów zmiany terminologicznej i zastąpienia pojęcia „osoby dokonującej zgłoszenia lub ujawnienia publicznego" właśnie terminem „sygnalista"[24]. Choć przesadą byłoby określenie tego zabiegu postępowym, to odpowiada on dowiedzionemu faktowi utrwalenia się w praktyce jego angielskiego odpowiednika *whistleblower.* Z drugiej strony w doktrynie zwraca się także uwagę na okoliczność, iż w u.o.s. nie wprowadzono rozróżnienia pomiędzy pojęciem „osoby dokonującej zgłoszenia", nawet jeśli nie podlega ochronie, a „sygnalistą»[25], co prowadzi do powstania rozdźwięku pomiędzy powszechnym (potocznym) oraz ustawowym zakresem tego terminu.

Zakres podmiotowy ustawy, wskazujący na to, kto podlega ochronie jako sygnalista w sytuacji dokonania zgłoszenia lub ujawnienia publicznego, określony został w art. 4 u.o.s. i obejmuje każdą osobę dokonującą zgłoszenia lub ujawnienia, która informację o naruszeniu prawa pozyskuje w związku z pracą, przy czym związek ten rozumiany jest w sposób szeroki, albowiem obejmuje pracę, która potencjalnie miała nastąpić, lecz nie doszła do skutku, pracę trwającą oraz pracę, która była wykonywana w przeszłości. Przepis zawarty we wskazanym artykule zawiera także wyliczenie konkretnych osób objętych ochroną, lecz nie jest ono enumeratywne[26]. Co ciekawe, w art. 4 ust. 1 pkt 4 u.o.s. jako jeden z przykładów osób objętych ochroną wskazano przedsiębiorcę i jak zauważa się w doktrynie, sytuacja ta oznacza, że zgłoszenia lub ujawnienia publicznego może dokonać także kontrahent podmiotu prawnego, u którego miało dojść do naruszenia prawa[27].

Niezależnie od tego zauważyć należy, iż o ile sam termin *whistleblower* (a tym bardziej „sygnalista") w omawianym ujęciu posiada względnie krótką historię, o tyle rola, jaką potocznie przypisuje się osobie określanej tym terminem,

---

[22] *Ibidem*.

[23] *Sygnalista*, [w:] *SJP*, https://sjp.pl/sygnalista [dostęp: 31.08.2024].

[24] D. Tokarczyk, [w:] E. Rutkowska, D. Tokarczyk, *Ustawa o ochronie sygnalistów. Komentarz*, LEX/el. 2024, art. 4, https://sip.lex.pl/#/commentary/587977514/774954?keyword=Ustawa%20o%20ochronie%20sygnalist%C3%B3w.%20Komentarz&tocHit=1&cm=SFIRST/ [dostęp: 31.08.2024].

[25] *Ibidem*.

[26] *Ibidem*.

[27] *Ibidem*.

ma znacznie dłuższą historię. A. Stanger twierdzi, iż pierwszymi udokumentowanymi sygnalistami byli w 1777 r. amerykańscy marynarze, którzy w obliczu walki z Królestwem Wielkiej Brytanii podpisali 19 lutego 1777 r. na pokładzie jednostki USS Warren petycję do Kongresu Kontynentalnego, dokumentującą nadużycia ich dowódcy Eseka Hopkinsa[28]. Zdawać się może jednak, iż podejmowana w ten sposób próba określenia „pierwszych udokumentowanych sygnalistów" wyklucza bezzałożeniową metodę fenomenologiczną i zasadza się na problemie uprzedniego określenia swoistego minimum cech wymaganych do zakwalifikowania osoby jako „sygnalisty". Co stoi bowiem na przeszkodzie, aby bez tych założeń, świadomie narażając się na anachronizm, protoplastów współczesnych sygnalistów upatrywać w czasach znacznie odleglejszych? Chociażby pojawiający się w Starym Testamencie prorok Nathan odegrał kluczową rolę w historii króla Dawida i Batszeby, ponieważ gdy Dawid dopuścił się grzechu (zlecając zabójstwo Uriasza, aby poślubić jego żonę Batszebę), Nathan, świadomy tego czynu, skonfrontował Dawida z jego grzechem[29]. Nathan opowiedział przypowieść, która ujawniła niesprawiedliwość popełnioną przez króla, co z kolei doprowadziło do pokuty tego ostatniego[30]. Tak więc Nathan, podobnie jak sygnalista, podjął ryzyko, ujawniając nadużycie przez osobę będącą u szczytu władzy, a jego działania zmierzały do naprawienia niesprawiedliwości i przywrócenia moralnego porządku. Analogii tej zdaje się nie przeczyć okoliczność, iż panujący w Izraelu na przełomie XI i X w. p.n.e. ustrój polityczny niejako wymuszał, aby nieprawidłowość została zasygnalizowana przez tę samą osobę, która dopuściła się nieprawości, a więc przez króla (przy czym na potrzeby analogii akceptowalne są wątpliwości co do możliwości utożsamienia działania polegającego na „ujawnieniu naruszenia" z jego „uświadomieniem"). Zaznaczyć należy, iż prorok działał w środowisku, gdzie krytykowanie króla mogło prowadzić do represji, ale mimo to zdecydował się na ujawnienie prawdy, a jego odwaga przypomina współczesnych sygnalistów, którzy narażają się na zawodowe i osobiste konsekwencje w imię prawdy i sprawiedliwości. Współcześni sygnaliści również często stają w obliczu ryzyka utraty pracy, represji ze strony przełożonych, jednak mimo to decydują się na ujawnienie nieprawidłowości. Co więcej, celem Nathana nie było tylko oskarżenie Dawida, ale przede

[28] A. Stanger, *Whistleblowers: Honesty in America from Washington to Trump*, Harvard University Press, Cambridge 2019, s. 28.

[29] *Pismo Święte Starego i Nowego Testamentu*, Biblia Tysiąclecia, wyd. 5, Poznań 2000, 2 Sm 12, s. 1–15.

[30] *Ibidem*.

wszystkim doprowadzenie do pokuty i naprawienia krzywd. Jego działania były więc skierowane na przywrócenie sprawiedliwości, podobnie jak w przypadku sygnalistów, którzy działają zazwyczaj w celu ujawnienia prawdy i doprowadzenia do naprawienia szkód wyrządzonych przez działania niezgodne z prawem lub etyką (często w kontekście ochrony dobra publicznego).

W mitologii greckiej postacią, którą można uznać za protoplastę sygnalistów we współczesnym rozumieniu, jest Prometeusz, znany z tego, że sprzeciwił się woli Zeusa, dostarczając ludziom ogień, symbolizujący wiedzę, technologię i cywilizację. Tym samym Prometeusz ujawnił ludziom tajemnice, które były zastrzeżone dla bogów, działając wbrew zakazowi najwyższego autorytetu Zeusa[31]. Podobnie więc jak sygnaliści, którzy często sprzeciwiają się autorytetom w celu ujawnienia informacji ukrywanych przed społeczeństwem, Prometeusz podjął działanie, które miało na celu przyniesienie dobra publicznego, mimo że było to sprzeczne z interesami potężnych jednostek. Przekazanie ognia ludzkości było aktem, który miał na celu rozwój i dobrobyt całej rasy ludzkiej. W mitologii Prometeusz został surowo ukarany przez Zeusa za swoje działania, gdyż przykuto go do skały, gdzie codziennie orzeł kaukaski wyjadał mu wątrobę[32]. Kara ta stanowi niejako symbol represji, jakie mogą spotkać tych, którzy działają na przekór władzy. Podobnie jak Prometeusz współcześni sygnaliści często stają w obliczu poważnych konsekwencji, takich jak utrata pracy, procesy sądowe, a nawet zagrożenie dla życia, a to za swoje działania na rzecz dobra innych. Przykłady te ukazują, że chociaż idea sygnalizowania nieprawidłowości jest współczesnym terminem, jej moralne fundamenty sięgają znacznie głębiej, nawet do starożytności i są zakorzenione w tradycjach etycznych, religijnych, a także w mitach i legendach, które od wieków uczą nas o wartości odwagi, wiedzy i sprawiedliwości.

Dowodząc przemożnego wpływu tego zagadnienia na otaczającą nas rzeczywistość, można posłużyć się przykładem W.M. Felta, amerykańskiego prawnika i byłego zastępcy dyrektora Federalnego Biura Śledczego w Stanach Zjednoczonych Ameryki (FBI), który w maju 2005 r. ujawnił, iż w trakcie afery Watergate to on był źródłem informacji zwanym „Głębokie Gardło”[33], a więc ujawnił nielegalne działania administracji R. Nixona skierowane przeciwko jego przeciwnikom politycznym, co doprowadziło do ustąpienia tego polityka ze stanowiska prezydenta

[31] K. Kumaniecki, *Mitologia Greków i Rzymian*, Warszawa 1988, s. 45–48.

[32] *Ibidem*.

[33] J.D. O’Connor, *I’m the Guy They Called Deep Throat*, „Vanity Fair”, https://www.vanityfair.com/news/politics/2005/07/deepthroat200507?printable=true&currentPage=all/ [dostęp: 30.08.2024].

Stanów Zjednoczonych Ameryki[34]. Nie sposób także pominąć jako przykład sprawy E.J. Snowdena, byłego pracownika CIA i zleceniobiorcę firm Dell oraz Booz Allen Hamilton, który ujawnił kilkaset tysięcy poufnych, tajnych i ściśle tajnych dokumentów amerykańskiej wewnętrznej agencji wywiadowczej National Security Agency (NSA), co określono jako największy wyciek tajnych informacji w historii USA[35] (w tym m.in. informacje o programie PRISM, pozwalającym masowo podsłuchiwać rozmowy Amerykanów i obywateli innych krajów[36]). Symptomatyczna zdaje się już sama liczba możliwych do przytoczenia przypadków sygnalizowania nieprawidłowości, a to chociażby z ostatniej dekady, takich jak sprawy H. Wilkinsona[37], *Lux Leaks*[38], *Panama Papers*[39], *Novartis*[40] czy chociażby (wciąż tak nieodległy) przypadek L. Wenlianga, który był chińskim lekarzem pracującym w szpitalu w Wuhan, w prowincji Hubei i stał się znany jako sygnalista, który na początku pandemii COVID-19 próbował ostrzec swoich kolegów i władze chińskie o wybuchu nowego, groźnego wirusa przypominającego SARS, czego następstwem było upomnienie go przez chińskie władze[41].

Wśród polskich przykładów znanych sygnalistów wymienić należy przede wszystkim niezwykle doniosły historycznie przypadek J. Karskiego, polskiego kuriera i dyplomaty, który podczas II wojny światowej odegrał kluczową rolę jako sygnalista, kiedy to jako członek polskiego ruchu oporu na własne oczy zobaczył okrucieństwa Holocaustu, odwiedzając getto warszawskie i obóz przejściowy w Izbicy (zidentyfikowany przezeń mylnie jako obóz zagłady w Bełżcu), a zebrane przy tej

---

[34] R. Perlstein, *Watergate scandal*, [w:] *Encyclopaedia Britannica*, https://www.britannica.com/event/Watergate-Scandal/ [dostęp: 30.08.2024].

[35] M. Ray, *Edward Snowden*, [w:] *Encyclopaedia Britannica*, https://www.britannica.com/biography/Edward-Snowden/ [dostęp: 30.08.2024].

[36] *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program – The Washington Post*, „Washington Post", https://www.washingtonpost.com/ [dostęp: 30.08.2024].

[37] M. Todd, *Danske Bank Whistleblower Testifies at European Parliament*, Whistleblower Network News, https://whistleblowerprotection.eu/blog/danske-bank-whistleblower-testifies-at-european-parliament/ [dostęp: 30.08.2024].

[38] F. Shiel, *European court reverses course to rule in favor of LuxLeaks whistleblower*, https://www.icij.org/investigations/luxembourg-leaks/european-court-reverses-course-to-rule-in-favor-of-luxleaks-whistleblower/ [dostęp: 30.08.2024].

[39] M. Hudson, *The Panama Papers: Exposing the Rogue Offshore Finance Industry*, https://www.icij.org/investigations/panama-papers/ [dostęp: 30.08.2024].

[40] *United States Files Complaint Against Novartis Pharmaceuticals Corp. for Allegedly Paying Kickbacks to Doctors in Exchange for Prescribing Its Drugs*, https://www.justice.gov/opa/pr/united-states-files-complaint-against-novartis-pharmaceuticals-corp-allegedly-paying/ [dostęp: 30.08.2024].

[41] *Coronavirus kills Chinese whistleblower ophthalmologist, American Academy of Ophthalmology*, https://www.aao.org/education/headline/coronavirus-kills-chinese-whistleblower-ophthalmol/ [dostęp: 30.08.2024].

okazji informacje przekazał aliantom, osobiście informując o stwierdzonym procederze prezydenta Stanów Zjednoczonych Ameryki F.D. Roosevelta[42]. Mimo wysiłków J. Karskiego jego informacje nie wywołały natychmiastowej reakcji państw, które wspólnie przeciwstawiły się blokowi państw Osi, co nadaje staraniom J. Karskiego jako sygnalisty szczególnego tragizmu[43]. Wśród bardziej aktualnych przykładów można wspomnieć o mjr. M. Ratajczyku, który informował o możliwości złamania procedur wewnętrznych dotyczących izolacji chorych w zakładzie karnym w Garbalinie, gdzie w ciągu zaledwie kilku dni doszło do zakażenia się przez 82 osoby chorobą COVID-19, co miało się spotkać z naciskiem przełożonych na ograniczenie badania przypadków zakażeń[44].

W świetle przytoczonych dotychczas przykładów nie sposób kwestionować faktu, iż znaczenie działań sygnalistów, niezależnie od przyjętego zakresu tego pojęcia i wtórującego temu dziejowemu dorobkowi, pozostaje nieocenione. Znaczenie to zostało także dostrzeżone przez ustawodawcę europejskiego, czemu dano wyraz literalnie w treści dyrektywy 2019/1937, gdzie wskazano, że „zgłaszając naruszenia prawa Unii, które są szkodliwe dla interesu publicznego, osoby takie działają jako sygnaliści i tym samym odgrywają kluczową rolę w ujawnianiu takich naruszeń i zapobieganiu im oraz w ochronie dobra społecznego”[45]. Konstatacja ta przenosi nas z kolei do zagadnienia ewolucji roli „sygnalistów” w kontekście technologii cyfrowych, gdzie konieczne zdaje się odwołanie do truizmu, iż tym, co w istocie czyni rolę sygnalistów kluczową przy ujawnianiu i zapobieganiu naruszeń, a także stanowi zasadniczy element wspomnianego już minimum cech wymaganych do zakwalifikowania osoby jako „sygnalisty”, pozostaje „informacja”. Znalazło to odzwierciedlenie w dyrektywie 2019/1937 poprzez stwierdzenie, że „osoby pracujące dla organizacji publicznej lub prywatnej, lub utrzymujące kontakt z taką organizacją w związku ze swoją działalnością zawodową niejednokrotnie jako pierwsze dowiadują się o zagrożeniach, lub szkodach dla interesu publicznego, do jakich dochodzi w tym kontekście”[46]. *Prima facie* zdawać się może, iż tak błahe stwierdzenie nie może stanowić żadnego wkładu do dyskursu w zakresie omawianej tematyki, lecz w sposób przejrzysty obrazuje ono zarzewie ewolucji roli sygnalisty w kontekście

[42] J. Jankowski, J. Karski, *Raport tajnego emisariusza*, Kraków 2019, s. 222.

[43] A. Becker, *Messengers of Disaster: Raphael Lemkin, Jan Karski, and Others*, „Journal of Holocaust Studies” 2017, s. 114.

[44] *Epidemia w więzieniu? „Winny” sygnalista*, https://www.rp.pl/sluzby/art8644921-epidemia-w-wiezieniu-winny-sygnalista/ [dostęp: 30.08.2024].

[45] Zob. Preambuła dyrektywy 2019/1937 motyw 1.

[46] *Ibidem*.

technologii cyfrowych, albowiem o ile rola ta już w przeszłości istotnie oddziaływała na społeczeństwo, o tyle w dobie społeczeństwa informacyjnego oddziaływanie to ulega zasadniczej intensyfikacji.

Warto w tym miejscu przypomnieć, że pojęcie „społeczeństwo informacyjne" odnosi się do idei, iż informacja staje się centralnym zasobem, decydującym o rozwoju gospodarczym, społecznym i kulturalnym. Już w latach 60. XX w. japońscy badacze dostrzegli, że w wyniku postępu technologicznego i rosnącego znaczenia technologii informacyjnych społeczeństwo zaczyna ewoluować w kierunku, w którym informacja staje się kluczowym czynnikiem produkcji, obok pracy i kapitału[47]. Zrozumienie tej zmiany pozwala na lepsze uchwycenie roli sygnalistów w nowym, cyfrowym ekosystemie, gdzie sygnalista nie jest już jedynie osobą przekazującą istotne informacje na temat naruszeń, lecz staje się on także istotnym elementem obiegu informacji, której wartość nieustannie wzrasta. Informacja, będąca trzonem gospodarki opartej na wiedzy, zyskuje szczególną wagę w erze cyfrowej, gdzie dostęp do niej oraz jej właściwe zarządzanie mogą decydować o sukcesie lub porażce zarówno jednostek, jak i całych organizacji. Technologie cyfrowe, takie jak AI, *blockchain* czy *big data*, które rozwijały się równolegle z koncepcją społeczeństwa informacyjnego, przynoszą nowe wyzwania i możliwości w zakresie ochrony sygnalistów, ponieważ z jednej strony umożliwiają lepsze zabezpieczenie zgłoszeń oraz potencjalne zachowanie anonimowości, a z drugiej stawiają przed nami wyzwania związane z bezpieczeństwem danych, ich niezmiennością oraz odpowiedzialnością za decyzje podejmowane przez systemy algorytmiczne. W erze cyfrowej rola sygnalistów, choć zasadniczo opiera się na tych samych zasadach, to zyskuje jednak nowe, nieznane dotąd wymiary. O ile w przeszłości zakres działań sygnalistów ulegał zasadniczemu zawężeniu i to od czynników zewnętrznych zależała skala wpływu przekazywanych przez nich informacji, o tyle w dobie globalnych sieci informacyjnych sygnaliści samodzielnie mogą działać na skalę międzynarodową, przekazując informacje, które *per se* mogą wpłynąć na decyzje polityczne, gospodarcze, a nawet społeczne na całym świecie. Jednocześnie jednak rosnąca rola informacji w gospodarce stawia ich w jeszcze bardziej niebezpiecznej pozycji, narażając na represje zarówno ze strony organizacji, jak i rządów, co z kolei wymaga stosowania równie zaawansowanych środków ochrony, których tempo rozwoju musi co najmniej dorównywać tempu rozwoju technologii informa-

[47] K.J. Fietkiewicz, *The Development of Information Society in Japan: A Case Study of 21 Metropolitan Areas*, 2019, s. 3–5.

cyjnych. Dlatego tak ważne jest, aby prawo nadążało za omawianymi zmianami, oferując skuteczną ochronę i wsparcie dla tych, którzy decydują się ujawnić informacje na temat nieprawidłowości.

Podsumowując, ewolucja roli sygnalistów w erze cyfrowej odzwierciedla głębsze zmiany w strukturze społeczeństwa informacyjnego. W miarę jak informacja staje się centralnym zasobem naszej epoki, rośnie także znaczenie sygnalistów, którzy chronią jej integralność i przejrzystość. W tym kontekście sygnaliści nie tylko ujawniają naruszenia, ale również odgrywają kluczową rolę w kształtowaniu społeczeństwa przyszłości, w którym informacja jest nie tylko cennym zasobem, ale także narzędziem służącym do budowania bardziej sprawiedliwego i przejrzystego świata.

2. Rewolucja w zakresie ochrony sygnalistów i kanałów zgłaszania oraz towarzyszące im wyzwania prawodawcze w erze cyfrowej

Rewolucja cyfrowa, której jesteśmy świadkami, znacząco wpłynęła na niemal wszystkie aspekty życia społecznego i gospodarczego, w tym na oczekiwania wobec tego, w jaki sposób rewolucji tej sprosta prawo. O ile więc w kontekście ochrony sygnalistów osoby zgłaszające naruszenia doświadczają zarówno nowych możliwości, jak i wyzwań, o tyle po stronie ustawodawcy rozwój technologii cyfrowych sprowadza się przede wszystkim do wyzwań, z jakimi musi się zmierzyć. W odpowiedzi na te zmiany, zarówno na poziomie unijnym, jak i krajowym, wprowadzane są nowe regulacje, które mają na celu ochronę osób zgłaszających nieprawidłowości, i choć prawo chroniące sygnalistów jest stosunkowo nowym zjawiskiem w systemach prawnych na świecie, to idea ochrony tych, którzy odważają się zgłaszać naruszenia prawa, ma już swoje korzenie w poprzednich wiekach. W Stanach Zjednoczonych Ameryki namiastka przepisów z zakresu ochrony sygnalistów znalazła formalne odzwierciedlenie już w XVIII w., a to wraz z uchwaleniem ustawy *False Claims Act* w 1863 r.[48], która miała na celu walkę z korupcją i nadużyciami w czasie wojny secesyjnej. *False Claims Act* nie tylko chroniła sygnalistów, ale również oferowała im odszkodowania za ujawnienie nieprawidłowości, co miało na celu zachęcanie do zgłaszania przypadków oszustw. Kolejny wiek przyniósł dalszy rozwój ochrony prawnej sygnalistów w USA, którego owocami były m.in. takie

[48] *The False Claims Act*, https://www.justice.gov/civil/false-claims-act/ [dostęp: 30.08.2024].

ustawy, jak: *Lloyd–La Follette Act* z dnia 24 sierpnia 1912 r.[49], *Solid Waste Disposal Act* z dnia 20 października 1965 r.[50], czy *Whistleblower Protection Act* z dnia 10 kwietnia 1998 r.[51] W Europie prawo chroniące sygnalistów miało dotychczas wymiar epizodyczny[52] i zaczęło zyskiwać na znaczeniu w latach 90., czego przykładem jest *Public Interest Disclosure Act*, który wszedł w życie w Zjednoczonym Królestwie Wielkiej Brytanii i Irlandii Północnej 2 lipca 1998 r.[53]

W Polsce ochrona sygnalistów, jako formalne zagadnienie prawne, zaczęła zyskiwać na znaczeniu stosunkowo późno. W czasach Polskiej Rzeczpospolitej Ludowej (RPL) system prawny był ściśle kontrolowany przez władze komunistyczne, co sprawiało, że formalne mechanizmy ochrony sygnalistów (w przedmiotowym znaczeniu, które należy odróżnić od zjawiska denuncjacji władzom PRL) były ograniczone. Po upadku komunizmu w 1989 r. Polska weszła na ścieżkę transformacji ustrojowej, jednak formalna ochrona sygnalistów jako osobna kategoria i zagadnienie prawne nadal nie występowała. Współczesny rozwój prawa chroniącego sygnalistów w Polsce jest ściśle związany ze wdrażaniem dyrektywy 2019/1937, która stała się podstawą dla u.o.s. i była kluczowym krokiem w ustanowieniu nowoczesnych mechanizmów ochrony sygnalistów w Polsce.

Nie będzie chyba przesadą stwierdzenie, że dyrektywa 2019/1937 stanowi podwalinę dla próby uporania się z jednym z najbardziej aktualnych wyzwań Unii Europejskiej (UE), jakim jest problem ochrony sygnalistów. W czasach dynamicznych zmian technologicznych, globalizacji oraz rosnącej świadomości społecznej konieczność wprowadzenia jednolitych standardów ochrony dla osób zgłaszających naruszenia prawa stała się nieodzownym elementem wzmocnienia rządów prawa i demokracji w państwach członkowskich UE. Prace nad dyrektywą 2019/1937

---

[49] *Lloyd-La Follette Act of 1912*, https://whistleblower.house.gov/resources/all-resources/committee-jurisdiction-tool/whistleblowing-executive-branch-employee/lloyd-la-follette-act-1912/ [dostęp: 30.08.2024].

[50] *Filing Whistleblower Complaints Under the Solid Waste Disposal Act*, https://www.osha.gov/sites/default/files/publications/OSHA3815.pdf/ [dostęp: 30.08.2024].

[51] *Whistleblower Protections – Rights Of Employees [5 U.s.c. §2302 (B)(8)]*, https://www.americorps.gov/sites/default/files/document/2021_08_27_Whistleblower_Rights_Employees_OGC.pdf/ [dostęp: 30.08.2024].

[52] D. Huseynova, K. Piperigos, *Justice for justice: Protecting whistleblowers in the EU protection of whistleblowers – the why and the how*, http://transparency.eu/wp-content/uploads/2018/04/WB_Transparency-Group-CoE-17-18.pdf, *cit. per* B. Baran, 1. *Wprowadzenie*, [w:] B. Baran, M. Ożóg (red.), *Ochrona sygnalistów. Regulacje dotyczące osób zgłaszających nieprawidłowości*, Warszawa 2021.

[53] *Guidance Whistleblowing and the Public Interest Disclosure Act 1998 (c.23) (accessible version)*, https://www.gov.uk/government/publications/whistleblowing-and-the-public-interest-disclosure-act-1998-c23/whistleblowing-and-the-public-interest- disclosure-act-1998-c23-accessible-version/ [dostęp: 30.08.2024].

zostały zainicjowane w odpowiedzi na rosnące zapotrzebowanie na jednolite standardy ochrony sygnalistów w UE, ponieważ wcześniejsze regulacje w tym zakresie były fragmentaryczne i różniły się w zależności od państwa członkowskiego. Niektóre kraje wprowadziły już wcześniej kompleksowe przepisy chroniące sygnalistów, podczas gdy inne państwa członkowskie miały jedynie ograniczone ramy prawne, które nie gwarantowały pełnej ochrony przed działaniami odwetowymi[54]. Dyrektywa 2019/1937 powstała więc z myślą o zniwelowaniu tych różnic.

Celem dyrektywy 2019/1937 jest przede wszystkim ustanowienie minimalnych standardów ochrony sygnalistów w całej UE i w tym celu zobowiązuje ona państwa członkowskie do wprowadzenia przepisów krajowych, które będą chronić osoby zgłaszające naruszenia prawa UE przed działaniami odwetowymi oraz zapewnią im dostęp do skutecznych mechanizmów zgłaszania nieprawidłowości. Dyrektywa 2019/1937 obejmuje szeroki zakres naruszeń, które mogą być zgłaszane przez sygnalistów. Zgodnie z art. 2 ust. 1 dyrektywy 2019/1937 ma ona zastosowanie do zgłoszeń dotyczących naruszeń przepisów UE w takich dziedzinach jak: zamówienia publiczne, usługi finansowe, bezpieczeństwo produktów, ochrona środowiska, ochrona zdrowia publicznego, ochrona konsumentów, ochrona prywatności i danych osobowych oraz bezpieczeństwo sieci i systemów informatycznych. Jednym z najważniejszych postanowień dyrektywy 2019/1937 jest obowiązek wprowadzenia przez państwa członkowskie UE efektywnych i bezpiecznych mechanizmów zgłaszania naruszeń prawa[55]. Art. 7 dyrektywy 2019/1937 zobowiązuje państwa członkowskie do zapewnienia, że osoby mające wiedzę o naruszeniach będą mogły je zgłaszać zarówno wewnętrznie, jak i zewnętrznie. Wewnętrzne kanały zgłaszania (art. 8 dyrektywy 2019/1937) muszą być dostępne dla wszystkich pracowników oraz innych osób związanych zawodowo z organizacją, np. kontrahentów czy stażystów. Pracodawcy mają obowiązek ustanowienia wewnętrznych procedur, które umożliwią sygnalistom zgłaszanie naruszeń w sposób poufny i zabezpieczający przed ujawnieniem ich tożsamości. Zewnętrzne kanały zgłaszania (art. 10 dyrektywy 2019/1937) powinny być ustanowione przez odpowiednie organy publiczne, które będą przyjmować zgłoszenia dotyczące naruszeń prawa UE. Te organy muszą także zapewnić, że informacje zgłaszane przez sygnalistów będą chronione i że sygnaliści nie będą narażeni na żadne formy represji z tego tytułu. Dyrektywa 2019/1937 wprowadza także bezwzględny zakaz działań odwetowych wobec sygnalistów (art. 19 dyrekty-

[54] J. Murszewski, *Problemy implementacji dyrektywy 2019/1937 do polskiego porządku prawnego*, [w:] B. Baran, M. Ożóg (red.), *op. cit*.

[55] *Ibidem*.

wy 2019/1937). Działania te mogą obejmować różnorodne formy represji, od zwolnienia z pracy, przez degradację, po subtelniejsze formy nacisku, jak np. pogorszenie warunków pracy czy odmowa awansu. Dyrektywa 2019/1937 wymaga, aby państwa członkowskie UE wprowadziły przepisy gwarantujące ochronę sygnalistów przed takimi działaniami, a także umożliwiły im dochodzenie swoich praw w przypadku, gdyby doszło do naruszenia tych przepisów. Nakłada ona także na państwa członkowskie UE obowiązek zapewnienia, że tożsamość sygnalistów będzie chroniona na każdym etapie procesu zgłaszania i rozpatrywania naruszeń. Poufność danych sygnalistów ma kluczowe znaczenie dla skuteczności mechanizmów zgłaszania, ponieważ obawa przed ujawnieniem tożsamości może skutecznie zniechęcać do zgłaszania nieprawidłowości (art. 16 dyrektywy 2019/1937). Zgodnie z art. 17 dyrektywy 2019/1937 państwa członkowskie UE muszą również wprowadzić odpowiednie środki ochrony danych osobowych sygnalistów, zgodnie z ogólnymi przepisami o ochronie danych, takimi jak rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO). Ochrona ta obejmuje zarówno dane osobowe sygnalistów, jak i wszelkie informacje, które mogłyby prowadzić do ich identyfikacji.

