

P
ME

4/2022

Redakcja Kwartalnika Naukowego Prawo Mediów Elektronicznych

Redaktor naczelny: prof. dr hab. *Jacek Gołaczyński*, UW

Sekretarz Redakcji: dr *Aleksandra Klich*, USz

Członek Redakcji: dr *Krzysztof Garstka*, Uniwersytet w Cambridge

Członkowie rady programowej:

Przewodniczący: dr hab. *Wojciech Wiewiórowski* (UG, Europejski Inspektor Ochrony Danych)

Członkowie:

r.pr. *Włodzimierz Chróścik*

adv. *Rafał Dębowski*

dr hab. *Sviatlana Fursa*, prof. nauk prawnych Kijowskiego Narodowego Uniwersytetu im. Tarasa Szewczenki

dr hab. prof. *Marlena Jankowska*, prof. nadzw. UŚ

adv. *Xawery Konarski*

prof. Avv. *Michele Angelo Lupoi*, Uniwersytet Boloński

prof. dr hab. *Jacek Mazurkiewicz*, UZ

prof. dr hab. *Radim Polcak*, Uniwersytet w Brnie

dr hab. *Grzegorz Sibiga*, INP PAN

dr hab. *Piotr Stec*, prof. nadzw. UO

dr hab. *Dariusz Szostek*, prof. nadzw. UO

prof. dr hab. *Grażyna Szpor*, UKSW

prof. dr hab. *Andreas Wiebe*, Uniwersytet w Getyndze

Recenzenci:

dr hab. *Andrzej Adamski*, prof. nadzw. UMK

prof. *Zsolt Balogh*, Uniwersytet Corvinus Budapeszt

prof. dr hab. *Sławomir Cieślak*, UŁ

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

prof. dr hab. *Jacek Górecki*, UŚ

prof. em. dr *Wolfgang Kilian*, University of Hannover

prof. hab. dr *Vytautas Nekrosius*, Uniwersytet Wileński

dr hab. *Marek Świerczyński*, prof. nadzw. UKSW

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

Adres redakcji:

Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii,

Centrum Badań Problemów Prawnych i Ekonomicznych

Komunikacji Elektronicznej

ul. Uniwersytecka 22/26, 51-145 Wrocław

e-mail: pme@beck.pl



C.H.BECK

Wydawca:

Wydawnictwo C.H. Beck

ul. Bonifraterska 17

00-203 Warszawa

tel.: 22 33 77 600

www.czasopisma.beck.pl

Nakład: 250 egz.

Spis treści

Ćwierć wieku ewolucji prawa w kontekście rozwoju technologii cyfrowych i aspiracji społecznych dr inż. <i>Kajetan Wojsyk</i>	4
Projekt ustawy o wolności słowa w internetowych serwisach społecznościowych – remedium na walkę z bezprawnymi treściami? <i>Kamila Brylak-Hudyma</i>	13
Obowiązki informacyjne przedsiębiorcy charakterystyczne dla świadczenia usług drogą elektroniczną na rzecz konsumenta <i>a plain language</i> i warstwowe obowiązki informacyjne jako próba rozwiązania problemu tzw. <i>information overkill</i> <i>Laura Słocka</i>	25
Ochrona konsumenta zawierającego umowy elektroniczne <i>Marlena Sobczak</i>	34
Odpowiedzialność cywilnoprawna <i>host providera</i> <i>Wiktor Żochowski</i>	42
Charakter prawny umowy <i>Software as a Service</i> w polskim systemie prawnym <i>Stanisław Małkowski</i>	49

Contents

Quarter of a century of evolution of law in the context of the development of digital technologies and social aspirations dr inż. <i>Kajetan Wojsyk</i>	4
Draft law on the freedom of speech in social media – remedy for combating unlawful content? <i>Kamila Brylak-Hudyma</i>	13
Entrepreneurs' information obligations characteristic to the electronic provision of services to the consumer and plain language and layered information obligations as a proposed solution to the so-called information overkill problem <i>Laura Słocka</i>	25
Protecting consumers who enter into electronic contracts <i>Marlena Sobczak</i>	34
Civil liability of the hosting provider <i>Wiktor Żochowski</i>	42
Legal nature of a <i>Software as a Service</i> contract in the Polish legal system <i>Stanisław Małkowski</i>	49

Szanowni Państwo,

Zapraszam Państwa do lektury kolejnego, czwartego w 2022 r. numeru czasopi-
sma naukowego Prawo Mediów Elektronicznych. Tym razem mam dla Państwa
pięć artykułów dotyczących zróżnicowanej tematyki, ale powiązanej z zagadnie-
niami wpływu nowych technologii na prawo.

Ciekawą wypowiedź znajdziecie Państwo w artykule pt. *Ćwierć wieku ewolucji
prawa w kontekście rozwoju technologii cyfrowych i aspiracji*, *Kajetana Wojsyka*.
Chodzi oczywiście o opis rozwoju technologii cyfrowych i jego wpływu na admi-
nistrację publiczną. Natomiast w artykule *Marleny Sobczak* zawarte są rozważa-
nia dotyczące ochrony konsumenta zawierającego umowy elektroniczne. Z arty-
kułu *Laury Słockiej* pt. *Obowiązki informacyjne przedsiębiorcy charakterystyczne
dla świadczenia usług drogą elektroniczną na rzecz konsumenta a plain langu-
age i warstwowe obowiązki informacyjne jako próba rozwiązania problemu
dowiemy się o świadczeniu usług drogą elektroniczną w zakresie obowiązków
informacyjnych, czyli problemu tzw. information overkill*. W artykule *Kamili Brylak-
Hydymy* pt. *Projekt ustawy o wolności słowa w internetowych serwisach społecz-
nościowych – remedium na walkę z bezprawnymi treściami? przeczytamy o wą-
pliwościach, jakie wiążą się z tym projektem*. W końcu artykuł *Stanisława
Małkowskiego* dotyczący charakteru prawnego umowy *Software as a Service*
w polskim systemie prawnym dotyczy problematyki nowego sposobu korzysta-
nia z praw autorskich za pośrednictwem Internetu.

Zapraszam Państwa do interesującej lektury
prof. dr hab. *Jacek Gołaczyński*
Redaktor naczelny

Ćwierć wieku ewolucji prawa w kontekście rozwoju technologii cyfrowych i aspiracji społecznych

dr inż. *Kajetan Wojsyk*¹

W niniejszym opracowaniu autor – który pracował w administracji publicznej (niezależnie od równoległej pracy naukowej i dydaktycznej związanej z zastosowaniami informatyki w różnych dziedzinach) ponad ćwierć wieku i brał bezpośredni, aktywny udział w jej przemianie od całkowicie „papierowej” do całkowicie „elektronicznej” w różnych podmiotach – dzieli się swoimi doświadczeniami. Artykuł jest retrospektywną próbą opisu poczynionych spostrzeżeń i zdobytych doświadczeń.

Uwagi wstępne

Jedną z cech człowieka, będącą motorem postępu i rozwoju (obok tzw. twórczego lenistwa), jest naturalna chęć ułatwiania sobie wykonywania codziennych czynności, szczególnie tych często powtarzanych, uciążliwych, monotonna, lub niewykonywania czynności w istocie swej zbędnych, ale wykonywanych siłą przyzwyczajenia czy tradycji „bo zawsze tak się robiło...”. Wspomniana cecha jest uniwersalna i dotyczy ludzi wykonujących prace w każdym obszarze, w tym w administracji.

Dwudziesta rocznica działalności Centrum Badań Komunikacji Elektronicznej wydaje się doskonałą okazją do spojrzenia z dłuższej perspektywy czasowej na proces przemian, jakie administracja różnych podmiotów przechodziła przez te 20 lat. Jest jednak przede wszystkim okazją do podjęcia próby przewidzenia dalszego kierunku rozwoju środków komunikacji elektronicznej – i nie tylko komunikacji jako takiej (ponieważ skuteczna komunikacja wymaga nadawców i odbiorców informacji), ale przede wszystkim przyszłych sposobów działania administracji publicznej i sposobów jej komunikacji z otoczeniem – z użyciem dokumentów.

Początek obserwacji – etap 0

Punktem wyjścia i początkiem obserwacji była praca dydaktyczna (1991 r. – 11 lat przed przyjęciem ustawy o świadczeniu usług drogą elektroniczną) w Instytucie Edukacji Technicznej na Wydziale Matematyczno-Przyrodniczym ówczesnej Wyższej Szkoły Pedagogicznej w Częstochowie i utworzenie Wydziałowej Pracowni Komputerowej – miejsca ćwiczeń studentów całego wydziału. Jest oczywiste, że różnego rodzaju prace laboratoryjne z wykorzystaniem komputerów pozwoliły na zorientowanie się w skali możliwości ułatwienia pracy w każdym niemal obszarze, w tym w administracji (dziekany wszystkim wydziałów, Dział Nauczania, Rektorat, administracja uczelni itd.).

W owym czasie nie istniała jeszcze sieć miejska CzestMAN², której projekt rozpoczęto dopiero w 1992 r. Do

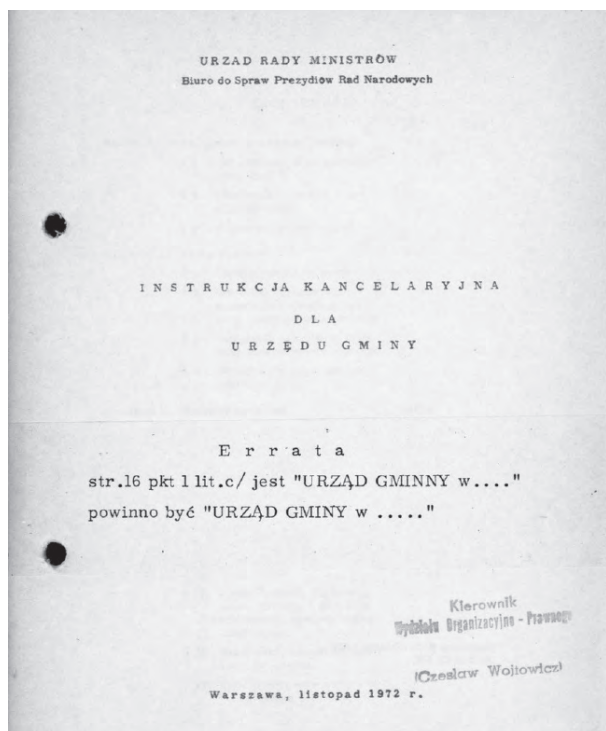
przenoszenia danych z poszczególnych dziekanatów (znajdujących się w odległych budynkach) do Działu Nauczania Wyższej Szkoły Pedagogicznej, gdzie następowało scalanie danych w zbiór wszystkich studentów uczelni, służyły dyskietki 3,5”. Podejmowanie kolejnych, niewielkich projektów informatycznych, w tym tworzenie lokalnych sieci komputerowych i rozpoczęcie wykorzystywania modemów, pozwalało na obejmowanie przetwarzaniem danych coraz większych obszarów informacyjnych. Równolegle pracownicy administracji, widząc możliwości przetwarzania danych (łatwe tworzenie różnego rodzaju list, np. stypendialnych, raportów, zestawień oraz dokonywania obliczeń) i porównując je z dawnym, dotychczasowym sposobem tworzenia tego samego typu list i raportów, szybko dostrzegli, że dzięki wykorzystaniu komputerów ten sam (a nawet znacząco lepszy, pozbawiony także błędów, które dawniej zdarzały się przy „ręcznym” przetwarzaniu) efekt można uzyskać znacząco mniejszym wysiłkiem, w dodatku samodzielnie. Zaczęli coraz odważniej stawiać pytania „czy dałoby się ...”, „czy możliwe byłoby...” itd. itp.

Należy w tym miejscu zwrócić uwagę na fakt, że sytuacja znaczącej poprawy szybkości i jakości przetwarzania danych była dobrze widoczna i odczuwalna szczególnie w okresach tworzenia się kolejek studentów przed dziekanatami (koniec semestru, składanie wniosków o miejsce w akademiku, stypendium itp.). Nagła, skokowa poprawa warunków pracy połączona z szybkim, ale skutecznym szkoleniem stanowiskowym, była niezwykle mobilizująca i tworzyła sprzyjającą atmosferę do dalszego rozwoju systemów, w szczególności poprawiała poczucie władz uczelni, że inwestycja w informatykę (nie tylko dla celów kształcenia studentów, co było koniecznością, ale właśnie dla poprawy działania administracji) ma sens: zadowoleni, chwalcący nowe rozwiązania pracownicy potrafili dzielić się doświadczeniami. W kontekście tego doświadczenia (początek lat 90. XX w.) można przyjąć tezę, że

¹ Autor jest doktorem nauk technicznych, nauczycielem akademickim, a od 1994 r. równoległe pracownikiem administracji publicznej zajmujący się jej informatyzacją. ORCID: 0000-0003-2523-8034

² Zob. <https://pl.wikipedia.org/wiki/CzestMAN> (dostęp z 30.12.2022 r.).

sukces we wdrożeniu rozwiązań informatycznych jest bezpośrednio i silnie zależny od wsparcia kierownika podmiotu i otwarcia się na nowe rozwiązania przyszłych użytkowników systemu. Wsparcie kierownika podmiotu polega na jego osobistym zaangażowaniu się – poprzez rozpoczęcie korzystania z nowego systemu, domaganiu się tego samego od podległych mu pracowników, a także na stanowiskowym przeszkoleniu administratora nowego systemu i liderów, pracowników komórki organizacyjnej, którzy w pierwszej kolejności zdobędą wiedzę i umiejętności (potrzebne w korzystaniu – nie „obsłudze”! – z nowego systemu), którymi będą się dzielili ze współpracownikami.



Można zatem przyjąć, że „etap 0” był etapem „radosnej fascynacji” dostępnymi już wówczas nowoczesnymi, elektronicznymi środkami mogącymi technicznie wspomagać pracę w administracji, mającymi tyle wspólnego z realizacją procedur administracyjnych, ile długopisy, pieczątki, papierowe rejestry, segregatory, spinacze, zszywacze, dziurkacze, klej, znaczki, naklejki itp. akcesoria biurowe.

Wątpliwości prawne – etap 1

Na tym etapie istotnym doświadczeniem były często wyrażane uwagi sceptyków, formułowane zazwyczaj jako wątpliwości, „czy stosowanie narzędzi informatycznych jest zgodne z prawem?”. Jaki przepis prawa mówi, że można tego rodzaju systemy stosować „zamiast”, a nie „obok”, „czy to jest bezpieczne, bo jeżeli coś się stanie z systemem i praca pójdzie na marne, to jak odtworzymy...”, „a co w razie kontroli...”, „co będzie, gdy wyłączą prąd...” itd., itp. Instrukcje kancelaryjne w owym czasie nie przewidywały używania

jakichkolwiek elektronicznych narzędzi, natomiast dość dokładnie opisywały procedury postępowania z dokumentami papierowymi. Wsparcie kierownika podmiotu (w tym przypadku rektora), a w drugiej kolejności kierownika komórki organizacyjnej było podstawowym i wystarczającym warunkiem trwałych i pozytywnych przemian. Należy zaznaczyć, że wobec niejasności prawa podjęcie decyzji o informatyzacji administracji wymagało nie tylko pewnej odwagi i wzięcia na siebie odpowiedzialności za ewentualne negatywne skutki przez kierownika podmiotu, ale z drugiej strony skłaniało do poszukiwania rozwiązania tej trudnej sytuacji, rozwiązania polegającego między innymi na próbach interpretacji niejasnych przepisów zgodnie z duchem zachodzących przemian. Istotny też był fakt, iż – jak już wyżej wspomniano – aktualnie obowiązujące wówczas instrukcje kancelaryjne wyraźnie traktowały o dokumentach w postaci papierowej (wskazywały na to słowa takie jak „maszyna do pisania”, „kartka papieru” itp.). Przykładowo jedynym ciągiem znaków, w którym występował ciąg „elektr” w instrukcji kancelaryjnej dla urzędów gmin z 1972 r., było hasło klasyfikacyjne „Elektryfikacja wsi” (605, kat. B10). W późniejszej o 18 lat instrukcji kancelaryjnej stanowiącej załącznik do nieopublikowanego zarządzenia Nr 40 Prezesa Rady Ministrów z 19.7.1990 r. w sprawie wykonywania czynności kancelaryjnych w urzędach gmin, związków komunalnych i sejmików samorządowych jedynym skojarzeniem ze środkami elektronicznego przekazu było wskazanie wśród czynności kancelaryjnych czynności takich jak „przyjmowanie i nadawanie telegramów, telefonogramów, dalekopisów, telefaxów”. Zarządzenie to utraciło moc w wyniku wydania rozporządzenia Prezesa Rady Ministrów z 22.12.1999 r. wchodzącego w życie 1.1.2000 r.³ W rozporządzeniu tym istotnie zmieniło się podejście do środków komunikacji elektronicznej, do tego nawet stopnia, że pojawił się „Rozdział XVI – Wykorzystanie informatyki w czynnościach kancelaryjnych”, w którym znajdujemy: „§ 52. Dopuszcza się szerokie wykorzystanie informatyki w urzędach, pod warunkiem ochrony przechowywanych w zbiorach informatycznych danych, w tym zwłaszcza danych osobowych, jeżeli ich gromadzenie dopuszcza ustawa”. Co więcej, w kolejnym paragrafie znajduje się nawet zalecenie: „§ 53.1. Zaleca się wykorzystanie informatyki w celu: [tu zakres, w jakim się zaleca...].” Rozporządzenie to, przy właściwej interpretacji i dobrej woli kierowników podmiotów dawało już bardzo wiele możliwości. Niestety, brakowało jeszcze dwóch istotnych elementów – zapewnienia integralności przesyłanych treści i niezaprzeczalności udziału konkretnych osób w realizacji procedur administracyjnych.

³ Dz.U. Nr 112, poz. 1319.

Wspomniane zarządzenie Nr 40 Prezesa Rady Ministrów nie dotyczyło oczywiście administracji uczelnianych, ale pozwalało zorientować się, jakie miejsce w owym czasie środki komunikacji elektronicznej znajdowały w zastosowaniach kancelaryjnych. Praktycznie środków tych nie było, gdyż do praktyki administracji pierwsze konta e-mailowe weszły pod koniec 1996 r. Wcześniej z poczty elektronicznej zaczęli korzystać głównie pracownicy naukowcy, współpracujący z innymi ośrodkami zagranicznymi – nie był to wprawdzie obszar administracji publicznej, ale nie rozważamy na tym etapie procedur właściwych dla dziedziny, ale narzędzia – środki techniczne, które co do zasady niczym nie powinny się różnić, gdyż są wyrazem aktualnego stanu cywilizacyjnego. Jeśli o integralność dokumentów chodzi, mogły być one tworzone z wykorzystaniem komputerów, ale później musiały być drukowane ze wszystkimi tego dalszymi konsekwencjami – pieczętowaniem, ręcznym podpisywaniem i przewożeniem z miejsca wytworzenia do miejsca docelowego. Praktycznie, poza estetyką i wygodą tworzenia – korzyści ekonomicznych nie było.

Elektroniczne środki i narzędzia pracy biurowej – etap 2

Należy wspomnieć, że w administracji w owym czasie stosowanych było kilka tzw. procesorów tekstu, takich jak TAG⁴ – produkcji polskiej firmy InfoService czy QR-Tekst⁵, aplikacja produkcji również polskiej firmy Malkom s.c. Oba wymienione produkty istniały na rynku zaledwie kilka lat – i choć drugi z nich był dość mocno wspierany i zalecany do stosowania w administracji (stosowały go między innymi Sejm i Senat RP, Ministerstwo Łączności, Główny Urząd Statystyczny, Główny Urząd Ceuł, Generalna Dyrekcja Lasów Państwowych, Urząd Rady Ministrów, Policja oraz wiele urzędów wojewódzkich, a także niektóre urzędy gmin), ostatecznie zostały wyparte przez MS Word. Oczywiście głównie chodziło o wykorzystanie tzw. procesorów tekstu, później nazwanych edytorami tekstów, które to teksty – zapisane w postaci elektronicznej – łatwo poddawały się korekcie, modyfikacji, umożliwiały tworzenie korespondencji seryjnej i były to bardzo mocne argumenty za odejściem od mechanicznych, a nawet elektronicznych maszyn do pisania. Od tworzenia plików w postaci elektronicznej do dokumentów elektronicznych (bo jeszcze – z uwagi na brak powszechnego stosowania podpisu elektronicznego mieliśmy do czynienia jedynie z projektami dokumentów, a nie dokumentami w ich ścisłym rozumieniu) do upowszechnienia się komunikacji elektronicznej droga nie była już tak bardzo daleka. Potrzebne były jeszcze 2 elementy: adresy elektroniczne oraz podpisy elektroniczne.