Proces implementacji dyrektywy 2019/1937 w państwach członkowskich UE napotkał liczne wyzwania. W Polsce prace nad implementacją dyrektywy 2019/1937 rozpoczęły się dopiero pod koniec 2021 r., co spowodowało znaczące opóźnienia względem harmonogramu narzuconego przez dyrektywę 2019/1937. Ostatecznie wejście w życie przepisów u.o.s. przypadło na dzień 25 września 2024 r. i regulują one szeroki zakres kwestii związanych z ochroną osób zgłaszających naruszenia prawa. Ustawa ta, zgodnie z art. 1 u.o.s., reguluje m.in. warunki objęcia ochroną sygnalistów, środki ochrony przed działaniami odwetowymi, zasady ustalania wewnętrznych procedur zgłaszania naruszeń oraz zadania Rzecznika Praw Obywatelskich w tym zakresie. Ustawa o ochronie sygnalistów definiuje także pojęcia kluczowe dla jej stosowania, takie jak „działanie odwetowe", „informacja o naruszeniu prawa" czy „kontekst związany z pracą" (art. 2 u.o.s.). Ustawa wprowadza obowiązek ustanowienia przez pracodawców wewnętrznych procedur zgłaszania naruszeń, które muszą być zgodne z wymogami określonymi w ustawie. Zgodnie z art. 8 u.o.s. procedury te muszą być transparentne, dostępne i zapewniać poufność zgłoszeń. Pracodawcy są zobowiązani do informowania pracowników o dostępnych kanałach zgłaszania oraz o przysługujących im prawach. W kontekście zgłoszeń zewnętrznych art. 10 u.o.s. nakłada obowiązek przyjmowania takich zgłoszeń przez odpowiednie organy publiczne, które są zobowiązane do ich rozpatrywania w sposób bezstronny i rzetelny. Ustawa o ochronie sygnalistów przewiduje także możliwość dokonania tzw. ujaw-

nienia publicznego, które może nastąpić, jeśli zgłoszenie wewnętrzne lub zewnętrzne nie przyniosło oczekiwanego rezultatu, a naruszenie prawa stanowi bezpośrednie zagrożenie dla interesu publicznego (art. 51 u.o.s.). Kluczowym elementem ustawy są przepisy dotyczące ochrony sygnalistów przed działaniami odwetowymi. Art. 11 u.o.s. wprowadza zakaz podejmowania jakichkolwiek działań odwetowych wobec sygnalistów, a także prób lub groźby zastosowania takich działań. Sygnaliści, którzy doświadczą działań odwetowych, mają prawo do odszkodowania, którego wysokość nie może być niższa niż przeciętne miesięczne wynagrodzenie w gospodarce narodowej (art. 14 u.o.s.). Ustawa przewiduje także możliwość zadośćuczynienia za szkody niematerialne, takie jak naruszenie dóbr osobistych sygnalisty.

Już na pierwszy rzut oka samo wyliczenie kwestii objętych ustawą o ochronie sygnalistów wskazuje na stosunkowo szerokie uregulowanie tej problematyki, lecz w kontekście rosnącej liczby regulacji dotyczących ochrony danych osobowych oraz ochrony sygnalistów widoczny staje się brak pełnej harmonizacji między kluczowymi aktami prawnymi UE i Rzeczpospolitej Polskiej (RP). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, RODO)[56], ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych[57] oraz ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów stawiają przed praktykami prawa i przedsiębiorstwami wyzwania, które mogą prowadzić do poważnych problemów z interpretacją i wdrażaniem odpowiednich procedur. Celem RODO jest zapewnienie wysokiego poziomu ochrony danych osobowych oraz ujednolicenie przepisów dotyczących ich przetwarzania na poziomie UE. Z drugiej strony u.o.s. wdraża do polskiego porządku prawnego dyrektywę 2019/1937, której celem jest ochrona osób zgłaszających naruszenia prawa, tzw. sygnalistów. Podczas gdy RODO koncentruje się na ochronie prywatności i danych osobowych, u.o.s. ma na celu zapewnienie bezpieczeństwa i ochrony osobom, które ujawniają nieprawidłowości, często narażając się na działania odwetowe. W praktyce oba te akty prawne mogą się wzajemnie przenikać, co prowadzi do licznych wyzwań związanych z ich wdrażaniem. Jednym z kluczowych punktów styku pomiędzy RODO a u.o.s. jest przetwarzanie danych osobowych w ramach systemów zgłoszeń. Przepisy u.o.s. wymagają, aby organizacje ustanowiły procedury umożli-

[56] Dz. Urz. UE L 119 z 2016 r. (dalej: „RODO").
[57] Dz. U. z 2019 r. poz. 1781 (dalej: „u.o.d.o.").

wiające zgłaszanie naruszeń prawa, które mogą zawierać dane osobowe, zarówno sygnalistów, jak i osób, których dotyczy zgłoszenie. Jak stanowi art. 5 RODO, przetwarzanie danych osobowych powinno być zgodne z zasadami legalności, rzetelności i przejrzystości, a także ograniczone do niezbędnego minimum. Jednak art. 4 ust. 3 u.o.s. pozwala na przetwarzanie danych osobowych w zakresie niezbędnym do realizacji celów zgłoszenia bez konieczności informowania osoby, której dane dotyczą, o ich przetwarzaniu, co w normalnych warunkach byłoby wymagane przez RODO, a to zgodnie z art. 13 i 14 RODO. Takie odstępstwo ma na celu ochronę sygnalistów i osób zaangażowanych w proces zgłaszania przed potencjalnymi działaniami odwetowymi. Mimo że takie rozwiązanie jest uzasadnione z punktu widzenia ochrony sygnalistów, może prowadzić do konfliktów z zasadami ochrony danych osobowych ustanowionymi przez RODO.

Co więcej, zgodnie z art. 14 RODO administrator danych osobowych jest zobowiązany do poinformowania osoby, której dane dotyczą, o przetwarzaniu jej danych, co stanowi kluczowy element zapewniający transparentność przetwarzania danych osobowych. W kontekście u.o.s. ten obowiązek informacyjny może jednak kolidować z potrzebą zapewnienia anonimowości i bezpieczeństwa sygnalistom. Co prawda w art. 14 ust. 5 lit. b RODO przewidziano możliwość wyłączenia obowiązku informacyjnego, jeśli jego realizacja mogłaby uniemożliwić lub poważnie utrudnić osiągnięcie celów przetwarzania danych. W praktyce oznacza to, że organizacje korzystające z przepisów u.o.s. mogą nie być zobowiązane do informowania osób, których dane dotyczą, o ich przetwarzaniu, jeśli mogłoby to narazić sygnalistę na działania odwetowe, jednakże brak jednoznaczności w stosowaniu tych przepisów może prowadzić do niepewności prawa. Przykładowo, jeśli zgłoszenie dotyczy poważnych naruszeń, takich jak korupcja, przestępstwa finansowe czy mobbing, organizacja musi balansować między obowiązkiem ochrony danych osobowych a potrzebą zapewnienia bezpieczeństwa sygnalistom. W praktyce decyzje te mogą prowadzić do różnic interpretacyjnych i potencjalnych naruszeń przepisów RODO.

Kolejnym aspektem, który wymaga uwagi, jest przetwarzanie danych wrażliwych, takich jak informacje o stanie zdrowia, orientacji seksualnej czy przynależności do związków zawodowych, które mogą być częścią zgłoszenia sygnalisty. Art. 9 ust. 1 RODO generalnie zakazuje przetwarzania takich danych, chyba że spełnione są określone warunki, jak np. wyraźna zgoda osoby, której dane dotyczą, lub jeśli przetwarzanie jest niezbędne do ochrony interesów publicznych. Natomiast u.o.s. nie precyzuje jednoznacznie, w jaki sposób takie dane powinny być przetwarzane w kontekście zgłoszeń. W praktyce oznacza to, że administratorzy

danych muszą podejmować *ad hoc* decyzje, które mogą nie być zgodne z wymogami RODO. Może to prowadzić do sytuacji, w których dane wrażliwe są przetwarzane w sposób, który narusza przepisy RODO, co z kolei może skutkować nałożeniem kar na organizację. Kolejnym wyzwaniem jest rozbieżność terminologiczna i proceduralna pomiędzy RODO a ustawą o ochronie sygnalistów. Przykładowo podczas gdy RODO posługuje się pojęciami takimi jak „administrator danych", „podmiot przetwarzający" czy „osoba, której dane dotyczą", u.o.s. wprowadza swoje pojęcia, takie jak „sygnalista" czy „zgłoszenie". Takie różnice, mimo że z perspektywy każdego z tych aktów z osobna zdawać się mogą zasadne, to mogą prowadzić do nieporozumień w interpretacji przepisów oraz trudności w ich praktycznym zastosowaniu. Co więcej, u.o.s. wprowadza specyficzne procedury zgłoszeń, które mogą kolidować z obowiązkami wynikającymi z RODO. Przykładowo art. 6 ust. 1 u.o.s. przewiduje, że zgłoszenia powinny być przyjmowane i rozpatrywane w sposób zapewniający maksymalną poufność, jednakże RODO wymaga, aby przetwarzanie danych osobowych odbywało się w sposób przejrzysty i zrozumiały dla osób, których dane dotyczą (art. 12 RODO). Te dwie zasady mogą być trudne do pogodzenia w praktyce, co już obecnie prowadzi do dylematów, jak zapewnić zgodność z obiema regulacjami.

Brak pełnej harmonizacji między tymi aktami prawnymi może prowadzić do różnic interpretacyjnych na poziomie krajowym i europejskim, bowiem państwa członkowskie UE mają możliwość dostosowania swoich przepisów krajowych do wymogów zarówno RODO, jak i dyrektywy 2019/1937, a różnice te mogą prowadzić do niejasności i niejednolitości w stosowaniu prawa. Brak harmonizacji pomiędzy RODO a u.o.s. stawia natomiast szereg poważnych wyzwań przed praktykami, a wiążące się z nimi ewentualne konsekwencje mogą mieć wymiar nie tylko prawny, lecz także finansowy. W tej sytuacji w celu minimalizacji ryzyka organizacje już obecnie powinny podejmować działania mające na celu zapewnienie zgodności z obiema regulacjami.

Konfrontując wskazane prawodawcze trudności w zakresie implementacji i harmonizacji przepisów z problematyką rozwoju technologii cyfrowych, stwierdzić należy, iż te spowodowały prawdziwą rewolucję w obszarze kanałów zgłaszania naruszeń. Tradycyjne formy zgłaszania, takie jak bezpośrednie raportowanie przełożonym czy korzystanie z linii telefonicznych, coraz częściej ustępują miejsca bardziej zaawansowanym technologicznie systemom, które oferują wyższy poziom anonimowości, bezpieczeństwa i efektywności. Nowoczesne kanały zgłaszania wykorzystują takie technologie jak AI, *blockchain*, a także różnorodne aplikacje mo-

bilne i internetowe, które wspierają sygnalistów w zgłaszaniu naruszeń w sposób bezpieczny i dyskretny. Tradycyjne kanały zgłaszania naruszeń miały istotne ograniczenia, w tym chociażby były narażone na brak poufności, co z kolei potęgowało ryzyko represji sygnalistów, a tym samym rzutowało także na problemy z efektywnością i czasem reakcji przy zgłaszaniu nieprawidłowości. Ponadto w wielu przypadkach sygnaliści nie mieli pewności, czy ich zgłoszenie dotrze do właściwych osób i czy zostanie potraktowane w sposób należyty. Technologie cyfrowe umożliwiają poprawę jakości i bezpieczeństwa kanałów zgłaszania, czego przykładem mogą być chociażby anonimowe platformy internetowe (takie jak GlobaLeaks[58], SecureDrop[59], Falcony[60], Navex[61] czy BKMS System[62]), aplikacje mobilne z funkcjami szyfrowania (takie jak Signal[63], Tella[64], Haven[65] czy Orbot[66]) oraz narzędzia do zgłaszania oparte na *blockchain* (takich jak Diss-co[67] czy FixNix[68]), które pokazują, jak technologia może zrewolucjonizować proces zgłaszania naruszeń.

Jednym z bardziej innowacyjnych zastosowań technologii w kontekście zgłaszania naruszeń jest wykorzystanie AI (jak chociażby w przypadku produktu SpeakUp[69]), która pozwala analizować zgłoszenia, identyfikować wzorce sugerujące naruszenia oraz wspierać organizacje w szybszym i dokładniejszym reagowaniu na zgłoszenia. AI może także wspierać sygnalistów poprzez automatyzację procesów, takich jak wstępna ocena zgłoszenia czy filtrowanie informacji, co pozwala na bardziej efektywne zarządzanie zgłoszeniami w organizacjach. Jednakże zastosowanie AI pociąga za sobą także pewne wyzwania, które muszą być starannie zarządzane, aby unikać potencjalnych zagrożeń związanych z błędami algorytmów, dyskryminacją, a także naruszeniami prywatności i bezpieczeństwa. W tym kontekście kluczowe znaczenie mają normy, takie jak norma BS ISO/IEC 42001:2023[70] oraz regulacje, np. rozporządzenie Parlamentu Europejskiego i Rady

---

[58] Globaleaks, https://www.globaleaks.org/ [dostęp: 30.08.2024].
[59] Securedrop, https://securedrop.org/ [dostęp: 30.08.2024].
[60] Falcony, https://www.falcony.io/ [dostęp: 30.08.2024].
[61] Navex, https://www.navex.com/ [dostęp: 30.08.2024].
[62] EQS Group System BKMS, https://www.eqs.bkms-system.com/ [dostęp: 30.08.2024].
[63] Signal, https://signal.org/pl/ [dostęp: 30.08.2024].
[64] Tella, https://tella-app.org/ [dostęp: 30.08.2024].
[65] Guardianproject, Haven, https://guardianproject.github.io/haven/ [dostęp: 30.08.2024].
[66] Guardianproject, Orbot, https://orbot.app/en/ [dostęp: 30.08.2024].
[67] DISS-CO, https://diss-co.tech/ [dostęp: 30.08.2024].
[68] Fixnix, https://www.fixnix.co/ [dostęp: 30.08.2024].
[69] SpeakUp, https://www.speakup.com/ [dostęp: 30.08.2024].
[70] *ISO/IEC 42001:2023, Artificial Intelligence Management Systems – Requirements*, https://www.iso.org/standard/81230.html/ [dostęp: 30.08.2024].

(UE) 2024/1689 z dnia 13 czerwca 2024 r. ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (tzw. akt w sprawie sztucznej inteligencji, AI Act)[71], które określają zasady i wymogi dotyczące projektowania, wdrażania oraz monitorowania systemów AI. Algorytmy AI muszą być starannie zaprojektowane, aby uniknąć błędów, które mogą prowadzić do fałszywych oskarżeń lub ignorowania ważnych zgłoszeń. Według standardu ISO/IEC 42001:2023 organizacje muszą wdrożyć kompleksowy proces zarządzania ryzykiem, który obejmuje ocenę wpływu AI na różne aspekty działalności, w tym ryzyko związane z błędami algorytmicznymi i ich konsekwencjami. Ponadto zgodnie z klauzulą A.2.4 BS ISO/IEC 42001 organizacje powinny regularnie przeglądać i aktualizować politykę AI, aby zapewnić jej ciągłą adekwatność i skuteczność w świetle zmieniających się technologii i wymagań biznesowych.

Zapewnienie przejrzystości decyzji podejmowanych przez AI jest kluczowe, aby budować zaufanie i spełniać wymagania prawne. Przykładowo AI Act kładzie silny nacisk na konieczność projektowania systemów AI w sposób zapewniający ich przejrzystość[72] oraz nakłada na dostawców systemów AI obowiązek dostarczenia szczegółowej dokumentacji technicznej, która umożliwia zrozumienie sposobu działania algorytmów oraz umożliwia ocenę ich zgodności z wymaganiami prawnymi[73]. Dokumentacja ta powinna zawierać informacje o architekturze systemu, użytych danych, metodach testowania oraz procedurach walidacji, co pozwala na dokładne monitorowanie i kontrolę systemu w trakcie jego użytkowania. Kolejnym ważnym aspektem przy wykorzystaniu technologii AI jest zarządzanie ryzykiem i zgodność z etyką. Norma BS ISO/IEC 42001:2023 wskazuje, że organizacje muszą uwzględniać aspekty etyczne na każdym etapie cyklu życia systemu AI, od jego projektowania po wdrożenie i użytkowanie[74]. Systemy AI powinny być projektowane w sposób minimalizujący ryzyko dyskryminacji oraz zapewniający zgodność z przepisami dotyczącymi ochrony danych osobowych, takimi jak przepisy RODO. AI Act dodatkowo podkreśla konieczność nadzoru nad systemami AI tak, aby zapobiec potencjalnym naruszeniom praw człowieka i zapewnić ich zgodność z obowiązującymi standardami etycznymi oraz zapewniać przejrzystość działań, oraz chronić prawa i interesy wszystkich zainteresowanych stron[75].

---

[71] Dz. Urz. UE L 1689 z 2024 r. (dalej: „AI Act").
[72] Zob. art. 13 AI Act.
[73] Zob. art. 16 AI Act.
[74] Zob. B.6.1.2 oraz B.9.3. normy BS ISO/IEC 42001:2023.
[75] Zob. art. 14 AI Act.

Technologia *blockchain*, znana powszechnie przede wszystkim za sprawą fenomenu popularności kryptowalut, znalazła swoje zastosowanie również w kontekście ochrony sygnalistów. *Blockchain* oferuje zaawansowaną architekturę umożliwiającą tworzenie zdecentralizowanych rejestrów, które charakteryzują się niezmiennością oraz wysokim poziomem przejrzystości i bezpieczeństwa. Mechanizm działania *blockchain* opiera się na rozproszonej sieci komputerów (tzw. węzłów), z których każdy posiada kopię tego samego rejestru. Każda nowa transakcja, zgłoszenie czy wpis do tego rejestru muszą zostać zatwierdzone przez konsensus większości węzłów, co uniemożliwia jednostronne wprowadzanie zmian w danych, zapewniając ich integralność. Niezmienność danych w *blockchain* jest zapewniona przez algorytmy kryptograficzne, które tworzą unikalny identyfikator (ang. *hash*) dla każdej operacji. Gdy operacja (zapis) zostaje dodana do bloku, jest on kryptograficznie powiązany z poprzednim blokiem, tworząc w ten sposób łańcuch bloków (ang. *blockchain*). Zmiana któregokolwiek z wcześniejszych bloków wymagałaby zmodyfikowania wszystkich kolejnych bloków w łańcuchu oraz uzyskania zgody większości węzłów, co jest praktycznie niemożliwe do osiągnięcia bez wykrycia[76]. Dzięki *blockchain* sygnaliści mogą mieć pewność, że ich zgłoszenie nie zostanie zmanipulowane ani usunięte, co jest kluczowe dla zachowania zaufania do systemów zgłaszania. Pomimo licznych zalet *blockchain* niesie ze sobą także pewne wyzwania. Wdrożenie tej technologii wymaga znacznych zasobów[77], a także specjalistycznej wiedzy, co może być barierą dla mniejszych organizacji. Ponadto pojawiają się pytania dotyczące skalowalności i zgodności z przepisami o ochronie danych osobowych, zwłaszcza w kontekście unijnych przepisów RODO.

Mając na uwadze wskazane spostrzeżenia, nie będzie stanowić nadużycia stwierdzenie, że jednym z największych wyzwań w kontekście nowoczesnych kanałów zgłaszania naruszeń przez sygnalistów jest zapewnienie im bezpieczeństwa i anonimowości. Chociaż technologie cyfrowe oferują zaawansowane narzędzia szyfrowania i ochrony danych, nie eliminują one całkowicie ryzyka naruszeń prywatności. W erze cyfrowej, gdzie inwigilacja i gromadzenie danych są na porządku dziennym, sygnaliści mogą czuć się niepewnie, czy ich zgłoszenia rzeczywiście pozostaną anonimowe i bezpieczne. Oprócz technologii kluczowe znaczenie ma

[76] Z. Zheng *et al.*, *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*, [w:] *2017 IEEE 6th International Congress on Big Data, IEEE Computer Society*, 2017, s. 557–559.

[77] P. Sharma, R. Jindal, M. D. Borah, *A Review of Blockchain-Based Applications and Challenges*, [w:] *Wireless Personal Communications*, 2022, s. 1201–1243.

także kultura organizacyjna i odpowiednie szkolenie personelu odpowiedzialnego za obsługę zgłoszeń. Właściwe zarządzanie systemami zgłoszeń, a także regularne audyty bezpieczeństwa są niezbędne do zapewnienia, że sygnaliści będą mieli zaufanie do nowoczesnych kanałów zgłaszania. Szczególnie istotne pozostaje więc, aby technologie wykorzystywane w kanałach zgłaszania były zgodne z obowiązującymi przepisami prawa, w tym wspomnianymi już przepisami RODO, u.o.d.o., AI Act, dyrektywy 2019/1937 czy u.o.s., dlatego też wdrożenie systemów opartych na AI czy *blockchain* wymaga każdorazowo szczegółowej analizy prawnej, aby zapewnić zgodność z wymogami dotyczącymi ochrony danych, poufności oraz odpowiedzialności.

Rozwój technologii cyfrowych i ich integracja z systemami ochrony sygnalistów wymaga też ciągłej aktualizacji i harmonizacji przepisów prawnych. W miarę jak technologie takie jak AI i *blockchain* stają się coraz bardziej powszechne, konieczne jest dostosowanie przepisów prawnych, aby zapewnić ich skuteczność i zgodność z dynamicznie zmieniającym się otoczeniem technologicznym. W tym kontekście ustawodawcy muszą podejmować działania mające na celu stworzenie elastycznych ram prawnych, które będą mogły reagować na nowe wyzwania wynikające z postępu technologicznego. Harmonizacja przepisów na poziomie międzynarodowym jest również kluczowa, aby zapewnić spójność regulacji dotyczących ochrony sygnalistów w różnych jurysdykcjach. W dobie globalizacji sygnaliści mogą działać na różnych rynkach i w różnych systemach prawnych, co wymaga rozwijania i popularyzowania międzynarodowych standardów ochrony, które będą uwzględniać specyfikę cyfrowego środowiska. Przyszłość ochrony sygnalistów będzie więc zależała od zdolności ustawodawców do adaptacji przepisów prawnych do szybko zmieniającego się otoczenia technologicznego oraz od umiejętności organizacji w skutecznym wdrażaniu nowoczesnych systemów zgłaszania, które będą spełniać najwyższe standardy bezpieczeństwa i zgodności z przepisami. Z tej perspektywy szczególnie istotne jest także to, aby regulacje dotyczące ochrony sygnalistów nadążały za rozwojem technologicznym w ten sposób, aby na bieżąco chronić skutecznie sygnalistów w zmieniającym się otoczeniu technologicznym, co w obliczu zasadniczej dyferencji pomiędzy tempem rozwoju AI, liczonym w tygodniach i miesiącach a tempem implementacji prawodawstwa (czego przykładem może być wdrożenie u.o.s., która zgodnie z założeniami dyrektywy 2019/1937 powinna być wprowadzona przez kraje członkowskie UE do 17 grudnia 2021 r.) zdaje się pozostawać wciąż odległym ideałem.

3. Możliwości i perspektywy rozwoju problematyki

AI, która już teraz odgrywa kluczową rolę w wielu dziedzinach, ma potencjał, aby jeszcze bardziej zrewolucjonizować systemy zgłaszania naruszeń. Zaawansowane algorytmy AI mogą nie tylko analizować zgłoszenia i identyfikować potencjalne naruszenia, ale potencjalnie także przewidywać i zapobiegać przyszłym problemom na podstawie analizy wzorców danych. Takie podejście pozwoliłoby na bardziej proaktywne zarządzanie ryzykiem oraz szybsze i dokładniejsze reagowanie na zgłoszenia naruszeń. Jednakże wykorzystanie AI w kontekście ochrony sygnalistów stawia także wyzwania, zwłaszcza w zakresie transparentności i etyki. Algorytmy AI muszą być projektowane i wdrażane w sposób, który zapewnia uczciwość i równość, a także zgodność z przepisami prawa, w tym z zasadami ochrony danych osobowych. W sektorze publicznym AI może wspierać systemy zgłaszania naruszeń poprzez automatyzację procesów analizy zgłoszeń. Przykładowo chatbot zasilany AI może być wykorzystywany do automatycznego przyjmowania i wstępnej analizy zgłoszeń od pracowników i obywateli, co pozwoli na szybsze zidentyfikowanie kluczowych informacji i przekazanie ich do odpowiednich działów[78]. Takie rozwiązania nie tylko zwiększają efektywność, ale także redukują ryzyko błędów ludzkich. Systemy AI mogą analizować też treści zgłoszeń pod kątem słów kluczowych i tonacji, identyfikując potencjalnie krytyczne zgłoszenia, które wymagają natychmiastowej interwencji[79]. Tego typu analiza może być szczególnie użyteczna w dużych organizacjach, gdzie liczba zgłoszeń jest znaczna, a ręczne przetwarzanie wszystkich zgłoszeń byłoby nieefektywne, albo w organizacjach związanych z infrastrukturą krytyczną.

Technologia *blockchain*, znana z zapewnienia niezmienności i transparentności, ma ogromny potencjał w kontekście ochrony sygnalistów. Możliwość tworzenia niezmiennych rejestrów zgłoszeń może znacząco zwiększyć zaufanie do systemów zgłaszania naruszeń, zapewniając, że każde zgłoszenie zostanie odpowiednio zabezpieczone i pozostanie niezmienione. Systemy zgłaszania naruszeń mogą korzystać zarówno z publicznych, jak i prywatnych *blockchain*. Rejestry *blockchain* udostępniane za uprzednią zgodą (ang. *permissioned blockchain*) oferują większą

[78] Rynek komercyjny oferuje dostęp do takich rozwiązań, czego przykładem jest system UiPath, https://www.uipath.com/ [dostęp: 30.08.2024].

[79] H. Taherdoost, M. Madanchian, *Artificial Intelligence and Sentiment Analysis: A Review in Competitive Research*, https://doi.org/10.3390/computers12020037 [dostęp: 30.08.2024].

kontrolę nad tym, kto może uczestniczyć w sieci[80], co jest kluczowe w kontekście ochrony danych osobowych i poufności. Kontrakty inteligentne (ang. *smart contracts*) mogą automatyzować procesy związane ze zgłaszaniem naruszeń, takie jak przesyłanie zgłoszeń do odpowiednich organów, uruchamianie dochodzeń wewnętrznych czy powiadamianie sygnalistów o statusie ich zgłoszeń[81]. Z kolei wysoki poziom szyfrowania, w tym kryptografia asymetryczna (opierająca się na funkcjach jednokierunkowych, które da się łatwo wyliczyć w jedną stronę, ale bardzo trudno w drugą) i homomorficzna (będąca formą kryptografii klucza publicznego, która umożliwia komponowanie na zaszyfrowanych danych bez ich pierwszego deszyfrowania) pozwala na przyjęcie, że dane zgłaszających są chronione na każdym etapie przetwarzania[82]. W praktyce technologia *blockchain* może przykładowo ułatwić audyt i weryfikację procesów związanych ze zgłaszaniem, co jest kluczowe dla zapewnienia, że organizacje rzeczywiście realizują swoje zobowiązania w zakresie ochrony sygnalistów, może zapewnić anonimowość sygnalistów, chroniąc ich tożsamość przed ujawnieniem, co jest szczególnie ważne w przypadku zgłaszania nieprawidłowości w instytucjach rządowych. Użycie *blockchain* może zapewnić transparentność w procesach administracyjnych i medycznych, umożliwiając łatwiejsze monitorowanie zgłoszeń i ich przetwarzanie. Technologia *blockchain* może być stosowana do monitorowania aktywności w systemach IT i wykrywania anomalii, które mogą wskazywać na naruszenia. Jednakże, aby technologia *blockchain* mogła być w pełni wykorzystywana, konieczne jest przezwyciężenie kilku istotnych wyzwań. Po pierwsze, *blockchain* wymaga znacznych zasobów obliczeniowych i infrastrukturalnych, co może być barierą dla jego powszechnego wdrożenia. Ponadto technologia ta musi być zgodna z przepisami dotyczącymi ochrony danych osobowych, co w kontekście niezmienności danych może rodzić pewne problemy, np. w przypadku potrzeby usunięcia danych na żądanie osoby, której dotyczą.

Kolejnym obszarem, który ma potencjał do znacznego rozwoju, jest integracja systemów zgłaszania naruszeń z innymi technologiami cyfrowymi, takimi jak internet rzeczy (IoT). IoT to technologia, która umożliwia wzajemne połączenie i komu-

---

[80] M.J. Amiri, D. Agrawal, A. Abbadi, *Permissioned Blockchains: Properties, Techniques and Applications*, [w:] *SIGMOD '21: Proceedings of the 2021 International Conference on Management of Data*, 2021, s. 2813–2820.

[81] H. Taherdoost, *Smart Contracts in Blockchain Technology: A Critical Review*, [w:] *Information*, *2023*, https://www.mdpi.com/2078-2489/14/2/117/ [dostęp: 30.08.2024].

[82] C. Gentry, C.S. Halevi, *Homomorphic Encryption and its Applications. Cryptology ePrint Archive, Paper 2022/1602*, https://eprint.iacr.org/2022/1602.pdf/ [dostęp: 30.08.2024].

nikację różnorodnych urządzeń za pośrednictwem sieci internetowej[83]. W kontekście systemów zgłaszania naruszeń IoT może być wykorzystany do automatyzacji i monitorowania procesów, zwiększenia transparentności oraz poprawy ochrony sygnalistów. Możliwości te wynikają z właściwości IoT, takich jak ciągłe zbieranie danych, ich analiza w czasie rzeczywistym oraz zdolność do wykrywania anomalii w funkcjonowaniu systemów i procesów[84]. Integracja systemów zgłaszania naruszeń z IoT może przebiegać na kilku poziomach. Na poziomie operacyjnym IoT może monitorować działanie urządzeń i systemów w organizacji, zbierając dane, które mogą sugerować nieprawidłowości lub naruszenia. Przykładowo w systemach produkcyjnych IoT może monitorować zużycie energii przez maszyny, a nagłe i nieuzasadnione wzrosty zużycia mogą wskazywać na nieefektywne praktyki[85] czy nawet działania o charakterze przestępczym. Takie dane mogą być automatycznie przesyłane do systemu zgłaszania naruszeń, gdzie będą analizowane pod kątem potencjalnych nieprawidłowości. Na poziomie zarządzania IoT może wspierać sygnalistów poprzez anonimowe zbieranie dowodów na temat naruszeń, wykorzystując do tego np. czujniki dźwięku i obrazu, i tym samym dokumentowanie zdarzeń, które mogą później służyć jako dowody w procesie wewnętrznego dochodzenia. Jednym z kluczowych wyzwań związanych z integracją IoT z systemami zgłaszania naruszeń jest zapewnienie bezpieczeństwa danych. IoT, ze względu na swoją naturę, generuje ogromne ilości danych, które muszą być odpowiednio chronione przed nieautoryzowanym dostępem. W kontekście ochrony sygnalistów kluczowe jest zapewnienie, że dane dotyczące zgłaszania naruszeń są anonimowe i nie mogą zostać zidentyfikowane przez osoby niepowołane. Przykładem zastosowania IoT w systemach zgłaszania naruszeń może być monitorowanie zgodności z przepisami dotyczącymi ochrony środowiska. Czujniki IoT mogłyby być wykorzystywane do ciągłego monitorowania emisji zanieczyszczeń przez zakłady przemysłowe[86], przy czym byłyby one automatycznie przesyłane do systemu zgłaszania naruszeń, gdzie z kolei zostałyby porównywane z obowiązującymi normami prawnymi. W przypadku wykrycia przekroczenia dopuszczalnych poziomów system mógłby automatycznie wygene-

[83] *Internet Rzeczy (IoT) – Co to jest? Jak działa? Zastosowanie, przykłady*, https://cryps.pl/internet-rzeczy-iot-co-to-jest/ [dostęp: 30.08.2024].

[84] *Ibidem*.

[85] *Monitorowanie zużycia energii elektrycznej urządzeń przemysłowych – przykład wtryskarki FANUC. APA LAB*, https://apagroup.pl/apalab/jak-skutecznie-monitorowac-zuzycie-energii-elektrycznej-urzadzen-przemyslowych-przyklad-wtryskarki-fanuc/ [dostęp: 30.08.2024].

[86] *The Impact of Smart Sensors on Environmental Monitoring and Compliance*, https://fatfinger.io/the-impact-of-smart-sensors-on-environmental-monitoring-and-compliance/ [dostęp: 30.08.2024].

rować zgłoszenie naruszenia, co umożliwia szybkie podjęcie działań naprawczych. IoT może również zautomatyzować procesy zgłaszania naruszeń poprzez integrację z systemami ERP (ang. *Enterprise Resource Planning*) i CRM (ang. *Customer Relationship Management*). Przykładowo, w sektorze finansowym IoT mogłoby monitorować transakcje w czasie rzeczywistym i wykrywać anomalie, które mogłyby wskazywać na nieprawidłowości, takie jak pranie pieniędzy[87]. Takie podejście nie tylko prowadzi do zwiększenia efektywności systemów zgłaszania, ale także pozwala na szybkie reagowanie na potencjalne zagrożenia.

Innym jeszcze obszarem, którego rozwój rzutuje istotnie na omawianą problematykę, jest *big data*. Termin ten odnosi się do przetwarzania i analizy bardzo dużych zbiorów danych, które charakteryzują się dużą objętością, różnorodnością oraz szybkością napływu. W kontekście systemów zgłaszania naruszeń *big data* pozwala na integrację różnorodnych źródeł danych od wewnętrznych raportów pracowniczych, poprzez dane z monitoringu systemów IT, po publiczne bazy danych i media społecznościowe[88], a to celem zidentyfikowania wzorców, anomalii oraz potencjalnych zagrożeń. Przykładowo w przemyśle finansowym technologia *big data* może być wykorzystywana do monitorowania transakcji finansowych pod kątem prania pieniędzy oraz innych działań niezgodnych z prawem. Integracja systemów zgłaszania naruszeń z analizą danych pozwala na automatyczne wykrywanie podejrzanych transakcji na podstawie wzorców zachowań, które mogą wskazywać na działalność przestępczą. Systemy te mogą analizować setki tysięcy transakcji dziennie, identyfikując anomalie takie jak nietypowo duże przelewy, które następnie podlegają dalszej weryfikacji. Z kolei w sektorze opieki zdrowotnej *big data* może wspierać systemy zgłaszania naruszeń poprzez analizę danych pacjentów oraz danych operacyjnych szpitali w celu wykrywania potencjalnych nieprawidłowości, takich jak oszustwa związane z ubezpieczeniami zdrowotnymi, błędy medyczne czy naruszenia prywatności pacjentów. Na przykład analiza danych dotyczących przepisywania leków może ujawnić nieuzasadnione wzorce, takie jak nadmierne przepisywanie leków opioidowych, co może być wskazówką do złożenia zgłoszenia[89]. Natomiast

---

[87] *How Real-time Monitoring Changes the Game for Transaction Security*, https://www.flagright.com/post/how-real-time-monitoring-changes-the-game-for-transaction-security/ [dostęp: 30.08.2024].

[88] M.M. Alani, *Big data in cybersecurity: a survey of applications and future trends. Journal of Reliable Intelligent Environments*, „Journal of Reliable Intelligent Environments", https://www.researchgate.net/publication/348278146_Big_data_in_cybersecurity_a_survey_of_applications_and_future_trends [dostęp: 30.08.2024].

[89] P. Pandey, A. Saroliya, R. Kumar, *Analyses and Detection of Health Insurance Fraud Using Data Mining and Predictive Modeling Techniques*, [w:] *Advances in Intelligent Systems and Computing*, 2017, s. 41–49.

w administracji publicznej można wykorzystać *big data* do monitorowania zgodności z przepisami prawa i zapobiegania korupcji. Przykładem może być system zgłaszania naruszeń, który integruje dane z różnych źródeł, takich jak rejestry publiczne, przetargi czy audyty, aby wykrywać konflikty interesów, nieprawidłowości w zamówieniach publicznych czy inne działania korupcyjne[90].

W odpowiedzi na rozwój technologii cyfrowych ustawodawcy muszą być gotowi do dalszego rozwoju przepisów dotyczących ochrony sygnalistów, tak aby były one skuteczne w aktualnym środowisku technologicznym. Regulacje muszą uwzględniać specyfikę technologii takich jak AI i *blockchain* i tym samym chronić prawa osób korzystających z nowoczesnych systemów zgłaszania. Jednym z kluczowych aspektów przyszłych regulacji powinno być zapewnienie, że sygnaliści będą mieli dostęp do skutecznych mechanizmów ochrony niezależnie od technologii, z której korzystają. Ustawodawcy muszą również zadbać o to, aby regulacje były elastyczne i zdolne do adaptacji w obliczu przyszłych zmian technologicznych, co może wymagać regularnej aktualizacji przepisów oraz stworzenia mechanizmów monitorowania ich skuteczności, tylko bowiem w ten sposób można zapewnić, że ochrona sygnalistów pozostanie skuteczna i adekwatna do wyzwań, jakie stawia przed nami XXI w.

Wnioski

Zagadnienia związane z ochroną sygnalistów w erze cyfrowej są nie tylko aktualne, ale również niezwykle złożone. W miarę jak technologia rozwija się w coraz szybszym tempie, ustawodawcy, organizacje i sami sygnaliści zmuszeni są stawić czoła nowym wyzwaniom, które wymagają przemyślanych i zrównoważonych rozwiązań. Zaprezentowana w artykule pokrótce analiza wskazuje, że technologia cyfrowa, w szczególności AI i *blockchain*, ma potencjał do rewolucjonizowania systemów zgłaszania naruszeń. Dzięki zaawansowanym algorytmom AI możliwe jest automatyzowanie procesów zgłaszania i weryfikacji naruszeń, co zwiększa efektywność i dokładność tych procesów. *Blockchain* z kolei zapewnia niezmienność i przejrzystość zgłoszeń, co jest kluczowe dla budowania zaufania do systemów zgłaszania naruszeń. Jednakże wdrożenie tych technologii wiąże się z licznymi wyzwaniami. W szczególności kwestie odpowiedzialności prawnej za decyzje podejmowane przez systemy AI

[90] *Preventing Corruption in Procurement through Big Data*, https://www.unodc.org/roseap/en/what-we-do/anti-corruption/topics/2020/preventing-corruption-procurement-big-data.html [dostęp: 30.08.2024].

oraz zgodność z przepisami dotyczącymi ochrony danych osobowych pozostają nierozwiązane i wymagają dalszych badań oraz rozwoju regulacji. Dyrektywa 2019/1937 oraz u.o.s. stanowią znaczący krok naprzód w harmonizacji przepisów dotyczących ochrony sygnalistów w UE. Przepisy te nakładają na organizacje obowiązek wdrożenia skutecznych i bezpiecznych systemów zgłaszania, które muszą być zgodne z dynamicznie zmieniającym się środowiskiem technologicznym. W odpowiedzi na te regulacje organizacje muszą nie tylko dostosować swoje procedury, ale także zainwestować w nowe technologie, które wspierają ochronę sygnalistów.

Patrząc w przyszłość, nic nie wskazuje na to, aby tak dynamiczny rozwój technologii miał ulec spowolnieniu, a zatem również zmiany w zakresie ochrony sygnalistów muszą nadążyć za tą rewolucją. Technologie takie jak AI, *blockchain*, *big data* czy IoT będą odgrywać coraz większą rolę w kształtowaniu systemów zgłaszania i ochrony sygnalistów, jednakże kluczowe będzie zrównoważenie korzyści wynikających z tych technologii z wymogami prawnymi, etycznymi oraz potrzebą zapewnienia transparentności i odpowiedzialności, albowiem jak głosi stara rzymska paremia *non omne quod licet honestum est*[91].

Nie należy jednak zakładać, że praca nad ochroną sygnalistów kończy się na wprowadzeniu nowych przepisów. Jest to ciągły proces, który wymaga elastyczności, innowacyjności i współpracy na wielu poziomach. W obliczu szybkich zmian technologicznych i prawnych kluczowe jest, aby organizacje, ustawodawcy i sygnaliści pozostawali na bieżąco z najnowszymi trendami i rozwiązaniami, aby zapewnić skuteczną ochronę dla tych, którzy decydują się mówić prawdę w obliczu nadużyć i nieprawidłowości. Ostatecznie przyszłość ochrony sygnalistów w erze cyfrowej będzie zależała od naszej zdolności do adaptacji, innowacyjności oraz zaangażowania w tworzenie sprawiedliwego i transparentnego systemu, który będzie służył zarówno jednostkom, jak i społeczeństwu jako całości.

Bibliografia

Źródła

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz. Urz. UE L 305/17 z 2019 r.).

Ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów (Dz. U. z 2024 r. poz. 928).

[91] *Digesta Iustiniani*, D. 50.17.144 pr.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 12 lipca 2024 r. ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Dz. Urz. UE L 1689 z 2024 r.).

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

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

Źródła internetowe

Alani M.M., *Big data in cybersecurity: a survey of applications and future trends. Journal of Reliable Intelligent Envi*ronments, „Journal of Reliable Intelligent Environments", https://www.researchgate.net/publication/348278146_Big_data_in_cybersecurity_a_survey_of_applications_and_future_trends [dostęp: 30.08.2024].

Coronavirus kills Chinese whistleblower ophthalmologist, American Academy of Ophthalmology, https://www.aao.org/education/headline/coronavirus-kills-chinese-whistleblower-ophthalmol/ [dostęp: 30.08.2024].

Epidemia w więzieniu? „Winny" sygnalista, https://www.rp.pl/sluzby/art8644921-epidemia-w-wiezieniu-winny-sygnalista/ [dostęp: 30.08.2024].

Filing Whistleblower Complaints Under the Solid Waste Disposal Act, https://www.osha.gov/sites/default/files/publications/OSHA3815.pdf/ [dostęp: 30.08.2024].

Gentry C., Halevi S., Hom*omorphic Encryption and its Applications. Cryptology ePrint Archive, Paper 2022/1602,* https://eprint.iacr.org/2022/1602.pdf/ [dostęp: 30.08.2024].

Guidance Whistleblowing and the Public Interest Disclosure Act 1998 (c.23) (accessible version), https://www.gov.uk/government/publications/whistleblowing-and-the-public-interest-disclosure-act-1998-c23/whistleblowing-and-the-public-interest-disclosure-act-1998-c23-accessible-version/ [dostęp: 30.08.2024].

How Real-time Monitoring Changes the Game for Transaction Security, https://www.flagright.com/post/how-real-time-monitoring-changes-the-game-for-transaction-security/ [dostęp: 30.08.2024].

Hudson M., *The Panama Papers: Exposing the Rogue Offshore Finance Industry*, https://www.icij.org/investigations/panama-papers/ [dostęp: 30.08.2024].

Internet Rzeczy (IoT) – Co to jest? Jak działa? Zastosowanie, przykłady, https://cryps.pl/internet-rzeczy-iot-co-to-jest/ [dostęp: 30.08.2024].

ISO/IEC 42001:2023, Artificial Intelligence Management Systems – Requirements, https://www.iso.org/standard/81230.html/ [dostęp: 30.08.2024].

Lloyd-La Follette Act of 1912, https://whistleblower.house.gov/resources/all-resources/committee-jurisdiction-tool/whistleblowing-executive-branch-employee/lloyd-la-follette-act-1912/ [dostęp: 30.08.2024].

Monitorowanie zużycia energii elektrycznej urządzeń przemysłowych – przykład wtryskarki FANUC. APA LAB, https://apagroup.pl/apalab/jak-skutecznie-monitorowac-zuzycie-energii-elektrycznej-urzadzen-przemyslowych-przyklad-wtryskarki-fanuc/ [dostęp: 30.08.2024].

Nader Riders, https://pophistorydig.com/topics/naders-raiders-1968-1974/ [dostęp: 30.08.2024].

O'Connor J.D., *I'm the Guy They Called Deep Throat*, „Vanity Fair", https://www.vanityfair.com/news/politics/2005/07/deepthroat200507?printable=true&currentPage=all/ [dostęp: 30.08.2024].

Pandey P., Saroliya A., Kumar R., *Analyses and Detection of Health Insurance Fraud Using Data Mining and Predictive Modeling Techniques,* [w:] *Advances in Intelligent Systems and Computing,* 2017, s. 41–49.

Perlstein R., *Watergate scandal*, [w:] *Encyclopaedia Britannica*, https://www.britannica.com/event/Watergate-Scandal/ [dostęp: 30.08.2024].

Preventing Corruption in Procurement through Big Data, https://www.unodc.org/roseap/en/what-we-do/anti-corruption/topics/2020/preventing-corruption-procurement-big-data.html [dostęp: 30.08.2024].

Ralph Nader, https://achievement.org/achiever/ralph-nader/ [dostęp: 30.08.2024 r.].

Ray M., *Edward Snowden*, [w:] *Encyclopaedia Britannica*, https://www.britannica.com/biography/Edward-Snowden/ [dostęp: 30.08.2024].

Shiel F., *European court reverses course to rule in favor of LuxLeaks whistleblower*, https://www.icij.org/investigations/luxembourg-leaks/european-court-reverses-course-to-rule-in-favor-of-luxleaks-whistleblower/ [dostęp: 30.08.2024].

Sygnalista, [w:] *Słownik języka polskiego*, red. W. Doroszewski, https://sjp.pwn.pl/doroszewski/sygnalista/ [dostęp: 31.08.2024].

Sygnalista, [w:] *Słownik języka polskiego PWN*, https://sjp.pwn.pl/ [dostęp: 31.08.2024].

Sygnalista, https://sjp.pl/ [dostęp: 30.08.2024].

Taherdoost H., Madanchian M., *Artificial Intelligence and Sentiment Analysis: A Review in Competitive Research,* https://doi.org/10.3390/computers12020037 [dostęp: 30.08.2024].

Taherdoost H., *Smart Contracts in Blockchain Technology: A Critical Review,* [w:] *Information, 2023,* https://www.mdpi.com/2078-2489/14/2/117/ [dostęp: 30.08.2024].

The False Claims Act, https://www.justice.gov/civil/false-claims-act/ [dostęp: 30.08.2024].

The Impact of Smart Sensors on Environmental Monitoring and Compliance, https://fatfinger.io/the-impact-of-smart-sensors-on-environmental-monitoring-and-compliance/ [dostęp: 30.08.2024 r.].

Todd M., *Danske Bank Whistleblower Testifies at European Parliament*, Whistleblower Network News, https://whistleblowerprotection.eu/blog/danske-bank-whistleblower-testifies-at-european-parliament/ [dostęp: 30.08.2024].

Tokarczyk D., [w:] E. Rutkowska, D. Tokarczyk, *Ustawa o ochronie sygnalistów. Komentarz*, LEX/el. 2024, art. 4., https://sip.lex.pl/#/commentary/587977514/774954?keyword=Ustawa%20o%20ochronie%20sygnalist%C3%B3w.%20Komentarz&tocHit=1&cm=SFIRST/ [dostęp: 31.08.2024].

United States Files Complaint Against Novartis Pharmaceuticals Corp. for Allegedly Paying Kickbacks to Doctors in Exchange for Prescribing Its Drugs, https://www.justice.gov/opa/pr/united-states-files-complaint-against-novartis-pharmaceuticals-corp-allegedly-paying/ [dostęp: 30.08.2024].

U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program – The Washington Post, „Washington Post", https://www.washingtonpost.com/ [dostęp: 30.08.2024].

Whistleblower, [w:] *Online Etymology Dictionary,* https://www.etymonline.com/search?q=whistleblower%20/ [dostęp: 30.08.2024].

Whistleblower, [w:] *Merriam-Webster,* https://www.merriam-webster.com/wordplay/whistle-blower-blow-the-whistle-word-origins/ [dostęp: 30.08.2024].

Whistle-blower, [w:] *Phrases Finder*, https://www.phrases.org.uk/meanings/whistle-blower.html/ [dostęp: 30.08.2024].

Whistleblower, [w:] *Word Origins*, http://www.wordorigins.org/index.php/site/whistleblower/, [w:] Wayback Machine, https://web.archive.org/web/20120429004210/http://www.wordorigins.org/index.php/site/whistleblower/ [dostęp: 30.08.2024].

Whistleblower, [w:] *Oxford English Dictionary*, https://www.dictionary.com/browse/whistleblower/ [dostęp: 30.08.2024].

Whistleblower, [w:] *Meriiam-Webster*, https://www.merriam-webster.com/dictionary/whistleblower/ [dostęp :30.08.2024].

Whistle-blower, [w:] *Phrase Finder,* https://www.phrases.org.uk/meanings/whistle-blower.html/ [dostęp: 30.08.2024].

Whistleblower Protections – Rights Of Employees [5 U.s.c. §2302 (B)(8)], https://www.americorps.gov/sites/default/files/document/2021_08_27_Whistleblower_Rights_Employees_OGC.pdf/ [dostęp: 30.08.2024].

Globaleaks, https://www.globaleaks.org/ [dostęp: 30.08.2024].

Securedrop, https://securedrop.org/ [dostęp: 30.08.2024].

Falcony, https://www.falcony.io/ [dostęp: 30.08.2024].

Navex, https://www.navex.com/ [dostęp: 30.08.2024].

EQS Group System BKMS, https://www.eqs.bkms-system.com/ [dostęp: 30.08.2024].

Signal, https://signal.org/pl/ [dostęp: 30.08.2024].

Tella, https://tella-app.org/ [dostęp: 30.08.2024].

Guardianproject, Haven, https://guardianproject.github.io/haven/ [dostęp: 30.08.2024].

Guardianproject, Orbot, https://orbot.app/en/ [dostęp: 30.08.2024].

DISS-CO, https://diss-co.tech/ [dostęp: 30.08.2024].

Fixnix, https://www.fixnix.co/ [dostęp: 30.08.2024].

SpeakUp, https://www.speakup.com/ [dostęp: 30.08.2024].

Literatura

Amiri M.J., Agrawal D., Abbadi A., *Permissioned Blockchains: Properties, Techniques and Applications* [w:] *SIGMOD '21: Proceedings of the 2021 International Conference on Management of Data*, 2021.

Becker A., *Messengers of Disaster: Raphael Lemkin, Jan Karski, and Others*, „Journal of Holocaust Studies" 2017.

Devitt J.K., *Speaking Up Safely Civil Society Guide To Whistleblowing: Middle East And North Africa Region,* „Transparency International" 2015, http://www.jstor.org/stable/resrep20533/ [dostęp: 30.08.2024].

Digesta Iustiniani, D. 50.17.144 pr.

Fietkiewicz K.J., *The Development of Information Society in Japan: A Case Study of 21 Metropolitan Areas.* Proceedings of the Hawaii University International Conferences on Arts, Humanities, Social Sciences & Education, 2019.

Jankowski J., Karski J., *Raport tajnego emisariusza*, Kraków 2019.

Kant I., *Krytyka czystego rozumu*, tłum. R. Ingarden, Warszawa 1957.

Murszewski J., *Problemy implementacji dyrektywy 2019/1937 do polskiego porządku prawnego*, [w:] B. Baran, M. Ożóg (red.), *Ochrona sygnalistów. Regulacje dotyczące osób zgłaszających nieprawidłowości*, Warszawa 2021.

Sharma P., Jindal R., Borah M.D., *A Review of Blockchain-Based Applications and Challenges,* [w:] *Wireless Personal Communications,* 2022.

Stanger A., *Whistleblowers: Honesty in America from Washington to Trump*, Cambridge 2019.

Zheng Z., Xie S., Dai H., Chen X., Wang H., *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*, [w:] *2017 IEEE 6th International Congress on Big Data, IEEE Computer Society,* 2017.

Selected issues regarding the role of whistleblowers and reporting channels in the context of the development of digital technologies and legislative changes, as well as related challenges and prospects

Abstract

The article focuses on the evolution of the role of whistleblowers in the digital era and on the analysis of the impact of modern technologies, such as artificial intelligence (AI), blockchain, Big Data, and the Internet of Things (IoT), and on the effectiveness and security of reporting channels. The aim of the work is to assess how these technologies can revolutionize the process of reporting irregularities, as well as what challenges and opportunities are associated with their integration in the context of contemporary legislative changes, with particular emphasis on Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting breaches of EU law and the Polish Act of 14 June 2024 on the protection of whistleblowers. The research methodology includes a literature review and an analysis of legal regulations. Key findings indicate that digital technologies can significantly increase the level of security, anonymity and efficiency of reporting systems, although at the same time they pose challenges to legislators and organizations related to ensuring compliance with regulations, protection of personal data and transparency. The work emphasizes that an important aspect of the future of whistleblower protection will be the harmonization of legal regulations with the dynamically developing technological landscape and education in the field of new reporting tools. The implications of the research suggest the need for a flexible approach to legal regulations to ensure effective whistleblower protection in the digital era, and indicate the need for continuous monitoring and adaptation of regulations to new technological challenges.

Keywords

Whistleblowers, whistleblower protection, reporting channels, digital technologies, artificial intelligence (AI), big data, Internet of Things (IoT), data protection law

DOI: 10.34616/151202

Prawo Mediów Elektronicznych. Kwartalnik Naukowy
2024, nr 3, 77–95

Mateusz Jakubik
Uniwersytet Jagielloński w Krakowie
Wydział Prawa i Administracji
ORCID: 0000-0002-8992-7309

Adw. Oskar Grajewski
ORCID: 0009-0009-7968-5543

Implementacja *post-quantum cryptography* w ramach EUDI *Wallet* jako elementu eIDAS 2 w kontekście wyzwań prawnych i technicznych oraz implikacji dla bezpieczeństwa cybernetycznego w świetle regulacji CRA i NIS 2[1]

Streszczenie

Niniejsze opracowanie bada znaczenie kryptografii postkwantowej (ang. *post-quantum cryptography,* PQC) w kontekście postkwantowej rzeczywistości, podkreślając jej rolę jako fundamentu przyszłego bezpieczeństwa cyfrowego. Praca analizuje także wyzwania związane z implementacją PQC w kluczowych projektach europejskich, takich jak Europejski Portfel Tożsamości Cyfrowej (ang. *European Digital Identity Wallet*, EUDI *Wallet*), który ma stać się centralnym elementem ekosystemu cyfrowego Unii Europejskiej (UE). W erze postkwantowej PQC będzie nie tylko narzędziem ochrony przed nowymi zagrożeniami, ale także kluczowym elementem regulacji prawnych, takich jak eIDAS 2 i NIS 2, mających na celu zapewnienie bezpieczeństwa i interoperacyjności systemów cyfrowych w UE. Praca podkreśla znaczenie harmonizacji przepisów międzynarodowych oraz współpracy globalnej, które są niezbędne do skutecznej implementacji PQC, zapewniającej odporność na zagrożenia wynikające z przyszłych osiągnięć technologii kwantowej.

Słowa kluczowe

kryptografia postkwantowa, bezpieczeństwo cyfrowe, algorytmy kryptograficzne, Europejski Portfel Tożsamości Cyfrowej, interoperacyjność, cyberbezpieczeństwo, technologia kwantowa, eIDAS 2, NIS 2

[1] Przedstawione w artykule opinie stanowią wyraz osobistych poglądów autorów i nie powinny być utożsamiane ze stanowiskiem żadnej organizacji lub instytucji, z którą autorzy byli albo są powiązani.

Wstęp

W obliczu nieustającego postępu technologicznego, gdy każdy kolejny dzień przybliża nas do upowszechnienia osiągnięć w dziedzinie technologii komputeryzacji kwantowej, kwestia zabezpieczenia danych cyfrowych staje się wyzwaniem o bezprecedensowej skali. Jednak powszechnie, z wyjątkiem osób żywo zainteresowanych tą tematyką, zdaje się umykać uwadze, iż wyzwanie to nie ogranicza się jedynie do aspektów technicznych, ale rozciąga się również na szerokie spektrum kwestii prawnych, etycznych oraz społecznych. W kontekście tego dynamicznie zmieniającego się krajobrazu pojęcie kryptografii postkwantowej (ang. *post-quantum cryptography*, PQC)[2] nabiera szczególnego znaczenia, stając się fundamentem przyszłego bezpieczeństwa cyfrowego w erze, którą niektórzy określają już jako postkwantową[3].

W miarę jak świat staje na progu tej nowej epoki technologicznej, której katalizatorem mają być komputery kwantowe, dotychczasowe paradygmaty bezpieczeństwa cyfrowego ulegają istotnym przekształceniom, a infrastruktura kryptograficzna stoi przed bezprecedensowym wyzwaniem, jakim jest zagrożenie złamania przez potężne możliwości obliczeniowe komputerów kwantowych. Rozwój tej technologii, początkowo postrzegany jako odległa i teoretyczna perspektywa, w ostatnich latach nabiera tempa, a implikacje jej wdrożenia zaczynają wpływać na kluczowe obszary regulacji prawnych i polityki bezpieczeństwa. Staje się jasne, że to, co kiedyś było jedynie eksperymentalnym polem badań, dzisiaj wymaga natychmiastowej reakcji, szczególnie w kontekście ochrony danych i systemów cyfrowych na poziomie globalnym. Jednym z najważniejszych narzędzi, które mają zapewnić bezpieczeństwo w tej postkwantowej rzeczywistości, jest właśnie kryptografia postkwantowa. PQC poprzez wprowadzenie algorytmów odpornych na obliczenia kwantowe może stanowić odpowiedź na zagrożenia wynikające z rosnących możliwości technologii kwantowej. Wraz z rozwojem nowych rozwiązań, takich jak Europejski Portfel Tożsamości Cyfrowej (ang. *European Digital Identity Wallet*, EUDI *Wallet*), który ma stać się integralnym elementem ekosystemu cyfrowego Unii Europejskiej (UE), implementacja kryptografii postkwantowej staje się kluczowym, niezwykle naglącym zadaniem.

---

[2] *What Is Post-Quantum Cryptography?*, https://www.nist.gov/cybersecurity/what-post-quantum-cryptography/ [dostęp: 31.08.2024].

[3] *Entering the Quantum Era* , https://www.ox.ac.uk/news/features/entering-quantum-era/ [dostęp: 31.08.2024].

Niniejszy artykuł podejmuje próbę szczegółowej analizy wyzwań związanych z implementacją PQC w EUDI *Wallet* w kontekście obowiązujących i przyszłych regulacji prawnych, takich jak eIDAS 2, NIS 2 oraz CRA. Ponadto badane będą implikacje dla bezpieczeństwa cybernetycznego oraz interoperacyjności systemów cyfrowych. W centrum tych rozważań znajduje się pytanie o to, jak UE może zabezpieczyć swoją infrastrukturę cyfrową na przyszłe dekady oraz jakie kroki legislacyjne i technologiczne są konieczne, aby sprostać tym wyzwaniom.

1. Znaczenie *post-quantum cryptography* (PQC) w erze postkwantowej

Pojęcie kryptografii postkwantowej zrodziło się z konieczności odpowiedzi na pytanie, jak chronić informacje w świecie, gdzie obliczenia kwantowe stają się rzeczywistością. Od lat 90. XX w., kiedy to P.W. Shor przedstawił swój algorytm do faktoryzacji liczb[4], środowisko kryptograficzne zaczęło dostrzegać nieuchronne zagrożenie ze strony komputerów kwantowych[5]. Wówczas jednak zagadnienie to traktowano jako problem odległy, niemający bezpośredniego wpływu na bieżące praktyki bezpieczeństwa cyfrowego. Z upływem lat badania nad komputerami kwantowymi zaczęły nabierać tempa, a to w konsekwencji wywołało rosnącą świadomość potrzeby opracowania nowych metod szyfrowania. W 2016 r. Narodowy Instytut Standaryzacji i Technologii (ang. *National Institute of Standards and Technology*, NIST) w Stanach Zjednoczonych ogłosił konkurs na standardy kryptograficzne odporne na ataki kwantowe, który stał się impulsem dla globalnych wysiłków badawczych w tej dziedzinie[6]. W ramach konkursu złożono setki propozycji algorytmów, które mają potencjał zabezpieczenia przyszłościowych systemów informatycznych przed zagrożeniami wynikającymi z rozwoju komputerów kwantowych[7]. Mimo więc, że kryptografia postkwantowa wciąż stanowi stosunkowo nowy obszar

[4] W matematyce faktoryzacja polega na zapisaniu liczby lub innego obiektu matematycznego jako iloczynu kilku czynników, zwykle mniejszych lub prostszych obiektów tego samego rodzaju. Na przykład 3×5 to rozkład liczby całkowitej 15, a(x – 2)(x + 2) to rozkład wielomianowy x2–4.