Logicznie rzecz biorąc, nic jednak nie stało na przeszkodzie, by tworzyć dokumenty za pomocą dostępnych wówczas edytorów tekstu, drukować je i dalej postępować jak z dokumentami tworzonymi z użyciem mechanicznych czy elektronicznych maszyn do pisania. Był to zatem etap zamiany jedynie środków technicznych wspomagających prace biurowe, ułatwiający pracę, niemający wprawdzie istotnego wpływu na przekształcenie tradycyjnej administracji „papierowej” w „elektroniczną”, ale będący zacinem zmian idących w kierunku stopniowej eliminacji mechanicznych, a w dalszej kolejności elektronicznych maszyn do pisania, coraz słabiej czytelnych kopii (max. 7), taśm barwiących, korektorów... Drobne, ale jednak ciągle idące w tę samą stronę działania (likwidacja materialnego składnika procesu tworzenia dokumentu) tworzyły podatny grunt dla dalszych przemian, szczególnie w sferze mentalnej pracowników administracji.

Opisany wyżej proces pozwolił zdobyć cenne doświadczenie: o ostatecznym sukcesie wdrożenia systemów informatycznych decydowało oficjalne, zdecydowanie wsparcie kierownika podmiotu pozwalające przełamywać mentalne opory pracowników, otrzymujących nowe narzędzia pracy, co zawsze wiązało się z chwilowym dodatkowym obciążeniem, ale z uzasadnioną obietnicą: „im szybciej opanujesz narzędzie, tym szybciej zdecydowanie poprawisz sobie warunki pracy, bo nie chodzi o to, by do dotychczasowych obowiązków dodać nowe, równoległe, ale by jak najszybciej zamienić archaiczne techniki pracy nowymi – wygodniejszymi, bardziej ergonomicznymi...”.

Słowa uczą, przykłady pociągają – etap 3

Kolejny, dający się dość dokładnie określić krok w stronę e-administracji to pojawienie się możliwości wykorzystania poczty elektronicznej w administracji (pracownicy uczelni wprawdzie wcześniej zaczęli korzystać z poczty elektronicznej, ale w niniejszym artykule koncentrujemy się na administracji publicznej). Nie chodzi tu o datę (koniec pierwszej połowy lat 90. XX w.), lecz o sam fakt akceptacji takiego środka przekazywania zarówno informacji, pojedynczych zdań, treści wpisywanych bezpośrednio, jak i dołączania przesyłek większych, kopii dokumentów w różnych formatach, własnych, jak też obcych.

Z natury rzeczy łatwiejsze w tworzeniu przesyłki e-mailowe upowszechniły się w administracji dość szybko, jednak bez głębszej refleksji użytkowników poczty elektronicznej nad bezpieczeństwem tych przesyłek (w rozumieniu integralności) i pewności co do tożsamości nadawcy czy od-

⁴ Zob. [https://pl.wikipedia.org/wiki/TAG_\(edytor_tekstu\)](https://pl.wikipedia.org/wiki/TAG_(edytor_tekstu)) (dostęp z 30.12.2022 r.).

⁵ Zob. <https://pl.wikipedia.org/wiki/QR-Tekst> (dostęp z 30.12.2022 r.).

biorcy (bezpieczeństwo prawne). Głównym czynnikiem „wspomagającym” była łatwość tworzenia przesyłki elektronicznej w porównaniu z trudnością stworzenia poprawnie sformatowanego i wypełnionego treścią pisma „urzędowego”. Ułatwienie z jednej strony – potencjalne (aczkolwiek często nieuświadomione) zagrożenie z drugiej wyraźnie pokazywało przewagę owego ułatwienia nad bezpieczeństwem. Sama możliwość szybkiego, natychmiastowego przesłania jakichś treści choćby „na koniec świata” i oczywiście rozmowa o tym we własnych środowiskach skłaniała do zakładania kont pocztowych w różnych serwisach, bez nadmiernego rozważania nad tym, kto administruje serwerem pocztowym, jakie prawa i obowiązki ma każda ze stron umowy o świadczeniu usług, umowy często akceptowanej bez jej czytania...

Szczególne znaczenie miała też stale rosnąca mobilność pracowników, częstość zmiany miejsca pracy, konieczność dostosowania się do warunków nowego miejsca pracy. Stałymi elementami „środowiska pracy” były dokumenty papierowe, tworzone, przesyłane, przyjmowane, rejestrowane i przechowywane tradycyjnie, zgodnie z instrukcją kancelaryjną i archiwalną, ale już komunikacja między pracownikami (nawet nieformalna), dzięki stale upowszechniającej się możliwości wykorzystywania poczty elektronicznej, zarówno służbowej, jak i prywatnej (wielu w ogóle się nad tym nie zastanawiało) znacząco poprawiła przepływ informacji, jednocześnie znacząco zwiększając wolumen przesyłanych treści.

Dedykowane systemy wspomagające procesy realizowane przez administrację – etap 4

Kolejnym, istotnym kamieniem milowym w procesie przemiany administracji „papierowej” w „elektroniczną” była prawna możliwość tworzenia i wykorzystania w praktyce tzw. Systemów Obiegu Dokumentów (SOD, e-SOD itp.). Tak je nazywano, gdyż mentalnie ich twórcy, lecz bardziej użytkownicy ciągle pojmowali dokumenty jako obiekty będące w „obiegu” między pracownikami, obiegu kojarzonym z ruchem w przestrzeni kartezjańskiej – z punktu A do punktu B, pomiędzy pracownikami w różnej lokalizacji – jak w poczcie elektronicznej czy przesyłaniu dokumentów za pośrednictwem gońca – o tym jednak mowa będzie dalej z uwagi na inny mechanizm owego „obiegu”. Trudno było wyjaśnić pracownikom administracji, że to nie sam dokument przemieszcza się, znajduje się na serwerze w tym samym miejscu, ale dokonuje się proces tworzenia i przekazywania dostępu do tego dokumentu z różnego rodzaju uprawnieniami nadawanymi pracownikom (np. do odczytu, modyfikacji, komentowania itp.) z jednoczesnym rejestrowaniem w tle czasu i charakteru dokonywanych przez

kolejne osoby czynności, wraz z automatycznym zapisem kolejnych wersji.

Mentalnie pracownicy administracji fakt przekazania „dokumentu” kojarzyli ciągle z przemieszczaniem tego „dokumentu” w przestrzeni – bo zawsze tak działało się to z dokumentami papierowymi. Problem, jaki się pojawił, to zupełnie różne rozwiązania techniczne owych SOD-ów. Nie wypracowano bowiem wcześniej i nie ogłoszono standardów dokumentów, ich formatów, zakresów danych (i ich formatów!), właściwych w konkretnych sprawach, które to zakresy danych pokazywane byłyby we właściwych, czytelnie opisanych podzbiorach. Należy jednak zauważyć, że dostawcy owych „SOD-ów” w różnych sposób starali się upodobnić środowisko pracy (interfejs) do używanych wcześniej formularzy w formie tekstów w ramkach, z sekcjami umożliwiającymi wybór różnych parametrów czy wprowadzanie niezbędnych danych (data wybierana z kalendarza, następny w procedurze pracownik lub komórka organizacyjna z listy rozwijanej, różne pola jedno- lub wielokrotnego wyboru itd.).

Wynikiem wspomnianego problemu i niczym nieskrępowanej inwencji dostawców rozwiązań informatycznych była faktyczna niekompatybilność tworzonych systemów i niemożność stosunkowo prostego przenoszenia dokumentów, metadanych tych dokumentów, relacji między nimi i relacji do osób związanych z przetwarzaniem dokumentów (zapewnienie integralności i rozliczalności) do systemów innych producentów. Świadomość wspomnianego problemu była znaczącym czynnikiem spowalniającym proces przemiany administracji publicznej. Kierownicy podmiotów z jednej strony chcieli unowocześnić działanie podległych sobie podmiotów, jednak z drugiej strony obawiali się sytuacji, w której firma „komputeryzująca” z jakiegokolwiek przyczyny zaprzestanie świadczenia swoich usług i urząd pozostanie bez wsparcia, gdyż wtedy pojawi się nowy dostawca (z zupełnie innym w sensie wizualnym, a częściowo i innym funkcjonalnie produktem), który będzie chciał zaczynać całkowicie od nowa, od „pustej kartki”, konfiguracji swojego systemu, szkoleń wg innej filozofii działania innego systemu stworzonego dla realizacji teoretycznie tego samego celu, do jakiego służył system wcześniej używany. Jest wiadomo i wielokrotnie sprawdzono w praktyce, pracownicy nie chcą co kilka lat przechodzić z jednego systemu na drugi służący do realizacji tego samego zadania; jest to marnowanie energii, czasu, pieniędzy, żeby już o stratach informacji nie wspominać. W takich sytuacjach z reguły rynek zdobywały „elastyczne” firmy informatyczne, które potrafiły przejść niemal w całości zasób bazodanowy – zaimportować go do swojego systemu i zminimalizować wszelkie różnice mogące być przeszkodą w opanowaniu nowego systemu. Zawsze wiązało się to z pewnym nakładem pracy, ale pozwalało uratować w znacznym stopniu włożoną już pracę.

Początki nowego spojrzenia na „dokument” – etap 5

Jednocześnie, niejako w tle, trwała dyskusja użytkowników różnych, mniej lub bardziej zaawansowanych „SOD-ów” nad koniecznością stworzenia reguł, które pozwoliłyby ucivilizować dziki rynek dostawców systemów dedykowanych administracji przynajmniej w zakresie obiektów (podmioty, jednostki organizacyjne, identyfikowalni pracownicy, identyfikowalne dokumenty) i relacji między nimi w sposób umożliwiający z jednej strony zabezpieczenie się przed „zabetonowaniem się” dotychczasowego dostawcy (*vendor lock*), który mógł tak kształtować zakres i ceny swoich usług, by ich odbiorcy nie opłacało się przenosić do innego dostawcy, z drugiej, by – niezależnie od dostawcy, zachować pewną jednolitą filozofię postępowania z dokumentami w podmiocie. Właśnie, z „dokumentami”⁶. Problem w tym, że dokumentami zaczęto nazywać różne byty, byty o całkowicie innej fizycznej naturze – zarówno dające się dotknąć, ująć dłonią, jak i byty elektroniczne, widzialne jedynie na ekranie monitora. Ponadto mylono procedury komunikacyjne z dokumentami. Należało także mieć na względzie fakt, iż ostatecznie, zgodnie z ustawą z 14.7.1983 r. o narodowym zasobie archiwalnym i archiwach⁷ pewna część dokumentów (kategorii archiwalnej „A”) będzie musiała być przekazana do Archiwów Państwowych (AP). Pojawiło się naturalne w tej sytuacji pytanie – jak spójnie przekazywać do AP zbiory dokumentów należących do konkretnych spraw, by nie doszło do ich dezintegracji? Równie naturalnie pojawiła się na to pytanie odpowiedź: należy sprawy rozpoczęte „papierowo” kończyć także „papierowo”, a sprawy nowe, jeśli warunki techniczne stosowanego „SOD” już na to pozwalają, trzeba prowadzić „elektronicznie”. Kwestie techniczne i prawne dla tak rozdzielonych zasobów były już stosunkowo łatwe do uregulowania.

Na tym etapie rozwojowym e-administracji bardziej świadomi uczestnicy procesów tworzenia i przesyłania dokumentów zaczęli zastanawiać się nad problemem różnorodności punktów wejścia i wyjścia w całym procesie przetwarzania dokumentów – od ich wytworzenia czy wpłynięcia – do archiwizacji. Inaczej bowiem wygląda sprawa dokumentów wewnętrznych, gdzie wszystko daje się jednoznacznie uregulować, a inaczej, gdy różne strony pewnego procesu są na innych etapach technicznego rozwoju, a nawet rozumienia pojęć takich jak „dokument” czy „podpis” – i to zarówno w odniesieniu do dokumentów papierowych, jak i elektronicznych. Całość dokumentacji w danej sprawie powinna mieć taką samą, jednolitą postać – papierową lub elektroniczną. Ten problem również dało się pokonać względnie łatwo; wystarczyło uświadomić sobie oczywisty fakt, że istotą przekazu komunikacyjnego jest niesiona treść, a nie sam nośnik jako taki, gdyż służy on jedynie utrwaleniu treści. Nośnik spełnia więc jedynie rolę pomocniczą „pojemnika”

na niesioną treść. Nie ma znaczenia, jakiego rodzaju pojemnika czy nośnika użyjemy do przeniesienia informacji (treści dokumentu) przy zachowaniu kilku istotnych warunków: zapewnieniu niezmienności niesionej treści przekazu (integralność) oraz wiarygodnej rejestracji czynności wykonanych przez konkretne osoby w odniesieniu do tego dokumentu (rozliczalność).

Nowe regulacje dotyczące formatów dokumentów – etap 6

Wszystkie wspomniane problemy czy nawet tylko wątpliwości stały się asumptem do stworzenia stosownych regulacji dotyczących wspomnianych już formatów dokumentów, niezbędnych elementów struktury, wyjaśnienia, czym jest formularz, a czym wzór dokumentu... Można zatem stwierdzić, że stopniowo dopracowane zostały (w sensie technicznym i prawnym) niemal wszystkie elementy całego e-środowiska pozwalającego na tworzenie, przekazywanie, archiwizację jednoznacznych, czytelnych dokumentów wraz z niezbędnymi ich elementami, takimi jak różne rodzaje i typy podpisów elektronicznych.

Komunikacja elektroniczna to jednak pojęcie bardziej złożone – i w tym miejscu należy wskazać na inne rozwiązania, które w naturalnej konsekwencji uzupełniły paletę możliwości, jakie zostały oddane do dyspozycji interesantów i samych pracowników administracji.

Przede wszystkim znaczącą rolę odegrały strony podmiotowe strony WWW, podmiotowe strony BIP oraz strona główna BIP. Faktem jest, że wiarygodna informacja jest „artykułem pierwszej potrzeby” – istnieje na nią ciągle zapotrzebowanie tak silne, że niemal każdy jest skłonny przyjmować napływającą z dowolnego źródła informację i trzeba zwykle dłuższego czasu, by nauczył się odróżniać rzeczywistą informację i prawdę od jakiegokolwiek, nawet fałszywego przekazu. Umiejętność weryfikacji treści nie jest umiejętnością powszechną, podobnie jak umiejętność znajdowania właściwych, wiarygodnych źródeł. Autor niniejszego miał okazję brać udział w tworzeniu tzw. Białej Księgi BIP⁸ i pracach mających na celu stworzenie systemu, którego celem było udostępnianie informacji wiarygodnej, podawanej w sposób jednolity co do zakresu i formy tak, by nie trzeba było zastanawiać się nad przekazem, nad jego wiarygodnością, źródłem – i by było wiadomo, kto personalnie za ów przekaz odpowiada.

⁶ Zob. <https://epodrecznik.mc.gov.pl/mediawiki/index.php?title=Dokument> (dostęp z 30.12.2022 r.).

⁷ T.j. Dz.U. z 2020 r. poz. 164 ze zm.

⁸ Zob. https://bip2.wokiss.pl/koninip/zasoby/files/archiwum/biuletyn-informacji-publicznej/przyszlosc-bip/biala-ksiega-nowego-bip/biala_ksiega_nowego_bip.pdf (dostęp z 30.12.2022 r.).

Na tym etapie rozwoju systemów informacji publicznej (nierozzerwalnie związanych z systemami komunikacji elektronicznej) tym, co wymagało szczególnego wysiłku, było wyjaśnianie, czym jest „informacja”, a czym „quasi-informacja”, przekaz PR-owy, swoista reklama działalności danego podmiotu czy jego jednostek organizacyjnych. Pamiętać należy, że podmiotowe strony i podstrony WWW, chociaż tworzone były albo przez samo źródło informacji (np. urząd gminy), albo na zlecenie przez jakiś podmiot biznesowy, były zawsze budowane z intencją nie tylko przekazania informacji, ale miały tworzyć pozytywny wizerunek danego podmiotu. Wszystko „na plus”, bez pokazywania potknięć, niedoróbek, braków, słabości organizacyjnej... I ten przekaz nie był ograniczony praktycznie niczym; dowolna kolorystyka, czcionka, układ treści na stronie. Każda strona podmiotowa charakteryzowała się własną filozofią dostępu do przekazywanych treści. Inaczej miała się rzecz z Biuletynem Informacji Publicznej, którego zakres informacyjny wynikał z przepisów, a nawet sposób oznaczania Strony Podmiotowej BIP i jej wyróżnienie oraz powiązanie ze Stroną Główną BIP i podmiotową stroną WWW musiały być utworzone tak, by można było jednym kliknięciem pomiędzy tymi stronami się przemieszczać. To już tworzyło załączek pewnego porządku znacząco ułatwiającego docieranie do poszukiwanej informacji lub osoby za udostępnienie informacji odpowiedzialnej.

Systemy regionalne i ogólnopolskie – etap 7

Kolejnym etapem systemów komunikacji elektronicznej stały się regionalne „wrota”, obejmujące terytoria województw, np. Wrota Mazowska, Wrota Małopolski, Wrota Warmii i Mazur, Wrota Podlasia, SEKAP (dziś już nieistniejący System Elektronicznej Komunikacji Administracji Publicznej woj. śląskiego) itp., które jednak znacząco różniły się zarówno wyglądem, jak i zakresem informacyjnym.

Systemy te budowane były podobnie jak systemy miejskie, gminne, ale obejmowały swoim zakresem szerszy terytorialnie zakres e-usług świadczonych przez różne podmioty. Rzecz w tym, że nie wszystkie podmioty, które powinny były świadczyć e-usługi, były do tego właściwie przygotowane. Przez „właściwe przygotowanie” rozumie się tu udostępnienie e-usługi do jej realizacji w trybie on-line (całkowita realizacja usługi bez jakiegokolwiek udziału pracownika merytorycznego) lub off-line, z konieczną interakcją jednego lub więcej pracowników. Według podobnej filozofii działania jak system SEKAP zbudowany został system ogólnopolski – elektroniczna Platforma Usług Administracji Publicznej⁹ (ePUAP). System ten, od momentu jego produkcyjnego udostępnienia (2008 r.) był już kilku-

krotnie przebudowywany – zarówno jeśli chodzi o interfejs użytkownika, jego wygląd i kolorystykę, jak i zaimplementowane w nim mechanizmy. Przykładowo w pierwszej jego edycji osoba zakładająca konto nie mogła wybrać sobie niezajętego jeszcze loginu (unikatowego identyfikatora osoby fizycznej); był on narzucany i przyjmował postać trudnego do zapamiętania alfanumerycznego ciągu (liter alfabetu łacińskiego i cyfr). Sam system ePUAP, jako taki, traktowany był jako „trudna” poczta elektroniczna – bez rozumienia, że w istocie jest czymś innym – systemem świadczenia usług wyposażonym w różne dodatkowe mechanizmy zarządzania zasobami, tworzenia dokumentów elektronicznych na podstawie wzorów tychże, zamieszczonych w Centralnym Repozytorium Wzorów Dokumentów Elektronicznych (CRWDE), mechanizmu walidacji podpisu elektronicznego i innych (np. importowalnej listy Elektronicznych Skrzynek Podawczych). Nie ma tu potrzeby szerszego opisywania funkcjonalności ePUAP; istotne jest jedynie pokazanie kolejnego etapu rozwoju e-administracji, wykorzystującej rozbudowane funkcjonalności dostępne dla każdego, kto spełni elementarne wymagania – pozwoli się w sposób pewny „zidentyfikować systemowi” poprzez użycie loginu i hasła, i certyfikatu uzyskanego w ramach wiarygodnej procedury. Przez identyfikację „pewną” w sensie prawnym należy rozumieć identyfikację i uwierzytelnienie z wykorzystaniem np. tzw. Profilu Zaufanego lub podobnej procedury, zapewniającej udział zaufanej strony trzeciej w wytworzeniu certyfikatu podpisu elektronicznego. Celem wprowadzenia Profilu Zaufanego było stworzenie sytuacji, w której osoba fizyczna przedkładająca dokument w jakimkolwiek podmiocie realizującym zadania publiczne będzie mogła być jednoznacznie nie tylko zidentyfikowana, ale przedkładany dokument (lub zbiór dokumentów) zostanie zabezpieczony podpisem elektronicznym (w istocie jest to pieczęć elektroniczna ministra właściwego ds. informatyzacji, związana z danymi podpisującego) w sposób zapewniający integralność przesyłki i związaną jej z osobą wnioskodawcy.

Trzeba w tym miejscu podkreślić, że ePUAP od początku zaprojektowany został w sposób umożliwiający wysyłanie nawet bardzo dużych objętościowo zbiorów dokumentów (np. spakowany zbiór mógł mieć w pierwszej edycji systemu ePUAP objętość do 200 MB, a później do 500 MB); przesyłanie odbywało się za pośrednictwem mechanizmu FTP (File Transfer Protocol). Innymi słowy, w treści pisma ogólnego (często pełniącego także funkcję pisma przewodniego) znajdował się link (aktywny odnośnik) do pliku wysłanego mechanizmem FTP. Istotą tego rozwiązania było usunięcie ograniczeń dotyczących wielkości przesyłanych plików. Stosowane rozwiązania poczty elektronicznej, niez-

⁹ Zob. <https://epuap.gov.pl/wps/portal> (dostęp z 30.12.2022 r.).

leżnie od innego typu zagrożeń bezpieczeństwa informacji, nie pozwalały na przesyłanie plików o wspomnianej wyżej objętości.

Wymienione do tej pory rozwiązania wprowadzane były do praktyki administracji publicznej w sposób miękki, w oparciu na argumente ergonomii, ułatwień mających zwiększać sprawność administracji, narzędzi i środków komunikacji znanych z zastosowań prywatnych (poczta elektroniczna). Wprowadzanie do przepisów prawa owych ułatwień zacierało różnice pomiędzy sferą prywatną a służbową, co mogło prowadzić do różnego rodzaju zagrożeń dla poufności informacji (przesyłanie dokumentów służbowych na prywatne konta i rozsyłanie ich bez zachowania rozliczalności, co potencjalnie mogło skutkować lub skutkowało tzw. wyciekami – naruszeniem ochrony należnej danym osobowym i innym danym chronionym odrębnymi przepisami).

Co gorsza, wspomniana wcześniej mobilność pracowników i wybory polityczne, wprowadzanie na stanowiska urzędnicze (w tym decyzyjne) osób niemających przygotowania do pracy w administracji, nierozumiejących zależności działania administracji i ochrony informacji od procedur, stosowanych narzędzi i umiejętności posługiwania się nimi prowadziło do dość chaotycznego wdrażania rozwiązań poprzez np. narzucanie przez szefów systemów znanych im z poprzedniego miejsca pracy lub wdrażanych jedynie z uwagi na fakt, że dany system używany był w jednostce nadrzędnej. Argumentem za zastosowaniem takiego czy innego rozwiązania była raczej marka i czas istnienia na rynku danego dostawcy niż rzeczywiste walory konkretnego rozwiązania. Należy w tym miejscu wskazać np. walkę rynkową pomiędzy różnego rodzaju dostawcami edytorów tekstu czy arkuszy kalkulacyjnych oraz systemów bazodanowych, nawet rodzimej, polskiej produkcji, a rozwiązaniami firm światowych – dotyczyło to wszelkich produktów, nie tylko IT.

Mobilność pracowników i odmiejscowienie usług – etap 8

Pojawianie się na rynku urządzeń mobilnych – laptopów, notebooków, tabletów i smartfonów uruchomiło kolejną falę przemian w konstrukcji aplikacji – nie tyle przeznaczonych dla pracowników administracji, ile dla klientów administracji, obywateli, by mogli w dogodniejszy dla siebie sposób komunikować się z administracją dowolnego szczebla.

W tym miejscu należy zwrócić uwagę na fakt „samoobrony” niektórych obszarów przetwarzania informacji przed zmianami zgodnymi z ogólnymi tendencjami rozwojowymi informatyki i postępem technicznym; zjawisko to można zaobserwować w odniesieniu do systemów dedykowanych, zbudowanych do przetwarzania danych

w pewnym, dającym się wyróżnić obszarze, np. ubezpieczeniach społecznych (np. PUE ZUS), w sądownictwie (np. systemy rejestrów sądowych, rejestry dedykowane dla przedsiębiorców itp.). Każdy resort czy urząd centralny tworzył rozwiązania mające umożliwić pełne zarządzanie danymi i dokumentami w jego silosowym rozwiązaniu. Od pewnego czasu trwa proces łączenia owych silosowych rozwiązań pod wspólnym „patronatem” czy może wspólną myślą przewodnią KPRM, co przejawia się w ujednoceniu interfejsów, kolorystyce rozwiązań, podobieństwie ikon, a przede wszystkim w stosowaniu tego samego narzędzia identyfikacji – Profilu Zaufanego, który na pewnym etapie został wyodrębniony z ePUAPu właśnie w celu stworzenia jednego sposobu logowania się do różnych rozwiązań odrębnych, stworzonych w latach wcześniejszych i możliwości podpisywania składanych dokumentów – tak jak musi się to odbywać przy realizacji usług elektronicznych.

W omawianym okresie (od końcowych lat 90. XX w.), z uwagi na znaczące zróżnicowanie zaawansowania technologicznego podmiotów przygotowujących się do świadczenia e-usług lub już usługi te świadczących, wielokrotnie dochodziło do nieporozumień wynikających z odmiennych interpretacji pojęć takich jak „dokument”, „dokument elektroniczny”, „elektroniczne odwzorowanie”, „wzór dokumentu”, „podpis”, „podpis elektroniczny” (przez jednych nazywany „certyfikowanym”, przez innych „kwalifikowanym” itp.). Obserwacja owych różnic w pojmowaniu istoty wspomnianych pojęć skłoniła autora niniejszego artykułu do opracowania sieciowego e-Podręcznika¹⁰ zawierającego obowiązujące definicje wynikające bezpośrednio z przepisów prawa, jeśli takowe istniały. W wielu jednak przypadkach trzeba było odwołać się do Wikipedii (pojęcia techniczne, takie jak base64, MD5, SHA-256 itp.). Istnieje też wiele pojęć, a nawet opisów technicznych, które również wymagały komentarza. Komentarze i opisy pozwoliły wyjaśnić pozorne niezgodności definicyjne, a także praktycznie wyjaśnić pojęcia związane z e-usługami tak, by w razie wątpliwości można było wybrać właściwy sposób realizacji e-usługi lub stwierdzić jej wiarygodność, ustalić, kto i na jakiej podstawie z usługi może skorzystać. Podręcznik jest aktualizowany, gdyż, jak to już było wcześniej opisane, prawo stale zmienia się nadążnie za nowymi osiągnięciami techniki – szczególnie w obszarach związanych z mobilnością i stosowanymi narzędziami identyfikacji i walidacji.

Ostatnie trendy wyraźnie pokazują, że ogromna część e-usług (na realizację e-usługi składają się między innymi usługa komunikacji elektronicznej, usługa identyfikacji stron i walidacji podpisu) może być realizowana za pomocą urządzeń powszechnie już dostępnych dla każdego; jedy-

¹⁰ Zob. <https://epodrecznik.mc.gov.pl> (dostęp z 30.12.2022 r.).

ne, co jest potrzebne, to umiejętność ich użytkowania – a to elementarne przeszkolenie zapewniają z reguły członkowie najbliższego otoczenia. Umiejętności korzystania z tabletów, a szczególnie smartfonów i wykorzystywania udostępnionych e-usług zdobywane są w sposób najbardziej naturalny, bez jakichkolwiek kursów i szkoleń – inaczej, niż działo się to w przypadku korzystania z komputerów. Taki stan rzeczy, przy równoczesnym porządkowaniu zasobów bazodanowych, zarówno gminnych, jak i w rozwiązaniach silosowych (dedykowanych, budowanych w oderwaniu od pierwotnych źródeł danych, a korzystających z danych deklaracyjnych) umożliwia tworzenie aplikacji smartfonowych, w tym aplikacji wykorzystujących dokumenty elektroniczne (dokumenty zestrukturizowane w formacie xml, których zawartość może być analizowana przez odpowiednio skonstruowane systemy informatyczne, automatycznie sięgające do rejestrów, „umiejące” analizować dane i na podstawie właściwych algorytmów podejmować stosowne działania).

W kontekście powyższego wyraźnie widoczna staje się pewna odmienność działania administracji publicznej i sądownictwa, bardzo zachowawczego i wyraźnie separującego się od ogólnego trendu rozwojowego dotyczącego wykorzystywania środków komunikacji elektronicznej oraz dokumentów elektronicznych, tak jakby niemożliwe było utrzymywanie się w ogólnym tempie zmian wynikających z postępu technicznego. Dokument o zapewnionej integralności zawsze będzie dokumentem o zapewnionej integralności – niezależnie od miejsca jego wytworzenia ani treści w nim zapisanych. System informatyczny zapewniający rozliczalność działań jego użytkowników będzie takim systemem niezależnie od tego, czy będzie stosowany w administracji, bankowości czy sądownictwie. Portal Rejestrów Sądowych, udostępniony 1.7.2021 r. przez Ministerstwo Sprawiedliwości na podstawie ustawy z 4.4.2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych¹¹ umożliwia już całkowicie elektroniczne składanie wniosków. Nastąpiło to niemal 20 lat po przyjęciu ustawy z 18.9.2001 r. o podpisie elektronicznym¹² uchylonej później ustawą z 5.9.2016 r. o usługach zaufania oraz identyfikacji elektronicznej¹³. W tym kontekście może dziwić trwanie w przypadku pism procesowych przy archaicznych, znacznie słabszych, a przede wszystkim kosztownych i uciążliwych sposobach postępowania z dokumentami – potrzebą ich własnoręcznego podpisywania.

Podsumowanie

Obserwując całe spektrum zmian od 1991 do 2022 r., można dostrzec bardzo wyraźnie zmiany roli narzędzi in-

formatycznych w dowolnym obszarze (gromadzenie i analiza danych, zabezpieczanie dokumentów w sensie ich integralności i niezaprzeczalności, przesyłanie dokumentów i ich archiwizację oraz wielu innych) z czysto technicznych – w kompleksowe systemy, bez których wiele dzisiaj naturalnych usług e-administracji (tzw. usługi on-line, realizowane bez bezpośredniego działania urzędnika) nie byłoby możliwych do wykonania. Jeśli np. dzisiaj możemy, znajdując się w dowolnym miejscu świata, pod warunkiem dostępu do internetu skorzystać z usług własnego banku, urzędu gminy czy z rejestrów centralnych (np. zaświadczenie o zameldowaniu na pobyt stały), czy nawet aplikacji mobilnych takich jak mObywatel, w ramach których możemy uzyskać istotne dokumenty, takie jak Unijny Certyfikat Covid, eReceptę, mPrawo Jazdy, mPojazd itp., a nawet bilety kolejowe, widzimy, jaką drogę musiało przejść nasze mentalne oderwanie się od papieru jako nośnika informacji.

W świetle powyższego bardzo niekorzystnie prezentuje się wynik analizy orzecznictwa dotyczącej wnoszenia pism procesowych, który prowadzi do wniosku, że dopuszczalne jest wniesienie pisma procesowego drogą elektroniczną lub opatrzenie go podpisem elektronicznym – w każdej z procedur sądowych, jednak pismo to wywoła skutek dopiero po uzupełnieniu jego braku formalnego poprzez własnoręczne podpisanie przez wnoszącego. Wówczas pismo zostanie uznane za złożone z datą sporządzenia jego wydruku przez pracownika sądu¹⁴. Skoro wiemy, że wszystkie elementy związane z rejestracją czasu jakiegoś zdarzenia (np. wniesienie pisma), z jego integralnością, z rozliczalnością całego procesu – dzięki powszechności profilu zaufanego, łatwości uzyskania certyfikatu kwalifikowanego służącego do składania podpisu kwalifikowanego, upowszechnianiu się podpisu osobistego jesteśmy w stanie kontrolować i weryfikować z dokładnością do 1 sekundy, utrzymywanie tego typu relikwów wiążących człowieka z jakimś punktem w przestrzeni, z kartką papieru drukowaną przez pracownika sądu przypomina związanie chłopca pańszczyźnianego z rolą, odebranie swobody zarządzania czasem, najcenniejszym, bo nieodnawialnym zasobem. Korzyścią jednak wypływającą z tej analizy jest wyraźne uwidocznienie, gdzie i co powinno ulec w polskim prawie zmianie, by – bez zmiany celu – osiągać go szybciej, taniej, zgodnie z potrzebami i aspiracjami rozwiniętego społeczeństwa informacyjnego.

¹¹ Dz.U. poz. 848.

¹² Dz.U. Nr 130, poz. 1450.

¹³ Dz.U. poz. 1579.

¹⁴ A. Mejka, Składanie pism procesowych drogą elektroniczną, Lex/el. 2020.

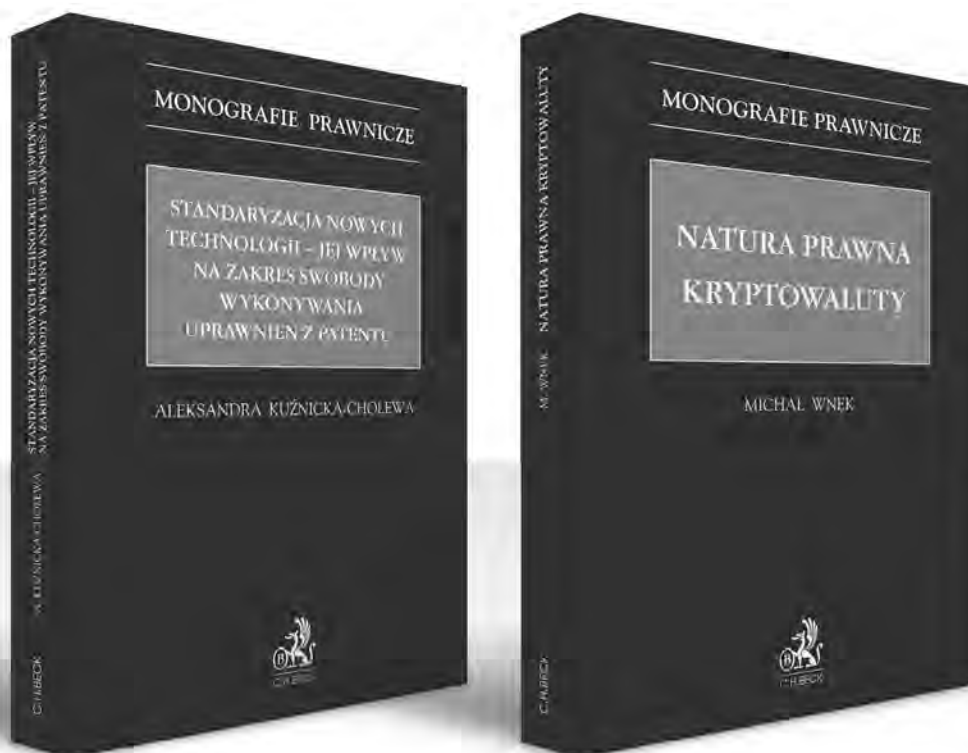
Słowa kluczowe: e-administracja, ewolucja prawa, prawo informatyczne, informatyzacja.

Quarter of a century of evolution of law in the context of the development of digital technologies and social aspirations

In the present article, the author – who worked in public administration (independently from simultaneous scientific and educational work connected with the use of computer science in different areas) for over a quarter of a century, directly and actively took part in its transformation from a completely “paper” to completely “digital” system in different areas – shares his experience. The article is a retrospective attempt to describe his observations and experience.

Key words: e-administration, evolution of law, legal informatics, computerisation.

Monografie Prawnicze



ksiegarnia.beck.pl

Zadzwonić: 81 46 13 300 • E-mail: kontakt@beck.pl



Projekt ustawy o wolności słowa w internetowych serwisach społecznościowych – remedium na walkę z bezprawnymi treściami?

Kamila Brylak-Hudyma¹

Walka z nielegalnymi treściami udostępnianymi na platformach internetowych jest aktualnym i palącym tematem, z którym ustawodawstwa krajowe, jak też europejskie próbują się zmierzyć. Dotychczasową i podstawową regulacją w przedmiocie platform internetowych była dyrektywa e-Commerce, a w polskim porządku prawnym dodatkowo ustawa o świadczeniu usług drogą elektroniczną. W ostatnich miesiącach nader często dochodziło do usuwania, blokowania nie tylko publikowanych na portalach społecznościowych treści, ale także kont użytkowników tychże portali. W ocenie niektórych środowisk takie arbitralne działania i decyzje platform społecznościowych stanowią zagrożenie dla wolności słowa gwarantowanej w Konstytucji RP oraz Europejskiej Konwencji Praw Człowieka. Na szczęblu unijnym trwają prace nad rozporządzeniem w przedmiocie określenia zasad przejrzystości decyzji dotyczących moderacji treści (Digital Service Act). Niemniej po ogłoszeniu projektu rozporządzenia Digital Service Act Ministerstwo Sprawiedliwości złożyło projekt ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych mającej na celu walkę z bezprawnymi treściami na platformach społecznościowych. Niniejszy artykuł ma na celu przedstawienie i omówienie najważniejszych regulacji dotyczących tej ustawy wraz z uwzględnieniem ryzyk i wątpliwości wiążących się z ewentualnym przyjęciem ustawy.

Uwagi wstępne

Podkreślanie roli, jaką platformy społecznościowe odgrywają w obecnych czasach, wydaje się truizmem. Świadczą o tym chociażby dane przedstawione w raporcie Hootsuite „Digital 2022”. W Polsce z Internetu korzysta 32,86 mln, co stanowi niemal 87% całkowitej populacji. W styczniu 2022 r. odnotowano 27,20 mln użytkowników social mediów, co stanowiło blisko 72% całkowitej populacji. Wskazano także, że liczba użytkowników social mediów w porównaniu do 2021 r. wzrosła o 1,3 mln². Używanie social mediów należy już raczej do monotonii dnia. Często zaraz po przebudzeniu niemal nałogowo sprawdza się powiadomienia, wiadomości i aktualności na serwisach społecznościowych. Co więcej, trudno wyobrazić sobie codzienne funkcjonowanie bez tego medium. Świadczyć może o tym chociażby sytuacja, która zdarzyła się 4.10.2021 r. Nastąpiła wówczas tzw. wielka awaria Facebooka (obecnie Mety), a za nim także Instagrama, Whats Appa, Messengera, w trakcie której kilka miliardów użytkowników straciło na kilkanaście godzin dostęp do swoich kont³. Co ciekawe, za utratę dostępu do kont obwiniano sam Internet (dostawców Internetu), a nie błąd czy problemy techniczne po stronie platform. Oznacza to, że dla wielu platformy są „trwalsze” niż sam Internet. Poza tym nie można zapomnieć, jak ważne są te platformy dla biznesu. Każda chwila uniemożliwiająca dostęp do Facebooka (Mety) czy Instagrama stanowi wymierne straty⁴. Niemniej oprócz zapewne wielu pozytywnych aspektów funkcjonowania social mediów nie można zapomnieć o zagrożeniach z nimi

związanych. W ostatnich latach szczególnie podkreśla się negatywny wpływ platform na zdrowie psychiczne, zwłaszcza młodych ludzi, którzy nieustannie porównują się do zakłamanej w social mediach rzeczywistości i sztucznych ideałów⁵, a wiele osób powtarza niezwyfikowane informacje, przez co w społeczeństwie rozwija się dezinformacja. Było to silnie widoczne w czasie pandemii COVID-19, kiedy w Internecie pojawiały się zagrażające zdrowiu sposoby na walkę z wirusem, np. „picie wybielaczy lub czystego alkoholu może wyleczyć zakażenie koronawirusem”, „instalacje sieci 5G sprzyjają rozprzestrzenianiu się wirusa”⁶. Zgodnie z wynikami raportu pt. Dezinformacja w sieci, według analizy wiarygodności kanałów informacyjnych przygotowanej przez IAB Polska, opublikowanej w lipcu 2018 r., ponad połowa internautów zapytanych, gdzie najczęściej zdarzało im się natrafić na nieprawdziwe informacje, wskazywała media społecznościowe.