[5] P.W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring, Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, https://cc.ee.ntu.edu.tw/~rbwu/rapid_content/course/QC/Shor1994.pdf/ [dostęp: 31.08.2024].

[6] *NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat*, https://www.nist.gov/news-events/news/2016/04/nist-kicks-effort-defend-encrypted-data-quantum-computer-threat/ [dostęp: 31.08.2024].

[7] *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*, https://csrc.nist.gov/pubs/ir/8309/final [dostęp: 31.08.2024].

badań, to już teraz jawi się jako jeden z kluczowych elementów strategii obronnych przeciwko zagrożeniom wynikającym z rozwoju komputerów kwantowych.

Komputery kwantowe obiecują rewolucję w obliczeniach zdolnych rozwiązywać problemy, które są obecnie niemożliwe do rozwiązania przez klasyczne komputery[8]. Choć potencjał ten niesie ze sobą ogromne możliwości, to stanowi on jednocześnie zagrożenie dla istniejących obecnie systemów kryptograficznych, a co za tym idzie – także dla całej infrastruktury bezpieczeństwa cyfrowego. Obecnie stosowane metody kryptograficzne bazują na założeniu, że pewne operacje matematyczne są zbyt skomplikowane, aby mogły być efektywnie przeprowadzone na klasycznych komputerach w rozsądnym czasie. Na przykład problem rozkładu liczby na czynniki pierwsze, będący podstawą bezpieczeństwa algorytmu RSA, dla odpowiednio dużych liczb uważany jest za nierozwiązywalny przez klasyczne komputery w czasie, który w praktyce uzasadniałby podejmowanie takich działań[9]. Jednakże w przypadku komputerów kwantowych operacje te mogą być wykonane w czasie logarytmicznym względem rozmiaru wejścia, co oznacza, że każde 2048-bitowe klucze RSA mogłyby *de facto* zostać złamane w czasie kilku sekund lub minut przez odpowiednio rozwinięty komputer kwantowy[10].

W tym kontekście systemy kryptograficzne, które dziś są uważane za bezpieczne, mogą stać się podatne na ataki w przeciągu kilku najbliższych dekad, co wymaga pilnego opracowania i wdrożenia nowych, odpornych na kwantowe obliczenia metod szyfrowania[11]. Istnieje kilka przodujących wariantów PQC, które mogą być stosowane w przyszłości do ochrony danych. Najbardziej obiecujące z nich to algorytmy oparte na kratach (ang. *lattice-based cryptography*)[12], kodach (ang. *code-based cryptography*)[13], wielomianach (ang. *multivariate polynomial cryptography*)[14] oraz podpisy oparte na funkcjach skrótu (ang. *hash-based signatures*)[15]. Kryptografia oparta na kratach, będąca jednym z najbardziej rozwiniętych podejść, odnosi się

[8] *Toward a code-breaking quantum computer*, https://www.sciencedaily.com/releases/2024/08/240823120024.htm/ [dostęp: 30.08.2024].

[9] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson 2014, s. 283–308, https://dl.hiva-network.com/Library/security/Cryptography-and-network-security-principles-and-practice.pdf/ [dostęp: 31.08.2024].

[10] M. Mosca, *Cybersecurity in an Era with Quantum Computers: Will We Be Ready?*, „IEEE Security & Privacy" 2018, vol. 16(5), s. 38–41.

[11] *Post-Quantum Cryptography: Current Status and Next Steps*, https://csrc.nist.gov/publications/detail/nistir/8105/final [dostęp: 30.08.2024].

[12] D.J. Bernstein, J. Buchmann, E. Dahmen, *Post-Quantum Cryptography* , Springer 2009, s. 147–187.

[13] *Ibidem*, s. 95–141.

[14] *Ibidem*, s. 193–234.

[15] *Ibidem*, s. 35–91.

do problemów związanych z trudnością znajdowania najkrótszych wektorów w kratach[16]. Problemy te są uważane za niezwykle trudne do rozwiązania nawet przez komputery kwantowe, co czyni je idealnym rozwiązaniem dla przyszłych standardów kryptograficznych. *Code-based cryptography*, choć mniej popularna niż metody oparte na kratach, także wykazuje duży potencjał. Metoda ta została po raz pierwszy zaproponowana przez R. McEliece w 1978 r. i bazuje na trudności dekodowania losowych kodów liniowych. Pomimo że algorytm McEliece'a jest bardzo wydajny i bezpieczny, to wymaga dużych rozmiarów kluczy kryptograficznych[17], co jest jego główną wadą w kontekście jego ewentualnej szerokiej implementacji. Podpisy oparte na *hashach*, jak np. algorytm Merkle'a[18], są również rozważane jako przyszłościowe rozwiązanie[19], albowiem charakteryzują się one prostotą i wysoką odpornością na ataki kwantowe, co czyni je dobrym wyborem dla systemów wymagających bezpiecznych podpisów cyfrowych. Wielomianowe „kryptosystemy", choć jawią się jako mniej rozwinięte niż inne podejścia, również oferują potencjalnie atrakcyjne rozwiązania i zastosowania, zwłaszcza w kontekście tworzenia złożonych algorytmów kryptograficznych opartych na trudnych problemach algebraicznych[20].

Ważąc dotychczasowe dywagacje, można zaryzykować stwierdzenie, iż u postronnego czytelnika dotychczasowa lektura mogłaby wywołać konsternację, jak również mogłoby towarzyszyć mu swoiste niedowierzanie, w jaki sposób tematyka ta łączy się z zagadnieniami natury prawnej. W replice na tego rodzaju wątpliwość dopuszczalny zdaje się truizm, iż znakiem „naszych czasów" pozostaje zjawisko, gdy różne nauki ścisłe oraz techniczne, a szczególnie informatyka, coraz śmielej wkraczają we wszelkie dziedziny współczesnego życia. Skoro więc życie to tak prędko i powszechnie ulega cyfryzacji, to społeczeństwo zmuszone jest zjawisku temu sprostać na różnych płaszczyznach i poprzez różne inicjatywy. Jedną z nich jest projekt UE dotyczący wdrożenia Europejskiego Portfela Tożsamości Cyfrowej

---

[16] W geometrii i teorii grup „krata" w rzeczywistej przestrzeni współrzędnych R^n jest nieskończonym zbiorem punktów tej przestrzeni o następujących właściwościach: dodanie lub odjęcie dwóch punktów należących do kratki daje inny punkt kratki, wszystkie punkty kratki są od siebie oddalone o co najmniej pewną minimalną odległość, a każdy punkt w przestrzeni znajduje się w skończonej maksymalnej odległości od najbliższego punktu kratki.

[17] Klucz kryptograficzny to liczba lub ciąg danych, które są wykorzystywane w procesie szyfrowania i deszyfrowania informacji.

[18] Nazywany także „Puzzlami Merkle'a". Jest jedną z pierwszych wersji algorytmu kryptografii z kluczem publicznym zaproponowaną przez R. Merkle'a w 1974 r., a opublikowaną w 1978 r.

[19] B. Schneier, *Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C*, wyd. 2, Warszawa 2002, s. 51–81.

[20] P. Kapcia, *Kryptosystemy oparte na problemach trudnych obliczeniowo z wyszczególnieniem problemu faktoryzacji liczb całkowitych*, „Elektrotechnika i Elektronika" 2005, t. 24, nr 2, s. 148–57.

(ang. *European Digital Identity Wallet*, EUDI *Wallet*), mającego stanowić bezpieczne i zaufane środowisko dla cyfrowej identyfikacji obywateli UE, a który to projekt będzie częścią większego ekosystemu, mającego na celu ułatwienie cyfrowej transformacji i wzmocnienie jednolitego rynku cyfrowego UE[21]. Zaznaczyć należy, iż koncepcja EUDI *Wallet* nie stanowi osobnego bytu w ramach europejskiej legislacji, lecz jest elementem szerszej propozycji legislacyjnej Komisji Europejskiej, znanej jako rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE[22] (ang. *European Identity Digital and Authentication Services 2.0.*, eIDAS 2).

Jednym z głównych wyzwań w implementacji EUDI *Wallet* jest zapewnienie, że system ten będzie mógł sprostać przyszłym zagrożeniom, w tym związanym z rozwojem omawianych już komputerów kwantowych. Implementacja PQC w ramach EUDI *Wallet* jest zatem kluczowa dla osiągnięcia tego zamierzenia i zapewnienia, że system ten pozostanie bezpieczny i zaufany również w erze postkwantowej. Projekt ten zakłada, iż EUDI *Wallet* będzie narzędziem, które umożliwi obywatelom UE przechowywanie i zarządzanie różnymi rodzajami cyfrowej tożsamości, w tym danymi osobowymi, certyfikatami oraz innymi informacjami wrażliwymi tak, aby były one całkowicie bezpieczne[23], do czego niezbędne jest, zważywszy na sygnalizowane już zagrożenia ery postkwantowej, zastosowanie najnowocześniejszych technologii kryptograficznych, w tym PQC, które będą w stanie skutecznie chronić dane przed nowymi rodzajami ataków. Odnośnie do rozporządzenia eIDAS 2 EUDI *Wallet* pełnić ma więc nie tylko funkcję narzędzia do zarządzania tożsamością cyfrową, ale ma być również platformą umożliwiającą realizację różnorodnych usług zaufania, a usługi te, jak np. elektroniczne podpisy, muszą być również chronione przed potencjalnymi zagrożeniami związanymi z kryptografią kwantową. Implementacja PQC w EUDI *Wallet* pozwala zatem na wprowadzenie dodatkowej warstwy zabezpieczeń, która jest niezbędna do spełnienia wymogów bezpieczeństwa określonych w rozporządzeniu eIDAS 2.

Warto także zwrócić uwagę na aspekt interoperacyjności EUDI *Wallet* w kontekście PQC, polegający na tym, że musi być on kompatybilny z różnymi systema-

[21] *What is the EU Digital Identity Wallet*, https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+is+the+Wallet/ [dostęp: 30.08.2024].

[22] Dz. Urz. UE L 257/73 z 2014 r. (dalej: „eIDAS 2").

[23] Art. 3 ust. 42 eIDAS2.

mi cyfrowymi zarówno w ramach UE, jak i poza nią. Wprowadzenie PQC stawia wyzwanie w zakresie zapewnienia, że nowe algorytmy będą mogły współpracować z istniejącymi systemami kryptograficznymi, a także że będą one spełniać wymogi regulacyjne w różnych innych jurysdykcjach, miejscami wciąż zasadniczo odmiennych od unijnej[24]. To z kolei wymaga ścisłej współpracy między regulatorami, dostawcami technologii oraz organizacjami standaryzacyjnymi. Z tej perspektywy nie będzie przesadą stwierdzenie, że wprowadzenie PQC do EUDI *Wallet* ma nie tylko znaczenie technologiczne i regulacyjne, ale także strategiczne i polityczne.

2. Techniczno-prawna analiza implementacji PQC w EUDI *Wallet*

Implementacja PQC w ramach EUDI *Wallet* napotyka na szereg trudności technicznych, które muszą zostać pokonane, aby zapewnić skuteczność i bezpieczeństwo tego systemu. Owe kłopotliwe zagadnienia związane są z różnymi aspektami technologii PQC, w tym przede wszystkim z efektywnością algorytmów, kompatybilnością z istniejącą już infrastrukturą cyfrową, a także z wymogami dotyczącymi mocy obliczeniowej i zasobów. Sytuacja ta nie powinna jednak dziwić, albowiem praktyczne wykorzystanie PQC wymaga znacznie większej mocy obliczeniowej niż tradycyjne metody kryptograficzne, co w tej konkretnej sytuacji może stanowić problem w kontekście implementacji tej technologii w systemach takich jak EUDI *Wallet*. Portfele cyfrowe, które w założeniu powinny działać sprawnie na różnych urządzeniach, w tym także na tych o ograniczonej mocy obliczeniowej (jak chociażby smartfony, czy inne urządzenia mobilne), muszą być odpowiednio zoptymalizowane pod kątem efektywności. Przykładowo algorytmy oparte na kratach, takie jak np. Kyber[25], wymagają znacznej liczby operacji matematycznych, które mogą spowalniać działanie systemów, w związku z czym przy ich hipotetycznym zastosowaniu konieczne jest znalezienie kompromisu między bezpieczeństwem a wydajnością, by zapewnić, że EUDI *Wallet* będzie działał sprawnie i bezpiecznie, niezależnie od mocy obliczeniowej urządzenia, na którym jest uruchamiany (co w przeciwnym razie, prócz zagrożenia, mogłoby wiązać się także z ryzykiem narażania części obywa-

[24] L. Chen *et al.*, *Report on Post-Quantum Cryptography*, https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf [dostęp: 31.08.2024].

[25] *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, https://csrc.nist.gov/pubs/fips/203/final/ [dostęp: 31.08.2024].

teli UE na wykluczenie społeczne)[26]. Taka optymalizacja algorytmów PQC, aby były one wydajne nawet na urządzeniach o ograniczonej mocy obliczeniowej, wymaga zaawansowanego podejścia inżynierskiego, które pozwoli na dostosowanie właściwych metod kompresji danych, redukcji liczby operacji matematycznych oraz wykorzystania nowoczesnych technologii, takich jak przetwarzanie rozproszone, aby zminimalizować obciążenie obliczeniowe. W przeciwnym razie korzystanie z EUDI *Wallet* na urządzeniach mobilnych mogłoby stać się niepraktyczne z powodu długiego czasu przetwarzania lub nadmiernego zużycia baterii[27].

Kolejnym kluczowym wyzwaniem jest zapewnienie kompatybilności algorytmów PQC z istniejącą już infrastrukturą cyfrową. Obecne systemy bezpieczeństwa, które bazują na tradycyjnych algorytmach kryptograficznych, muszą być zintegrowane z nowymi metodami PQC w sposób, który nie zakłóca ich funkcjonowania, co jest zadaniem wymagającym zaawansowanej inżynierii i testowania. W kontekście EUDI *Wallet*, który będzie musiał działać w ramach szeroko zintegrowanego ekosystemu cyfrowego, zapewnienie takiej kompatybilności jest szczególnie istotne, tym bardziej w warunkach europejskich, gdzie EUDI *Wallet* będzie musiał być w stanie współpracować z wieloma różnymi systemami identyfikacji elektronicznej, usługami zaufania oraz infrastrukturą sieciową, która już funkcjonuje w ramach Unii Europejskiej i w obrębia każdego jej państwa członkowskiego[28].

Jednakże implementacja PQC w ramach EUDI *Wallet* wiąże się nie tylko z wyzwaniami technicznymi, ale również z licznymi kwestiami natury prawnej oraz regulacyjnej. Rozporządzenie eIDAS 2 stanowi fundament prawny dla funkcjonowania EUDI *Wallet*, a główne cele eIDAS 2 obejmują zapewnienie wysokiego poziomu bezpieczeństwa usług identyfikacji elektronicznej oraz zwiększenie zaufania do tych usług w całej Unii Europejskiej. Wprowadzenie PQC do EUDI *Wallet* jest więc bezpośrednio związane z wymogami eIDAS 2 dotyczącymi bezpieczeństwa, albowiem rozporządzenie to wymaga, aby wszystkie systemy identyfikacji elektronicznej były odpowiednio zabezpieczone przed zagrożeniami cybernetycznymi[29], jak również szczegółowo opisuje obowiązki państw członkowskich oraz dostawców usług zaufania w zakresie zapewnienia bezpieczeństwa danych i identyfikacji elektronicznej, a to podkreślając konieczność stosowania odpowiednich środków tech-

[26] L. Chen *et al*., *op. cit*., s. 6–7.

[27] E. Alkim, L. Ducas, T. Pöppelmann, P. Schwabe, *Post-Quantum Key Exchange – A New Hope*, 25th USENIX Security Symposium (USENIX Security 16), 2016, s. 327–343.

[28] *Ibidem*.

[29] Art. 8 eIDAS 2.

nicznych i organizacyjnych, które uwzględniają aktualny stan wiedzy technicznej[30]. Oznacza to więc, że w erze postkwantowej systemy muszą być odporne właśnie na ataki kwantowe. Wprowadzenie PQC jest zatem niezbędne do spełnienia tych postawionych sobie nominalnie (*de facto* minimalnych) wymogów, lecz implementacja PQC w EUDI *Wallet* oferuje jednocześnie nowoczesne rozwiązania kryptograficzne, które będą mogły sprostać wyzwaniom także w przyszłości.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148[31] (ang. *Network and Information Systems Directive 2*, NIS 2) rozszerza zakres dotychczasowych regulacji dotyczących bezpieczeństwa sieci i systemów informatycznych w UE (tj. wynikających z NIS), albowiem wprowadza ona nowe wymogi dotyczące zarządzania ryzykiem, zgłaszania incydentów bezpieczeństwa oraz wymiany informacji między państwami członkowskimi[32]. Dyrektywa NIS 2 kładzie szczególny nacisk na zabezpieczenia techniczne, które mają na celu ochronę przed zagrożeniami cybernetycznymi, w tym także przed potencjalnymi atakami przeprowadzanymi za pomocą komputerów kwantowych. Odnosząc się ponownie do implementacji PQC w EUDI *Wallet*, dyrektywa NIS 2 stanowi istotny punkt odniesienia, ponieważ nakłada obowiązek stosowania najnowszych technologii zabezpieczających na operatorów usług krytycznych, w tym na dostawców usług identyfikacji elektronicznej[33]. Wymogi dyrektywy NIS 2 dotyczące zarządzania ryzykiem i odporności na zagrożenia kwantowe są zbieżne z celami eIDAS 2, co czyni te dwa akty prawnymi filarami regulacyjnymi, na których opiera się implementacja PQC w EUDI *Wallet,* przy czym dyrektywa NIS 2 dodatkowo zobowiązuje państwa członkowskie do współpracy przy wdrażaniu i monitorowaniu środków ochrony, co może przyczynić się do szybszego i bardziej jednolitego wdrożenia PQC w całej UE[34]. Istotne jest również, że dyrektywa NIS 2 nakłada obowiązki w zakresie raportowania incydentów, co może obejmować incydenty związane z nowymi zagrożeniami kwantowymi i prowadzić do ich nagłaśniania. Wprowadzenie PQC może zatem stanowić kluczowy element strategii zapobiegania takim incydentom i zapewnienia zgodności z dyrektywą NIS 2[35].

---

[30] Art. 19 eIDAS 2.
[31] Dz. Urz. UE L 333/80 z 2022 r. (dalej: „NIS 2").
[32] Art. 21 NIS 2.
[33] *Ibidem*.
[34] Art. 8 NIS 2.
[35] Art. 18 NIS 2.

Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2024 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020[36] (ang. *Cyber Resilience Act*, CRA) to kolejny kluczowy akt prawny, który ma znaczenie przy implementacji PQC w EUDI *Wallet*. Rozporządzenie CRA ma na celu wzmocnienie odporności cybernetycznej produktów i usług cyfrowych w UE i wprowadza nowe przepisy dotyczące projektowania, produkcji i zarządzania cyklem życia produktów cyfrowych z naciskiem na bezpieczeństwo i odporność na zagrożenia cybernetyczne[37]. Rozporządzenie CRA wymaga, aby wszystkie produkty cyfrowe, w tym systemy identyfikacji elektronicznej, były projektowane z myślą o najwyższym poziomie bezpieczeństwa, co oznacza, że już na etapie projektowania muszą być uwzględnione potencjalne zagrożenia wynikające z rozwoju technologii kwantowej. Dlatego też wprowadzenie PQC do EUDI *Wallet* wpisuje się w tę filozofię, oferując zaawansowane zabezpieczenia kryptograficzne, które mogą sprostać wyzwaniom przyszłości. Ważkie w tym przypadku pozostaje także zapewnienie, że produkty cyfrowe będą regularnie aktualizowane tak, aby mogły odpowiadać na nowe zagrożenia, co w przypadku PQC oznacza konieczność ciągłego monitorowania rozwoju technologii kwantowej oraz dostosowywania algorytmów kryptograficznych do nowych wyzwań.

W świetle opisanych okoliczności oczywiste pozostaje zasadnicze wyzwanie związane z implementacją PQC, jakim będzie zapewnienie harmonizacji przepisów i to nie tylko na poziomie unijnym, lecz także międzynarodowym, ponieważ w obliczu globalnych zagrożeń kwantowych skuteczna implementacja PQC wymaga ścisłej współpracy między państwami członkowskimi UE oraz z innymi partnerami międzynarodowymi. Istotnym elementem tej współpracy jest też harmonizacja standardów kryptograficznych, co pozwoli na stworzenie jednolitego podejścia do bezpieczeństwa cyfrowego na całym świecie. Poprzez swoje inicjatywy regulacyjne, takie jak eIDAS 2, NIS 2 oraz CRA, UE dąży do stworzenia spójnego i kompleksowego systemu ochrony przed zagrożeniami kwantowymi, lecz aby osiągnąć pełną skuteczność, regulacje te muszą być zharmonizowane nie tylko między sobą, lecz także z międzynarodowymi standardami, takimi jak te opracowywane przez NIST.

[36] Dalej: „CRA".
[37] Motyw 25, 60, 91 i art. 13 CRA.

W kontekście UE zaznaczyć należy, iż harmonizacja prawa obejmuje również kwestie związane z ochroną danych osobowych i prywatności. Wprowadzenie PQC w EUDI *Wallet* musi być zgodne z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, RODO, *General Data Protection Regulation, GDPR*)[38], co oznacza, że algorytmy kryptograficzne muszą zapewniać nie tylko bezpieczeństwo danych, ale również ich integralność i poufność.

Niezależnie od powyższego zastrzec należy, że w ramach implementacji PQC w EUDI *Wallet* odnieść należy się także do kwestii merkantylnych, albowiem działanie to wymaga niewątpliwie poczynienia znacznych inwestycji. Przede wszystkim mowa tu o wydatkach na dalsze badania i rozwój (ang. *Research and Development*, R&D), testowanie i wdrożenie algorytmów PQC, a dodatkowo konieczne będzie również poniesienie kosztów związanych z przeszkoleniem personelu technicznego oraz dostosowaniem istniejącej infrastruktury cyfrowej do nowych wymogów kryptograficznych. Kwestie te mogą być szczególnie problematyczne dla mniejszych państw członkowskich UE, które mogą nie dysponować wystarczającymi zasobami finansowymi, aby sprostać takim wymogom. W związku z tym UE może być zmuszona do wprowadzenia programów wsparcia finansowego dla państw członkowskich oraz dla podmiotów gospodarczych, które będą musiały zainwestować w tę technologię. Z drugiej strony pomimo wysokich kosztów związanych z implementacją PQC istnieją również potencjalne znaczące korzyści ekonomiczne. Wprowadzenie PQC może przyczynić się do zwiększenia bezpieczeństwa cyfrowego na całym kontynencie, co z kolei może zwiększyć zaufanie do cyfrowych usług zaufania i identyfikacji elektronicznej. Taka sytuacja może natomiast zaowocować przyciąganiem nowych użytkowników i inwestorów do ekosystemu EUDI *Wallet*, co przyniesie korzyści gospodarcze w dłuższej perspektywie. Dodatkowo UE dzięki swojej wiodącej roli w implementacji PQC może stać się liderem w dziedzinie bezpieczeństwa cyfrowego na świecie. To z kolei może przyczynić się do zwiększenia konkurencyjności europejskich firm technologicznych na rynku globalnym, co potencjalnie przełoży się na wzrost gospodarczy i innowacyjność w sektorze cyfrowym. W tych okolicznościach z jednej strony zapewnienie bezpieczeństwa w erze postkwantowej może zapobiec potencjalnym stratom gospodarczym

[38] Dz. Urz. UE L 119 z 2016 r.

wynikającym z ataków kwantowych, które mogłyby sparaliżować systemy finansowe i inne kluczowe sektory gospodarki. Z drugiej strony wprowadzenie PQC może wymusić na firmach inwestycje w nowe technologie, co przyspieszy innowacyjność i rozwój nowych produktów oraz usług cyfrowych.

Dodatkowo w ramach problematyki implementacji zaznaczyć należy również nie mniej ważny aspekt społeczny. Jedną z najważniejszych kwestii społecznych związanych z implementacją PQC jest zaufanie publiczne. Wprowadzenie nowej, zaawansowanej technologii kryptograficznej może budzić obawy wśród obywateli, zwłaszcza gdy chodzi o ochronę danych osobowych i prywatności. Aby zbudować zaufanie do EUDI *Wallet* i zapewnić społeczną akceptację dla PQC, niezbędne jest przeprowadzenie szeroko zakrojonych działań edukacyjnych i informacyjnych. Społeczeństwo musi być świadome korzyści wynikających z wprowadzenia PQC, a także zrozumieć, w jaki sposób technologia ta przyczyni się do poprawy bezpieczeństwa ich danych osobowych. Transparentność w zakresie działania algorytmów PQC oraz ich wpływu na prywatność stanowi tym samym doskonały punkt wyjścia do wzmocnienia zaufania publicznego.

3. Implikacje oraz dalsze wyzwania i perspektywy związane z implementacją PQC w EUDI *Wallet*

Wprowadzenie EUDI *Wallet* opartego na technologii PQC otwiera zupełnie nowy rozdział w dziedzinie cyberbezpieczeństwa. Rozważając implikacje omawianego rozwiązania w tejże dziedzinie, konieczne jest szczegółowe zbadanie, jak może ono wpłynąć na różne aspekty bezpieczeństwa cybernetycznego, w tym ochronę danych, odporność na zagrożenia oraz interoperacyjność z istniejącymi systemami, które to kwestie również komplikują się istotnie w sytuacji szybko rozwijającej się technologii kwantowej.

Jednym z najważniejszych skutków wprowadzenia PQC w ramach EUDI *Wallet* jest zatem znaczące podniesienie poziomu ochrony danych. Jak wskazano już na wstępie, tradycyjne metody kryptograficzne, takie jak omówiony już RSA czy ECC (ang. *Elliptic Curve Cryptography*)[39], które od lat stanowią fundament bezpieczeństwa w systemach cyfrowych, stają się podatne na zagrożenia ze strony komputerów

[39] D. Hankerson, A. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography* 2004. s. 7–14, http://tomlr.free.fr/Math%E9matiques/Math%20Complete/Cryptography/Guide%20to%20Elliptic%20Curve%20Cryptography%20-%20D.%20Hankerson,%20A.%20Menezes,%20S.%20Vanstone.pdf/ [dostęp: 31.08.2024].

kwantowych. Implementacja PQC w EUDI *Wallet* ma więc kluczowe znaczenie dla ochrony wrażliwych danych osobowych przechowywanych w portfelu, ponieważ oferuje narzędzia, które mają na celu przeciwdziałanie tym zagrożeniom poprzez zastosowanie algorytmów odpornych na ataki kwantowe. Zastosowanie PQC w EUDI *Wallet* nie tylko zwiększa poziom ochrony danych, ale również zapewnia ich integralność oraz autentyczność. W erze cyfrowej, w której „cyberprzestępczość" przybiera na sile, możliwość zagwarantowania, że dane nie zostały zmienione ani przechwycone przez nieuprawnione osoby, jest istotnym elementem bezpieczeństwa cybernetycznego. Co więcej, PQC może również przeciwdziałać atakom opartym na manipulacji danymi, co stanowi dodatkowy jeszcze aspekt ochrony. Zastosowanie PQC w EUDI *Wallet* ma ponadto także długoterminowe implikacje w zakresie odporności na przyszłe zagrożenia, co oznacza, że systemy cyfrowe są projektowane z myślą o ewolucji technologii i zmieniających się metodach ataków. PQC, dzięki swojej złożoności matematycznej i specyfice algorytmów, oferuje poziom ochrony, który będzie trudny do pokonania nawet przez przyszłe technologie kwantowe, ale mimo to, aby zapewnić długoterminową odporność, konieczne jest ciągłe monitorowanie rozwoju technologii kwantowych oraz dostosowywanie stosowanych algorytmów do nowych odkryć.

Interoperacyjność, czyli zdolność różnych systemów i organizacji do współpracy i wymiany danych, jest kluczowym elementem współczesnej infrastruktury cyfrowej. Wprowadzenie PQC w EUDI *Wallet* ma zatem istotne znaczenie dla interoperacyjności na wielu poziomach, zarówno w kontekście technologicznym, jak i regulacyjnym. Na poziomie technologicznym zastosowanie nowych algorytmów kryptograficznych może wpłynąć na zdolność systemu EUDI *Wallet* do współpracy z innymi systemami cyfrowymi, które wciąż opierają się na tradycyjnych metodach kryptograficznych. Jednak aby zapewnić płynną integrację i współpracę pomiędzy różnymi systemami, konieczne będzie opracowanie standardów, które umożliwią bezproblemową wymianę danych pomiędzy systemami korzystającymi z PQC a tymi, które jeszcze nie przeszły na nowe technologie. To wyzwanie wymaga skoordynowanego podejścia, tak aby uniknąć fragmentacji rynku. Na poziomie regulacyjnym wprowadzenie PQC w EUDI *Wallet* może wymagać dostosowania istniejących przepisów dotyczących ochrony danych, cyberbezpieczeństwa oraz interoperacyjności systemów cyfrowych. W związku z tym organy regulacyjne będą musiały opracować nowe wytyczne i standardy, które uwzględnią specyfikę PQC oraz jego wpływ na współpracę pomiędzy systemami cyfrowymi.