¹ Doktorantka w jednostce naukowo-badawczej Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej (CBKE) działającej w ramach Uniwersytetu Wrocławskiego. ORCID: 0000-0002-2631-7159.

² Zob. <https://datareportal.com/reports/digital-2022-poland> (dostęp z 6.6.2022 r.).

³ Zob. <https://polskatimes.pl/awaria-facebook-co-sie-stalo-nie-dzialaly-tez-instagram-messenger-i-whatsapp/ar/c1-15835813> (dostęp z 6.6.2022 r.).

⁴ Zob. <https://spidersweb.pl/2021/10/awaria-facebook-nie-dziala-paraliz.html> (dostęp z 6.1.2022 r.).

⁵ Zob. <https://cyberdefence24.pl/bezpieczenstwo-informacyjne/facebook-od-dawna-wie-ze-instagram-jest-toksyczny-dla-nastolatkow> (dostęp z 6.6.2022 r.).

⁶ Zob. https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_pl#przyklady-dezinformacji (dostęp z 26.6.2022 r.).

Media społecznościowe są zatem głównym źródłem nieprawdziwych informacji z kraju i ze świata⁷. Były one wskazywane przez 58% pytanym, drugie miejsce (39%) zajęły portale informacyjne. Co więcej, serwisy społecznościowe umożliwiają szerzenie treści nielegalnych i tych uznanych za szkodliwe, ponieważ ich bieżące usuwanie czy blokowanie z uwagi na ich ilość zdaje się zgoła niemożliwa, a algorytmy nie są w stanie zweryfikować wszystkich naruszeń. Ponadto pojawiła się obawa, że monopolistyczne platformy staną się zagrożeniem dla podstawowych praw i wolności obywatelskich, jak swoboda i wolność wypowiedzi czy swoboda prowadzenia działalności gospodarczej. Nic więc dziwnego, że poszczególne państwa⁸ postanowiły wprowadzić własne regulacje w przedmiocie uregulowania serwisów społecznościowych. W ślad za nimi poszło polskie Ministerstwo Sprawiedliwości, które chwilę po ogłoszeniu przez KE – w grudniu 2020 r. – projektu rozporządzenia Digital Service Act⁹ (DSA) przedstawiło pierwszą wersję swojej propozycji, mającej na celu uregulowanie rynku usług cyfrowych¹⁰.

Dlaczego temat regulacji platform stał się istotny?

Rola platform społecznościowych znacząco ewoluowała. Początkowo miały głównie pełnić funkcję komunikatora dla osób, które na co dzień nie mają ze sobą kontaktu i nie mogą utrzymywać relacji. Poprzez umożliwienie tworzenia kont, a następnie udostępnianie na nich zdjęć, filmów, relacji użytkownicy portali mogą natychmiast dzielić się ze światem swoją prywatnością. Jednakże obecnie poprzez platformy społecznościowe publikowane są nie tylko zdjęcia czy nagrania z wakacji, z rodzinnych wyjazdów, imprez okolicznościowych. Platformy te są teraz miejscem do wyrażania opinii, recenzji, poglądów, a także do przekazywania i rozpowszechniania informacji o aktualnych wydarzeniach z kraju i świata. Jeśli przekazywane informacje byłyby wiarygodne i rzetelne, a wyrażane w komentarzach opinie nie szerzyłyby mowy nienawiści, treści o charakterze terrorystycznym, stanowiąc forum do dyskusji, wówczas wirtualny świat tworzony przez platformy społecznościowe przypominałby idyllę. Niestety, rzeczywistość jest zgoła inna.

Aktualny stan prawny w zakresie świadczenia usług drogą elektroniczną, w tym w szczególności udostępnianiu internetowych serwisów społecznościowych, reguluje przede wszystkim ustawa z 18.7.2002 r. o świadczeniu usług elektroniczną¹¹, wdrażająca dyrektywę 2000/31/WE z 8.6.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego na rynku wewnętrznym („dyrektywa o handlu elektronicznym”)¹². Mając na uwadze rozwój Internetu, a przy tym platform społecznościowych, których rola w globalnym

i industrialnym społeczeństwie znacząco wzrosła, wydaje się, że obowiązujące regulacje (zarówno unijne, jak i krajowe) zdają się przestarzałe i nie odpowiadać na aktualne problemy w sieci. Z jednej strony istnieje zagrożenie, że nielegalne treści nie będą niezwłocznie usuwane z platformy, ale z drugiej strony jest obawa, że prywatna platforma będzie usuwała treści arbitralnie, naruszając tym samym prawo do wolności słowa zagwarantowane chociażby w art. 54 Konstytucji RP oraz w art. 10 Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności. Pojawia się więc pytanie, kto, w jaki sposób powołany, za pomocą jakich mechanizmów powinien stać na straży wolności słowa, a jednocześnie bezpieczeństwa udostępnianych w Internecie treści.

Prace nad projektem

Podczas konferencji prasowych, mających miejsce 17.12.2020 r. oraz 15.1.2021 r., Minister Sprawiedliwości zapowiedział projekt ustawy mającej na celu ochronę wolności słowa na internetowych serwisach społecznościowych. Informacja ta stała się medialną sensacją i rzekomo m.in. ze względu na liczne zapytania ze strony prasy i innych zainteresowanych stron, w lutym 2021 r. na stronie rządowej Ministerstwa Sprawiedliwości został opublikowany tekst projektu ustawy pt. Ustawa o ochronie wolności użytkowników serwisów społecznościowych¹³. Po wielu tygodniach oczekiwania, tj. 27.9.2021 r., projekt ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych został wpisany do wykazu prac Rady Ministrów pod numerem UD293¹⁴, wywołując tym samym ponowne poruszenie opinii publicznej. Niemniej 10.1.2022 r. opublikowano nową

⁷ Krajowa Rada Radiofonii i Telewizji: „Fake news – dezinformacja online próby przeciwdziałania tym zjawiskom z perspektywy instytucji międzynarodowych oraz wybranych państw UE, w tym Polski”, Warszawa 2018.

⁸ Tak np. niemiecka ustawa NetzDG – Network Enforcement Act (dalej jako: niemiecka ustawa lub NetzDG), <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html> (dostęp z 6.1.2022 r.); Francja – ustawa o zwalczaniu manipulowania informacją z 22.12.2018 r. (dalej jako: francuska ustawa), <https://www.legifrance.gouv.fr/eli/loi/2018/12/22/2018-1202/jo/texte> (dostęp z 26.6.2022 r.).

⁹ Pl.: „Akt o usługach cyfrowych”.

¹⁰ Z uwagi na ramy niniejszego artykułu i w celu zachowania przejrzystości, autorka nie będzie odnosiła się do treści o charakterze przestępnym, zdefiniowanych w art. 3 ust. 1 pkt 6.

¹¹ T.j. Dz.U. z 2020 r. poz. 344 ze zm.; dalej jako: ŚwUsłElekU. Istotną rolę w tym zakresie odgrywa również Kodeks cywilny, ustawa z 16.7.2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2022 r. poz. 1648 ze zm.; dalej jako: PrTelU) oraz ustawa z 10.5.2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019 r. poz. 1781 ze zm.).

¹² Dz.Urz. WE L Nr 178, s. 1; dalej jako: dyrektywa E-commerce.

¹³ Zob. <https://www.gov.pl/web/sprawiedliwosc/zachecamy-do-zapoznania-sie-z-projektem-ustawy-o-ochronie-wolnosci-uzytownikow-serwisow-spoecznościowych> (dalej jako: projekt UWSł albo projekt), (dostęp z 22.5.2022 r.).

¹⁴ Zob. <https://legislacja.rcl.gov.pl/projekt/12351757/katalog/12819479#12819479> (dostęp z 22.5.2022 r.).

wersję projektu ustawy z 3.1.2022 r. wraz ze zmodyfikowanym uzasadnieniem projektu¹⁵. Żadnych uwag do projektu nie złożył KRS, NSA oraz PK, natomiast RPD zadeklarował, iż przedmiot projektowanej regulacji pozostaje poza zakresem jego właściwości. Natomiast uwagi zostały zgłoszone przez KRRIT, RMIŚP, RPO, SN, UKE, UODO, UOKIK.

Uzasadnienie projektu

W uzasadnieniu projektu (zarówno do wersji projektu z 2021 r., jak i 2022 r.) podkreślono, że prawda jest fundamentalnym prawem człowieka stanowiącym o godności człowieczeństwa i chronionym przez wiele dokumentów, a zjawisko masowego blokowania treści w przestrzeni internetowej wymaga wprowadzenia narzędzi, które zapewnią ochronę wyrażonej w art. 54 Konstytucji RP zasady wolności wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji. Podkreślono, iż mimo że w doktrynie prawa konstytucyjnego wolność wypowiedzi gwarantowana w art. 54 Konstytucji RP jest wartością fundamentalną dla państwa prawa, nie jest wartością absolutną¹⁶. Ograniczenia wolności wypowiedzi mogą pochodzić z instrumentów prawnych przewidzianych w zakresie zarówno prawa prywatnego, jak i prawa karnego¹⁷. Wszelka ingerencja w upowszechnione treści, będąca niewątpliwie formą ograniczenia konstytucyjnych wolności, może zostać wprowadzona pod warunkami określonymi w art. 31 ust. 3 Konstytucji RP. Zgodnie z treścią tej regulacji ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego bądź dla ochrony środowiska, zdrowia i moralności publicznej albo wolności i praw innych osób. Co istotne, ograniczenia te nie mogą naruszać istoty wolności i praw. Niemniej w uzasadnieniu projektu nie odniesiono się do art. 10 Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności¹⁸ (EKPC). Wnioskodawca podkreśla, że informacje umieszczane przez użytkowników portali społecznościowych są często uważane za najważniejsze źródło wiedzy w przedmiocie aktualnych wydarzeń dla szerokiej części społeczeństwa. Ponadto stanowią relevantne miejsce, w którym może się odbywać debata dotycząca aktualnych zagadnień społecznych i politycznych. Dlatego też wnioskodawca wskazuje, że „kluczowe znaczenie ma zatem przeciwdziałanie arbitralnemu oraz bezpodstawnemu izolowaniu określonych podmiotów od podstawowych źródeł informacji, funkcjonujących szeroko w obecnym życiu publicznym”¹⁹. Głównym celem projektu UWSł jest zapewnienie warunków dla zagwarantowania wolności wypowiedzi, zapewnienie prawa do prawdziwej informacji, poprawa ochrony wolności i praw człowieka w udostępnianych w Polsce internetowych serwisach społecznościowych oraz przestrzeganie przez nie wolności do wyrażania poglądów,

opinii, pozyskiwania informacji, rozpowszechniania informacji, wyrażania przekonań religijnych, światopoglądowych i filozoficznych oraz wolności komunikowania się²⁰. Według wnioskodawcy portale społecznościowe notorycznie usuwają arbitralnie treści publikowane przez ich użytkowników, które nie powinny zostać usunięte. Takie postępowanie portali ma stanowić przykład naruszania konstytucyjnie gwarantowanych wolności i praw innych osób. Stąd też relevantnym celem projektu UWSł jest zapewnienie użytkownikom portali ochrony przed wymierzonymi w nich „bezprawnymi działaniami, które nie mieszczą się w realizacji wolności wyrażania opinii, a tym samym nie mogą korzystać z ochrony prawnej”²¹. Sposobem urzeczywistnienia ww. celów mają być przede wszystkim przewidziane w projekcie UWSł regulacje dot. Rady Wolności Słowa, instytucja zaufanych podmiotów sygnalizujących nowe obowiązki dla platform, w tym m.in. obowiązek sprawozdawczy, kary pieniężne oraz instytucja tzw. ślepego pozwu.

Rada Wolności Słowa

Rada Wolności Słowa (RWS), zgodnie z art. 4 projektu, ma być organem administracji publicznej stojącym na straży przestrzegania przez usługodawców²² wolności do wyrażania poglądów, pozyskiwania informacji, rozpowszechniania informacji, wyrażania przekonań religijnych, światopoglądowych i filozoficznych oraz wolności komunikowania się. Ma ona być organem objętym sześcioletnią kadencją i składać się z Przewodniczącego i czterech członków, wobec których projekt przewiduje pewne wymagania, jak: wyłącznie polskie obywatelstwo, korzystanie z pełni praw publicznych, pełną zdolność do czynności prawnych, niekaralność, brak powiązań z organami bezpieczeństwa państwa w rozumieniu art. 2 ustawy z 18.10.2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944–1990 oraz treści tych dokumentów²³ w okresie od 22.7.1944 r. do 31.7.1990 r.; nieposzlakowaną opinię, wyższe wykształcenie prawnicze lub niezbędną wiedzę w zakresie językoznawstwa

¹⁵ Zob. <https://legislacja.rcl.gov.pl/projekt/12351757/katalog/12819479#12819479> (dostęp z 22.5.2022 r.).

¹⁶ L. Garlicki, Konstytucja Rzeczypospolitej Polskiej. Komentarz, Warszawa 2016.

¹⁷ Uzasadnienie projektu UWSł z 3.1.2022 r., s. 1–2, [za:] wyrok TK z 11.10.2006 r., P 3/06, Legalis.

¹⁸ Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie 4.11.1950 r., zmieniona następnie Protokołami Nr 3, 5 i 8 oraz uzupełniona Protokołem Nr 2 (Dz.U. z 1993 r. Nr 61 poz. 284).

¹⁹ Uzasadnienie projektu UWSł z 3.1.2022 r., s. 4.

²⁰ Art. 1 projektu.

²¹ Zob. uzasadnienie projektu z 3.1.2022 r., s. 7.

²² Osoby fizyczne, osoby prawne albo jednostki organizacyjne nieposiadające osobowości prawnej, które świadczą usługę internetowego serwisu społecznościowego (art. 3 pkt 1 projektu).

²³ T.j. Dz.U. z 2021 r. poz. 1633 ze zm.

lub nowych technologii. Zgodnie z uzasadnieniem projektu UWSł wszystkie ww. wymagania muszą zostać spełnione kumulatywnie. Niemniej członkiem RWS nie może być minister, sekretarz stanu, podsekretarz stanu, poseł, senator, poseł do PE, a także radny, wójt (burmistrz, prezydent miasta), zastępca wójta (burmistrza, prezydenta miasta), sekretarz gminy, skarbnik gminy, członek zarządu powiatu, sekretarz powiatu, skarbnik powiatu, członek zarządu województwa, skarbnik województwa, sekretarz województwa oraz osoba należąca do partii politycznej lub osoba, której interesy mogą pozostawać w konflikcie z pełnieniem funkcji członka RWS (zob. art. 6). Według założeń projektu członkowie RWS mają być powoływani przez Sejm RP większością 3/5 głosów w obecności co najmniej połowy ustawowej liczby posłów na wspólną kadencję. Natomiast jeśli w pierwszym głosowaniu kandydat na członka RWS nie uzyskał większości 3/5 głosów albo zgłoszono więcej niż jednego kandydata na członka Rady, a żaden z kandydatów nie uzyskał większości 3/5 głosów, wówczas głosowanie przeprowadza się ponownie, ale Sejm RP powołuje członka RWS już zwykłą większością głosów. Kandydaci na członka RWS zgłaszani są Marszałkowi Sejmu, który najpóźniej na dwa miesiące przed końcem kadencji członków RWS obwieszcza o możliwości składania przez kandydatów zgłoszeń o powołanie do Rady. Do zgłoszenia kandydatów uprawniona jest grupa co najmniej 2000 obywateli RP, którzy ukończyli osiemnaście lat, mają pełną zdolność do czynności prawnych i korzystają z pełni praw publicznych. W tym przypadku nie ma już wymagania, aby w skład grupy wchodziły jednostki, które mają wyłącznie polskie obywatelstwo, ale z brzmienia regulacji wynika, że zagraniczne podmioty, zamieszkujące na terenie Polski, nie będą uprawnione do zgłaszania kandydatów na członków RWS. Projekt przewiduje zamknięty katalog sytuacji, w jakich może dojść do wygaśnięcia członkostwa w RWS – analogicznie ma to miejsce, w sytuacji gdy choć jedna z ww. kryteriów przewidzianych dla kandydatów na członka RWS zostanie naruszona, np. członek nabędzie obywatelstwo innego państwa. Ponadto członkostwo w RWS wygasa z upływem 30 dni od dnia złożenia rezygnacji. Wygaśnięcie członkostwa w RWS niezwłocznie stwierdza postanowieniem Marszałek Sejmu RP. W przypadku wygaśnięcia członkostwa w RWS powołuje się nowego członka na okres, jaki pozostaje do dnia upływu trwającej kadencji członków RWS.

Co istotne, w art. 4 wskazano, iż Przewodniczący prowadzi listę ekspertów RWS, do których RWS może się zwrócić o sporządzenie opinii, gdy na potrzeby postępowania potrzebuje wiadomości specjalnych. Ekspert ma siedem dni na wydanie decyzji²⁴. Ekspertem RWS może być osoba, która korzysta z pełni praw publicznych, ukończyła 25 lat, posiada teoretyczne i praktyczne wiadomości specjalne, w szczególności z zakresu medycyny, prawa, praw człowieka, językoznawstwa, rynku finansowego, bezpieczeństwa publicznego,

informatyki i telekomunikacji²⁵, daje rękojmię należytego wykonywania obowiązków eksperta Rady oraz wyrazi pisemną zgodę na sprawowanie tej funkcji. W ust. 4 art. 14 projektodawca wskazał podmioty, które mogą zgłaszać kandydatów na ekspertów²⁶.

Nie można także pominąć regulacji dotyczących postępowania przed RWS, które zostały umieszczone w rozdziale 6 projektu. Niemniej, w celu zachowania przejrzystości niniejszego artykułu, postępowanie to zostanie przybliżone w dalszej części artykułu.

Zaufane podmioty sygnalizujące

Institucja zaufanych podmiotów sygnalizujących ma działać w interesie publicznym w celu przeciwdziałania dezinformacji rozpowszechnianej za pośrednictwem internetowych serwisów społecznościowych. W celu dokładniejszej analizy roli zaufanych podmiotów sygnalizujących w walce o bezpieczne portale społecznościowe autor przybliży ustaloną w projekcie UWSł definicję „dezinformacji”. Z brzmienia ww. przepisu wynika, iż podmioty będą mogły zgłaszać tylko treści dot. dezinformacji. Takie założenie potwierdza także treść art. 25 ust. 1²⁷ oraz uzasadnienia projektu²⁸. Należy więc uznać, iż „oddelegowanie” zaufanych podmiotów sygnalizujących do monitorowania jedynie dezinformacji było zabiegiem celowym. Niemniej, dezinformacja wg projektodawców jest klasyfikowana jako treść o charakterze bezprawnym. Zgodnie z definicją treści o charakterze bezprawnym są to treści naruszające dobra osobiste, o charakterze przestępnym, treści, które naruszają dobre obyczaje²⁹, w szczególności rozpowszechniają lub pochwalają przemoc, cierpienie lub poniżenie oraz właśnie dezinformacja. Takie ujęcie dezinformacji stoi w sprzeczności z poglądami unijnymi. W raporcie opracowanym przez niezależną Grupę Wysokiego Szczebla ds.

²⁴ Art. 29 ust. 2 projektu.

²⁵ Posiadanie wiadomości specjalnych ma być udowodnione poprzez przedłożenie dokumentów lub ew. innych dowodów (projekt nie uściśla, o jakich „innych dowodach” mowa. Natomiast, ocena dostatecznego wykazania posiadania wiadomości specjalnych należy do Przewodniczącego RWS.

²⁶ Do tych podmiotów należą: NIL, NIA, GIF, GIS, GIOŚ, NRA, KIRP, RPP, KRS, Pierwszy Prezes SN; RPO, RPD, KNE, Rzecznik Finansowy, Prezes UOKiK, Prezes UKE, Szef ABW, rektorzy uczelni publicznych oraz ministrowie kierujący działami administracji rządowej.