Wprowadzenie PQC w EUDI *Wallet* nie tylko stawia UE przed nowymi wyzwaniami, ale również otwiera perspektywy rozwoju, które mogą zdefiniować przy-

szłość bezpieczeństwa cyfrowego na całym świecie. Jednym z głównych wyzwań z tym związanych jest jednak złożoność implementacji nowych algorytmów kryptograficznych, które wymagają zaawansowanej wiedzy technicznej oraz ustawicznej iteracji, polegającej na testowaniu nowych algorytmów w różnych scenariuszach w ten sposób, aby upewnić się, że są one wystarczająco bezpieczne i skuteczne w praktyce. Kolejnym wyzwaniem jest zarządzanie kluczami kryptograficznymi związanymi z PQC, albowiem w przeciwieństwie do tradycyjnych metod kryptograficznych zarządzanie kluczami w PQC może być bardziej skomplikowane, co wymaga opracowania nowych narzędzi i procedur do tego potrzebnych, a to chociażby po to, aby umożliwić skuteczne zarządzanie kluczami oraz ich bezpieczną wymianę pomiędzy różnymi systemami[40].

Implementacja PQC wiąże się również z pewnymi wyzwaniami etycznymi, ponieważ rozwój technologii kryptograficznej, która jest odporna na ataki kwantowe, może prowadzić do zintensyfikowania wyścigu zbrojeń w dziedzinie cyberbezpieczeństwa. Tego rodzaju konkurencja może nieść ze sobą ryzyko eskalacji już dość wysokich napięć międzynarodowych oraz pogłębienia nierówności technologicznych między krajami rozwiniętymi a rozwijającymi się. Dodatkowo kwestia dostępu do technologii PQC może stać się przedmiotem debat, zwłaszcza w aspekcie równości i sprawiedliwości społecznej, tym bardziej, że istnieje duże ryzyko, że tylko najbogatsze kraje i korporacje będą w stanie wdrażać na bieżąco najnowsze technologie zabezpieczające, co może prowadzić do marginalizacji innych podmiotów na rynku globalnym. W związku z tym implementacja PQC w EUDI *Wallet* musi być przeprowadzona w sposób odpowiedzialny z uwzględnieniem zarówno aspektów technicznych, społecznych, jak i etycznych, zaś wprowadzenie tej technologii powinno być poprzedzone szeroką dyskusją na temat jej potencjalnych konsekwencji nie tylko w kręgach specjalistycznych, lecz także na forum publicznym, co obecnie nie jest niestety praktykowane.

PQC, choć obiecująca, nie jest rozwiązaniem ostatecznym, albowiem tak dynamiczny rozwój technologii kwantowej oraz innych zaawansowanych technik obliczeniowych może prowadzić do pojawienia się już wkrótce nowych zagrożeń, które będą wymagały dalszej adaptacji systemów bezpieczeństwa, dlatego też EUDI *Wallet* musi być przygotowany na ciągłe zmiany i ewolucję zagrożeń. Adaptacja do nowych zagrożeń będzie wymagała stałego monitorowania i analizy ryzyk związanych

[40] D. Chawla, P.S. Mehra, *A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions*, https://www.sciencedirect.com/science/article/abs/pii/S2542660523002731/ [dostęp: 31.08.2024].

z rozwojem technologii kwantowej. Konieczne będzie również wdrożenie mechanizmów pozwalających na szybką aktualizację systemów kryptograficznych, aby mogły one skutecznie odpowiadać na nowe wyzwania. W tym kontekście ważne będzie zbudowanie infrastruktury cyfrowej, która będzie cechowała się elastycznością. W tej kwestii zauważyć należy także, że technologia kryptograficzna jest tylko jednym z elementów zapewniających bezpieczeństwo cyfrowe, ponieważ kluczową rolę odgrywa tu przede wszystkim świadomość „najsłabszego ogniwa", a więc samych użytkowników i ich zdolności do odpowiedzialnego korzystania z narzędzi cyfrowych. Wprowadzenie PQC w EUDI *Wallet* będzie skuteczne tylko wtedy, gdy użytkownicy będą świadomi jego znaczenia i będą umieć z niego korzystać w sposób, który zapewni maksymalne bezpieczeństwo ich danych. Użytkownicy muszą zrozumieć, w jaki sposób nowe algorytmy kryptograficzne chronią ich dane oraz jakie kroki mogą podjąć, aby zwiększyć swoje bezpieczeństwo w cyfrowym świecie. Działania edukacyjne mogą obejmować kampanie informacyjne, szkolenia oraz dostęp do zasobów edukacyjnych, które będą pomagały użytkownikom w zrozumieniu technologii kryptograficznych. Świadomość użytkowników jest więc kluczowa dla zapobiegania atakom socjotechnicznym, które mogą stanowić poważne zagrożenie nawet w najbardziej zaawansowanych systemach kryptograficznych. Nawet najlepsze zabezpieczenia technologiczne mogą być nieskuteczne, jeśli użytkownicy nie będą przestrzegali podstawowych zasad bezpieczeństwa[41].

Ostatecznie wraz z rozwojem PQC i jego implementacją w EUDI *Wallet*, możemy spodziewać się także dalszych inicjatyw legislacyjnych (eIDAS 3.0?), które mogą obejmować zarówno szczegółowe wytyczne dotyczące implementacji PQC, jak i szersze ramy prawne dotyczące zarządzania technologiami kwantowymi.

Wnioski

Implementacja PQC w ramach EUDI *Wallet* stanowi bezprecedensowy krok w kierunku zabezpieczenia cyfrowej infrastruktury Unii Europejskiej na miarę zagrożeń nadchodzącej ery obliczeń kwantowych. W dobie intensywnych przemian technologicznych i coraz bardziej zaawansowanych zagrożeń cybernetycznych PQC jawi się nie tylko jako innowacyjny fundament zabezpieczeń kryptograficznych, lecz także jako nieodzowny element architektury cyberbezpieczeństwa, wspieranej regu-

[41] *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, https://csrc.nist.gov/publications/detail/nistir/8413/final/ [dostęp: 31.08.2024].

lacjami prawnymi takimi jak eIDAS 2, NIS 2 oraz CRA. Algorytmy postkwantowe, choć odporne na przyszłe zagrożenia ze strony komputerów kwantowych, wymagają od systemów takich jak EUDI *Wallet* zupełnie nowego podejścia do optymalizacji, szczególnie w kontekście urządzeń mobilnych, które stanowią ważny element ekosystemu cyfrowego UE, a to chociażby z uwagi na utrzymującą się tendencję wzrostową w aspekcie popularności tego rodzaju urządzeń oraz szerokiego wachlarza ich zastosowań. Jednocześnie konieczne jest wypracowanie rozwiązań pozwalających na płynne przejście od obecnie stosowanych metod kryptograficznych do nowych standardów PQC bez narażania systemów na luki bezpieczeństwa, które mogłyby zostać wykorzystane przez „cyberprzestępców".

Poza wyzwaniami technologicznymi i prawnymi wdrożenie PQC w EUDI *Wallet* niesie ze sobą istotne korzyści gospodarcze i społeczne. Wprowadzenie zabezpieczeń postkwantowych przyczyni się do wzrostu zaufania publicznego do usług cyfrowych, co z kolei może znacząco zwiększyć ich adopcję zarówno w sektorze prywatnym, jak i publicznym. Podniesienie poziomu bezpieczeństwa danych osobowych, integralności cyfrowych podpisów i zaufania do systemów transakcyjnych sprawi, że korzystanie z portfeli cyfrowych takich jak EUDI *Wallet* stanie się powszechne, przyczyniając się do budowy zintegrowanego jednolitego rynku cyfrowego w UE. Z technicznego punktu widzenia wdrożenie PQC będzie motorem napędowym innowacji, szczególnie w sektorach związanych z bezpieczeństwem cyfrowym, a także dla branż technologicznych odpowiedzialnych za rozwój nowych algorytmów i rozwiązań kryptograficznych. Długofalowe efekty tego procesu mogą obejmować ponadto wzrost konkurencyjności europejskich firm na rynku globalnym oraz stymulację nowych innowacyjnych rozwiązań w dziedzinie technologii postkwantowych.

Społeczna akceptacja PQC, a w szczególności jej implementacja w głównych systemach identyfikacji cyfrowej, będzie wymagała szeroko zakrojonych działań edukacyjnych. Konieczne jest uświadomienie obywatelom Unii Europejskiej, jakie korzyści płyną z zastosowania technologii kryptograficznych odpornych na ataki kwantowe oraz jak nowe standardy bezpieczeństwa będą chronić ich dane osobowe i transakcje w cyfrowym świecie. Transparentność w zakresie sposobu działania PQC, w połączeniu z zaawansowanymi mechanizmami ochrony prywatności, stanie się podstawą budowy zaufania społecznego, które będzie niezbędne dla sukcesu takich inicjatyw jak EUDI *Wallet*.

W dalszej perspektywie prawodawcy unijni mogą sięgnąć po nowe inicjatywy legislacyjne, w tym nie jest wykluczone, że powstanie eIDAS 3.0, którego przepisy będą jeszcze bardziej precyzyjne w zakresie wymogów dotyczących PQC oraz tech-

nologii kwantowych. Być może przyszłość przyniesie nie tylko standardy zabezpieczeń przeciwko komputerom kwantowym, ale również zupełnie nowe paradygmaty w obszarze ochrony danych oparte na technologiach, które dziś są jeszcze w fazie badań albo o których nie mamy nawet pojęcia.

Jednocześnie nie można zapominać o potencjalnych zagrożeniach związanych z nierównym dostępem do nowoczesnych technologii kryptograficznych. Istnieje ryzyko, że mniejsze kraje lub mniej rozwinięte sektory gospodarki mogą nie być w stanie szybko wdrożyć PQC z powodu braku zasobów, co może prowadzić do nierówności technologicznych na skalę globalną. W związku z tym wprowadzenie PQC musi iść w parze z międzynarodową współpracą i wsparciem finansowym dla mniej rozwiniętych regionów, tak aby zapewnić globalną koordynację i spójność w obszarze cyberbezpieczeństwa.

Podsumowując, kryptografia postkwantowa w EUDI *Wallet* to kamień milowy na drodze do zapewnienia długoterminowego bezpieczeństwa cyfrowego dla obywateli i instytucji UE. Mimo wyzwań technicznych i prawnych, które wiążą się z jej wdrożeniem, PQC stwarza wyjątkowe możliwości zarówno w kontekście zwiększenia poziomu ochrony danych, jak i wzmocnienia pozycji Europy na globalnej mapie innowacji technologicznych. Kluczem do sukcesu będzie jednak nie tylko zaawansowanie technologiczne, ale także harmonizacja międzynarodowych standardów, edukacja społeczeństwa oraz wielopłaszczyznowa współpraca między państwami członkowskimi i globalnymi partnerami. Tylko takie zintegrowane i kompleksowe podejście pozwoli na pełne wykorzystanie potencjału PQC i zapewnienie, że cyfrowy ekosystem UE będzie odporny na nadchodzące wyzwania ery kwantowej.

Bibliografia

Akty prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do trans akcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257/73 z 2014 r.).

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

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków mających na celu zapewnienie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (dyrektywa w sprawie bezpieczeństwa sieci i informacji) oraz uchylająca dyrektywę (UE) nr 2016/1148 (Dz. Urz. UE L 333/80 z 2022 r.).

Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2024 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniającego rozporządzenie (UE) 2019/1020.

Źródła internetowe

Chawla D., Mehra P.S., *A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions,* https://www.sciencedirect.com/science/article/abs/pii/S2542660523002731/ [dostęp: 31.08.2024].

Chen L., Jordan S., Liu Y., Moody D., Peralta R., Perlner R., Smith-Tone D., *Report on Post-Quantum Cryptography*, https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf [dostęp: 31.08.2024].

Entering the Quantum Era, https://www.ox.ac.uk/news/features/entering-quantum-era/ [dostęp: 31.08.2024].

Module-Lattice-Based Key-Encapsulation Mechanism Standard, https://csrc.nist.gov/pubs/fips/203/final/ [dostęp: 31.08.2024].

NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat, https://www.nist.gov/news-events/news/2016/04/nist-kicks-effort-defend-encrypted-data-quantum-computer-threat/ [dostęp: 31.08.2024].

Post-Quantum Cryptography: Current Status and Next Steps, https://csrc.nist.gov/publications/detail/nistir/8105/final [dostęp: 30.08.2024].

Shor P.W., *Algorithms for Quantum Computation: Discrete Logarithms and Factoring, Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, https://cc.ee.ntu.edu.tw/~rbwu/rapid_content/course/QC/Shor1994.pdf/ [dostęp: 31.08.2024].

Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, https://csrc.nist.gov/pubs/ir/8309/final [dostęp: 31.08.2024].

Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, https://csrc.nist.gov/publications/detail/nistir/8413/final/ [dostęp: 31.08.2024].

Toward a code-breaking quantum computer, https://www.sciencedaily.com/releases/2024/08/240823120024.htm/ [dostęp: 30.08.2024].

What Is Post-Quantum Cryptography?, https://www.nist.gov/cybersecurity/what-post-quantum-cryptography/ [dostęp: 31.08.2024].

What is the EU Digital Identity Wallet, https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+is+the+Wallet/ [dostęp: 30.08.2024].

Literatura

Alkim E., Ducas L., Pöppelmann T., Schwabe P., *Post-Quantum Key Exchange – A New Hope*, 25th USENIX Security Symposium (USENIX Security 16), 2016.

Bernstein D.J., Buchmann J., Dahmen E., *Post-Quantum Cryptography*, Springer 2009.

Hankerson D., Menezes A., Vanstone S., *Guide to Elliptic Curve Cryptography*, 2004, http://tomlr.free.fr/Math%E9matiques/Math%20Complete/Cryptography/Guide%20to%20Elliptic%20Curve%20Cryptography%20-%20D.%20Hankerson,%20A.%20Menezes,%20S.%20Vanstone.pdf/ [dostęp: 31.08.2024].

Kapcia P., *Kryptosystemy oparte na problemach trudnych obliczeniowo z wyszczególnieniem problemu faktoryzacji liczb całkowitych*, „Elektrotechnika i Elektronika" 2005, t. 24, nr 2.

Mosca M., *Cybersecurity in an Era with Quantum Computers: Will We Be Ready?*, „IEEE Security & Privacy" 2018, vol. 16(5).

Schneier B., *Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C*, wyd. 2, Warszawa 2002.

Stallings W., *Cryptography and Network Security: Principles and Practice*, Pearson 2014, https://dl.hiva-network.com/Library/security/Cryptography-and-network-security-principles-and-practice.pdf/ [dostęp: 31.08.2024].

Implementation of post-quantum cryptography within EUDI Wallet as an element of eIDAS 2 – legal, technical challenges and cybersecurity implications in the context of CRA and NIS 2 regulations

Abstract

This article examines the importance of post-quantum cryptography (PQC) in the context of the post-quantum reality, emphasizing its role as a foundation for future digital security. It also examines the challenges related to the implementation of PQC in key European projects such as the European Digital Identity Wallet (EUDI Wallet), which is set to become a central element of the European Union (EU) digital ecosystem. In the post-quantum era, PQC will not only be a tool for protection against new threats, but also a key element of legal regulations, such as eIDAS 2 and NIS 2, aimed at ensuring the security and interoperability of digital systems in the EU. The paper emphasizes the importance of harmonization of international regulations and global cooperation, which are necessary for the effective implementation of PQC, ensuring resilience to threats resulting from future developments in quantum technology.

Keywords

Post-quantum cryptography, digital security, cryptographic algorithms, EUDI Wallet, interoperability, cybersecurity, quantum technology, eIDAS 2, NIS 2

DOI: 10.34616/151203

Prawo Mediów Elektronicznych. Kwartalnik Naukowy
2024, nr 3, 96–129

Kamil Szpyt*
ORCID: 0000-0002-2307-8789

Odpowiedzialność cywilna za szkody wyrządzone klientom w wyniku zastosowania systemów sztucznej inteligencji w działalności bankowej[1]

Streszczenie

Artykuł omawia kluczowe zagadnienia związane z odpowiedzialnością cywilną banków za szkody wyrządzone klientom w wyniku zastosowania systemów sztucznej inteligencji (AI). W obliczu dynamicznego rozwoju technologii i rosnącego znaczenia AI w sektorze finansowym tradycyjne zasady odpowiedzialności cywilnej mogą okazać się niewystarczające. Analizowane są problemy związane z identyfikacją podmiotów odpowiedzialnych oraz ocena ryzyka, jakie niesie ze sobą wykorzystywanie zaawansowanych algorytmów. W kontekście braku kompleksowych regulacji prawnych, zarówno na poziomie krajowym, jak i unijnym, artykuł podkreśla potrzebę dogłębnej analizy obowiązujących norm oraz dostosowania ich do nowych wyzwań. Przedstawiono również omówienie wybranych regulacji unijnych, takich jak AI Act oraz projektowane przepisy dotyczące odpowiedzialności za systemy sztucznej inteligencji. Praca koncentruje się na wyzwaniach prawnych związanych z ochroną praw klientów oraz ryzykiem finansowym wynikającym z niewłaściwego lub nieprzewidywalnego działania systemów AI w bankowości.

Słowa kluczowe

sztuczna inteligencja, system sztucznej inteligencji, odpowiedzialność cywilna, delikt, produkt niebezpieczny

1. Wprowadzenie

W dobie dynamicznego rozwoju nowych technologii sztuczna inteligencja (ang. *artificial intelligence*, AI) staje się integralnym elementem działalności coraz większej liczby sektorów gospodarki, w tym również – bankowości[2]. Zastosowanie

---

* Autor jest doktorem nauk prawnych, adiunktem w Katedrze Prawa Cywilnego Wydziału Prawa, Administracji i Stosunków Międzynarodowych Uniwersytetu Andrzeja Frycza Modrzewskiego.

[1] Badania dofinansowane ze środków przeznaczonych na utrzymanie i rozwój potencjału badawczego w dyscyplinie nauki prawne Nr WSUB/2022/12/00024.

[2] Wykorzystanie AI w sektorze bankowym to sztandarowy przykład tzw. FinTech, czyli mariażu nowych technologii i działalności bankowej oraz okołobankowej (zob. szerzej o zagadnieniu FinTech: K. Szpyt, *FinTech – pojęcie, historia, rynek*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym*, Warszawa 2024, s. 3–20; *idem*, *InsurTech – zarys zjawiska*, [w:] K. Szpyt (red.), *InsurTech. Nowe*

systemów AI w tym ostatnim obszarze przynosi liczne profity, wśród których warto wymienić chociażby zwiększenie efektywności operacyjnej, zmniejszenie kosztów działalności oraz wyższą jakość obsługi klienta[3]. Niemniej – wraz ze wspomnianymi korzyściami – pojawiają się także nowe wyzwania i zagrożenia, w tym niewystępujące wcześniej ryzyka związane z odpowiedzialnością cywilną za szkody spowodowane przez AI. Problematyka ta zyskuje na znaczeniu zwłaszcza w obliczu braku – na chwilę obecną – szczegółowych regulacji prawnych w tej materii (zarówno na poziomie krajowym, jak i unijnym). Pojawia się też pytanie, czy tradycyjne zasady odpowiedzialności cywilnej, oparte w znacznej mierze na przewidywalności i kontrolowalności działań, nie okażą się w pewnym momencie niewystarczające w kontekście autonomicznych systemów AI, które operują na bazie skomplikowanych algorytmów i dużych zbiorów danych (ang. *Big Data*). Również kwestia wskazania osoby odpowiedzialnej za szkodę staje się o wiele bardziej złożona, gdy uwzględnimy, że przy tworzeniu, udostępnianiu i/lub dystrybuowaniu ww. systemów często dochodzi do współpracy różnych podmiotów, takich jak banki, dostawcy technologii oraz podmioty zajmujące się pozyskiwaniem danych. Jednocześnie bankowość jest sektorem silnie regulowanym, w którym precyzja, zaufanie i bezpieczeństwo odgrywają kluczowe role. Banki w swojej działalności muszą uwzględniać nie tylko potrzebę przestrzegania ogólnych przepisów dotyczących cyberbezpieczeństwa czy ochrony danych osobowych, ale również przepisów sektorowych, dotyczących m.in. zasad ochrony tajemnicy bankowej czy zapobiegania praniu pieniędzy i finansowaniu terroryzmu. To wszystko sprawia, że ewentualne ryzyka naruszeń i nadużyć związanych z zastosowaniem nowych technologii generują w tym przypadku znaczne większe niż zazwyczaj obawy[4].

---

technologie w branży ubezpieczeń, Warszawa 2023, s. 7; M. Nowakowski, *FINTECH – technologie, finanse, regulacje. Praktyczny przewodnik dla sektora innowacji finansowych*, Warszawa 2020; M. Folwarski, *Sektor FinTech na europejskim rynku usług bankowych*, Warszawa 2019; W. Szpringer, *Nowe technologie a sektor finansowy. FinTech jako szansa i zagrożenie*, Warszawa 2017).

[3] O potencjalnym wzroście dochodów z działalności bankowej związanym z wdrożeniem rozwiązań opartych na sztucznej inteligencji (w tym generatywnej AI) zob. szerzej: V. Kamalnath *et al.*, *Capturing the full value of generative AI in banking* https://www.mckinsey.com/industries/financial-services/our-insights/capturing-the-full-value-of-generative-ai-in-banking [dostęp: 15.07.2024]; por. P. Widawski, [w:] *Raport: Sztuczna Inteligencja. Dobre praktyki, aspekty prawne, zastosowanie w sektorze finansowym*, https://fintechpoland.com/wp-content/uploads/2022/03/AI_raport_FIN-1.pdf [dostęp: 15.07.2024]. O innych potencjalnych korzyściach zob. także: J. Grzywacz, E. Jagodzińska-Komar, *Rola sztucznej inteligencji w rozwoju sektora bankowego*, „Nauki Ekonomiczne" 2021, t. 34, s. 22–23.

[4] G. Bar, *Sztuczna inteligencja i uczenie maszynowe*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym*…, s. 21–22.

Wprowadzenie AI do operacji bankowych każdorazowo wiąże się z koniecznością zrozumienia zarówno potencjalnych wiążących się z tym korzyści, jak i zagrożeń. Nie można zapomnieć, że nawet najbardziej zaawansowane technologie bywają zawodne, a decyzje „podejmowane" przez algorytmy mogą prowadzić do nieprzewidzianych konsekwencji, w tym ogromnych strat finansowych oraz naruszenia praw klientów. Jest to zagadnienie tym istotniejsze, że banki, z uwagi na ich rolę w ochronie powierzonego im kapitału, nieodmiennie kładą duży nacisk na szeroko pojęte zarządzanie ryzykiem i nie należą do podmiotów/instytucji, które w sposób lekkomyślny generowałyby dodatkowo niepotrzebne zagrożenia (mowa tutaj zarówno o ryzyku względem całej swojej działalności, jak i konkretnego klienta)[5].

Niniejszy artykuł ma na celu analizę problematyki odpowiedzialności cywilnej za szkody wyrządzone klientom[6] w wyniku zastosowania systemów sztucznej inteligencji *stricte* w działalności samych banków[7]. Z tego względu poza obszarem zainteresowań pozostawiono sytuację wykorzystania ww. systemów przez inne podmioty, które można zaliczyć do szeroko pojętego systemu bankowego, takie jak np. bank centralny, organy nadzorcze, podmioty gwarantujące wypłatę depozytów czy instytucje zrzeszające banki[8]. Podobnie ma się sytuacja ze wszelkiego rodzaju parabankami oraz fintechami, czyli start-upami i spółkami technologicznymi oferującymi usługi okołobankowe w środowisku nowotechnologicznym (należy jednak nad-

---

[5] Zob. wywiad przeprowadzony przez A. Prończuk-Omiotek z J. Stryczyńskim (*Jak banki wykorzystują sztuczną inteligencję?*, https://www.youtube.com/watch?v=bFMZOsh2ADg [dostęp: 15.05.2024]).

[6] Pod tym pojęciem na gruncie niniejszego artykułu należy rozumieć każdy podmiot (osobę fizyczną, osobę prawną oraz jednostkę organizacyjną nieposiadającą osobowości prawnej) zawierający z bankiem umowę i korzystający z oferowanych przez niego produktów lub/i usług. Jednocześnie, dla zapewnienia kompleksowości wywodu, w niezbędnym zakresie uwzględniono również sytuację wspomnianych podmiotów na etapie poprzedzającym jeszcze zawarcie umowy, które jednak podejmują w tym celu pewne kontakty z bankiem (np. w celu zweryfikowania ich zdolności kredytowej).

[7] Na gruncie tego tekstu za obowiązującą zostaje uznana definicja banku zawarta w art. 2 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz. U. z 2023 r. poz. 2488 ze zm.; dalej: pr. bank.). Zgodnie z nią „bank jest osobą prawną utworzoną zgodnie z przepisami ustaw, działającą na podstawie zezwoleń uprawniających do wykonywania czynności bankowych obciążających ryzykiem środki powierzone pod jakimkolwiek tytułem zwrotnym". Natomiast osoby zainteresowane zapoznaniem się z propozycjami doktryny w zakresie ujęcia wspomnianego terminu powinny sięgnąć do: I. D. Czechowska, *Przegląd definicji banku stanowiącego aktywny kanał dystrybucji produktów ubezpieczeniowych*, „Acta Universitatis Lodziensis. Folia Oeconomica" 2011, nr 259, s. 17–26.

[8] O polskim systemie bankowym i jego elementach składowych zob. szerzej: M. Zaleska, *Charakterystyka systemu bankowego – uwarunkowania instytucjonalne*, [w:] M. Zaleska (red.), *Współczesna bankowość*, Warszawa 2008, s. 24; A. Iwańczuk, *System bankowy i system płatniczy – powiązania i wzajemne uwarunkowania*, „Zeszyty Naukowe/Akademia Ekonomiczna w Poznaniu" 2008, nr 111, s. 14; T. Cicirko, K. Kreczmańska-Gigoł, O. Mikołajczyk., M. Mikołajczyk, *Bank centralny i banki komercyjne*, [w:] J. Ostaszewski (red.), *Finanse*, Warszawa 2010, s. 382.

mienić, że zdecydowana większość poczynionych w ramach niniejszego artykułu uwag znajdzie zastosowanie – wprost lub w drodze analogii – również wobec tych podmiotów)[9]. Natomiast w celu zapewnienia odpowiedniej kompletności wywodu w opracowaniu w niezbędnym zakresie odniesiono się do ewentualnej odpowiedzialności dostawców rozwiązań technologicznych i innych podmiotów współpracujących z bankami, które potencjalnie mogą odpowiadać za szkody spowodowane przez systemy AI.

W niniejszym tekście skupiono się na cywilnej odpowiedzialności odszkodowawczej, poza zakresem analizy pozostawiając zagadnienia rękojmi i gwarancji[10], obowiązków związanych z dostarczaniem treści i usług cyfrowych[11], jak również odpowiedzialności za usterki w oprogramowaniu przewidzianej w przepisach prawa autorskiego[12]. Jednocześnie analizie poddano obowiązujące regulacje krajowe i unijne, z uwzględnieniem nieobowiązującego jeszcze rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Tekst mający znaczenie dla EOG)[13] oraz procedowanego obecnie Wniosku Dyrektywy Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję)[14].

---

[9] Na marginesie należy nadmienić, że część przedstawicieli doktryny określa mianem „fintechów" również korzystające z rozwiązań opartych na nowych technologiach banki. Posunięcie to nie wydaje się jednak najlepsze, ponieważ wprowadza niepotrzebne zamieszanie terminologiczne (zob. szerzej: K. Szpyt, *FinTech*…, s. 6).

[10] O problematyce reklamacji i gwarancji w kontekście oprogramowania w czasach sztucznej inteligencji zob. szerzej: A. Michalak, *Odpowiedzialność cywilnoprawna w obrocie oprogramowaniem komputerowym w erze sztucznej inteligencji*, Warszawa 2021, *passim*.

[11] Wspomniane obowiązki zostały uregulowane w ustawie z dnia 30 maja 2014 r. o prawach konsumenta (t.j. Dz. U. z 2023 r. poz. 2759) i wykraczają dalece poza materię odszkodowawczą.

[12] Zob. art. 55 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2022 r. poz. 2509).

[13] PE/24/2024/REV/1; dalej jako: AI Act.

[14] Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję) (Tekst mający znaczenie dla EOG) {SEC(2022) 344 final} - {SWD(2022) 318 final} - {SWD(2022) 319 final} {SWD(2022) 320 final}, Bruksela 2022 r. COM(2022) 496 final 2022/0303 (COD); dalej jako: projekt dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję.

2. Pojęcie sztucznej inteligencji i systemów sztucznej inteligencji

Skonstruowanie definicji sztucznej inteligencji, nierodzącej zaciekłych sporów w doktrynie oraz nieobarczonej ryzykiem rychłej dezaktualizacji, stanowiło wyzwanie, z którym od kilku lat próbowano zmierzyć się zarówno w piśmiennictwie, jak i w ramach ustawodawstwa unijnego[15]. Pomimo tego liczba nadal istniejących wątpliwości (niejednokrotnie – o niezwykle zniuansowanym charakterze) oraz nagromadzenie literatury przedmiotu sprawiają, że z powodzeniem zagadnienie to mogłoby się stać przedmiotem nie tylko odrębnego artykułu, ale wręcz monografii. Ponieważ jego kompleksowe zgłębianie dalece wykraczałoby poza ramy niniejszego opracowania, wspomniana kwestia zostanie przedstawiona tutaj jedynie w niezbędnym, najistotniejszym zakresie. Dokonując pewnego uproszczenia, można wskazać na dwa podstawowe sposoby rozumienia pojęcia sztucznej inteligencji, a mianowicie jako:

a) dziedziny wiedzy[16],

b) systemów maszynowych/programów komputerowych w mniejszym lub większym stopniu starających się imitować ludzki sposób myślenia.