²⁷ Art. 25. 1. „(...) zaufany podmiot sygnalizujący niezadowolony ze sposobu rozpatrzenia w wewnętrznym postępowaniu kontrolnym reklamacji w przedmiocie rozpowszechniania dezinformacji (...)”.

²⁸ „Oprócz zdefiniowania pojęcia dezinformacji, podmiotom powołanym do jej zwalczania w interesie publicznym, tj. zaufanym podmiotom sygnalizującym, które będą certyfikowane przez fachowe organy państwowe, przyznano szczególne uprawnienia” – zob. uzasadnienie, s. 5.

²⁹ Uwagi do definicji treści bezprawnych zgłosił także Prezes UOKiK, który zwraca uwagę na potencjalne problemy związane z brakiem rozgraniczenia kompetencji pomiędzy Prezesem UOKiK a Radą Wolności Słowa, które mogą odmiennie ocenić naruszenie przez opublikowaną treść do- brych obyczajów z obszaru ochrony konsumentów.

falszywych wiadomości i dezinformacji w Internecie (ang. *independent High level Group on fake news and online disinformation*) pt. *A multi-dimensional approach to disinformation* z 2018 r. przedstawiono i omówiono problematykę zjawiska dezinformacji, jego definicje, skalę zagrożenia, którą za sobą niesienie, oraz przedstawiono sposoby, które dotychczas zostały podjęte do zwalczania dezinformacji, jak też te, które mogłyby zostać wprowadzone. W Raporcie podkreślono, iż pomiędzy dezinformacją a fake newsami nie może zostać postawiony znak równości. Autorzy raportu wskazują, że obecne debaty na temat fake newsów obejmują spektrum rodzajów informacji; są to zarówno treści o stosunkowo niskim ryzyku, takie jak pomyłki reporterów, stroniczy dyskurs polityczny, jak i treści o wysokim ryzyku, jak np. działania obcych państw lub grup krajowych, które próbują osłabić proces polityczny w państwach członkowskich UE i w UE, wykorzystując różne formy złośliwych fabrykacji, infiltracji. Raport koncentrował się przede wszystkim na dezinformacji, która niesie za sobą ryzyko szkód obejmujących zagrożenia dla demokratycznych procesów politycznych i wartości, które mogą dotyczyć różnych sektorów, takich jak zdrowie, nauka, edukacja, finanse i inne. Ryzyko to wynika z produkcji i promocji dezinformacji dla korzyści ekonomicznych lub celów politycznych czy ideologicznych, ale może być także zaostrzone przez sposób, w jaki różni odbiorcy przekazują informacje³⁰. Dezinformacja jest definiowana w raporcie jako fałszywa, niedokładna lub błędna informacja zaprojektowana, prezentowana i promowana w celu wyrządzenia szkody społeczeństwu lub dla zysku³¹. Dezinformacja, zgodnie z ww. definicją, obejmuje formy wypowiedzi, które nie są już nielegalne, ale mimo to mogą być szkodliwe. W ujęciu unijnym więc dezinformacja nie stanowi (lub nie musi stanowić) treści nielegalnej. Natomiast w polskim projekcie dezinformacja, zgodnie z literalnym brzmieniem art. 3 ust. 1 pkt 1, powinna stanowić treść o charakterze nielegalnym, co stanowi znaczące ograniczenie dla monitorowania treści na portalach społecznościowych przez zaufane podmioty sygnalizujące. Zwłaszcza że jak zostało ujęte w raporcie, nie tylko nielegalne treści mogą być szkodliwe. Warto zwrócić uwagę, że projektodawca wskazał w uzasadnieniu, iż definicja dezinformacji została skonstruowana na podstawie Unijnego kodeksu postępowania w zakresie zwalczania dezinformacji z 2018 r.³². Niemniej w Kodeksie tym również nie sklasyfikowano dezinformacji jako treści o charakterze bezprawnym.

Podsumowując, mimo twierdzeń projektodawców co do tego, iż polska propozycja definicji dezinformacji jest węższa i precyzyjniejsza od unijnych uregulowań, wydaje się ona nie brać pod uwagę będących dezinformacją treści, które nie są jednocześnie bezprawne. Niemniej te treści (pomimo braku charakteru bezprawności), jeśli niosą za sobą szkodę i krzywdę, również powinny być poddane kontroli i ew. zablokowane, usunięte. Oczywiście wciąż mając na uwadze „konstytucyjne

wymogi, zezwalające na ingerowanie w rozpowszechnianie jakichkolwiek informacji, jedynie wtedy, gdy jest to niezbędne w demokratycznym państwie prawnym i nie narusza istoty prawa do wolności słowa³³.

Wracając do regulacji *stricte* dot. instytucji zaufanych podmiotów sygnalizujących, w pierwszej kolejności należy wspomnieć, iż pierwszy projekt ustawy, tj. z grudnia 2021 r., nie przewidywał takiej instytucji. Została ona wprowadzona w drugiej wersji projektu z 2022 r. i zgodnie z tą wersją zaufanym podmiotem sygnalizującym może zostać osoba fizyczna, która posiada specjalistyczną wiedzę, w szczególności z zakresu medycyny, prawa, praw człowieka, rynku finansowego lub bezpieczeństwa publicznego, ale także organizacja społeczna, do której statutowych celów należy zwalczanie dezinformacji w przestrzeni publicznej³⁴. Projektodawca przedstawił zamknięty katalog podmiotów (tzw. podmiotów certyfikujących), które mogą wyznaczyć zaufane podmioty sygnalizujące i jest to FGIF, GIS, GIOŚ, RPP, RPO, RPP, KNF, Prezes UOKiK, Szef ABW, ministrowie kierujący działami administracji rządowej. Podmioty te zgłaszają RWS wybrane zaufane podmioty sygnalizujące po wyrażeniu przez nie

³⁰ W raporcie termin „fake news” został pominięty celowo z dwóch powodów. Po pierwsze, termin ten jest nieodpowiedni do uchwycenia złożonego problemu dezinformacji, który obejmuje treści, które nie są w rzeczywistości lub całkowicie „fałszywe”, lecz stanowią sfabrykowane informacje zmieszane z faktami, a także praktyki, które wykraczają daleko poza wszystko, co przypomina „wiadomości”, i obejmują pewne formy automatycznych kont, które mogą być wykorzystane np. do zorganizowanego trollingu. Może również obejmować cały wachlarz zachowań cyfrowych, które w większym stopniu polegają na rozpowszechnianiu dezinformacji niż na jej wytwarzaniu, począwszy od zamieszczania postów, komentowania, udostępniania, tweetowania i re-tweetowania itp (za: C. Wardle, H. Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Report to the Council of Europe 2017, <https://shorensteincenter.org/information-disorder-framework-for-research-and-policy-making/> (dostęp z 19.6.2022 r.)). Po drugie, termin „fake news” jest nie tylko nieadekwatny, lecz także mylący, ponieważ został zawłaszczony przez niektórych polityków i ich zwolenników, którzy używają go do odrzucania informacji, z którymi się nie zgadzają, i stał się w ten sposób bronią, za pomocą której wpływowe podmioty mogą ingerować w obieg informacji oraz atakować i osłabiać niezależne media informacyjne. Badania wykazały, że obywatele kojarzą termin „fake news” z partyzancką debatą polityczną i słabym dziennikarstwem, a nie z bardziej szkodliwymi i precyzyjnie zdefiniowanymi formami dezinformacji (R.K. Nielsen, L. Graves, *News You Don't Believe: Audience Perspectives on Fake News*, Oxford 2017).

³¹ Zob. Raport, s. 10.

³² Code of Practice on Disinformation 2018, <https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation> (dostęp z 19.6.2022 r.); dalej jako: Kodeks. Definicja dezinformacji zawarta w Kodeksie natomiast w głównej mierze odnosi się do komunikatu Komisji Europejskiej „Zwalczanie dezinformacji w internecie: podejście europejskie” z 2018 r. <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52018DC0236&qid=1556211423628&from=PL> (dostęp z 19.6.2022 r.). Kodeks odnosi się także do rekomendacji Komisji zawartych w ww. komunikacie, że sygnatariusze mają świadomość podstawowego prawa do wolności wypowiedzi i otwartego internetu, a także delikatnej równowagi, którą należy zachować przy podejmowaniu starań na rzecz ograniczenia rozpowszechniania i wpływu treści, które są zgodne z prawem (zob. Kodeks, s. 1).

³³ Zob. Uzasadnienie, s. 16.

³⁴ Zob. art. 15 projektu.

zgody, z urzędu. Lista zaufanych podmiotów sygnalizacyjnych ma być publikowana w BIP. Co istotne, podmiotom certyfikującym przysługują uprawnienia zaufanego podmiotu sygnalizującego³⁵. Mówiąc o „uprawnieniach”, projektodawca proponuje regulację, zgodnie z którą, jeśli zaufane podmioty sygnalizujące zgłoszą daną treść do usługodawcy, wówczas zarówno ich zgłoszenia, jak i ew. reklamacje powinny być traktowane jako te „zaufane”, ponieważ od wykwalifikowanych, wyspecjalizowanych podmiotów, i przez to priorytetowe (a więc przed zgłoszeniami np. użytkowników ów portalu społecznościowego). Jeśli więc ww. podmiotom certyfikującym mają zostać przyznane uprawnienia zaufanych podmiotów sygnalizujących, które to, jak zostało wyżej wspomniane, mogą zgłaszać jedynie bezprawną dezinformację, to należy domniemać, iż podmioty certyfikujące będą mogły zgłaszać analogicznie takie same treści. Ponadto projekt nie precyzuje, czy zaufany podmiot sygnalizujący będzie uprawniony do zgłaszania wszystkich treści czy też tylko tych, w których się specjalizuje. Idąc dalej, zastanawiające jest, czy KNF jako podmiot certyfikujący posiadający uprawnienia zaufanego podmiotu sygnalizującego będzie mogła zgłaszać tylko treści z obszaru rynku finansowego, czy też będzie mogła także (korzystając z przywilejów zaufanego podmiotu zgłaszającego) zgłosić treści z zakresu prawa autorskiego. Ponadto zaufane podmioty sygnalizujące będą uprawnione do wnoszenia do RWS skarg na rozstrzygnięcia usługodawców w sprawie rozpowszechniania dezinformacji. Usługodawcy są również zobowiązani do wprowadzenia niezbędnych środków technicznych i organizacyjnych, aby zapewnić priorytetowe i niezwłoczne rozpatrywanie zgłoszeń oraz reklamacji zaufanych podmiotów sygnalizujących (art. 22 ust. 6).

Należy również wspomnieć, iż instytucja dot. zaufanych podmiotów sygnalizujących (ang. *trusted flaggers*) nie jest *novum*, na szczeblu unijnym bowiem została ona przewidziana w Digital Service Act (DSA)³⁶, a wcześniej także chociażby w Zaleceniach Komisji (UE) 2018/334 z 1.3.2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w Internecie³⁷. Ponadto portale społecznościowe jak np. YouTube już w 2012 r. zaczęły prowadzić swój własny program pt. Heroes trusted flagger³⁸. Brak w projekcie w wersji z 2021 r. regulacji w przedmiocie „zaufanych podmiotów sygnalizujących” podkreślił RPO w swojej opinii do projektu UWSŁ z 26.10.2021 r.³⁹.

W art. 19 ust. 1 DSA, w wersji z czerwca 2022 r.⁴⁰, wskazuje, iż dostawcy platform internetowych (ang. „*providers of online platform*”) powinni podjąć niezbędne środki techniczne i organizacyjne w celu zapewnienia, aby zawiadomienia składane przez zaufane podmioty sygnalizujące (ang. „*trusted flaggers*”), działające w ramach wyznaczonego obszaru wiedzy specjalistycznej, za pośrednictwem mechanizmów, o których mowa w art. 14, były przetwarzane i rozpatrywane w sposób priorytetowy i bez zbędnej zwłoki. W ww. art. 14

wspomniana jest procedura *notice and action*, stąd też przyjęto, iż *trusted flaggers* mają stanowić „przedłużenie” tej procedury. Niemniej takie brzmienie art. 19 ust. 1 nie było zaproponowane w pierwotnej wersji projektu z grudnia 2020 r.⁴¹. Po pierwsze, art. 19 odnosił się bezpośrednio do platform internetowych, a nie do dostawców platform internetowych jak obecnie. Po drugie, ustalono, iż *trusted flaggers* mogą działać, a dokładniej mieć uprawnienia, tylko w relacji do branży, która została im wyznaczona (np. tylko odnośnie do treści o charakterze terrorystycznym). Po trzecie, sprecyzowano, iż zawiadomienia zgłaszane przez *trusted flaggers* mają być rozpatrywane bez zbędnej zwłoki (wcześniej było jedynie wskazane, iż mają być rozpatrywane bez zwłoki). Status *trusted flagger* w świetle DSA przyznaje, na wniosek dowolnego podmiotu, Koordynator ds. usług cyfrowych w państwie członkowskim, w którym wnioskodawca ma siedzibę. Nie ma więc, tak jak w polskim projekcie UWSŁ, zamkniętego katalogu podmiotów mogących zgłaszać zaufane podmioty sygnalizujące. DSA nakłada również na *trusted flaggers* obowiązek publikacji, co najmniej raz w roku sprawozdania dotyczące zawiadomień złożonych zgodnie z art. 14 (a więc w trybie procedury *notice and action*). W sprawozdaniu podaje się co najmniej liczbę powiadomień skategoryzowanych według: (a) tożsamości podmiotu świadczącego usługi hostingowe; (b) rodzaju rzekomo nielegalnej treści, której dotyczy powiadomienie; (c) działań podjętych przez usługodawcę. Sprawozdania te zawierają wyjaśnienie procedur stosowanych w celu zagwarantowania, że *trusted flagger* zachowuje swoją niezależność. Istotne jest także, że w omawianym art. 19 DSA przewidziano także procedurę kontrolowania działań *trusted*

³⁵ Zob. art. 16 projektu.

³⁶ Projekt rozporządzenia DSA z grudnia 2020 r.

³⁷ „W uzupełnieniu odpowiednich organów również określone osoby fizyczne lub podmioty, w tym organizacje pozarządowe i stowarzyszenia handlowe, mogą posiadać szczególną wiedzę fachową i być gotowe do przejścia, na zasadach dobrowolności, określonej odpowiedzialności związanej ze zwalczaniem nielegalnych treści w internecie. W świetle wnoszonej przez te podmioty wartości dodanej i czasami wysokiej liczby przedmiotowych zawiadomień należy zachęcać do współpracy między takimi zaufanymi podmiotami sygnalizującymi i dostawcami usług hostingowych, zwłaszcza poprzez traktowanie realizowanych przez nich zgłoszeń w sposób priorytetowy i z odpowiednim stopniem zaufania, jeżeli chodzi o dokładność tych zgłoszeń. Jednak w związku z ich szczególnym statusem współpraca taka powinna być otwarta jedynie dla osób fizycznych i podmiotów przestrzegających wartości, na których opiera się Unia i które określono w art. 2 TUE, spełniających pewne odpowiednie warunki, które z kolei powinny być dostępne publicznie w sposób wyraźny i obiektywny” – pkt 28 Zaleceń Komisji (UE) 2018/334 z 1.3.2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w Internecie.

³⁸ Zob. <https://blog.youtube/news-and-events/growing-our-trusted-flagger-program/> (dostęp z 20.6.2022 r.).

³⁹ Stanowisko RPO w przedmiocie uwag do projektu UWSŁ z 26.10.2021 r., s. 11.

⁴⁰ Zob. <https://www.consilium.europa.eu/pl/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/> (dostęp z 20.6.2022 r.).

⁴¹ Zob. <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=COM:2020:825:FIN> (dostęp z 20.6.2022 r.).

flaggers oraz określono warunki i procedurę odebrania im statusu *trusted flagger*. W przypadku gdy dostawca platform internetowych posiada informacje wskazujące na to, że *trusted flagger* złożył znaczną liczbę nieprecyzyjnych, niedokładnych lub nieodpowiednio uzasadnionych zawiadomień w trybie art. 14, przekazuje te informacje koordynatorowi ds. usług cyfrowych, który przyznał danemu podmiotowi status *trusted flagger*. Na czas trwania postępowania status zaufanego podmiotu oflagowującego zostaje zawieszony na czas dochodzenia, które powinno zostać przeprowadzone bez zbędnej zwłoki. Natomiast projektowane polskie regulacje w przedmiocie zaufanych podmiotów sygnalizujących nie przewidują podobnych mechanizmów kontroli jak w przypadku DSA. W przeciwieństwie do polskiego projektu, w świetle DSA, status *trusted flagger* nie może zostać przyznany osobie fizycznej. Zarówno DSA, jak i projekt UWSI nie przewidują, by status ten miał charakter kadencyjny

Obowiązki usługodawców

Przez „usługodawcę” rozumie się osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę internetowego serwisu społecznościowego⁴². Natomiast przez „internetowy serwis społecznościowy” rozumie się usługę świadczoną drogą elektroniczną w rozumieniu ustawy o świadczeniu usług drogą elektroniczną, która umożliwia udostępnianie przez użytkowników dowolnych treści innym użytkownikom lub ogółowi, z której korzysta na terytorium RP co najmniej jeden milion użytkowników, którzy założyli profil użytkownika, chyba że usługa jest wyłącznie funkcją innej usługi, stanowiącej usługę główną, a ze względów obiektywnych lub technicznych nie można jej wykorzystać bez usługi głównej lub ma charakter wyłącznie wspierający funkcjonalność usługi głównej⁴³. Ta wersja definicji różni się od tej z projektu z 2020 r. Poprzednia nie zawierała w sobie żadnego wyłączenia, na co zwrócił uwagę RPO w swojej opinii do projektu z 2020 r. RPO wskazał, że zgodnie z definicją serwisu społecznościowego w wersji projektu UWSI zakresem ustawy objęte zostaną nie tylko portale społecznościowe, takie jak Facebook czy Twitter, ale również portale informacyjne umożliwiające komentowanie publikowanych artykułów czy komunikatory internetowe.

Projektodawca w art. 18 nakłada na usługodawców, którzy otrzymują w roku kalendarzowym ponad 100 zgłoszeń dotyczących rozpowszechniania treści o charakterze bezprawnym, obowiązek sporządzenia w języku polskim, co pół roku, sprawozdania w przedmiocie sposobu rozstrzygnięcia zgłoszeń i reklamacji w danym półroczu. Sprawozdanie to ma również zostać opublikowane w tymże internetowym serwisie społecznościowym. W ust. 2 art. 18 wskazane są elementy, które muszą znaleźć się w owym sprawozdaniu, przy czym są to elementy jedynie podstawowe i usługodawca może upublicz-

nić więcej danych⁴⁴. Ponadto w art. 19 ust. 1 przewidziano, że usługodawca jest obowiązany do udzielania odpowiedzi i wszelkich informacji organom państwowym uprawnionym na podstawie odrębnych przepisów na potrzeby prowadzonych przez nie postępowań. Niemniej przepis nie precyzuje, jakiego obszaru miałyby dot. zapytania i czy usługodawca będzie mógł odmówić przedłożenia odpowiedzi z uwagi na nadzwyczajne okoliczności lub swój interes biznesowy.

Kolejnym obowiązkiem, uregulowanym w rozdziale 5, jest zobowiązanie usługodawcy do ustanowienia w języku polskim skutecznego, zrozumiałego, tzw. wewnętrznego postępowania kontrolnego, pozwalającego na elektroniczne przesyłanie użytkownikom ów portali społecznościowych zgłoszeń⁴⁵ oraz reklamacji⁴⁶. Jeśli zgłoszenie albo reklamacja zawiera adres poczty elektronicznej, usługodawca ma niezwłocznie przesłać na ten adres potwierdzenie ich otrzymania. Niezwłocznie, czyli nie później niż w ciągu 48 godzin od dnia otrzymania zgłoszenia czy reklamacji, ponieważ usługodawca ma 48 godzin na rozpatrzenie zgłoszenia i reklamacji od chwili ich wniesienia. W tym samym czasie usługodawca ma przesłać drogą elektroniczną informację o sposobie ich rozpatrzenia, w tym na adres poczty elektronicznej, o ile został wskazany przez użytkownika. Niemniej w opinii autora przepis ten nie przesądza, czy termin 48 godzin obowiązuje także w przedmiocie obowiązku informacyjnego nałożonego na usługodawcę. Jeśli usługodawca miałby także informować, jaka decyzja zapadła do zgłoszonej treści, wówczas powinno to zostać uściślone⁴⁷. O sposobie rozpatrzenia zgłoszenia albo reklamacji usługodawca w każdym przypadku ma także informować użytkownika, który udostępnił treść lub założył profil użytkownika będące przedmiotem wewnętrznego postępowania kontrolnego. Z literalnego brzmienia regulacji nie wynika jednak, by usługodawca informował podmiot, który opublikował zgłoszoną treść, o danych zgłaszającego.