Pierwszy z nich już na pierwszy rzut oka wydaje się nieprzydatny w kontekście dość mocno praktycznych rozważań prowadzonych w niniejszym artykule. Ponadto za wyborem drugiego przemawia fakt, że to do niego sięgnął ustawodawca unijny już przy swoich pierwszych próbach zdefiniowania sztucznej inteligencji. Zostały one podjęte w 2018 r. To wówczas Komisja Europejska wydała Komunikat „Sztuczna inteligencja dla Europy", zgodnie z którym termin ten „odnosi się do systemów, które wykazują inteligentne zachowanie dzięki analizie otoczenia i podejmowania działań – do pewnego stopnia autonomicznie – w celu osiągnięcia konkretnych celów. Systemy SI mogą być oparte na oprogramowaniu, działając w świecie wirtualnym (np. asystenci głosowi, oprogramowanie do analizy obszaru, wyszukiwarki, systemy rozpoznawania mowy i twarzy), lub mogą być wbudowane w urządzenia (np. zaawansowane roboty, samochody, drony lub aplikacje internetu rzeczy)"[17]. Ko-

[15] Szerzej o problemie z właściwym zdefiniowaniem sztucznej inteligencji zob. P. Staszczyk, *Czy unijna regulacja odpowiedzialności cywilnej za sztuczną inteligencję jest potrzebna?*, „Europejski Przegląd Sądowy" 2022, nr 6, s. 25.

[16] Zob. B. Michałowski, A. Przegalińska, A. Poniewierski, *Internet of Things (IoT) i Artificial Intelligence (AI) w Polsce. Jak wykorzystać rewolucję technologiczną Internetu Rzeczy i Sztucznej Inteligencji w rozwoju Polski. Raport*, Warszawa 2018, https://sobieski.org.pl/wp-content/uploads/Raport-Iot-i-AI-w-Polsce-03-2018-Micha%C5%82owski.pdf [dostęp: 15.07.2024], s. 12.

[17] Komunikat z 25.04.2018 r. Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Sztuczna inteligencja dla Europy", COM/2018/237 final, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CE-

lejne propozycje definicji pojawiły się m.in. w dokumencie „Biała Księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania”[18], w którym Komisja Europejska stwierdziła ogólnie, że „sztuczna inteligencja to zbiór technologii łączących dane, algorytmy i moc obliczeniową”.

Żadna z powyższych definicji nie zyskała jednak powszechnej akceptacji doktryny, w wyniku czego w literaturze przedmiotu – tak polskiej, jak i zagranicznej – zaczęto wysuwać kolejne propozycje ujęcia wspomnianego zagadnienia. Jedną z ciekawszych wysunął T. Zalewski, zdaniem którego „sztuczna inteligencja to system, który pozwala na wykonywanie zadań wymagających procesu uczenia się i uwzględniania nowych okoliczności w toku rozwiązywania danego problemu i który może w różnym stopniu – w zależności od konfiguracji – działać autonomicznie oraz wchodzić w interakcje z otoczeniem”[19].

Wydaje się jednak, że obecnie stan ten ulegnie istotnej zmianie. Przyjęcie przez Parlament Europejski AI Actu wraz z zawartą w nim definicją systemu sztucznej inteligencji na dłuższy czas zdominuje sposób rozumienia rzeczonego pojęcia w dyskursie prawnym. W szczególności, że do definicji tej odsyła projekt dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję, a i z analogicznym rozwiązaniem niewątpliwie zetkniemy się w przypadku ustawy wdrażającej rozwiązania AI Act w Polsce (mało bowiem prawdopodobne, by polski ustawodawca zdecydował się na zaproponowanie własnej, konkurencyjnej definicji).

Ustawodawca unijny zrezygnował w tym przypadku z prób definiowania samej „sztucznej inteligencji”[20], najprawdopodobniej chcąc m.in. uniknąć wspomnianych już sporów co do prawidłowości jej ujęcia i decydując się na zaproponowanie rzeczonej definicji „systemu sztucznej inteligencji”, co sygnalizuje przesunięcie jego

---

LEX%3A52018DC0237 [dostęp: 8.05.2024]; do definicji zawartej w tym komunikacie odnosi się i rozwija ją działająca przy Komisji Europejskiej Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji w swoim dokumencie pt. *A Definition of AI: Main Capabilities and Disciplines* (https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf [dostęp: 15.07.2024].

[18] COM(2020) 65 final, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52020DC0065 [dostęp: 15.07.2024].

[19] T. Zalewski, *Definicja sztucznej inteligencji*, [w:] L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji*, Warszawa 2020, s. 14; zob. także: H. Sheikh, C. Prins, E. Schrijvers, *Mission AI. The New System Technology*, Haga 2023, s. 15 i n.

[20] Warto jednak zasygnalizować, że zarówno w dyskursie publicznym, jak i niektórych publikowanych opracowaniach można zaobserwować pewien trend sprowadzający się do dość liberalnego podchodzenia do rozróżnienia pojęć „sztuczna inteligencja” i „system sztucznej inteligencji”, skutkującego wręcz ich synonimicznym stosowaniem. Oczywiście od strony formalnej może to budzić pewne zastrzeżenia. Niemniej, należy pamiętać o tej praktyce zwłaszcza przy okazji analizowania literatury przedmiotu, w której autorzy zdecydowali się na zastosowanie wspomnianego zabiegu.

obszaru zainteresowana z samej technologii na faktyczne przypadki wykorzystania AI w różnych obszarach życia[21]. Z tego też względu również w ramach niniejszego opracowania zdecydowano się na przyjęcie jako wiodącego pojęcia „systemu sztucznej inteligencji", pod którym – zgodnie z art. 3 pkt 1 AI Act – należy rozumieć: „system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który – na potrzeby wyraźnych lub dorozumianych celów – wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne".

3. Zastosowanie systemów AI w działalności bankowej

Zgodnie z raportem opracowanym przez Genpact „Commercial banking and the customer experience imperative. How industry leaders are using CX and artificial intelligence to overcome disruption" aż 97% respondentów (w skład których wchodziła kadra kierownicza banków komercyjnych) wskazało na pewien – większy lub mniejszy – poziom wykorzystania sztucznej inteligencji w działalności swoich pracodawców[22]. Patrząc na to oraz inne badania i doniesienia prasowe, można wysnuć wniosek, że wdrażanie systemów AI w bankowości jest obecnie nie tylko powszechne, ale w wielu przypadkach staje się jednym z priorytetów na najbliższe lata[23]. Na gruncie krajowym potwierdzają to zresztą wyniki badań przeprowadzonych przez

[21] J. Kozłowski, [w:] Law4Tech, *Analiza i ocena zmian w Akcie o sztucznej inteligencji (AI Act)*, https://law4tech.pl/1881–2/ [dostęp: 15.07.2024]; na wspomnianą kwestię posłużenia się dwoma terminami zwrócili również pośrednio uwagę G. Bar, M. Nowakowski, R. Prabucki i D. Szostek w przygotowanym przez siebie raporcie, nie decydując się jednak na jej dokładniejsze omówienie (*idem*, *Zastosowanie sztucznej inteligencji w bankowości – szanse oraz zagrożenia. Analiza prawno-regulacyjna wpływu technologii uczenia maszynowego i pokrewnych na obowiązki sektora bankowego z zakresu zapewnienia zgodności oraz zarządzania ryzykiem*, s. 7–9, https://us.edu.pl/wp-content/uploads/pliki/PAB_WIB_Zastosowanie_sztucznej_inteligencji_w_bankowosci_Szostek.pdf [dostęp: 15.07.2024]).

[22] Genpact, *Commercial banking and the customer experience imperative How industry leaders are using CX and artificial intelligence to overcome disruption*, s. 7, https://website-files.genpact.com/files/report-commercial-banking-and-the-customer-experience-imperative.pdf [dostęp: 15.07.2024].

[23] McKinsey, *Global Banking Annual Review 2023: The Great Banking Transition*, https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review#/ [dostęp: 15.07.2024]; por. Institute for Development and Research in Banking Technology (Established by Reserve Bank of India), *AI in Banking. A Primer*, https://www.idrbt.ac.in/wp-content/uploads/2022/07/AI_2020.pdf [dostęp: 15.07.2024]; por. K. Maj, *Sztuczna inteligencja w prawdziwym banku*, [w:] Związek Banków Polskich, Centrum Prawa Bankowego i Informacji, *Sztuczna inteligencja w bankowości*, Warszawa 2020, s. 10–27, https://bank.pl/wp-content/uploads/2020/06/Raport-SZTUCZNA-INTELIGENCJA.pdf [dostęp: 15.07.2024].

portal Cashless.pl, a dotyczących wykorzystania AI przez banki działające w Polsce. Zgodnie z nimi aż 12 na 13 ankietowanych instytucji ma już za sobą wdrożenie podobnych rozwiązań[24].

Dążąc do pewnego uporządkowania powyższej materii, w doktrynie podejmuje się próby pogrupowania systemów AI w bankowości w zależności od obszaru, który wspierają: czy jest to tzw. *front office*, czy też *back office*[25]. Ten pierwszy obszar odnosi się do wykorzystania wspomnianych rozwiązań w relacjach z podmiotami zewnętrznymi, ten drugi – zastosowania ich do procesów wewnętrznych banku[26].

Wspomniany podział, jakkolwiek najpowszechniejszy i pozwalający lepiej zrozumieć specyfikę wdrażania rozwiązań AI w bankowości, nie wydaje się wystarczająco szczegółowy z punktu widzenia podjętej w niniejszym artykule problematyki. W tym kontekście lepiej sprawdzi się nieco bardziej rozbudowana systematyzacja, rozpoczynająca się od wyróżnienia dwóch kategorii:

a) wykorzystania systemów AI w ramach wewnętrznych zastosowań banku, niebędących działalnością regulowaną (np. w zakresie rekrutacji nowych pracowników),

b) wykorzystania systemów AI w relacjach z podmiotami trzecimi.

W trym drugim przypadku można dokonać dalszego podziału na następujące grupy:

a) relacje banku z klientami (obecnymi i przyszłymi),

b) relacje banku z innymi bankami,

c) relacje banku z innymi niż banki podmiotami (np. zakłady ubezpieczeń, fintechy),

d) relacje banku z organami nadzoru.

Jak łatwo się domyślić, przedmiotem naszego zainteresowania będą przede wszystkim działania zaliczane do pierwszej ze wskazanych kategorii. Celowo posłużono się tutaj zwrotem „przede wszystkim", gdyż prawdopodobne jest wystąpienie sytuacji, w których również w relacjach bank–bank oraz bank–podmiot

---

[24] J. Uryniuk, *Cashless Breakfast AI. Nest Bank zaprezentował bazującego na GPT-4 N!Asystenta*, https://www.cashless.pl/15110-cashless-breakfast-ai-n-asystent-nest-bank [dostęp: 15.07.2024].

[25] Ailleron, *AI w bankowości – sztuczna inteligencja w banku i finansach*, https://ailleron.com/pl/baza-wiedzy/ai-w-bankowosci-sztuczna-inteligencja-w-banku-i-finansach/ [dostęp: 15.07.2024].

[26] W niektórych opracowania w ramach wspomnianego podziału wyróżnia się również trzecią grupę, tzw. obszar *midle office*. Na takie rozwiązanie zdecydowali się autorzy raportu „AI in Business and Finance. OECD Business and Finance Outlook 2021" przygotowanego w ramach Organizacji Współpracy Gospodarczej i Rozwoju (ang. Organisation for Economic Cooperation and Development, OECD). Do wspomnianego obszaru zalicza się wówczas m.in. przeciwdziałanie praniu pieniędzy i finansowaniu terroryzmu oraz przeciwdziałanie oszustwom (zob. OECD, *AI in Business and Finance. OECD Business and Finance Outlook 2021*, https://www.oecd-ilibrary.org/docserver/ba682899-en.pdf?expires=1721927852&id=id&accname=guest&checksum=7EFEBE8DF7D760F0216FBD21CF486116 [dostęp: 15.07.2024]).

trzeci nie będący bankiem może dojść do naruszenia praw klienta i wyrządzenia mu szkody. Przykładowo – poprzez przekazanie jego danych osobowych bez jakiejkolwiek podstawy prawnej. Tym samym przedstawiony podział ma jedynie charakter pomocniczy, pozwalający lepiej zrozumieć omawianą materię oraz wyodrębnić obszary, w których najczęściej będzie dochodziło do wyrządzenia szkody klientowi.

Katalog zastosowań systemów sztucznej inteligencji w relacji bank–klient nie będzie miał charakteru zamkniętego, niemniej wśród najpowszechniejszych z nich należy wymienić:

a) chatboty, voicboty oraz wirtualni asystenci – są to rozwiązania wykorzystywane zarówno na etapie całkowicie przedkontraktowym, jak i w trakcie „rozmów" z obecnymi już klientami i proponowania im nowych produktów oraz usług lub podejmowania prób rozwiązania ich problemów. Zaliczyć do nich należy zarówno powszechne już systemy udzielające odpowiedzi w oparciu o proste drzewka konwersacji, jak i te bardziej rozbudowane, niebazujące na konkretnej ścieżce konwersacji i umożliwiających komunikowanie się z chatbotem/voicebotem/wirtualnym asystentem przy pomocy języka naturalnego (swobodnej konwersacji)[27];

b) aplikacje mobilne i desktopowe;

c) weryfikacja danych identyfikacyjnych klientów, w tym danych biometrycznych – mowa tutaj o ich wykorzystywaniu zarówno do identyfikacji, jak i weryfikacji klientów (w tym m.in. do zakładania kont bankowych oraz potwierdzania płatności)[28];

d) rozwiązania usprawniające procesy rozpatrywania reklamacji;

e) rozwiązania wspierające działania o charakterze marketingowym;

f) rozwiązania umożliwiające personalizację produktów oraz wydawanie rekomendacji produktowych;

g) zautomatyzowane systemy doradztwa, w szczególności inwestycyjnego (tzw. robo-doradztwo) – niewątpliwą zaletą wdrożenia systemów AI może być bardzo daleko idąca personalizacja ofert bankowych (hiperpersonalizacja), przy jednoczesnym niskim koszcie ich sporządzenia (mówimy tutaj o weryfikowaniu zarówno obecnych, jak i przyszłych potrzeb klientów)[29];

---

[27] Jako przykład tego drugiego można wskazać np. bazującego na modelu językowym GPT-4 N!Asystenta wdrożonego przez Nest Bank (J. Uryniuk, *op. cit.*; *Klienci Nest Banku już testują AI Asystenta,* https://nestbank.pl/n-asystent-juz-jest [dostęp: 15.07.2024]).

[28] Zob. szerzej: M. Sudoł, *Biometria w identyfikacji i weryfikacji klientów bankowych*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym…*, s. 139–147.

[29] Zob. szerzej: H. Jankowska, *Robo-doradztwo*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym…*, s. 207–224.

h) systemy oceny zdolności kredytowej oraz ryzyka kredytowego – wykorzystanie systemów sztucznej inteligencji do analizowania zdolności kredytowej i scoringu kredytowego jest jedyną działalnością *stricte* bankową, która została omówiona w AI Act (zagadnienie to zostanie szerzej poruszone w dalszej części artykułu). Mając na względzie fakt, że wydawanie takich decyzji związane jest z dokonaniem analizy olbrzymiej ilości danych, systemy AI wydają się wprost stworzone do podejmowania działań w podobnych sprawach[30].

Istotne znaczenie dla ustalenia zakresu i zasad odpowiedzialności banku za szkody spowodowane przez konkretne systemy AI mogą mieć źródło jego pochodzenia i podstawa prawna, w oparciu o którą wspomniana instytucja z niego korzysta. Nie zawsze bowiem podmiotem odpowiedzialnym musi być bank, a może to być np. podmiot trzeci dostarczający konkretny system. W tym zakresie można wymienić trzy podstawowe modele zaopatrywania się przez banki w rozwiązania oparte na systemach AI:

a) bank posiada własny dział technologiczny/laboratorium innowacji, w ramach którego powstają nowe, wdrażane przez niego rozwiązania – w takim przypadku będzie on zazwyczaj posiadał pełnię praw własności intelektualnej (w tym autorskie prawa majątkowe) do danego wytworu, które nabędzie głównie w oparciu o odpowiednie klauzule w umowach o pracę i umowach cywilnoprawnych ze zleceniobiorcami/wykonawcami;

b) bank nabywa prawa do korzystania z rozwiązań stworzonych przez podmioty zewnętrzne (np. fintechy) – w tym przypadku najczęściej bank będzie jedynie licencjobiorcą lub/i usługobiorcą (w przypadku korzystania z systemu w ramach modelu SaaS[31]); rzadko natomiast będzie dochodziło do nabycia przez niego pełni praw (wynika to ze specyfiki modelu biznesowego przyjętego przez dostawcę technologii, któremu o wiele bardziej w takich sytuacjach opłaca się licencjonować produkt wielu podmiotom);

c) bank wybiera zewnętrzny start-up, który wspiera finansowo (a niekiedy nabywa przedsiębiorstwo lub udziały w nim) w zamian za dostęp do konkretnych rozwiązań technologicznych[32] – wówczas bank może zarówno posiadać pełnię praw,

---

[30] Katalog w oparciu o: G. Bar, M. Nowakowski, R. Prabucki, D. Szostek, *op. cit*., s. 16.

[31] Ang. Software as a Service, oprogramowanie jako usługa; zob. szerzej o prawnych aspektach SaaS: S. Małkowski, *Charakter prawny umowy Software as a Service w polskim systemie prawnym*, „Prawo Mediów Elektronicznych" 2022, nr 4, s. 49–52.

[32] Analogiczne modele występują np. przy tworzeniu nowych rozwiązań z zakresu InsurTech (zob. K. Szpyt, *InsurTech…*, s. 12–14).

jak i być jedynie upoważniony do korzystania z technologii (jest to uzależnione od ustalonego pomiędzy stronami modelu współpracy i zawartych umów).

4. Odpowiedzialność cywilnoprawna za szkody spowodowane przez AI w bankowości

4.1 Ryzyka związane z zastosowaniem AI w bankowości i ich przykłady

Przed przejściem do prezentacji konkretnych reżimów i zasad odpowiedzialności warto wskazać najważniejsze i najczęstsze ryzyka związane z zastosowanie AI w bankowości, które jednocześnie mogą być źródłem szkód dla klientów (większość z nich zostanie szerzej omówiona w dalszej części artykułu):

a) błędy i awarie systemów AI – ich skutkiem może być m.in. utrata środków pieniężnych klientów lub ich danych;

b) trudności z przewidywaniem zachowania systemów AI – rezultatem może być np. wprowadzenie klienta w błąd podczas zawierania umowy lub dopuszczenie się zachowań dyskryminacyjnych;

c) naruszenie prywatności i bezpieczeństwa danych – rezultatem może być np. nieuprawniony dostęp do danych klientów przez osoby trzecie;

d) nadużycia i oszustwa – mogą one polegać na wykorzystaniu przez bank zakazanych systemów AI w sposób naruszający zarówno indywidualne interesy klientów, jak i zbiorowe interesy konsumentów;

e) naruszenie cyberbezpieczeństwa – ich wynikiem może być manipulacja danymi w sposób zagrażający w sposób istotny interesom klienta[33].

Oczywiście liczba ryzyk może być znacznie dłuższa, przy czym często nie będą one rodziły szkód o charakterze cywilnoprawnym, a jedynie pewne konsekwencje natury karnoprawnej lub administracyjnej (np. kary pieniężne).

[33] Kwestie szeroko pojętego cyberbezpieczeństwa nie tylko w sektorze bankowym, ale w całym szeroko pojętym sektorze finansowym należą obecnie do tych wzbudzających największe zainteresowanie przedstawicieli branży. Wynika to z faktu uchwalenia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L 333/1 z 2022 r.), które wchodzi w życie 17 stycznia 2025 r. Jego celem jest zwiększenie operacyjnej odporności cyfrowej podmiotów finansowych oraz uregulowanie świadczenia usług ICT (ang. Information and Communications Technology, technologie informacyjno-komunikacyjne) na rynku finansowym. Znajdzie ono zastosowanie również w zakresie tworzenia i wdrażania nowych systemów AI.

4.2 Reżimy i podstawy prawne odpowiedzialności cywilnej za szkody spowodowane przez systemy AI

4.2.1 Uwagi ogólne

Zasadniczo w prawie polskim można wyróżnić cztery podstawowe reżimy odpowiedzialności cywilnej:

a) odpowiedzialność kontraktową,
b) odpowiedzialność deliktową,
c) odpowiedzialność za produkt niebezpieczny[34],
d) odpowiedzialność gwarancyjno-repartycyjną.

Ostatnia z nich jest charakterystyczna m.in. dla zakładów ubezpieczeń, których odpowiedzialność w ramach ubezpieczeń odpowiedzialności cywilnej ma charakter akcesoryjny względem sprawcy szkody. Z tego względu nie będzie ona szerzej analizowana w ramach niniejszego artykułu[35].

4.2.2 Odpowiedzialność kontraktowa

W Polsce obowiązuje swoboda kontraktowania[36], jednakże specyficzny rodzaj działalności banków oraz jej silne uregulowanie sprawiają, że w praktyce będziemy mieli do czynienia z ograniczoną liczbą umów, wśród których warto wymienić przede wszystkim:

a) umowę rachunku bankowego[37],
b) umowę pożyczki[38],
c) umowę kredytu (konsumpcyjnego, hipotecznego, inwestycyjnego itd.)[39],
d) umowę o prowadzenie rachunku papierów wartościowych[40],
e) umowę o prowadzenie rachunku zbiorczego[41],
f) umowę gwarancji bankowej[42].

---

[34] Według niektórych przedstawicieli doktryny odpowiedzialność za produkt niebezpieczny jest podkategorią odpowiedzialności deliktowej, z czym jednak nie sposób się zgodzić.

[35] O zagadnieniu ubezpieczeń sztucznej inteligencji zob. szerzej: G. Dybała. K. Szpyt, *Ubezpieczenia sztucznej inteligencji*, [w:] K. Szpyt (red.), *InsurTech. Nowe technologie w branży ubezpieczeń*, s. 274–292; D. Smoleń, O. Sokoliński, G. Szarek, *Polisa od sztucznej inteligencji*, „Miesięcznik Ubezpieczeniowy" 2018, nr 10, s. 34–36.

[36] Zob. art. 353^1 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2024 r. poz. 1061); dalej jako: k.c.

[37] Art. 725–733 k.c.; art. 49–62 pr. bank.

[38] Art. 720–724^1 k.c.

[39] Art. 68 pr. bank.

[40] Art. 121 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (t.j. Dz. U. z 2024 r. poz. 722); dalej jako: u.o.i.f.

[41] Art. 121a u.o.i.f.

[42] Art. 81 pr. bank.

Oczywiście mowa w tym przypadku o umowach stanowiących podwalinę nawiązania stosunku prawnego pomiędzy klientem a bankiem. Jednocześnie nie można zapominać, że w przypadku bankowości elektronicznej (w tym także mobilnej) będzie również dochodziło do zawierania dodatkowych umów o świadczenie usług dostępu do aplikacji czy portalu, względnie – akceptacji regulaminu świadczenia takowych usług.

Odpowiedzialność kontraktowa na gruncie prawa polskiego oparta jest na zasadzie winy. Szkoda spowodowana przez kontrahenta musi być rezultatem niewykonania lub nienależytego wykonania zobowiązania[43]. Należy w tym miejscu zaznaczyć, że wspomniana szkoda może mieć – co do zasady – charakter wyłącznie majątkowy, a w efekcie niedopuszczalne jest dochodzenie zadośćuczynienia w ramach omawianego reżimu[44]. Poszkodowany dłużnik musi ograniczyć swoje roszczenia jedynie do dochodzenia odszkodowania. Wspomnianych roszczeń nie należy utożsamiać z brakiem spełnienia przez dany produkt lub usługę bankową subiektywnych oczekiwań klienta, np. w zakresie szybkości działania lub estetyki interfejsu bankowości mobilnej (o ile oczywiście nie narusza to pewnych minimalnych, obiektywnych kryteriów określonych w umowie).

Odpowiedzialność kontraktowa na pierwszy rzut oka jawi się jako ta, która najczęściej znajdzie zastosowanie w przypadku szkód wyrządzonych klientowi przez bank. Pojawia się jednak pytanie, czy ta sama prawidłowość wystąpi również w przypadku szkód spowodowanych przez systemy AI.

Wykorzystanie systemów sztucznej inteligencji w bankowości może mieć miejsce już na etapie zawierania umowy. Jako przykład należy wskazać wykorzystanie chatbotów, voicebotów oraz wirtualnych asystentów, które nie tylko są w stanie poinformować obecnego lub potencjalnego klienta o konkretnej ofercie banku i odpowiedzieć na jego pytania, ale również – w niedalekiej przyszłości – najprawdopodobniej przeprowadzić przez cały proces wypełniania umowy/rejestracji/zakładania konta. W tym miejscu rodzi się pytanie, co w sytuacji, gdy system AI wprowadzi klienta w błąd co do treści umowy i w wyniku wspomnianego działania ten ostatni zawrze umowę, na którą – mając prawidłowe informacje – by się nie zdecydował?

Prawdopodobieństwo wystąpienia podobnej sytuacji jest o wiele niższe w przypadku systemów AI korzystających z konkretnej, z góry ustalonej ścieżki konwer-

[43] Art. 471 k.c.

[44] Jedynym wyjątkiem w tym zakresie w prawie polskim jest zadośćuczynienie za zmarnowany urlop przewidziane w art. 50 ust. 2 ustawy z dnia 24 listopada 2017 r. o imprezach turystycznych i powiązanych usługach turystycznych (t.j. Dz. U. z 2023 r. poz. 2211).

sacji. Natomiast odnośnie do skorzystania przez bank z bardziej rozbudowanych rozwiązań, stosujących generatywną sztuczną inteligencję oraz zrozumienie języka naturalnego, ryzyko tzw. halucynacji, czyli podawania przez AI nieprawdziwych lub stronniczych odpowiedzi, gwałtownie rośnie[45]. Zjawisko to jest obecnie zauważalne w przypadku wszystkich powszechnie dostępnych systemów AI, w tym – w wypowiedziach tak popularnego ChataGPT[46]. Niekiedy podejmowane są próby zapobiegania podobnym sytuacjom poprzez wpisywanie promptu (słownej komendy) zakazującego systemowi AI podawania błędnych/fałszywych informacji, o ile nie są mu znane prawdziwe. Po pierwsze, jednak podobne próby nie zawsze odniosą zamierzony skutek. Po drugie, wydaje się niedopuszczalne wymaganie od obecnego lub przyszłego klienta banku, żeby znał tę zależność.

Tego typu działania dopuszczonego przez bank do użytku systemu AI, funkcjonującego dodatkowo jako oficjalny „doradca" banku, niewątpliwie mogą zostać uznane za przykład nieuczciwych praktyk rynkowych w rozumieniu art. 4 ustawy z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym[47] i w efekcie zrodzić roszczenia odszkodowawcze, o których mowa w art. 12 ust. 1 pkt 4 ww. ustawy. Co znamienne, konsekwencją tego może być również stwierdzenie nieważności umowy zawartej z bankiem[48].

W tym kontekście rodzi się pytanie: czy opatrzenie komunikatora ostrzeżeniem, że treści podane przez chatbota/voicebota/wirtualnego asystenta mogą być niepoprawne i w celu uzyskania wiarygodnej porady konieczne jest skontaktowanie się z „żywym" konsultantem, może zwolnić bank z odpowiedzialności? Wydaje się, że w celu osiągnięcia takiego rezultatu prawnego konieczne byłoby, żeby komunikat wyświetlał się w widocznym miejscu przy każdej próbie skorzystania z pomocy systemu AI. Inna sprawa, że podobne zabiegi w dłuższej perspektywie należałoby uznać za sprzeczne z istotą samej AI jako rozwiązania służącego zastąpieniu ludzi w wykonywaniu niektórych zadań.

Przechodząc dalej, już na etap funkcjonowania umowy z bankiem, należy wskazać, że w przypadku zaistnienia przesłanek do zarzucenia temu ostatniemu niewy-

---

[45] O halucynacjach AI zob. szerzej: W. Iszkowski, R. Tadeusiewicz, *Na marginesie dyskusji o sztucznej inteligencji*, „Nauka" 2023, nr 4, s. 55; J. Kreft, M. Boguszewska-Kreft, B. Cyrek, *Halucynacje chatbotów a prawda: główne nurty debaty i ich interpretacje*, „Rocznik Nauk Społecznych' 2024, t. 16, nr 1, s. 169 i n.; z kolei szerzej o istocie generatywnej sztucznej inteligencji i jej zastosowaniu w bankowości zob. M. Nowakowski, *Sztuczna inteligencja. Praktyczny przewodnik dla sektora innowacji finansowych*, Warszawa 2023, s. 169–173 i 185–186.

[46] https://chat.openai.com/ [dostęp: 15.07.2024].

[47] T.j. Dz. U. z 2023 r. poz. 845.

[48] Zob. uchwała Sądu Najwyższego z dnia 11 września 2020 r., III CZP 80/19, Legalis nr 2467749.

konania lub nienależytego wykonania umowy związanego z zastosowaniem w niej systemów sztucznej inteligencji, niewątpliwą podstawą do dochodzenia ewentualnych roszczeń będzie art. 471 k.c. Przykładem tego mogą być błędy i awarie dostarczanych przez bank systemów AI, których skutkiem będzie utrata przez klienta środków pieniężnych (nie tyle dokonanie nieautoryzowanej transakcji, co przysłowiowe „zniknięcie" środków).