Informacja o sposobie rozpatrzenia zgłoszenia albo reklamacji powinna zawierać przyczyny rozstrzygnięcia wskazujące w szczególności podstawy prawne z odwołaniem się do regulaminu internetowego serwisu społecznościowego oraz podstawy faktyczne rozstrzygnięcia wraz z uzasadnieniem (art. 22 ust. 5). W niemieckiej ustawie natomiast serwisy mają obowią-

⁴² Art. 3 ust. 1 pkt 2 projektu.

⁴³ Art. 3 ust. 1 pkt 1 projektu.

⁴⁴ Przykładowo sprawozdanie ma zawierać co najmniej ogólne informacje dotyczące działań podjętych przez usługodawcę w zakresie zapobiegania udostępnianiu treści o charakterze bezprawnym; łączną liczbę zgłoszeń i łączną liczbę reklamacji, które wpłynęły w okresie sprawozdawczym – zob. art. 18 ust. 2 projektu UWSI.

⁴⁵ Przedmiotem zgłoszenia jest rozpowszechnianie treści o charakterze bezprawnym (art. 23).

⁴⁶ Od rozstrzygnięcia wydanego w wyniku zgłoszenia użytkownikowi, który dokonał zgłoszenia albo udostępnił treść lub założył profil użytkownika będące przedmiotem zgłoszenia, przysługuje reklamacja.

⁴⁷ Przykładowo usługodawca rozpatruje zgłoszenia w terminie 48 godzin od ich wniesienia i w tym czasie przesyła także drogą elektroniczną informację o sposobie rozpatrzenia zgłoszenia.

zek usuwania treści (np. filmów i komentarzy), które są „w sposób oczywisty niezgodne z prawem”, w ciągu 24 godzin od powiadomienia. Jeśli legalność (lub jej brak) nie jest oczywista, dostawca ma maksymalnie siedem dni na podjęcie decyzji dotyczącej postępowania w danym przypadku. W wyjątkowych sytuacjach czas na podjęcie decyzji może być dłuższy – jeśli użytkownicy przesyłający treści, czyli użytkownicy, których filmy lub komentarze są zapisywane w YouTube (przesyłający), zostaną poproszeni o odniesienie się do uwag lub gdy decyzja jest przekazywana organizacji branżowej akredytowanej jako instytucja regulowania wewnętrznego⁴⁸.

W przypadku gdy użytkownik nie jest usatysfakcjonowany z wyniku wniesionej w wewnętrznym postępowaniu kontrolnym reklamacji czy też zaufany podmiot sygnalizujący nie jest zadowolony ze sposobu rozpatrzenia reklamacji, ale już tylko w przedmiocie rozpowszechniania dezinformacji mogą wnieść skargę do RWS w terminie siedmiu dni od otrzymania informacji o sposobie rozpatrzenia reklamacji⁴⁹. Użytkownik wnosi skargę do Rady na piśmie utrwalonym w postaci elektronicznej na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z 18.11.2020 r. o doręczeniach elektronicznych⁵⁰. Skargę opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym⁵¹. Skarga ma zawierać: imię i nazwisko, nazwę lub firmę użytkownika oraz jego przedstawiciela ustawowego lub ew. pełnomocnika, oznaczenie usługodawcy i pełnomocnika do doręczeń w kraju, opis naruszenia, wskazanie żądania, podpis i ew. wymienienie załączników. RWS jest uprawniona do pominięcia dowodów, które prowadziłyby do przedłużenia postępowania. Niemniej nie jest wskazane w projekcie, o jakiego rodzaju dowodach mowa, ani czy RWS będzie zobowiązana wyjaśnić, z jakich przyczyn uważała, że ów dowód może przedłużyć postępowanie; uzasadnienie projektu również nie rozwija regulacji (art. 29 ust. 3). Warto zwrócić uwagę, że projektodawca wskazał ścisły krąg podmiotów, którym przysługuje status strony postępowania przed RWS. Jest nią (1) użytkownik, któremu ograniczono dostęp do treści, albo (2) któremu ograniczono dostęp do profilu użytkownika, albo (3) zaufany podmiot sygnalizujący i (4) usługodawca⁵². Taki katalog podmiotów nie uwzględnia jednak samego zgłaszającego daną treść. O wniesionej skardze niezwłocznie zawiadamiany jest usługodawca⁵³, który ma 24 godziny na przekazanie RWS materiałów zgromadzonych w wewnętrznym postępowaniu kontrolnym, w tym reklamacji. Ustawa nie precyzuje, w jaki sposób te dane miałyby zostać przekazane.

Zgodnie z art. 30 postępowanie prowadzone przed RWS może zakończyć się decyzją w przedmiocie (1) nakazania zniesienia ograniczenia dostępu do treści albo (2) odmowy nakazania zniesienia tego ograniczenia; albo w przedmiocie (3) nakazania zniesienia ograniczenia dostępu do profilu użytkownika albo odmowy nakazania zniesienia tego ograni-

czenia. Jeśli natomiast zaufane podmioty sygnalizujące mogą zgłaszać jedynie dezinformację, to projektodawca wykluczył tę instytucję także ze zgłaszania danych profili użytkowników. Dlatego też decyzje RWS w przedmiocie zgłoszeń pochodzących od zaufanych podmiotów sygnalizujących mogą dotyczyć nakazania uniemożliwienia rozpowszechniania treści albo odmowy nakazania uniemożliwienia rozpowszechniania treści. Niemniej, jeśli na danym profilu użytkownika notorycznie są udostępniane treści dezinformacyjne, to nieekonomiczne i nieefektywne wydaje się zgłaszanie przez zaufany podmiot sygnalizujący każdej z tych treści. W takim przypadku zaufany podmiot sygnalizujący (którego kompetencje w walce z bezprawnymi treściami i tak zostały przez projekt znacznie ograniczone) mógłby zgłosić cały profil użytkownika, który szerzy dezinformację w sieci.

Projektodawca zobowiązał także usługodawcę do zapewnienia, aby reklamacje nie były rozpatrywane wyłącznie z wykorzystaniem zautomatyzowanych środków (art. 24 ust. 4). Z literalnego brzmienia regulacji wynika zatem, że automatyczne rozpatrywanie części reklamacji nie jest całkowicie wykluczone, niemniej nie uściślono, jaka część może być rozpatrywana w trybie zautomatyzowanym. Ponadto, zgodnie z art. 33, jeśli dana treść była już przedmiotem badań przed RWS, usługodawca nie może ponownie ograniczyć dostępu do tej treści. Niemniej można sobie wyobrazić sytuację, w której przedmiotem zgłoszenia jest treść, która narusza prawo do znaku towarowego, a zgłoszenia dokonuje użytkownik, który nie jest właścicielem tego znaku i nie ma do niego praw. Ostatecznie RWS stwierdza, iż ta treść nie narusza prawa, ale informacja o niej dochodzi do rzeczywistego właściciela znaku. Pytanie, czy w takim przypadku treść ponownie nie będzie mogła być zgłoszona. Wątpliwości budzi również zmiana okoliczności sprawy, aktualnej sytuacji na świecie czy też właśnie zmiana podmiotu zgłaszającego udostępnioną treść. Dlatego też przepis powinien precyzować, w jakich okolicznościach, w zależności od tego, jaki podmiot zgłasza treść, kolejne postępowanie w przedmiocie tożsamej treści przed RWS byłoby bądź nie byłoby dozwolone.

Rada ma doręczyć decyzję stronom⁵⁴ postępowania niezwłocznie, ale nie później niż w terminie 24 godzin od jej

⁴⁸ Zob. <https://transparencyreport.google.com/netzdg/youtube?hl=pl> (dostęp z 28.6.2022 r.).

⁴⁹ Art. 25 projektu.

⁵⁰ T.j. Dz.U. z 2022 r. poz. 569 ze zm.

⁵¹ Do skargi użytkownik obowiązany jest dołączyć informację o sposobie rozpatrzenia reklamacji, chyba że wnosi skargę, bo nie uzyskał na czas informacji w zakresie sposobu rozstrzygnięcia wniesionej reklamacji (zob. art. 25–26 projektu).

⁵² Art. 27 projektu.

⁵³ Jeżeli skarga została wniesiona przez zaufany podmiot sygnalizujący, wówczas usługodawca jest o tym informowany. Projekt nie precyzuje jednak, czy usługodawca jest informowany bezpośrednio o imieniu i nazwisku/nazwie zaufanego podmiotu sygnalizującego czy tylko generalnie o tym, że skargę wniosła ta instytucja.

⁵⁴ Taka regulacja art. 32 oznacza, że zgłaszający treść nie otrzyma informacji o finalnej decyzji RWS.

wydania. Usługodawca również zobowiązany jest wykonać decyzję RWS niezwłocznie, nie później niż w terminie 24 godzin od jej doręczenia. Ponadto usługodawca w terminie 24 godzin od upływu terminu do wykonania decyzji, o którym ma poinformować RWS o sposobie jej wykonania (art. 32 projektu)⁵⁵. W ocenie projektodawcy termin 24 godzin na wykonanie przez usługodawcę decyzji RWS będzie całkowicie wystarczający, gdyż „w tym terminie nie będzie podejmował dodatkowych czynności analitycznych, a jedynie, zgodnie z decyzją Rady, przywracał wcześniej ograniczony dostęp do treści lub ograniczony dostęp do profilu użytkownika”⁵⁶. Termin wprowadzenia 24 godzin uzasadniony został również tym, aby czas ograniczenia wolności słowa trwał jak najkrócej⁵⁷. Za brak subordynacji z przepisami projektu na usługodawców mogą zostać nałożone, na podstawie Kodeksu postępowania karnego, grzywny w wysokości od 50 000 zł do 50 000 000 zł i będą podlegały egzekucji administracyjnej na podstawie art. 2 § 1 pkt 2 ustawy z 17.6.1966 r. o postępowaniu egzekucyjnym w administracji⁵⁸. W sprawach nieuregulowanych w rozdziale dotyczącym postępowania przed RWS mają być stosowane przepisy Kodeksu postępowania administracyjnego ze wskazanymi wyłączeniami⁵⁹.

Strona niezadowolona z decyzji Rady będzie uprawniona do złożenia skargi do sądu administracyjnego⁶⁰. Natomiast, z uwagi na fakt, że zgłaszającemu daną treść nie został przyznany status strony, nie będzie mógł on złożyć skargi do WSA.

Ślepy pozew

Powództwo nie zostanie zainicjowane, jeżeli powód nie oznaczy prawidłowo pozwanego⁶¹. Dlatego też dochodzenie swoich praw przeciwko użytkownikom portali społecznościowych, którzy przez swoją aktywność naruszają prawa innych i szerzą treści bezprawne, często nie jest możliwe; wynika to bowiem z faktu, że powód nie jest w stanie dowiedzieć się albo zweryfikować danych potencjalnego pozwanego. Rozwiązaniem tego patu ma być instytucja pozwu ślepego, która miałaby zostać dodana do Kodeksu postępowania cywilnego w drodze art. 38 pkt 1 projektu, w części pierwszej, w księdze pierwszej Kodeksu postępowania cywilnego jako rozdział IX.

Pomysł wprowadzenia instytucji pozwu ślepego do polskiej procedury cywilnej nie stanowi *novum*. W dniu 17.5.2016 r. RPO wystąpił do Ministra Sprawiedliwości z inicjatywą podjęcia prac legislacyjnych w przedmiocie umożliwienia wprowadzenia instytucji ślepego pozwu⁶². Rzecznik podkreślił, że instytucja ta mogłaby się przyczynić do zminimalizowania ilości wszczynanych postępowań karnych, administracyjnych i sądowoadministracyjnych tylko w jednym celu – uzyskania w nich danych osobowych, które mogłyby zostać wykorzystywane w kolejnym postępowaniu⁶³. Wprowadzenie instytucji „ślepego pozwu” było także postulowane przez posłów „Nowoczesnej” w czerwcu 2017 r. w projekcie ustawy o zmianie ustawy – Kodeks postępowania

cywilnego oraz ustawy – Prawo telekomunikacyjne (druk Nr 1715)⁶⁴. Należy również przywołać uzasadnienie uchwały SN z 20.8.2020 r.⁶⁵, zgodnie z którym w obecnym stanie prawnym „powód dochodzący roszczeń o ochronę dóbr osobistych musi zidentyfikować osobę, której zarzuca czyn będący formą takiego naruszenia i wykazać, że pozwany dopuścił się zarzucanego mu czynu. Ustawodawca nie przewidział odmiennych zasad dochodzenia tego rodzaju roszczeń, gdy czyn naruszający dobra osobiste miał miejsce w sieci Internet. Także w takim przypadku powód musi zatem oznaczyć pozwanego już na etapie wniesienia pozwu”. W orzeczeniu tym SN przyjął dopuszczalność żądania od podmiotu związanego tajemnicą telekomunikacyjną informacji pozwalających zweryfikować twierdzenie powoda, że czynu naruszającego dobra osobiste dopuścił się pozwany w sprawie, na podstawie art. 159 ust. 2 pkt 4 PrTelU⁶⁶. Niemniej powód wciąż jest zobowiązany oznaczyć pozwanego w pozwie. Dlatego też jedynym remedium na zapewnienie możliwości wszczęcia postępowania przeciwko nieznanemu „hejterowi” ma być właśnie instytucja ślepego pozwu.

W świetle projektu regulacje w przedmiocie ślepego pozwu będą aplikowały wyłącznie do spraw o ochronę dóbr osobistych, które naruszono za pośrednictwem usługi świadczonej drogą elektroniczną i będą należały do właściwości sądów

⁵⁵ W zakresie nieuregulowanym w Rozdziale 6 (Postępowanie przed RWS) stosuje się odpowiednio przepisy Kodeksu postępowania administracyjnego – zob. art. 34 projektu.

⁵⁶ Zob. uzasadnienie, s. 37.

⁵⁷ *Ibidem*.

⁵⁸ T.j. Dz.U. z 2022 r. poz. 479 ze zm.

⁵⁹ Art. 8 § 2, art.10, art. 28, art. 31, art. 36, art. 38, art. 77 § 1, art. 79, art. 89–98, art. 114–122h., art. 217–220. Do decyzji RWS nie stosuje się art. 61 i art. 152 § 1 ustawy z 30.8.2002 r. Prawo o postępowaniu przed sądami administracyjnymi, t.j. Dz.U. z 2022 r. poz. 329 zd zm.; dalej jako: PrPostSądAdmU – zob. art. 34 projektu.

⁶⁰ Na podstawie art. 3 § 2 PrPostSądAdmU.

⁶¹ Art. 187 w zw. z 126 § 1 pkt 1 KPC.

⁶² Funkcjonującej w systemie anglosaskim instytucji tzw. ślepego pozwu (*John Doe lawsuit*)

⁶³ W mniemaniu RPO kluczowym problemem jest zwykle anonimowość osoby, która złamała prawo: ofiara nie wie i nie jest w stanie samodzielnie ustalić, kto dokonał obraźliwego bądź zniesławiającego ją wpisu. Rzecznik w swoim wystąpieniu nawiązał także do koncepcji ślepego pozwu, funkcjonującej z powodzeniem od wielu lat (w najbardziej klasycznej formie) w procesie anglosaskim – *John Doe lawsuit*. „Tożsamość pozwanego jest nieznaną we wstępnej fazie procesu, dopiero w trakcie postępowania sąd ustala wszelkie potrzebne dane osoby pozwanej. Instytucja ta zapewnia możliwość uzyskania danych anonimowego sprawcy szkody, jednak równocześnie chroni prywatność potencjalnego pozwanego – wykluczony jest wszelki automatyzm w korzystaniu z tego narzędzia prawnego” – wystąpienie RPO do Ministra Sprawiedliwości ws. zwalczania mowy nienawiści w Internecie z 17.5.2016 r., <https://bip.brpo.gov.pl/sites/default/files/Wystapienie%20do%20Ministra%20Sprawiedliwosci%20ws%20zwalczania%20mowy%20nienawisci%20w%20internecie%2017.05.2016.pdf> (dostęp z 20.6.2022 r.), [za:] *M. Mazzotta*, Balancing Act: Finding Consensus on Standards for Unmasking Anonymous Internet Speakers, 51 Boston College Law Rev. 833 (2010), s. 845 i n., <http://lawdigitalcommons.bc.edu/bclr/vol51/iss3/6> (dostęp z 20.6.2022 r.).

⁶⁴ Projekt ten został odrzucony w pierwszym czytaniu na 48. posiedzeniu Sejmu VIII kadencji 29.9.2017 r.

⁶⁵ III CZP 78/19, OSNC 2021, Nr 2, poz. 7.

⁶⁶ Zob. przypis Nr 11.

okręgowych. W pozwie zamiast imienia i nazwiska albo nazwy lub adresu miejsca zamieszkania albo siedziby pozwanego powód podaje informacje pozwalające ustalić osobę, która dopuściła się naruszenia, w szczególności nazwę profilu lub login użytkownika. Pozew powinien zawierać również (1) wniosek o zobowiązanie usługodawcy do wskazania (a) danych pozwanego określonych w art. 18 ust. 1 ŚwUsłElekU, (b) danych eksploatacyjnych określonych w art. 18 ust. 5 ŚwUsłElekU – w oparciu o podane przez powoda informacje⁶⁷; (2) oznaczenie usługodawcy świadczącego usługę drogą elektroniczną w sposób umożliwiający doręczenie zobowiązania do nadesłania danych pozwanego; (3) wskazanie publikacji naruszających dobra osobiste powoda, z podaniem adresu identyfikującego treść w zasobach danych internetowych, w których zostały opublikowane; (4) datę i godzinę publikacji, o której mowa w pkt (3), oraz nazwę profilu lub loginu użytkownika, jeśli wskazanie tych danych jest możliwe. Zgodnie z proponowanym brzmieniem nowego art. 755(5) KPC, w sprawach o ochronę dóbr osobistych, naruszonych za pośrednictwem usługi⁶⁸ świadczonej drogą elektroniczną, sąd może udzielić zabezpieczenia również poprzez: (1) nakazanie uniemożliwienia dostępu do publikacji, (2) nakazanie umieszczenia oświadczenia uprawnionego odnoszącego się do publikacji, (3) nakazanie umieszczenia oznaczenia informującego o spornym charakterze publikacji. Mając na uwadze powyższe, sąd zobowiąże więc usługodawcę świadczącego usługę drogą elektroniczną do wskazania danych, o których mowa w art. 505⁴¹ § 1 pkt 1⁶⁹, i zagrozi mu grzywną na wypadek, gdyby w wyznaczonym terminie ich nie wskazał. Po bezskutecznym upływie terminu wyznaczonego usługodawcy do wskazania danych sąd nałoży grzywnę i jednocześnie wyznaczy nowy termin do wskazania danych, z zagrożeniem surowszą grzywną. Jeśli ustawodawca nie wskazałby tych danych, wówczas, w wersji art. 505⁴³ § 2 z projektu z 2021 r., postępowanie miałyby podlegać umorzeniu. Nie było natomiast jasne, czy do umorzenia postępowania musiałoby dojść, nawet w przypadku gdy usługodawca podał tylko niektóre wymagane dane pozwanego. Sąd Najwyższy postulował, że w razie uznania, iż podanie niewystarczających danych prowadzi do umorzenia postępowania, należałoby rozważyć wprowadzenie mechanizmu przekazywania tych niekompletnych danych powodowi, co mogłoby mu ułatwić wytoczenie powództwa na zasadach ogólnych⁷⁰. Niemniej projektodawca, w wersji projektu z 2022 r., wskazał w art. 505⁴³ § 3 pkt 2, że sąd umarza postępowanie, jeżeli usługodawca świadczący usługę drogą elektroniczną nie wskazał wystarczających danych identyfikujących pozwanego, ich pozyskanie nie jest możliwe lub byłoby połączone z nadmiernymi trudnościami.

Projekt ma również nowelizować ustawę z 28.7.2005 r. o kosztach sądowych w sprawach cywilnych⁷¹. Zgodnie z proponowaną treścią art. 13f KosztSądSpCywU w sprawach dochodzonych w postępowaniu o ochronę dóbr osobistych przeciwko osobom o nieustalonej tożsamości, o którym mowa w części pierwszej w księdze pierwszej w tytule VII

w dziale VIII, rozdziale 2 KPC pobiera się opłatę stałą w kwocie 1000 zł. Projektodawca wyjaśnia, że określając wysokość opłaty, kierował się art. 26 ust. 1 pkt 3 KosztSądSpCywU. Przepis ten wskazuje, że opłata stała od pozwu o ochronę dóbr osobistych wynosi 600 zł, ale w tym przypadku sąd nie jest już zobligowany do dokonania dodatkowych czynności mających na celu ustalenia danych pozwanego (tj. osoby, która naruszyła dobra osobiste powoda na portalu)⁷².

Nie można również zapomnieć, że często konta tworzone na portalach i serwisach społecznościowych tworzone są przy użyciu fałszywych danych, a usługodawcy nie weryfikują ich, nie prowadzą rejestru danych używanych do założenia konta i analogicznie nie aktualizują go. Obowiązek takiej weryfikacji nie wynika także z przepisów prawa. Uwaga ta jest istotna z tego powodu, iż liczba profili, które zostały utworzone przy użyciu nieprawdziwych danych osobowych, jest znacząca. Dla przykładu w pierwszym kwartale 2021 r. Facebook na całym świecie dezaktywował 1,3 miliarda fałszywych kont, a w drugim już 1,7 miliarda⁷³. Istnieje więc prawdopodobieństwo, że pomimo uzyskania danych potencjalnego pozwanego nie będą one przydatne, ponieważ okażą się fałszywe, co prowadzi do błędnego koła. Niemniej trudno oczekiwać,

⁶⁷ Sąd zobowiąże usługodawcę do wskazania tych danych i zagrozi grzywną na wypadek, gdyby w wyznaczonym terminie ich nie wskazał. Po bezskutecznym upływie terminu wyznaczonego usługodawcy do wskazania danych sąd nałoży grzywnę i jednocześnie wyznaczy nowy termin do wskazania danych, z zagrożeniem surowszą grzywną. Grzywna jest powtarzana, jeżeli pomimo wyznaczenia nowego terminu usługodawca świadczący usługę drogą elektroniczną nadal bez usprawiedliwienia nie wskazał danych. Ogólna suma grzywien w tej samej sprawie nie może przewyższać 2 milionów zł. Natomiast w razie wskazania danych przez usługodawcę lub usprawiedliwienia powodów, dla których ich pozyskanie nie jest możliwe lub byłoby połączone z nadmiernymi trudnościami, grzywny niezapłacone do tego czasu ulegają umorzeniu [art. 505(43) § 1–2]

⁶⁸ W poprzedniej wersji projektu, zamiast pojęcia „usługi” w sformułowaniu z art. 505(40) § 1: „naruszenia dóbr osobistych za pośrednictwem usługi świadczonej drogą elektroniczną w rozumieniu ustawy o świadczeniu usług drogą elektroniczną”, użyto pojęcia „usługodawca w UośuDE”. W poprzednim sformułowaniu 505(40) § 1, wątpliwości praktyczne mogła budzić kwestia tego, czy zobowiązanie do podania danych pozwanego będzie mogło być skierowane do podmiotów, które jedynie umożliwiają dostęp do sieci Internet, nie świadcząc żadnych usług „drogą elektroniczną”. Na gruncie ustawy o świadczeniu usług drogą elektroniczną to właśnie podmioty zapewniające dostęp do sieci mogą dysponować wiarygodnymi danymi użytkowników Internetu (w szczególności ukrywających się pod określonym adresem IP), tj. nie tylko imieniem i nazwiskiem, tak jak sam usługodawca – zob. Uwagi SN do projektu ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych z 27.10.2021 r.

⁶⁹ Tj. tych wskazanych w art. 18 ust. 1 i 2 ŚwUsłElekU. W poprzedniej wersji projektu mowa była o danych od ust. 1 do ust. 5, co oznaczało, że projekt znacząco wykraczał poza te dane, które są niezbędne do wytoczenia powództwa. Niemniej projektodawca ograniczył w wersji projektu z 2022 r. dane, które usługodawca miałby udostępnić już tylko do tych wskazanych w ust. 1–2 art. 18 ŚwUsłElekU (nazwisko i imiona usługobiorcy; PESEL a przy jego braku numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość).

⁷⁰ Uwagi Sądu Najwyższego do projektu ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych z 27.10.2021 r., s. 15.

⁷¹ Tj. Dz.U. z 2022 r. poz. 1125) ze zm.; dalej jako: KosztSądSpCywU.

⁷² Uzasadnienie, s. 54.

⁷³ Zob. <https://transparency.fb.com/data/community-standards-enforcement/> (dostęp z 26.6.2022 r.).

że przy zakładaniu konta na portalu społecznościowym weryfikacja będzie przypominała tę, która jest wymagana np. w procedurze rejestracji na platformę ePUAP. Do tworzenia konta na portalu społecznościowym, najczęściej, wymagane jest wskazanie adresu e-mail, a tych można tworzyć wiele. Ponadto samej idei tworzenia kont społecznościowych towarzyszyły względy rozrywkowe i z pewnością mało kto mógł się spodziewać, jak rewolucyjna okaże się rola portali społecznościowych, w szczególności w zakresie dostępu do informacji i możliwości wyrażania swoich opinii.

Podsumowanie

Nie ulega wątpliwości, że aktualnie obowiązujące regulacje w przedmiocie dostawców usług hostingowych, tj. przede wszystkim platform społecznościowych, nie przystają do obowiązujących realiów. W szczególności mowa tu o monopolistycznych platformach, które nader często arbitralnie ograniczają bądź usuwają treści, które mimo że naruszają ich politykę i regulamin, obiektywnie nie powinny zostać uznane za bezprawne.

Pozycja tych platform sprawia, że nie wahają się one usunąć nie tylko treści, ale także konta osób globalnie znanych, chociażby ze świata polityki. Mowa oczywiście o incydencie związanym z usunięciem konta *D. Trumpa* z Twittera⁷⁴. W ostatnim czasie także profil polskiej partii – Konfederacji został zablokowany przez Facebooka. Z jednej strony można oceniać, że każdy użytkownik platform – bez względu na status społeczny czy pełniącą funkcję, jest traktowany przez te platformy w sposób równy, z drugiej jednak istnieje obawa, by platformy nie ograniczały tematów nie tyle bezprawnych, ile kontrowersyjnych i przez to mogących pozornie naruszać jej regulamin i politykę. Jak powszechnie wiadomo, granica pomiędzy wolnością słowa a szerzeniem treści bezprawnych jest niezwykle cienka i wciąż trudna do jednoznacznego zdefiniowania. Należy także mieć na względzie, że platformy społecznościowe to wciąż prywatne platformy. ETPCz orzekł⁷⁵, że art. 10 EKPC nie zapewnia żadnej „swobody wyboru forum” dla korzystania z prawa do wolności wypowiedzi, co oznacza, że art. 10 EKPC nie gwarantuje żadnego prawa do nadawania swoich treści na jakimkolwiek konkretnym forum prywatnym. Prywatne platformy nie mogą być zatem zmuszane do rozpowszechniania treści osób trzecich, nawet jeśli treści te nie są w rzeczywistości nielegalne, co jest logiczne⁷⁶.

Poszczególne usługodawcy, w zależności od własnego profilu światopoglądowego i promowanych przez siebie wartości, mogą w zasadniczych kwestiach często różnić się w diametralny sposób w odbiorze publikowanych przez ich użytkowników treści. Przez co dane treści, choć kontrowersyjne dla danej platformy, a obiektywnie legalne i rzeczywistnie art. 10 EKPC, mogą zostać usunięte przez platformę. Jakikolwiek usunięcie czy zablokowanie konta lub treści na danej platformie społecznościowej momentalnie wywołuje

fałę spekulacji i dyskusji, która dość często szerzy bezprawne treści, np. mowę nienawiści. Dlatego też tak newralgiczne jest wprowadzenie środków prawnych pozwalających z jednej strony na monitorowanie, a wręcz nadzorowanie treści udostępnianych online, ale z drugiej strony takich, które będą respektowały zasadę wolności słowa i prawa do swobody wypowiedzi. Z tego też względu należy docenić inicjatywę ustawodawczą Ministerstwa Sprawiedliwości w przedmiocie regulacji portali społecznościowych. Niemniej wersja regulacji przedstawiona przez Ministerstwo jest w wielu aspektach niespójna i niejednoznaczna, co zostało podniesione we wcześniejszej części artykułu. Wątpliwości budzi także pominięcie w regulacji projektu osoby zgłaszającego daną treść, ponieważ jego rola zaczyna i kończy się na etapie zgłoszenia danej treści. Nie jest on także uznany za stronę postępowania przed RWS, co, jak wskazano, blokuje go przed złożeniem skargi do WSA na decyzje RWS. Z drugiej strony, projekt nie reguluje odpowiedzialności zgłaszającego, w przypadku gdyby okazało się, że zgłoszona treść nie jest bezprawna. Może się jednak okazać, że zgłoszenia dokonał konkurent autora publikacji czy właściciela zakwestionowanego konta społecznościowego. Brak dostępu do opublikowanej treści czy też konta może wywołać katastrofalne skutki, nie tylko w sferze finansowej, ale również wizerunkowej. Co prawda można próbować dochodzić roszczeń na podstawie przepisów Kodeksu cywilnego czy ustawy z 16.4.1993 r. o zwalczaniu nieuczciwej konkurencji⁷⁷.

Pojawiają się także wątpliwości dotyczące sposobu wyegzekwowania od zagranicznych platform podporządkowania się pod krajowe regulacje. Wydaje się, że przymus zapłaty kwoty 50 mln zł dla takich gigantów jak Facebook (obecnie Meta) nie stanowiłby większego problemu, biorąc pod uwagę dochody firmy. W 2020 r. Facebook (Meta) odnotował przychód w wysokości 85 mld dolarów i zysk w wysokości 29 mld dolarów⁷⁸. Pytanie więc, jak zmusić platformy do respektowania krajowych rozwiązań. Niemniej, skoro platformy respektują obowiązki nałożone przez niemiecką ustawę, dlaczego miałyby

⁷⁴ Zgodnie z amerykańskim prawem działanie Twittera nie stanowiło naruszenia Pierwszej Poprawki, ponieważ nie było to działanie państwa <https://www.techdirt.com/2021/01/08/not-easy-not-unreasonable-not-censorship-decision-to-ban-trump-twitter/> (dostęp z 28.6.2022 r.).

⁷⁵ *Appleby and Others v. the United Kingdom*, no. 44306/98, ECHR 2003-V,I https://www.echr.coe.int/documents/research_report_article_10_eng.pdf (dostęp z 28.6.2022 r.).

⁷⁶ Trudno sobie wyobrazić, by platforma dla właścicieli psów była zmuszana do udostępniania zdjęć kotów, <https://verfassungsblog.de/twitter-trump-trump/> (dostęp z 28.6.2022 r.).

⁷⁷ T.j. Dz.U. z 2022 r. poz. 1233 ze zm.; zob. *M. Mielniczuk-Skibicka, R. Skibicki*, Jak nie wpaść w Kanał (Sportowy), czyli o odpowiedzialności za bezpodstawne zgłoszenie internetowego naruszenia praw autorskich do dostawcy usług pośredniczących na tle sprawy Kanał Sportowy v. Polsat – cz. I, PME 2021, Nr 1, *passim*; *M. Mielniczuk-Skibicka, R. Skibicki*, Jak nie wpaść w Kanał (Sportowy), czyli o odpowiedzialności za bezpodstawne zgłoszenie internetowego naruszenia praw autorskich do dostawcy usług pośredniczących na tle sprawy Kanał Sportowy v. Polsat – cz. II, PME 2021, Nr 2, *passim*.

⁷⁸Zob. <https://businessinsider.com.pl/wiadomosci/facebook-ile-zarabia-ile-placi-podatkow-w-polsce-dane-za-2019-r> (dostęp z 22.1.2022 r.).

nie podporządkować się pod polskie standardy, dla przykładu, YouTube publikuje raporty w przedmiocie przejrzystości co dwa lata. Raporty mają zawierać dane na temat organizacji i przyjętych procedur oraz ilości otrzymanych skarg i usuniętych treści oraz ogólne informacje o praktykach obowiązujących u usługodawcy oraz zasadach w zakresie usuwania treści⁷⁹. Polski projekt natomiast wymaga od usługodawcy, otrzymującego w roku kalendarzowym ponad 100 zgłoszeń w przedmiocie rozpowszechniania treści o charakterze bezprawnym, sporządzania sprawozdania w języku polskim, już co pół roku. Nie jest również wiadome, w jaki sposób weryfikować liczbę zgłoszeń, tj. czy przekroczy ona pułap 100 zgłoszeń.

Ponadto, w uproszczeniu, w przypadku niemieckiej ustawy obowiązki są nałożone na sieci społecznościowe liczące ponad dwa miliony zarejestrowanych użytkowników, a jeśli mowa o projekcie UWSł wiele obowiązków jest nałożonych na usługodawców posiadających już co najmniej jeden milion użytkowników, którzy założyli profil użytkownika, korzystając z usługi na terytorium Polski.

Mając na uwadze powyższe, wiele środowisk, począwszy od przedstawicieli różnych gałęzi biznesu, jak np. wydawcy prasowi, branża usług cyfrowych, organizacje przedsiębiorców, aż po organizacje zajmujące się ochroną praw człowieka apelują o zaniechanie prac nad projektem UWSł. Z takim apelem 24.1.2022 r. wystąpiła do Ministra Sprawiedliwości Krajowa Izba Gospodarcza, wskazując, że „projekt ustawy, wbrew deklaracjom projektodawców, nie doprowadzi do wzmocnienia praw użytkowników serwisów społecznościowych względem wielkich korporacji internetowych. Z dużym prawdopodobieństwem przyczyni się natomiast do wprowadzenia arbitralnej kontroli politycznej nad swobodą

wypowiedzi w Internecie oraz wprowadzenia rozwiązań niezgodnych z prawem UE⁸⁰.

Podsumowując, najlepszym rozwiązaniem wydaje się porzucenie, a przynajmniej zawieszenie prac nad projektem do czasu przyjęcia ostatecznej wersji rozporządzenia DSA. Dzięki temu regulacje w przedmiocie platform społecznościowych byłyby spójne na szczeblu unijnym. Co więcej, platformom po pierwsze, łatwiej byłoby „podporządkować” się pod regionalną regulację aniżeli krajową, a po drugie, platformy chociażby ze względów wizerunkowych, ale i finansowych poczuwałyby się do działania zgodnie z rozporządzeniem unijnym i są podstawy, by takiego podejścia od nich oczekiwać. Platformy społecznościowe jak np. Facebook, Twitter, Instagram, już podejmowały współpracę mającą na celu walkę z dezinformacją czy mową nienawiści. Świadczy o tym odpowiednio, Kodeks postępowania w zakresie dezinformacji z 2018 r., znowelizowany w 2022 r.⁸¹ oraz Unijny kodeks postępowania dotyczący zwalczania niezgodnego z prawem nawoływania do nienawiści w Internecie⁸². Mając na uwadze powyższe, niewykluczone, że rozporządzenie DSA, jeśli zostanie przyjęte, przyczyni się do zwiększenia bezpieczeństwa i świadomości użytkowników platform społecznościowych.

⁷⁹ Zob. <https://transparencyreport.google.com/netzdg/youtube?hl=pl> (dostęp z 22.6.2022 r.).

⁸⁰ Zob. <https://kig.pl/apel-o-zaniechanie-prac-nad-projektem-transparencyreport.google.com/netzdg/youtube?hl=pl> -ustawy-o-wolnosci-slova-w-serwisach-spoecznościowych/ (dostęp z 28.6.2022 r.).

⁸¹ Zob. <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation> (dostęp z 28.6.2022 r.).

⁸² Zob. https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-counter-illegal-hate-speech-online_pl (dostęp z 28.6.2022 r.).

Słowa kluczowe: wolność słowa, Akt o usługach cyfrowych, platformy społecznościowe, treści nielegalne, zaufane podmioty zgłaszające.

Draft law on the freedom of speech in social media – remedy for combating unlawful content?

The fight against illegal content provided on online platforms is a current and pressing topic that the national as well as European legislation is trying to tackle. The previous and basic regulation on the subject of Internet platforms has been the e-Commerce Directive and, in the Polish legal system, additionally the Act on the Provision of Electronic Services. In recent months, it has been all too common to remove or block not only the content published on social networks, but also the accounts of users of these portals. In the opinion of some circles, such arbitrary actions and decisions of social media platforms pose a threat to freedom of speech guaranteed by the Polish Constitution and the European Convention on Human Rights. At the EU level, work is underway on a regulation on defining the principles of transparency of decisions regarding content moderation (Digital Service Act). However, after the announcement of the Digital Service Act regulation draft, the Ministry of Justice submitted a draft law on the protection of freedom of expression in social network websites aimed at combating unlawful content on social media platforms. This article aims to present and discuss the most important regulations of this act along with the risks and uncertainties associated with the possible adoption of this act.

Key words: freedom of speech, Digital Service Act, social media platforms, illegal content, trusted flaggers.

Obowiązki informacyjne przedsiębiorcy charakterystyczne dla świadczenia usług drogą elektroniczną na rzecz konsumenta *a plain language* i warstwowe obowiązki informacyjne jako próba rozwiązania problemu tzw. *information overkill*

Laura Słocka¹

Świadczenie usług drogą elektroniczną w relacji przedsiębiorca – konsument charakteryzuje się brakiem jednoczesnej obecności stron, co skutkuje ograniczonym zaufaniem. Ustawodawca, wprowadzając różnorodne obowiązki informacyjne, próbuje zrekomensować ten brak zaufania, chroniąc tym samym konsumenta. W związku z powyższym konsument zarzucany jest ogromną ilością informacji, które są zazwyczaj dodatkowo niezrozumiałe i nieczytelne. Z drugiej strony nieprzekazanie konsumentowi informacji rodzi wiele negatywnych konsekwencji dla przedsiębiorcy. Zjawisko niewłaściwego spełniania obowiązków informacyjnych stało się tak powszechne, że doczekało się określenia *information overkill*. Przedsiębiorcy próbują więc sprostać wymogom prawnym i szukają różnych sposobów na lepsze sformułowanie komunikatów. W pierwszej części artykułu zostanie dokonana analiza przepisów prawnych pod kątem obowiązków informacyjnych przedsiębiorcy świadczącego usługi drogą elektroniczną, a następnie zostaną zaprezentowane konsekwencje niewłaściwego informowania konsumenta. W końcowej części zostaną przedstawione dwa wybrane narzędzia, które mogą stanowić rozwiązanie problemu tzw. *information overkill*.

Uwagi wstępne

Nie da się nie zauważyć, że pandemia koronawirusa COVID-19 w znacznej mierze przyczyniła się do gwałtownego rozwoju świadczenia usług drogą elektroniczną. W obliczu różnorodnych ograniczeń w funkcjonowaniu wielu zakładów pracy czy przemieszczaniu się obywateli, mających na celu przeciwdziałanie rozprzestrzenianiu się wirusa SARS-CoV-2, usługi, których charakter pozwalał na świadczenie ich bez równoczesnej obecności stron, przeniosły się do wirtualnego świata. Prawo zobowiązań charakteryzuje się tym, że zezwala stronom na dość dużą swobodę w kształtowaniu stosunku zobowiązaniowego i choć jest ono bardzo kompleksowo uregulowane, to wobec rozwoju nowych technologii zdaje się być już przestarzałe, a zatem i nieregulujące odpowiednio wielu aspektów umów elektronicznych². Cyfryzacja gospodarki nastąpiła o wiele szybciej, niż się tego można było spodziewać, stąd w ostatnim czasie o wiele łatwiej można było dostrzec problem nieprawidłowo realizowanych obowiązków informacyjnych.