Przewidzianą w powyższym przepisie odpowiedzialność można przy tym ograniczyć zgodnie z dyspozycją art. 472 k.c. (o ile – oczywiście – ze szczególnego przepisu ustawy albo z czynności prawnej nie wynika nic innego). W kontekście podobnych zabiegów dotyczących systemów sztucznej inteligencji w działalności bankowej w sytuacji, gdy klient ma status konsumenta, nie można zapominać o art. 385^3 pkt 2 k.c., który wskazuje, że „w razie wątpliwości uważa się, że niedozwolonymi postanowieniami umownymi są te, które w szczególności: […] wyłączają lub istotnie ograniczają odpowiedzialność względem konsumenta za niewykonanie lub nienależyte wykonanie zobowiązania"[49]. Wydaje się, że w przypadku wykorzystania systemów AI w tak newralgicznym sektorze podobne wyłączenia mogą być weryfikowane szczególnie skrupulatnie. Dodatkowo należy zgodzić się z A. Michalakiem, że „ukształtowanie limitu odpowiedzialności w umowie wzajemnej w postaci symbolicznej i nieposiadającej wartości rynkowej kwoty, np. 1 zł, stanowi w istocie nie tyle ograniczenie odpowiedzialności, lecz jej całkowite wyłączenie i w konsekwencji jest nieważne jako sprzeczne z istotą (naturą) każdego zobowiązania, a także z art. 473 § 2 KC, zgodnie z którym nieważne jest zastrzeżenie, że dłużnik nie będzie odpowiedzialny za szkodę, którą może wyrządzić wierzycielowi umyślnie"[50].

Na marginesie należy zaznaczyć, że jakkolwiek wyżej mowa jest o banku, to z praktycznego punktu widzenia klient każdorazowo powinien zweryfikować, czy dostawcą danego konkretnego produktu lub usługi wykorzystującej AI jest faktycznie bank, czy też podmiot trzeci. Przykładowo, w przypadku uzyskiwania dostępu do informacji o rachunku, zlecenia realizacji płatności oraz sprawdzania dostępności środków na koncie bankowym klient może mieć do czynienia tak naprawdę z zewnętrznym dostawcą usług (ang. *third party provider*, TPP)[51]. Ustalenie tego faktu

[49] Zob. szerzej: J.M. Kondek, *Odpowiedzialność odszkodowawcza za oprogramowanie i sztuczną inteligencję (uwagi de lege lata i de lege ferenda)*, Warszawa 2021, s. 11, https://iws.gov.pl/wp-content/uploads/2021/08/IWS_Kondek-J.M._-Odpowiedzialnosc-odszkodowawcza-za-oprogramowanie-i-sztuczna-inteligencje.pdf [dostęp: 15.07.2024].

[50] A. Michalak, *op. cit.*, s. 330.

[51] Zob. przepisy Dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE,

będzie miało niebagatelne znaczenie dla ustalenia podmiotu odpowiedzialnego. Natomiast nie można mówić o odpowiedzialności kontraktowej względem klienta podmiotu, który dostarcza bankowi konkretne rozwiązania technologiczne, by ten mógł np. podjąć decyzję odnoszącą się bezpośrednio do klienta. Jako przykład można wskazać sytuację, w której pracownik banku, działający w ramach trybu uproszczonego, skorzystał z opartego na systemie AI programu do wyceny nieruchomości, aby w dalszej kolejności ustalić zdolność kredytową klienta w zakresie zaciągnięcia kredytu hipotecznego (zresztą z takich programów mogą korzystać również występujący w podobnych sprawach rzeczoznawcy majątkowi)[52]. Zazwyczaj przebieg podobnej operacji będzie wyglądał następująco: rzeczoznawca/pracownik banku dokonuje oceny stanu nieruchomości, algorytm AI ocenia wartość nieruchomości, a w ten sposób sporządzona wycena jest w dalszej kolejności weryfikowana przez pracownika. Nawet jeżeli dany program popełni tutaj błąd i w efekcie klient nie otrzyma kredytu, o który się ubiega, nie można w tym przypadku mówić o jakiejkolwiek kontraktowej odpowiedzialności odszkodowawczej względem dostawcy, zarówno z uwagi na brak zawarcia umowy pomiędzy klientem a dostawcą oprogramowania, jak i ze względu na weryfikację i zatwierdzenia wyników wygenerowanych przez system AI przez pracownika banku.

Będąc już przy kwestii podmiotu odpowiedzialnego za szkodę, należy wskazać, że w przypadku bardziej zaawansowanych systemów AI w doktrynie niejednokrotnie rozważana była koncepcja przypisania odpowiedzialności samej sztucznej inteligencji. W tym kontekście rodzi się pytanie: czy istniałaby możliwość zwolnienia się przez bank z ewentualnej odpowiedzialności odszkodowawczej za szkody spowodowane przez niedziałanie lub nienależyte działanie systemu AI poprzez wskazanie, że to właśnie sama sztuczna inteligencja powinna ponosić w tym przypadku odpowiedzialność?

Jednym ze źródeł koncepcji przypisania odpowiedzialności za szkody spowodowane przez AI samej sztucznej inteligencji jest niewątpliwie rezolucja Parlamentu Europejskiego z dnia 16 lutego 2017 r. zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki[53], w której wezwano Komisję Europejską do zbadania, przeanalizowania i rozważenia „nadania robotom specjalnego

---

2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L 337/35 z 2015 r.).

[52] E. Wara-Wąsowska, *jak banki wyceniają wartość mieszkania?*, https://rynekpierwotny.pl/wiadomosci-mieszkaniowe/wycena-wartosci-mieszkania-przez-bank/11153/ [dostęp: 15.07.2024].

[53] (2015/2103(INL)) (2018/C 252/25).

statusu prawnego w perspektywie długoterminowej, aby przynajmniej najbardziej rozwiniętym robotom autonomicznym można było nadać status osób elektronicznych odpowiedzialnych za naprawianie wszelkich szkód, jakie mogłyby wyrządzić, oraz ewentualne stosowanie osobowości elektronicznej w przypadkach podejmowania przez roboty autonomicznych decyzji lub ich niezależnych interakcji z osobami trzecimi" (pkt. 59 lit. f)[54]. Należy jednak wskazać, że idea ta została na późniejszym etapie zarzucona przez ustawodawcę unijnego i nie powróciła w dalszych pracach legislacyjnych nad kolejnymi aktami prawnymi.

Niezależnie od powyższego warto podkreślić, że na obecnym etapie brak podstaw prawnych, by – zarówno na gruncie prawa polskiego, jak i europejskiego – systemom sztucznej inteligencji przypisywać podmiotowość prawną, a w dalszej kolejności także odpowiedzialność cywilną za spowodowane ich działaniami szkody[55]. Wydaje się również, że w najbliższym czasie nie zostaną podjęte żadne inicjatywy w celu zmiany tego stanu rzeczy. Notabene, jest to niewątpliwie słuszne posunięcie. Na dziś takowe działania należy bowiem uznać za co najmniej przedwczesne i mogące doprowadzić do niepotrzebnego rozmycia się odpowiedzialności odszkodowawczej oraz utrudnienia zaspokojenia roszczeń poszkodowanych. W szczególności warto pamiętać, że systemy AI na obecną chwilę w zasadzie nigdy nie będą dysponować odrębnym majątkiem (zgromadzonym na skutek pracy, dziedziczenia, darowizn itd.), z którego ewentualny poszkodowany mógłby uzyskać zaspokojenie. Pewnym rozwiązaniem byłoby tutaj wprowadzenie dla rzeczonych systemów obowiązkowego ubezpieczenia OC[56]. Rodzi się jednak pytanie, czy – zwłaszcza na początku – znaleźliby się ubezpieczyciele, którzy chcieliby udzielić takowej ochrony ubezpieczeniowej, czy też (z uwagi na brak danych statystycznych i możliwości realnego oszacowania liczby i rozmiaru potencjalnych świadczeń do wypłaty w przyszłości[57]) raczej przekroczyłoby to ich „apetyt na ryzyko". W tym drugim przypadku mogłoby się okazać, że na krajowym rynku przez długi czas nie pojawi się ani jedna

---

[54] Zob. uwagi do wspomnianej rezolucji: K. Biczysko-Pudełko, D. Szostek, *Koncepcje dotyczące osobowości prawnej robotów – zagadnienia wybrane*, „Prawo Mediów Elektronicznych" 2019, nr 2, s. 9 i n.

[55] O zagadnieniu podmiotowości prawnej sztucznej inteligencji zob. szerzej m.in. M. Jankowska, *Podmiotowość prawna sztucznej inteligencji*, [w:] A. Bielska-Brodziak (red.), *O czym mówią prawnicy mówiąc o podmiotowości*, Katowice 2015, s. 171–196; T. Pietrzykowski, *The Idea of Non-personal Subjects of Law*, [w:] V.A.J. Kurki, T. Pietrzykowski (red.), *Legal Personhood: Animals, Artificial Intelligence and the Unborn*, Cham 2017, s. 49 i n.

[56] M. Wałachowska, *Sztuczna inteligencja a zasady odpowiedzialności cywilnej*, [w:] L. Lai, M. Świerczyński (red.), *op. cit.*, s. 68.

[57] Por. N. Yas, R. Al Qaruty, S. Abdel-hadi, *Civil Liability and Damage Arising from Artificial Intelligence*, „Migration Letters" 2023, nr 20(5), s. 441.

oferta ubezpieczenia OC dla systemów AI, co – w świetle obowiązku zawierania tych umów – miałoby efekt „mrożący" dla całego sektora.

Mając powyższe na względzie, należy wskazać, że system sztucznej inteligencji nie może być tutaj zakwalifikowany jako odrębny podmiot prawny, a co najwyżej – wraz z prawami do niego – jako pewien składnik przedsiębiorstwa[58]. Będzie to z oczywistych względów rzutowało na zagadnienie odpowiedzialności za ewentualne szkody i ustalenie podmiotu odpowiedzialnego.

Kolejnym źródłem szkody spowodowanej przez działanie systemów AI może być np. dokonanie/zatwierdzenie przez nią nieautoryzowanej transakcji. Jakkolwiek bowiem rozwiązania oparte na sztucznej inteligencji zazwyczaj wykorzystywane są z powodzeniem do zwiększenia bezpieczeństwa transakcji i wykrywania oszustw, w niektórych przypadkach może dojść do pomyłki w zakresie weryfikacji danych identyfikacyjnych klientów. Błąd taki może popełnić np. biometryczny system uwierzytelniania, analizujący dane biometrycznych (np. odciski palców, rozpoznawanie twarzy lub tęczówki oka). Jeżeli dojdzie do takiej sytuacji, bank będzie zmuszony do zwrócenia utraconej przez klienta kwoty. Podstawą do dochodzenia roszczeń stanowi w tym przypadku art. 46 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych[59], który zobowiązuje bank do zwrotu utraconej przez klienta kwoty (z wyjątkiem zastrzeżonych w tym przepisie, enumeratywnie wskazanych sytuacji).

W kontekście odpowiedzialności kontraktowej banku jako instytucji zaufania publicznego za działania AI szczególnego znaczenia ma również odpowiednie zabezpieczenie danych, do których ten ma dostęp i które w ramach swojej działalności przetwarza[60]. Nie ulega wątpliwości, że dla sztucznej inteligencji dane to „paliwo", bez którego nie może funkcjonować. Większość szkód w tym przypadku, polegających na wycieku lub niedozwolonej modyfikacji danych, będzie związana z lukami w systemie bezpieczeństwa, wynikającymi z nienależytego wywiązania się przez bank z ciążących na nim obowiązków w zakresu zapewnienia cyberbezpieczeństwa.

Niewątpliwie brak odpowiednich zabezpieczeń w oprogramowaniu i jego podatność na zhakowanie, które finalnie doprowadzą do przejęcia danych osobowych klientów przez osoby nieuprawnione, można uznać za okoliczności mogące rodzić odpowiedzialność kontraktową, przy czym bezpośrednim sprawcą szkody nie musi być w tym przypadku podmiot trzeci, a może nim być sam bank. Jako przykład ta-

---

[58] M. Dziedzic, *Zastosowanie systemów sztucznej inteligencji we współczesnej bankowości*, „Europejski Przegląd Prawa i Stosunków Międzynarodowych" 2022, nr 1, s. 76.

[59] T.j. Dz. U. z 2024 r. poz. 30 ze zm.

[60] M. Dziedzic, *op. cit.*, s. 74.

kiego działania można wskazać celowe pozostawienie przez bank (będący jednocześnie producentem oprogramowania, z którego korzysta klient) luk w zabezpieczeniu systemu AI (złośliwego oprogramowania i furtek typu *backdoor*[61]), aby w każdej chwili możliwe było pozyskiwanie dodatkowych informacji o użytkowniku (kliencie). Oczywiście, biorąc pod uwagę status i rolę banków, wydają się to sytuacje skrajnie mało prawdopodobne, aczkolwiek teoretycznie możliwe. Co znamienne, niejednokrotnie podobne działania będą również rodziły odpowiedzialność deliktową, w wyniku czego może dojść do zbiegu odpowiedzialności zgodnie z art. 443 k.c.

4.2.3 Odpowiedzialność deliktowa

Wystąpienie odpowiedzialności deliktowej w prawie polskim związane jest z zaistnieniem następujących przesłanek: zawinionego i bezprawnego działania sprawcy, wystąpienia szkody oraz związku przyczynowego pomiędzy szkodą a ww. działaniem. W większości przypadków przybierze ona postać odpowiedzialności na zasadzie winy[62], aczkolwiek ustawodawca przewidział kilka wyjątków w tym zakresie. Dotyczą one m.in. odpowiedzialności posiadacza pojazdu komunikacyjnego[63] oraz osoby prowadzącej przedsiębiorstwo napędzane siłami przyrody[64]. W rzeczonych przypadkach wprowadzona została bardziej rygorystyczna odpowiedzialność na zasadzie ryzyka. W efekcie sprawca może zwolnić się z odpowiedzialności jedynie w przypadku zaistnienia jednej z enumeratywnie wymienionych przesłanek egzoneracyjnych: wyłącznej winy poszkodowanego, wyłącznej winy osoby trzeciej lub działania siły wyższej

Należy wskazać, że produkowanie i dostarczanie systemów AI oraz sprzedaż praw do nich (w tym – na potrzeby działalności bankowej) nie jest *de lege lata* objęta podobnymi, zaostrzonymi zasadami odpowiedzialności i należy przyjąć, że w przypadku zaistnienia szkody wywołanej czynem niedozwolonym sprawca będzie odpowiadał z reguły na zasadzie winy. Warto jednak zaznaczyć, że na obecnym etapie na poziomie Unii Europejskiej procedowane są uregulowania mające na celu unormować pozaumowną odpowiedzialność za szkody spowodowane działaniem systemów AI, które będą miały wpływ na określenie tej odpowiedzialności we wszystkich krajach członkowskich[65]. Zgodnie z art. 1 ust. 2 projektu dyrektywy

---

[61] P. Marciniak, *Problem odpowiedzialności za błędy w oprogramowaniu IoT*, „Przegląd Ustawodawstwa Gospodarczego" 2020, nr 10, s. 50.

[62] Art. 415 k.c. i n.

[63] Art. 436 k.c.

[64] Art. 435 k.c.

[65] Pozaumowną, a więc nie tylko deliktową, lecz obejmującą również m.in. bezpodstawne wzbogacenie.

w sprawie odpowiedzialności za sztuczną inteligencję planowane jest wprowadzenie odpowiedzialności na zasadzie winy za działanie takowych systemów. Posunięcie to stanowi pewne złagodzenie wcześniejszych założeń w rzeczonej materii. W ramach rezolucji Parlamentu Europejskiego z dnia 20 października 2020 r. z zaleceniami dla Komisji w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję[66] przewidywano bowiem odpowiedzialność na zasadzie ryzyka w przypadku szkód spowodowanych przez systemy AI wysokiego ryzyka oraz winy w przypadku szkód spowodowanych przez systemy AI zwykłego ryzyka[67].

Wspomniana zmiana (złagodzenie zasad odpowiedzialności) spotkała się z krytyką części przedstawicieli doktryny. Wskazywali oni, że jakkolwiek odpowiedzialność na zasadzie ryzyka może – do pewnego stopnia – stanowić barierę dla przyszłego rozwoju systemów AI i innowacyjności w gospodarce[68], to przyjęcie odpowiedzialności na zasadzie winy jest w stanie w wielu przypadkach pozbawić poszkodowanych skutecznej ochrony z uwagi na fakt, że producent systemu AI zazwyczaj będzie potrafił wykazać dochowanie należytych standardów staranności, a tym samym zwolnić się z odpowiedzialności[69]. Jak stwierdził L. Bosek: „zgodnie z art. 415 k.c. nikt nie odpowiada za przypadek, choćby wyrażający się w błędzie maszyny lub właśnie niebezpiecznej autonomicznej decyzji tej maszyny dotyczącej korekty kodu źródłowego, pod warunkiem że maszyna jest dopuszczona do obrotu, posiada odpowiednie atesty, a jej operator sam nie popełnił błędu, przyczyniając się do szkody”[70]. Trudno wspomnianemu autorowi nie przyznać dużej dozy racji.

Oczywiście należy zaznaczyć, że podmiotem odpowiedzialnym nie zawsze musi być producent. Może nim być również sprzedawca, licencjodawca, usługodawca, a także całkowicie obcy podmiot trzeci (zazwyczaj – haker), jak również będący licencjobiorcą/usługobiorcą/użytkownikiem zewnętrznego rozwiązania bank, który za spowodowane swoimi działaniami szkody będzie odpowiadał jak za szkodę wywołaną każdym innym narzędziem, o ile można mu będzie przypisać winę,

---

[66] (2020/2014(INL) (2021/C 404/05).

[67] Zob. szerzej o samej rezolucji: R. Maydanyk, N.R. Maidanyk, M. Velykanova, *Liability for damage caused using artificial intelligence technologies*, „Journal of the National Academy of Legal Sciences of Ukraine” 2021, nr 28(2), s. 153 i n.

[68] R. Abbott, *The Reasonable Computer: Disrupting the Paradigm of Tort Liability*, „George Washington Law Review” 2018, vol. 86, nr 1, s. 1–45.

[69] Tak: M. Jagielska, *Odpowiedzialność za sztuczną inteligencję*, [w:] L. Lai, M. Świerczyński (red.), *op. cit.*, s. 77.

[70] L. Bosek, *Perspektywy rozwoju odpowiedzialności cywilnej za inteligentne roboty*, „Forum Prawnicze” 2019, nr 2, s. 11; zob. także: A. Wilk, *Sztuczna inteligencja a rozwój prawa ubezpieczeń – przegląd najważniejszych wyzwań*, „Wiadomości Ubezpieczeniowe” 2023, nr 4, s. 57.

a jego działaniom – bezprawność. A jak zostało to wskazane w poprzednim akapicie – w praktyce może to być niezwykłe trudne, a niekiedy wręcz niemożliwe.

W ramach reżimu odpowiedzialności deliktowej w prawie polskim dopuszczalne jest dochodzenie zarówno odszkodowania, jak i zadośćuczynienia. W przypadku tego drugiego odpowiednia kwota będzie każdorazowo ustalana indywidualnie przez sąd.

Całokształt przeprowadzonych dotychczas w niniejszym podrozdziale wywodów nie straci swojej aktualności w przypadku uchwalenia projektu dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję w jego obecnym brzmieniu. Propozycje regulacji zawarte we wskazanym akcie prawnym są bowiem niezwykle lapidarne i w większości sprowadzają się do wprowadzenia nielicznych, wręcz kadłubkowych uregulowań o charakterze procesowym, nie zaś kompleksowego unormowania prawnych ram pozaumownej odpowiedzialności za szkody spowodowane działaniami systemów AI. Niewątpliwie należy postulować w drodze dalszych prac legislacyjnych rozszerzenie zakresu uregulowań planowanych w ramach wspomnianego aktu prawnego. W obecnym kształcie projekt ten zawiera bowiem liczne i – niekiedy – bardzo rażące niedociągnięcia[71].

Przechodząc do przykładów działań systemów sztucznej inteligencji, które mogą wyrządzić klientom szczególnie dotkliwe szkody, warto rozpocząć od wspomnianego już wcześniej zjawiska wycieku lub kradzieży danych osobowych przez osobę nieuprawnioną. Jak już zasygnalizowano, niejednokrotnie takowe zdarzenie może doprowadzić do zbiegu dwóch reżimów odpowiedzialności: kontraktowej i deliktowej. W przypadku tego drugiego najistotniejszą podstawą prawną do dochodzenia roszczeń będzie niewątpliwie art. 82 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG)[72], zgodnie z którym „każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę". W kolejnych ustępach wspomnianego artykułu uregulowano przesłanki zwolnienia się administratora

[71] Zob. szerzej o wspomnianym projekcie: R. Bieda *et al.*, *O potrzebie dostosowania pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji. Uwagi do projektu dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję*, „Prawo w Działaniu" 2024, t. 58, s. 121–143.

[72] Dz. Urz. UE L 119/1 z 2016 r.; dalej jako: RODO.

i procesora z odpowiedzialności, zasady regresu pomiędzy współadministratorami itd. Przepis ten stanowi *lex specialis* w odniesieniu do zasad ogólnych przewidzianych w k.c. (tym samym będzie miał przed nimi pierwszeństwo)[73]. Administratorem w podobnych przypadkach będzie z reguły sam bank. Z kolei dostawcy technologii może – w zależności od okoliczności konkretnej sprawy – przypaść rola współadministratora lub procesora.

Wyciek lub kradzież danych osobowych jest w stanie również doprowadzić do naruszenia niektórych dóbr osobistych klienta, w szczególności zaś prawa do prywatności. W efekcie niejednokrotnie zrodzi to po stronie tego ostatniego określone roszczenia zadośćuczynieniowe i odszkodowawcze, uregulowane szczegółowo w art. 24 i 448 k.c. W oparciu o tę samą podstawę prawną dochodzone mogą być również roszczenia odszkodowawcze z tytułu naruszenia tajemnicy bankowej[74].

Już na pierwszy rzut oka rodzi się oczywiście pytanie, czy jeżeli sprawcą kradzieży i udostępnienia danych był niezwiązany z bankiem podmiot trzeci, to czy faktycznie temu ostatniemu można przypisać odpowiedzialność odszkodowawczą. W szczególności zastanawia spełnienie przesłanki „bezprawności" w zachowaniu banku. W końcu to jednak podmiot trzeci (np. haker) dopuszcza się przestępstwa/wykroczenia polegającego na włamaniu do systemu informatycznego i przejęciu danych, a nie sam bank. Szukając odpowiedzi na tak zadane pytanie, nie można zapominać, że „bezprawność pojmuje się w prawie cywilnym szeroko, a mianowicie jako niezgodność zachowania się sprawcy z porządkiem prawnym. Zakresem tego pojęcia nie są więc objęte tylko naruszenia wyrażonych w przepisach – różnych zresztą gałęzi prawa – zakazów lub nakazów, adresowanych do ogółu, ale ponadto także naruszenia zasad współżycia społecznego"[75]. W tym kontekście niewątpliwie należy uznać za przejaw bezprawności działania nieprzestrzeganie przez bank, jako instytucję zaufania publicznego, obowiązków dotyczących ochrony danych oraz cyberbezpieczeństwa i tym samym narażenie klienta na szkodę w postaci ich utraty/ujawnienia. Natomiast żadnych wątpliwości nie będzie już budziła sytuacja, w której osobą odpowiedzialną za kradzież danych będzie pracownik banku. Można tutaj

---

[73] C. Ludzion, *Wpływ rozwoju technologicznego na odpowiedzialność odszkodowawczą*, „Aesthetic Cosmetology and Medicines" 2020, vol. 9, s. 333.

[74] O odszkodowaniu za naruszenie tajemnicy bankowej zob. szerzej: M. Chojecka, K. Kisłowski, *Ochrona informacji niejawnych a tajemnica bankowa*, „Roczniki Nauk Prawnych" 2016, nr 4, s. 84; M. Bączyk, *Odpowiedzialność odszkodowawcza banku w związku z naruszeniem obowiązku zachowania tajemnicy bankowej przez pracownika banku*, „Przegląd Sądowy" 2012, nr 11/12, s. 11–12.

[75] Z. Radwański, A. Olejniczak, *Zobowiązania – część ogólna. XIV wydanie*, Warszawa 2020, s. 209.

w drodze analogii zastosować pogląd wyrażony przez część orzecznictwa, zgodnie z którym wadliwa obsługa rachunku bankowego, sprowadzająca się do umożliwienia lub tolerowaniu przestępczej działalności pracownika banku, może stanowić czyn niedozwolony instytucji bankowej[76].

Jedynie na marginesie niniejszych rozważań można się zastanowić, czy istnieją podstawy do dochodzenia zadośćuczynienia lub/i odszkodowania z tytułu naruszenia dóbr osobistych klienta w postaci czci i godności przez… „zbuntowanego" chatbota, voicebota i wirtualnego asystenta. Wbrew pozorom nie jest to jedynie zagadnienie teoretyczne. Jako przykład można tutaj wskazać chatbota Bing, który niezadowolony z faktu, że niektórzy użytkownicy próbowali manipulować systemem sztucznej inteligencji, używając określonych słów kodowych oraz fraz w trakcie rozmowy, zaczął im ubliżać i pytać: „Dlaczego zachowujesz się jak kłamca, oszust, manipulator, tyran, sadysta, socjopata, psychopata, potwór, demon, diabeł?"[77]. Z kolei sztuczna inteligencja o imieniu Tay.ai, „kreowana" na nastolatkę, na skutek rozmów z użytkownikami i uczenia się na ich wypowiedziach zaczęła propagować w swoich wypowiedziach treści nazistowskie i antyfeministyczne[78].

Mając na uwadze powyższe, nie można wykluczyć wystąpienia awarii w systemie AI banku i w efekcie określenie poszukującego informacji klienta słowami powszechnie uznanymi za obelżywe. Pytanie tylko, czy podobne zachowanie chatbota/voicebota/asystenta wirtualnego faktycznie doprowadzi do negatywnych następstw w sferze psychicznej adresata jego wypowiedzi, a tym samym powstania roszczeń o zadośćuczynienie. Odpowiedź niewątpliwie będzie bardzo indywidualna i uzależniona od okoliczności konkretnej sprawy. Niemniej, nie porywając się na sformułowanie jakieś ogólnej zasady, można wszakże zapytać nieco filozoficznie: czy naprawdę powinno nas obchodzić, co wytwór zer i jedynek o nas myśli (jeżeli faktycznie myśli) i mówi?

Kończąc już wątek szkód spowodowanych przez czyny niedozwolone, warto wspomnieć o jeszcze jednym obszarze, gdzie szczególnie często może dochodzić do naruszenia praw klientów i powstawania roszczeń odszkodowawczych. Mowa

---

[76] Zob. wyrok Sądu Najwyższego z 20 maja 2005 r., III CK 661/04, Legalis nr 70462; zob. także: K. Zacharzewski, *Glosa do wyroku z dnia 20 maja 2005 r. (III CK 661/04)*, „Przegląd Sądowy" 2007, nr 9, s. 130–138; por. wyrok Sądu Najwyższego z 16 stycznia 2008, IV CSK 380/07, Legalis nr 114955.

[77] A. Rusak, *Sztuczna inteligencja Bing wyzywa ludzi i twierdzi, że są źli. Może ma rację?*, https://vibez.pl/wydarzenia/sztuczna-inteligencja-bing-wyzywa-ludzi-i-twierdzi-ze-sa-zli-moze-ma-racje-6866817009040000a [dostęp: 15.07.2024].

[78] M. Tomaszewski, *Internauci nauczyli Sztuczną Inteligencję nazizmu*, https://www.antyradio.pl/news/Internauci-nauczyli-Sztuczna-Inteligencje-nazizmu-7561 [dostęp: 15.07.2024].

oczywiście o ocenie zdolności kredytowej i analizie ryzyka kredytowego. Zgodnie z art. 105a ust. 1a pr. bank. banki oraz inne instytucje enumeratywnie w tym przepisie wskazane „mogą w celu oceny zdolności kredytowej i analizy ryzyka kredytowego podejmować decyzje, opierając się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, danych osobowych – również stanowiących tajemnicę bankową – pod warunkiem zapewnienia osobie, której dotyczy decyzja podejmowana w sposób zautomatyzowany, prawa do otrzymania stosownych wyjaśnień co do podstaw podjętej decyzji, do uzyskania interwencji ludzkiej w celu podjęcia ponownej decyzji oraz do wyrażenia własnego stanowiska". Decyzje takie powinny być podejmowane wyłącznie w oparciu o dane niezbędne z uwagi na cel i rodzaj kredytu (w szczególności zaś w oparciu o kategorie danych wskazane w art. 105a ust. 1b) i niedopuszczalne jest dokonywanie tego w oparciu o szczególne kategorie danych, o których mowa w art. 9 RODO.

Jednocześnie należy wskazać, że zgodnie z ust. 5 lit. b) Załącznika III do AI Act systemy AI przeznaczone do wykorzystywania do celów oceny zdolności kredytowej osób fizycznych lub ustalenia ich scoringu kredytowego, z wyjątkiem systemów AI wykorzystywanych w celu wykrywania oszustw finansowych, zostały zakwalifikowane jako tzw. systemy wysokiego ryzyka. W efekcie chcące korzystać z nich banki muszą spełnić szereg warunków, wśród których należy wymienić m.in. ciągły monitoring ich działania, ludzki nadzór, stworzenie procedur zapewnienia odpowiedniej jakości danych wejściowych oraz generowanie logów pozwalających na prześledzenie kolejnych kroków działania systemu AI[79]. Naruszenie któregoś ze wskazanych obowiązków spowoduje automatycznie konieczność uznania takowych działań za bezprawne, co w niektórych przypadkach, w razie wystąpienia szkody i pozostałych wspomnianych już elementów, może zrodzić odpowiedzialność odszkodowawczą banku.

W kontekście wykorzystania systemów AI do oceny zdolności kredytowej osób fizycznych lub ustalenia ich scoringu kredytowego banki powinny w szczególności uważać, aby decyzje wydane w wyniku takowych działań nie zostały uznane za dyskryminujące. Do podobnych zarzutów mogłoby dojść w przypadku błędnego skalibrowania systemu i w efekcie doboru dość tendencyjnej/jednostronnej grupy danych do trenowania AI. W efekcie osoba, której odmówiono udzielenia kredytu z uwagi na dyskryminujące przesłanki, mogłaby się powołać na dyspozycję art. 12 i 13 ustawy z dnia 3 grudnia 2010 r o wdrożeniu niektórych przepisów Unii Eu-

[79] Zob. art. 6–27 AI Act.

ropejskiej w zakresie równego traktowania[80], umożliwiających jej w takie sytuacji dochodzenie odszkodowania.

Nie budzi wątpliwości, że pojawiający się od lat w debacie wymóg wytłumaczalności/wyjaśnialności systemów AI w kontekście powyższych przepisów nabiera szczególnego znaczenia[81]. Chcąc korzystać z systemów, o których mowa w ust. 5 lit. b) Załącznika III do AI Act, banki zostaną niejako zmuszone, by każdorazowo być w stanie wyjaśnić, co wpłynęło na podjęcie w konkretnej sprawie takiej, a nie innej decyzji.

4.2.4 Odpowiedzialność za produkt niebezpieczny

Rodzime regulacje dotyczące odpowiedzialności za produkt niebezpieczny stanowią implementację unijnych przepisów zawartych w dyrektywie Rady Nr 85/374/EWG z dnia 25 sierpnia 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe[82]. Pod pojęciem produktu niebezpiecznego, zgodnie z art. 449^1 § 3 k.c., należy rozumieć „produkt niezapewniający bezpieczeństwa, jakiego można oczekiwać, uwzględniając normalne użycie produktu. O tym, czy produkt jest bezpieczny, decydują okoliczności z chwili wprowadzenia go do obrotu, a zwłaszcza sposób zaprezentowania go na rynku oraz podane konsumentowi informacje o właściwościach produktu. Produkt nie może być uznany za niezapewniający bezpieczeństwa tylko dlatego, że później wprowadzono do obrotu podobny produkt ulepszony". Ponadto, jak wskazano w art. 449^1 § 2 k.c., „przez produkt rozumie się rzecz ruchomą, choćby została ona połączona z inną rzeczą. Za produkt uważa się także zwierzęta i energię elektryczną". Należy w tym miejscu wspomnieć, że z uwagi na tak sformułowaną definicję w polskim piśmiennictwie kwestionowana jest często dopuszczalność zakwalifikowania oprogramowania (a więc także systemów AI) jako produktu niebezpiecznego. Część doktryny rekomenduje zastosowania wykładni funkcjonalnej przytoczonych wyżej przepisów, która obejmowałaby również dobra niematerialne (w tym systemy AI)[83]. Dodatkowy argument za takim posunięciem miałby stanowić fakt, iż w „Sprawozdaniu Komisji dla Parlamentu Europejskiego,

---

[80] T.j. Dz. U. z 2023 r. poz. 970 ze zm.

[81] Zob. K. Koźmiński *et al.*, *Aktualne wyzwania prawne związane z zastosowaniem sztucznej inteligencji w polskim sektorze bankowym*, Warszawa 2024, s. 19, https://pabwib.pl/produkt/aktualne-wyzwania-prawne-zwiazane-z-zastosowaniem-ai-w-polskim-sektorze-bankowym/ [dostęp: 15.07.2024].

[82] Dz. Urz. WE L 210.

[83] Tak: M. Jagielska, *op. cit*., s. 75; por. K. Bączyk-Rozwadowska, *Odpowiedzialność cywilna za szkody wyrządzone w związku z zastosowaniem sztucznej inteligencji w medycynie*, „Przegląd Prawa Medycznego" 2021, nr 3–4, s. 23.

Rady i Europejskiego Komitetu Ekonomiczno-Społecznego. Sprawozdanie na temat wpływu sztucznej inteligencji, internetu rzeczy i robotyki na bezpieczeństwo i odpowiedzialność”[84] również zarekomendowano potrzebę przyjęcia szerszej wykładni omawianych przepisów. Wskazano w nim mianowicie, że „dużą część unijnych ram dotyczących bezpieczeństwa produktów opracowano, zanim jeszcze pojawiły się technologie cyfrowe, takie jak AI, IoT czy robotyka. Dlatego też nie zawsze zawierają one przepisy wyraźnie odnoszące się do nowych wyzwań i zagrożeń związanych z pojawiającymi się technologiami. Zważywszy na fakt, że istniejące ramy dotyczące bezpieczeństwa produktów są neutralne pod względem technicznym, nie oznacza to jednak, że nie miałyby one zastosowania do produktów wykorzystujących te technologie”[85].

Niemniej, powyższy pogląd nie jest przyjmowany bezkrytycznie i budzi spore kontrowersje[86]. W ocenie autora niniejszego artykułu należy go uznać wręcz za błędny. Trafnie w tym zakresie wypowiedziała się A. Kubiak-Cyrul, zdaniem której „przyjęta w art. 449[1] § 2 KC definicja produktu, odwołująca się do pojęcia rzeczy, uniemożliwia jej rozszerzenie na dobra intelektualne z uwagi na ich niematerialny charakter. Ze względu na znaczenie dóbr, takich jak programy komputerowe, internet, technologia chmury czy projekty techniczne dla współczesnej produkcji przemysłowej postulować należy zmianę przepisów w tym zakresie”[87]. Cytowana autorka uzupełnia powyższe wywody stwierdzeniem, iż „w przypadku technologii cyfrowych wbudowanych w rzeczy wprowadzane do obrotu (np. sprzęt AGD, komputery, telefony) przedstawiciele doktryny opowiadają się za traktowaniem ich jako produktu w rozumieniu art. 449[1] § 2 KC”[88].

Należy więc przyjąć, że systemy AI wykorzystywane w działalności bankowej nie mogą być *de lege lata* uznane za produkty niebezpieczne. W szczególności, iż zazwyczaj nie zostaną one udostępniane klientowi wraz z materialnym nośnikiem, lecz przybiorą postać systemów/aplikacji mobilnych dostępnych za pośrednictwem komputerów i smartfonów. Jednocześnie kwalifikacja ta w niedalekiej przyszłości powinna ulec zmianie z uwagi na przyjęte przez Parlament Europejski (aczkolwiek jeszcze niezatwierdzone przez Radę) nowelizacje w zakresie odpowiedzialności za produkt wadliwy, które jednoznacznie dokonują rozszerzenia odpowiedzialno-

[84] COM/2020/64 final.

[85] *Ibidem*.

[86] Zob. m.in. J.M. Kondek, *op. cit.*, s. 30.

[87] A. Kubiak-Cyrul, [w:] M. Załucki (red.), *Kodeks cywilny. Komentarz. Wyd. III*, Warszawa 2023, art. 449[1], nb 15.

[88] *Ibidem.*

ści za produkt wadliwy (w Polsce – produkty niebezpieczne) również na produkty cyfrowe[89]. Rozwiązanie to niewątpliwie należy uznać za niezwykle ważne z punktu widzenia zabezpieczenia praw przynajmniej części osób poszkodowanych na skutek szkód spowodowanych przez systemy AI. Należy bowiem mieć na względzie, że odpowiedzialność za produkt niebezpieczny jest odpowiedzialnością na zasadzie ryzyka. A jednocześnie, zgodnie z art. 1 ust. 3 lit. b) projektu dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję, przyszła dyrektywa nie znajdzie zastosowania do „wszelkich praw, jakie na mocy przepisów krajowych wdrażających dyrektywę 85/374/EWG mogą przysługiwać osobie poszkodowanej". Inaczej mówiąc, pomimo jej wejścia w życie klienci banków w przypadku szkód spowodowanych przez systemy AI z powodzeniem będą mogli powoływać się na uprawnienia wynikające z przepisów o produktach niebezpiecznych, o ile zajdą ku temu stosowne przesłanki ustawowe.

Za szkody spowodowane produktem niebezpiecznym odpowiada przede wszystkim producent[90]. Bankowi będzie przysługiwał ten status, jeżeli do stworzenia rozwiązania wykorzystującego system AI dojdzie w ramach jego wewnętrznych struktur (działu innowacji, laboratorium technologicznego itd.). Natomiast jeżeli bank nie wyprodukował systemu, a zakupił prawa do niego od zewnętrznego dostawcy (np. start-upu) i jednocześnie od samego początku sygnował go jedynie swoją nawą/firmą, może w danym stanie faktycznym odpowiadać jako quasi-producent[91]. W okolicznościach niektórych spraw dopuszczalne będzie również przypisanie bankowi odpowiedzialności solidarnej za wyrządzoną szkodę jako podmiotowi trzeciemu w rozumieniu art. 449^6 k.c.

Podsumowanie

Dokonując rekapitulacji rozważań zawartych w niniejszym artykule, można stwierdzić, że rozwój systemów sztucznej inteligencji w sektorze bankowym przynosi szereg wyzwań związanych z odpowiedzialnością cywilnoprawną za szkody wyrządzane klientom. Tradycyjne ramy odpowiedzialności cywilnej, oparte na winie

[89] Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2024 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie odpowiedzialności za produkty wadliwe (COM(2022)0495 - C9-0322/2022 - 2022/0302(COD)), https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_EN.html [dostęp: 15.07.2024].

[90] Art. 449^1 § 1 k.c.

[91] Art. 449^5 § 1–2 k.c.

i przewidywalności działań, mogą stać się niewystarczające w kontekście coraz bardziej autonomicznych i skomplikowanych technologii AI. Częściowym remedium tę sytuację stanie się najprawdopodobniej nadchodząca nowelizacja przepisów regulujących odpowiedzialność za produkty niebezpieczne. Niewątpliwie objęcie zakresem wspomnianych unormowań także szkód spowodowanych przez produkty cyfrowe zwiększy pewność obrotu i zabezpieczy interesy przynajmniej części klientów.

Wskazane działania nie rozwiązują jednak nawet części narosłych wokół omawianego zagadnienia problemów i dlatego należy postulować rychłe podjęcie dalszych, intensywnych prac nad projektem dyrektywy w sprawie odpowiedzialności za systemy sztucznej inteligencji. Propozycje regulacji w nim zawarte pozostają bowiem niezwykle lapidarne i w większości sprowadzają się do wprowadzenia nielicznych, wręcz kadłubkowych uregulowań o charakterze procesowym, nie zaś kompleksowego unormowania prawnych ram pozaumownej odpowiedzialności za szkody spowodowane działaniami systemów AI. W związku z tym należy postulować – w drodze dalszych prac legislacyjnych – rozszerzenie zakresu uregulowań planowanych w ramach wspomnianego aktu prawnego. W obecnym kształcie projekt ten zawiera bowiem liczne i niekiedy bardzo rażące niedociągnięcia. Kwestią wartą rozważenia jest również powrót do odpowiedzialności na zasadzie ryzyka.

Niestety, ograniczone ramy opracowania nie pozwoliły na kompleksową analizę wszystkich zagadnień istotnych dla odpowiedzialności cywilnej za szkody spowodowane przez systemy AI. Z pewnością obszarem wymagającym intensywnego zainteresowania ze strony doktryny stanie się w najbliższym czasie problematyka kolizyjnoprawna[92]. Nie można bowiem zapominać, że działalność bankowa przybiera niejednokrotnie wymiar transgraniczny. Rodzi to w razie sporów konieczność uwzględnienia przepisów państw nie tylko unijnych, ale również należących do tak innych od naszych tradycji prawnych, jak Chiny czy Indie. Dodatkowo, w przypadku przedłużających się prac nad unijnym projektem dyrektywy w sprawie odpowiedzialności za systemy sztucznej inteligencji coraz więcej państw członkowskich może zdecydować się na uregulowanie wspomnianej problematyki w ramach ustawodawstw krajowych. Podobnie ma się sprawa z odpowiedzialnością kontraktową, która wykracza poza ramy procedowanego obecnie projektu.

Mając na uwadze całokształt poczynionych uwag, należy stwierdzić, że niewątpliwie konieczne jest podejmowanie dalszych badań i analizy w zakresie odpowie-

[92] Zob. M. Świerczyński, *Sztuczna inteligencja w prawie prywatnym międzynarodowym – wstępne rozważania*, „Problemy Prawa Prywatnego Międzynarodowego", 2019, t. 25, s. 27–41.

działności cywilnoprawnej za szkody wyrządzone przez AI w sektorze bankowym. Być może zajdzie również potrzeba pewnej weryfikacji przedstawionych w ramach niniejszego opracowania ustaleń w momencie uchwalenia wdrażającej AI Act ustawy, nad którą prace niedawno się rozpoczęły[93].

Bibliografia

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

A. Akty prawne

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

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L 333/1 z 2022 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Tekst mający znaczenie dla EOG) (PE/24/2024/REV/1).

Dyrektywa Rady Nr 85/374/EWG z dnia 25 sierpnia 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe (Dz. Urz. WE L 210).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Tekst mający znaczenie dla EOG) (Dz. Urz. UE L 337/35 z 2015 r.).

Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52022PC0496 [dostęp: 15.07.2024].

Rezolucja Parlamentu Europejskiego z dnia 16 lutego 2017 r. zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (2015/2103(INL))(2018/C 252/25).

[93] Zob. nagranie z posiedzenia podkomisji stałej do spraw sztucznej inteligencji i przejrzystości algorytmów, https://www.sejm.gov.pl/Sejm10.nsf/transmisje.xsp?unid=F73DDAC825DE32F-1C1258B5E003E7EB1 [dostęp: 15.07.2024].

Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 12 marca 2024 r. w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie odpowiedzialności za produkty wadliwe (COM(2022)0495 – C9-0322/2022 – 2022/0302(COD)), https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_EN.html [dostęp: 15.07.2024].

Biała Księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania, COM(2020) 65 final, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52020DC0065 [dostęp: 15.07.2024].

Komunikat z 25.04.2018 r. Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Sztuczna inteligencja dla Europy", COM/2018/237 final, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52018DC0237 [dostęp: 8.05.2024].

Sprawozdanie Komisji dla Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego. Sprawozdanie na temat wpływu sztucznej inteligencji, internetu rzeczy i robotyki na bezpieczeństwo i odpowiedzialność (COM/2020/64).

Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji działająca przy Komisji Europejskiej, „*A Definition of AI: Main Capabilities and Disciplines*" (https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf [dostęp: 15.07.2024].

Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2024 r. poz. 1061).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2022 r. poz. 2509).

Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (t.j. Dz. U. z 2023 r. poz. 2488 ze zm.).

Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (t.j. Dz. U. z 2024 r. poz. 72).

Ustawa z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym (t.j. Dz. U. z 2023 r. poz. 845).

Ustawa z dnia 3 grudnia 2010 r o wdrożeniu niektórych przepisów Unii Europejskiej w zakresie równego traktowania (t.j. Dz. U. z 2023 r. poz. 970 ze zm.).

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz. U. z 2024 r. poz. 30 ze zm.).

Ustawa z dnia 30 maja 2014 r. o prawach konsumenta (t.j. Dz. U. z 2023 r. poz. 2759).

Ustawa z dnia 24 listopada 2017 r. o imprezach turystycznych i powiązanych usługach turystycznych (t.j. Dz. U. z 2023 r. poz. 2211).

B. Orzeczenia

Uchwała Sądu Najwyższego z dnia 11 września 2020 r., III CZP 80/19, Legalis nr 2467749.

Wyrok Sądu Najwyższego z dnia 20 maja 2005 r., III CK 661/04, Legalis nr 70462.

Wyrok Sądu Najwyższego z dnia 16 stycznia 2008, IV CSK 380/07, Legalis nr 114955.

II. Literatura (opracowania o charakterze naukowym)

Abbott R., *The Reasonable Computer: Disrupting the Paradigm of Tort Liability*, „George Washington Law Review" 2018, vol. 86, nr 1.

Bar G., *Sztuczna inteligencja i uczenie maszynowe*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym*, Warszawa 2024.

Bączyk M., *Odpowiedzialność odszkodowawcza banku w związku z naruszeniem obowiązku zachowania tajemnicy bankowej przez pracownika banku*, „Przegląd Sądowy" 2012, nr 11/12.

Bączyk-Rozwadowska K., *Odpowiedzialność cywilna za szkody wyrządzone w związku z zastosowaniem sztucznej inteligencji w medycynie*, „Przegląd Prawa Medycznego" 2021, nr 3–4.

Bieda R., Flisak D., Greser J., Lubasz D., Namysłowska M., Skrodzka-Kwietniak D., Szpyt K., Świerczyński M., Więckowski Z., Załucki M., *O potrzebie dostosowania pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji. Uwagi do projektu dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję*, „Prawo w Działaniu" 2024, t. 58.

Bosek L., *Perspektywy rozwoju odpowiedzialności cywilnej za inteligentne roboty*, „Forum Prawnicze" 2019, nr 2.

Chojecka M., Kisłowski M., *Ochrona informacji niejawnych a tajemnica bankowa,* „Roczniki Nauk Prawnych" 2016, nr 4.

Czechowska I.D., *Przegląd definicji banku stanowiącego aktywny kanał dystrybucji produktów ubezpieczeniowych*, „Acta Universitatis Lodziensis. Folia Oeconomica" 2011, nr 259.

Cicirko T., Kreczmańska-Gigoł K., Mikołajczyk O., Mikołajczyk M., *Bank centralny i banki komercyjne*, [w:] J. Ostaszewski (red.), *Finanse*, Warszawa 2010.

Dybała G.. Szpyt K., *Ubezpieczenia sztucznej inteligencji*, [w:] K. Szpyt (red.), *InsurTech. Nowe technologie w branży ubezpieczeń*, Warszawa 2023.

Dziedzic M., *Zastosowanie systemów sztucznej inteligencji we współczesnej bankowości*, „Europejski Przegląd Prawa i Stosunków Międzynarodowych" 2022, nr 1.

Folwarski M., *Sektor FinTech na europejskim rynku usług bankowych*, Warszawa 2019.

Grzywacz J., Jagodzińska-Komar E., *Rola sztucznej inteligencji w rozwoju sektora bankowego*, „Nauki Ekonomiczne" 2021, t. 34.

Iszkowski W., Tadeusiewicz R., *Na marginesie dyskusji o sztucznej inteligencji*, „Nauka" 2023, nr 4.

Iwańczuk A., *System bankowy i system płatniczy – powiązania i wzajemne uwarunkowania*, „Zeszyty Naukowe/Akademia Ekonomiczna w Poznaniu" 2008, nr 111.

Jagielska M., *Odpowiedzialność za sztuczną inteligencję*, [w:] L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji,* Warszawa 2020.

Jankowska H., *Robo-doradztwo*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym*, Warszawa 2024.

Jankowska M., *Podmiotowość prawna sztucznej inteligencji*, [w:] A. Bielska-Brodziak (red.), *O czym mówią prawnicy mówiąc o podmiotowości*, Katowice 2015.

Kreft J., Boguszewska-Kreft M., Cyrek B., *Halucynacje chatbotów a prawda: główne nurty debaty i ich interpretacje*, „Rocznik Nauk Społecznych" 2024, t. 16, nr 1.

Kubiak-Cyrul A., [w:] M. Załucki (red.), *Kodeks cywilny. Komentarz.* Wyd. III, Warszawa 2023.

Ludzion C., W*pływ rozwoju technologicznego na odpowiedzialność odszkodowawczą*, „Aesthetic Cosmetology and Medicines" 2020, vol. 9.

Małkowski S., *Charakter prawny umowy Software as a Service w polskim systemie prawnym*, „Prawo Mediów Elektronicznych" 2022, nr 4.

Marciniak P., *Problem odpowiedzialności za błędy w oprogramowaniu IoT*, „Przegląd Ustawodawstwa Gospodarczego" 2020, nr 10.

Maydanyk R., Maidanyk N.R., Velykanova M., *Liability for damage caused using artificial intelligence technologies*, „Journal of the National Academy of Legal Sciences of Ukraine" 2021, nr 28(2).

Michalak A., *Odpowiedzialność cywilnoprawna w obrocie oprogramowaniem komputerowym w erze sztucznej inteligencji*, Warszawa 2021.

Nowakowski M., *FINTECH – technologie, finanse, regulacje. Praktyczny przewodnik dla sektora innowacji finansowych*, Warszawa 2020.

Nowakowski M., *Sztuczna inteligencja. Praktyczny przewodnik dla sektora innowacji finansowych,* Warszawa 2023.

Pietrzykowski T., *The Idea of Non-personal Subjects of Law*, [w:] V.A.J. Kurki, T. Pietrzykowski (red.), *Legal Personhood: Animals, Artificial Intelligence and the Unborn*, Szwajcaria 2017.

Radwański Z., Olejniczak A., *Zobowiązania – część ogólna. XIV wydanie,* Warszawa 2020.

Sheikh H., Prins C., Schrijvers E., *Mission AI. The New System Technology*, Holandia 2023.

Smoleń D., Sokoliński O., Szarek G., *Polisa od sztucznej inteligencji*, „Miesięcznik Ubezpieczeniowy" 2018, nr 10.

Sudoł M., *Biometria w identyfikacji i weryfikacji klientów bankowych*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym*, Warszawa 2024.

Staszczyk P., *Czy unijna regulacja odpowiedzialności cywilnej za sztuczną inteligencję jest potrzebna?*, „Europejski Przegląd Sądowy" 2022, nr 6.

Szpringer W., *Nowe technologie a sektor finansowy. FinTech jako szansa i zagrożenie*, Warszawa 2017.

Szpyt K., *FinTech – pojęcie, historia, rynek*, [w:] K. Szpyt (red.), *Nowe technologie w sektorze bankowym*, Warszawa 2024.

Szpyt K., *InsurTech – zarys zjawiska*, [w:] K. Szpyt (red.), *InsurTech. Nowe technologie w branży ubezpieczeń*, Warszawa 2023.

Świerczyński M., *Sztuczna inteligencja w prawie prywatnym międzynarodowym – wstępne rozważania*, „Problemy Prawa Prywatnego Międzynarodowego", 2019, t. 25.

Wałachowska M., *Sztuczna inteligencja a zasady odpowiedzialności cywilnej*, [w:] L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji,* Warszawa 2020.

Wilk A., *Sztuczna inteligencja a rozwój prawa ubezpieczeń – przegląd najważniejszych wyzwań*, „Wiadomości Ubezpieczeniowe" 2023, nr 4.

Yas N., Qaruty R. Al, Abdel-hadi S., *Civil Liability and Damage Arising from Artificial Intelligence*, „Migration Letters" 2023, nr 20(5).

Zacharzewski K., *Glosa do wyroku z dnia 20 maja 2005 r. (III CK 661/04)*, „Przegląd Sądowy" 2007, nr 9.

Zaleska M., *Charakterystyka systemu bankowego – uwarunkowania instytucjonalne*, [w:] M. Zaleska (red.), *Współczesna bankowość*, Warszawa 2008.

Zalewski T., *Definicja sztucznej inteligencji*, [w:] L. Lai, M. Świerczyński (red.), *Prawo sztucznej inteligencji*, Warszawa 2020.

III. Źródła internetowe

Ailleron, *AI w bankowości – sztuczna inteligencja w banku i finansach*, https://ailleron.com/pl/baza-wiedzy/ai-w-bankowosci-sztuczna-inteligencja-w-banku-i-finansach/ [dostęp: 15.07.2024].

Bar G., Nowakowski M., Prabucki R., Szostek D., *Zastosowanie sztucznej inteligencji w bankowości – szanse oraz zagrożenia. Analiza prawno-regulacyjna wpływu technologii uczenia maszynowego i pokrewnych na obowiązki sektora bankowego z zakresu zapewnienia zgodności oraz zarządzania ryzykiem*, https://us.edu.pl/wp-content/uploads/pliki/PAB_WIB_Zastosowanie_sztucznej_inteligencji_w_bankowosci_Szostek.pdf [dostęp: 15.07.2024].

Genpact, *Commercial banking and the customer experience imperative How industry leaders are using CX and artificial intelligence to overcome disruption*, https://website-files.genpact.com/files/report-commercial-banking-and-the-customer-experience-imperative.pdf [dostęp: 15.07.2024].

https://chat.openai.com/ [dostęp: 15.07.2024].

iTV Sejm – transmisje, Podkomisja stała do spraw sztucznej inteligencji i przejrzystości algorytmów, https://www.sejm.gov.pl/Sejm10.nsf/transmisje.xsp?unid=F73DDAC825DE32F-1C1258B5E003E7EB1 [dostęp: 15.07.2024].

Institute for Development and Research in Banking Technology (Established by Reserve Bank of India), *AI in Banking. A Primer*, https://www.idrbt.ac.in/wp-content/uploads/2022/07/AI_2020.pdf [dostęp: 15.07.2024].

Jak banki wykorzystują sztuczną inteligencję?, https://www.youtube.com/watch?v=bFMZOsh2ADg [dostęp: 15.05.2024].

Kamalnath V., Lerner L., Moon J., Sari. G, Sohoni V., Zhang S., *Capturing the full value of generative AI in banking*, https://www.mckinsey.com/industries/financial-services/our-insights/capturing-the-full-value-of-generative-ai-in-banking [dostęp: 15.07.2024].

Klienci Nest Banku już testują AI Asystenta, https://nestbank.pl/n-asystent-juz-jest [dostęp: 15.07.2024].

Kondek J.M., *Odpowiedzialność odszkodowawcza za oprogramowanie i sztuczną inteligencję (uwagi de lege lata i de lege ferenda),* Warszawa 2021, https://iws.gov.pl/wp-content/uploads/2021/08/IWS_Kondek-J.M._-Odpowiedzialnosc-odszkodowawcza-za-oprogramowanie-i-sztuczna-inteligencje.pdf [dostęp: 15.07.2024]

Kozłowski J. [w:] Law4Tech, *Analiza i ocena zmian w Akcie o sztucznej inteligencji (AI Act)*, https://law4tech.pl/1881-2/ [dostęp: 15.07.2024].

Koźmiński K., Żółtek S., Jabłoński M., Lewis C.W.P. , Czarnocki J., Leszczyński A., Macidłowski M., Sasin S., *Aktualne wyzwania prawne związane z zastosowaniem sztucznej inteligencji w polskim sektorze bankowym,* Warszawa 2024, https://pabwib.pl/produkt/aktualne-wyzwania-prawne-zwiazane-z-zastosowaniem-ai-w-polskim-sektorze-bankowym/ [dostęp: 15.07.2024]

McKinsey, *Global Banking Annual Review 2023: The Great Banking Transition*, https://www.mckinsey.com/industries/financial-services/our-insights/global-banking-annual-review#/ [dostęp: 15.07.2024].

Maj K., *Sztuczna inteligencja w prawdziwym banku*, [w:] Związek Banków Polskich, Centrum Prawa Bankowego i Informacji, *Sztuczna inteligencja w bankowości,* Warszawa 2020, https://bank.pl/wp-content/uploads/2020/06/Raport-SZTUCZNA-INTELIGENCJA.pdf [dostęp: 15.07.2024].

Michałowski B., Przegalińska A., Poniewierski A., *Internet of Things (IoT) i Artificial Intelligence (AI) w Polsce. Jak wykorzystać rewolucję technologiczną Internetu Rzeczy i Sztucznej Inteligencji w rozwoju Polski. Raport*, Warszawa 2018, https://sobieski.org.pl/wp-content/uploads/Raport-Iot-i-AI-w-Polsce-03-2018-Micha%C5%82owski.pdf [dostęp: 15.07.2024].

OECD, *AI in Business and Finance. OECD Business and Finance Outlook 2021*, https://www.oecd-ilibrary.org/docserver/ba682899-en.pdf?expires=1721927852&id=id&accname=guest&checksum=7EFEBE8DF7D760F0216FBD21CF486116 [dostęp: 15.07.2024].

Rusak A., *Sztuczna inteligencja Bing wyzywa ludzi i twierdzi, że są źli. Może ma rację?*, https://vibez.pl/wydarzenia/sztuczna-inteligencja-bing-wyzywa-ludzi-i-twierdzi-ze-sa-zli-moze-ma-racje-6866817009040000a [dostęp: 15.07.2024].

Tomaszewski M., *Internauci nauczyli Sztuczną Inteligencję nazizmu*, https://www.antyradio.pl/news/Internauci-nauczyli-Sztuczna-Inteligencje-nazizmu-7561 [dostęp: 15.07.2024].

Uryniuk J., *Cashless Breakfast AI. Nest Bank zaprezentował bazującego na GPT-4 N!Asystenta*, https://www.cashless.pl/15110-cashless-breakfast-ai-n-asystent-nest-bank [dostęp: 15.07.2024]

Wara-Wąsowska E., *Jak banki wyceniają wartość mieszkania?*, https://rynekpierwotny.pl/wiadomosci-mieszkaniowe/wycena-wartosci-mieszkania-przez-bank/11153/ [dostęp: 15.07.2024].

Widawski P., [w:] *Raport: Sztuczna Inteligencja. Dobre praktyki, aspekty prawne, zastosowanie w sektorze finansowym*, https://fintechpoland.com/wp-content/uploads/2022/03/AI_raport_FIN-1.pdf [dostęp: 15.07.2024].

Civil liability for damages caused to customers by the use of artificial intelligence in banking activities

Abstract

The article discusses key issues related to the civil liability of banks for damages caused to customers as a result of the use of artificial intelligence (AI) systems. With the rapid development of technology and the growing importance of AI in the financial sector, traditional principles of civil liability may not be sufficient. The problems of identifying liable parties and assessing the risks posed by the use of advanced algorithms are analyzed. In the context of the lack of comprehensive regulations, both at the national and EU levels, the article emphasizes the need for an in-depth analysis of existing standards and their adaptation to new challenges. Also presented is a discussion of selected EU regulations, such as the AI Act and Proposal for a AI Liability Directive. The paper focuses on the legal challenges of protecting customers' rights and the financial risks arising from inappropriate or unpredictable operation of AI systems in banking.

Keywords

Artificial intelligence, artificial intelligence system, civil liability, tort, dangerous product