Konieczność zmian w spełnianiu obowiązków informacyjnych wobec konsumenta

Brak równoczesnej obecności przedsiębiorcy i konsumenta przy zawieraniu umów drogą elektroniczną rodzi wysokie ryzyko wykorzystania braku umiejętności funkcjonowania w wirtualnym świecie nowych konsumentów. Dlatego też ustawodawca nałożył na przedsiębiorcę pewne obowiązki, które

mają zapewnić konsumentom bezpieczeństwo i zagwarantować właściwe wykonanie umów, rekompensując stronom zrozumiały brak wzajemnego zaufania przy zawieraniu umowy na odległość³. Sam cel przepisów wprowadzających obowiązki informacyjne jest słuszny, ale niekiedy nierealny. Konsument nie ma ani czasu, ani ochoty zapoznawać się z obowiązkami informacyjnymi każdego przedsiębiorcy, z którego usług korzysta online. Potrzebę zmian w przepisach dostrzegają nie tylko przedsiębiorcy, którzy muszą dołożyć wielu starań, aby sprostać oczekiwaniom stawianym przez prawo, ale także sami konsumenci otrzymujący już przy pierwszym kontakcie z przedsiębiorcą lub jego usługami zbyt dużo informacji. Organizacja Współpracy Gospodarczej i Rozwoju⁴ w badaniach nad e-commerce w czasach pandemii sformułowała postulat *de lege ferenda* o dostosowanie przepisów do innowacyjnych rozwiązań powstałych przede wszystkim podczas izolacji, w której musiał funkcjonować cały świat⁵. Oczywiście modyfikacje te

¹ Studentka V roku prawa na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. ORCID: 0000-0003-1432-4092.

² J. Gołczyński (red.), *Sporządzanie umów elektronicznych. Komentarz praktyczny, wzory umów, orzecznictwo*, Warszawa 2017, *passim*.

³ M. Węgiński, *Charakterystyka prawna umów zawieranych drogą elektroniczną*, Legalis/el. 2020.

⁴ Organizacja Współpracy Gospodarczej i Rozwoju (Organisation for Economic Co-operation and Development) to międzyrządowa organizacja zrzeszająca 38 państw w celu promowania polityki maksymalnie wspierającej gospodarkę. Organizacja ta z sukcesami działa na rzecz polepszenia standardów prawnych w zakresie gospodarki na arenie międzynarodowej.

⁵ Organisation for Economic Co-operation and Development, *E-commerce in the time of COVID-19*, <https://www.oecd.org/coronavirus/policy-responses/e-commerce-in-the-time-of-covid-19-3a2b78e8/> (dostęp z 25.4.2022 r.).

w pierwszej kolejności powinny utworzyć środowisko przyjazne dla nowych rozwiązań, ale *de facto* oznaczać to może także zmiany w zakresie objętości obowiązku informacyjnego. Obecnie przedsiębiorca musi spełniać wymogi wynikające z różnych aktów prawnych, których istnienia nie zawsze mogą być świadomi ze względu na liczbę przepisów powszechnie obowiązujących, więc być może uregulowanie kwestii przekazywania określonych informacji w jednym akcie prawnym byłoby rozwiązaniem. W tym miejscu powstaje jednocześnie pytanie, czy aby na pewno jest to konieczne. W dalszych rozważaniach przedstawione zostaną dwa narzędzia do pracy z tekstem. Mogą one rozwiązać problem braku czytelności i zrozumiałości obowiązków informacyjnych, których zakres zostanie omówiony na przykładzie aktów prawnych mających zastosowanie do świadczenia usług drogą elektroniczną na rzecz konsumenta⁶.

Zakres obowiązków informacyjnych wspólny dla większości przedsiębiorców świadczących usługi drogą elektroniczną

Świadczenie usług drogą elektroniczną na rzecz konsumenta to oczywiście zaledwie jeden z wielu aspektów wirtualnego świata gospodarki. Dotyczy on wyłącznie relacji przedsiębiorca – konsument, czyli części działalności przedsiębiorcy, który może również zawierać umowy z innymi przedsiębiorcami czy podmiotami sektora publicznego. Co więcej, usługi muszą być świadczone za pomocą sieci telekomunikacyjnej, zatem spełnienie świadczenia musi odbyć się elektronicznie, np. przez Internet.

Pierwszym aktem prawnym mającym zastosowanie do sytuacji będącej przedmiotem badań jest ustawa z 18.7.2002 r. o świadczeniu usług drogą elektroniczną⁷. Zgodnie z art. 1 w zw. z art. 2 ustawa ta ma zastosowanie do wykonania usług świadczonych bez jednoczesnej obecności stron (na odległość), jeżeli następuje przekaz danych na indywidualne żądanie usługobiorcy, przesyłanych i otrzymywanych za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, które są w całości nadawane, odbierane lub transmitowane za pomocą sieci telekomunikacyjnej w rozumieniu ustawy z 16.7.2004 r. Prawo telekomunikacyjne⁸. W tym miejscu należy podkreślić, że nie ma znaczenia sposób zawarcia umowy, lecz jej wykonanie. Umowa może zostać zawarta przy równoczesnej obecności stron, ale może zostać zawarta również na odległość⁹. Istotne jest to, żeby usługi świadczone były bez jednoczesnej obecności stron, czyli na odległość, aby ustawa ta miała zastosowanie.

Jeżeli usługi świadczone są na rzecz konsumenta¹⁰, to należy również wziąć pod uwagę przepisy ustawy z 30.5.2014 r. o prawach konsumenta¹¹. W przypadku świadczenia usług

drogą elektroniczną dochodzi zazwyczaj również do zawarcia umowy na odległość, tj. w ramach zorganizowanego systemu zawierania umów na odległość, bez jednoczesnej fizycznej obecności stron, z wyłącznym wykorzystaniem jednego lub większej liczby środków porozumiewania się na odległość do chwili zawarcia umowy włącznie (art. 1 w zw. z art. 2 ust. 1). Wobec tego przedsiębiorca musi dostosować swoją działalność również do przepisów prawa konsumenckiego.

Kolejne dwa akty prawne regulują zasady prowadzenia działalności gospodarczej przez przedsiębiorców na terenie Polski¹². Ustawa z 6.3.2018 r. Prawo przedsiębiorców¹³ określa zasady podejmowania, wykonywania i zakończenia działalności gospodarczej na terytorium Rzeczypospolitej Polskiej, w tym prawa i obowiązki przedsiębiorców oraz zadania organów władzy publicznej w tym zakresie, a zatem odnosi się do wszystkich przedsiębiorców i jednocześnie nakłada na nich jednakowe obowiązki. Z kolei Kodeks spółek handlowych odnosi się już jedynie do spółek handlowych, czyli do ograniczonej grupy form prawnych prowadzenia działalności gospodarczej, choć dość licznej, zwłaszcza biorąc pod uwagę działalność gospodarczą w wirtualnym świecie. Niemniej jednak oba akty prawne należy wziąć pod uwagę przy analizie problemu obowiązków informacyjnych przy świadczeniu usług drogą elektroniczną.

Na koniec wskazać należy także rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)¹⁴, które jako akt prawa unijnego stosowany bezpośrednio w relacjach horyzontalnych nakłada również znaczne obowiązki informacyjne na przedsiębiorców, którzy przetwarzają dane osobowe w związku ze świadczeniem usług na odległość. W przeważającej

⁶ Przykładem świadczenia usług drogą elektroniczną na rzecz konsumenta są usługi świadczone w modelu Software as a Service (SaaS), czyli np. korzystanie przez konsumenta z usług Office 365 świadczonych przez Microsoft Ireland Operations Limited.

⁷ T.j. Dz.U. z 2020 r. poz. 344 ze zm.; dalej jako: ŚwUsłElekU.

⁸ T.j. Dz.U. z 2022 r. poz. 1648 ze zm.

⁹ Por. M. Świerczyński, [w:] J. Gołaczyński (red.), Ustawa o świadczeniu usług drogą elektroniczną. Komentarz, Warszawa 2009, komentarz do art. 2 oraz wyrok SOKiK z 6.12.2021 r., XVII AmA 19/20, Legalis.

¹⁰ Konsument, zgodnie z art. 221 KC, to osoba fizyczna dokonująca z przedsiębiorcą czynności prawnej niezwiązanej bezpośrednio z jej działalnością gospodarczą lub zawodową. Dodatkowo przepisy konsumenckie mają zastosowanie do osoby fizycznej zawierającej umowę bezpośrednio związaną z jej działalnością gospodarczą, gdy z treści tej umowy wynika, że nie posiada ona dla tej osoby charakteru zawodowego, wynikającego w szczególności z przedmiotu wykonywanej przez nią działalności gospodarczej, udostępnionego na podstawie przepisów o CEIDG.

¹¹ T.j. Dz.U. z 2020 r. poz. 287 ze zm.; dalej jako: PrKonsU.

¹² Przedsiębiorca to osoba fizyczna, osoba prawna i jednostka organizacyjna, o której mowa w art. 331 § 1, prowadząca we własnym imieniu działalność gospodarczą lub zawodową zgodnie z art. 431 KC.

¹³ T.j. Dz.U. z 2021 r. poz. 162 ze zm.

¹⁴ Dz.Urz. UE L Nr 119, s. 1; dalej jako: RODO.

większości przypadków są oni w stanie zidentyfikować konsumenta będącego drugą stroną umowy, a zatem przepisy RODO będą miały również zastosowanie.

Choć każdą działalność przedsiębiorcy w sieci należy oceniać *in concreto*, to powyższe akty prawne cechuje pewnego rodzaju wspólność. Są one głównymi źródłami prawa, które przyznają osobom fizycznym będącym beneficjentem usług świadczonych na odległość określone uprawnienia do otrzymania pewnych informacji. Każdy akt prawny ze względu na swój obszar regulacji w innym stopniu i zakresie reguluje obowiązek informacyjny przedsiębiorcy wobec konsumenta. Mimo to można wyróżnić tożsamą część wszystkich obowiązków informacyjnych w zakresie identyfikacji przedsiębiorcy.

Poniższa tabela stanowi zestawienie informacji, które zgodnie z prawem przedsiębiorca powinien przekazać konsumentowi przed lub w związku z zawarciem umowy. Analiza obowiązków informacyjnych prowadzi do wniosku, że bezwzględnie konsument musi mieć możliwość poznania przynajmniej firmy i siedziby lub nawet dokładnego adresu przedsiębiorcy. Ponadto powtarza się także zobowiązanie przedsiębiorcy do ujawnienia adresu poczty elektronicznej czy numeru identyfikacji podatkowej (NIP), a także oznaczenia organu rejestrowego. Choć normy prawne odnoszą się do tych samych informacji, to jednak różnice w używanym przez ustawodawcę słownictwie odnoszącym się do tych samych *de facto* informacji mogą być mylące dla przedsiębiorcy i konsumenta.

Ustawa o świadczeniu usług drogą elektroniczną	Ustawa o prawach konsumenta	Kodeks spółek handlowych	Prawo przedsiębiorców	RODO
Artykuł 5 ust. 2, 3 i 5: 1) firma; 2) siedziba i adres; 3) adresy elektroniczne; 4) jeżeli usługodawcą jest przedsiębiorca, podaje on również informacje dotyczące właściwego zezwolenia i organu zezwalającego, w razie gdy świadczenie usługi wymaga, na podstawie odrębnych przepisów, takiego zezwolenia; 5) jeżeli usługodawcą jest osoba fizyczna, której prawo do wykonywania zawodu jest uzależnione od spełnienia określonych w odrębnych ustawach wymagań, podaje również: a) w przypadku ustanowienia pełnomocnika, jego imię, nazwisko, miejsce zamieszkania i adres albo jego nazwę lub firmę oraz siedzibę i adres; b) samorząd zawodowy, do którego należy; c) tytuł zawodowy, którego używa, oraz państwo, w którym został on przyznany; d) numer w rejestrze publicznym, do którego jest wpisany wraz ze wskazaniem nazwy rejestru i organu prowadzącego rejestr; e) informację o istnieniu właściwych dla danego zawodu zasad etyki zawodowej oraz o sposobie dostępu do tych zasad.	Artykuł 12 ust. 1: 1) firma; 2) adres przedsiębiorstwa; 3) adres poczty elektronicznej; 4) numer telefonu lub faksu, jeżeli są dostępne, pod którymi konsument może szybko i efektywnie kontaktować się z przedsiębiorcą; 5) organ, który zarejestrował działalność gospodarczą, numer, pod którym został zarejestrowany; 6) adres, pod którym konsument może składać reklamacje, jeżeli jest inny niż adres, o którym mowa w art. 12 ust. 1 pkt 3.	Artykuł 206 § 1, art. 300 ⁶¹ § 1, art. 374 § 1 i art. 127 § 5: 1) firma spółki; 2) siedziba i adres; 3) numer identyfikacji podatkowej (NIP); 4) numer telefonu lub faksu jeżeli są dostępne, pod którymi konsument może szybko i efektywnie kontaktować się z przedsiębiorcą; 5) oznaczenie sądu rejestrowego, w którym przechowywana jest dokumentacja spółki oraz numer pod którym spółka jest wpisana do rejestru; 6) wysokość kapitału zakładowego, a dla spółki, której umowę zawarto przy wykorzystaniu wzorca umowy, do czasu pokrycia kapitału zakładowego, także informację, że wymagane wkłady na kapitał zakładowy nie zostały wniesione. 7) oznaczenie grupy spółek, jeżeli spółka do niej należy ¹⁵ .	Artykuł 20 ust. 3: 1) firma; 2) siedziba albo adres ¹⁶ ; 3) numer identyfikacji podatkowej (NIP).	Artykuł 13 i 14: 1) tożsamość ¹⁷ ; 2) dane kontaktowe; 3) tożsamość i dane kontaktowe swojego przedstawiciela; 4) dane kontaktowe inspektora ochrony danych.

¹⁵ Artykuł 206 § 1 pkt 5 został dodany ustawą z 9.2.2022 r. (Dz.U. poz. 807 ze zm.), która weszła w życie 13.10.2022 r.

¹⁶ Nieostre określenie przez ustawodawcę zakresu obowiązkowych informacji, które należy umieszczać w ofercie, powoduje pewne wątpliwości natury interpretacyjnej. Nie jest jasne bowiem, o jaki dokładnie adres chodziło ustawodawcy, gdyż może to być rozumiane jako dokładny adres siedziby, którą rozumie się jako miejscowość (wówczas adresem byłby następujący zestaw danych: ulica, numer budynku, numer lokalu, kod pocztowy, miejscowość) lub jako adres jakiegokolwiek innego miejsca, gdzie przedsiębiorca prowadzi swoją działalność (por. *M. Zdyb, G. Lubeńczuk, A. Wołoszyn-Cichońska*, Prawo przedsiębiorców. Komentarz, Lex/el. 2019, komentarz do art. 20). Rozważania te są o tyle istotne, że w ustawie Prawo przedsiębiorców w przeciwieństwie do np. ustawy o świadczeniu usług drogą elektroniczną czy Kodeksu spółek handlowych ustawodawca zdecydował się zastosować spójnik „albo” zamiast spójnika „i” między siedzibą a adresem. Zatem przyjęcie w miejsce koniunkcji alternatywy rozłącznej i brak jednoznacznego określenia znaczenia słowa „adres” powodują, że obowiązek informacyjny zostanie spełniony, nawet jeżeli przedsiębiorca poda jakikolwiek adres, zamiast adresu siedziby, co może utrudnić identyfikację przedsiębiorcy.

¹⁷ Tożsamość administratora danych, którym jest przedsiębiorca, na gruncie przepisów Ogólnego rozporządzenia o ochronie danych rozumiana jest podobnie jak w przypadku ustaw wskazanych w powyższej tabeli. W doktrynie przyjmuje się, że administrator danych osobowych, realizując obowiązek informacyjny z art. 13 lub 14, powinien podać podmiotowi danych firmę przedsiębiorstwa oraz adres w rozumieniu dokładnego położenia geograficznego, a zatem ulicę, numer budynku, numer lokalu, kod pocztowy i miejscowość. Celem ustawodawcy jest zapewnienie podmiotowi danych (konsumentowi) informacji, gdzie może on znaleźć przedsiębiorcę [por. *P. Litwiński* (red.), Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Komentarz, Legalis/el. 2021, komentarz do art. 13].

Szczegółowe elementy obowiązków informacyjnych wynikające z poszczególnych aktów prawnych

Oprócz opisanych wyżej tożsamyh elementów obowiązków informacyjnych przedsiębiorcy świadczącego usługi drogą elektroniczną na rzecz konsumenta w zakresie identyfikacji przedsiębiorcy, warto zwrócić również uwagę na inne elementy, które powtarzają się niezależnie od charakteru usług zawsze wtedy, gdy: (1) usługi świadczone są drogą elektroniczną, (2) odbiorcą usług jest konsument, (3) w związku ze świadczeniem usług dochodzi do przetwarzania danych osobowych konsumenta.

Ustawa o świadczeniu usług drogą elektroniczną

W związku z faktem świadczenia usług drogą elektroniczną usługodawca (przedsiębiorca) jest obowiązany zapewnić usługobiorcy (konsumentowi) dostęp do:

- 1) informacji o szczególnych zagrożeniach związanych z korzystaniem z usługi świadczonej drogą elektroniczną (art. 6 pkt 1 ŚwUsłElekU);
- 2) informacji o funkcji i celu oprogramowania lub danych niebędących składnikiem treści usługi, wprowadzanych przez usługodawcę do systemu teleinformatycznego, którym posługuje się usługobiorca (art. 6 pkt 2 ŚwUsłElekU);
- 3) regulaminu świadczenia usług drogą elektroniczną (art. 8 ust. 1 ŚwUsłElekU), który zawiera w szczególności:
 - a) rodzaje i zakres usług świadczonych drogą elektroniczną (art. 8 ust. 3 pkt 1 ŚwUsłElekU),
 - b) warunki świadczenia usług drogą elektroniczną (art. 8 ust. 3 pkt 2 ŚwUsłElekU), w tym:
 - wymagania techniczne niezbędne do współpracy z systemem teleinformatycznym, którym posługuje się usługodawca,
 - zakaz dostarczania przez usługobiorcę treści o charakterze bezprawnym,
 - c) warunki zawierania i rozwiązywania umów o świadczenie usług drogą elektroniczną (art. 8 ust. 3 pkt 3 ŚwUsłElekU),
 - d) tryb postępowania reklamacyjnego (art. 8 ust. 3 pkt 4);
- 4) szczegółowych informacji o świadczonej przez przedsiębiorcę usłudze informacji handlowej (art. 9 ŚwUsłElekU).

Zazwyczaj wszystkie powyższe informacje znajdują odzwierciedlenie w regulaminie lub popularnej ostatnio podstronie tzw. helpdesk lub FAQ (Frequently Asked Questions), zwłaszcza w zakresie informacji o zagrożeniach (pkt 1 powyżej).

Ustawa o prawach konsumenta

Konsumenci w rozumieniu art. 221 KC oraz art. 38a PrKonsU powinni poza danymi identyfikującymi przedsię-

biorcę i informacjami wskazanymi w ustawie o świadczeniu usług drogą elektroniczną otrzymać także następujące informacje najpóźniej w chwili wyrażenia woli zawarcia umowy na odległość:

- 1) główne cechy świadczenia z uwzględnieniem przedmiotu świadczenia oraz sposobu porozumiewania się z konsumentem;
- 2) łączna cena lub wynagrodzenie za świadczenie wraz z podatkami, ewentualnie sposób obliczenia;
- 3) koszty korzystania ze środka porozumiewania się na odległość w celu zawarcia umowy, jeśli są wyższe niż stosowane zwykle;
- 4) sposób i termin zapłaty;
- 5) sposób i termin spełnienia świadczenia przez przedsiębiorcę;
- 6) procedura rozpatrywania reklamacji;
- 7) prawo do odstąpienia od umowy, w tym zwłaszcza brak prawa odstąpienia od umowy lub okoliczności jego utraty;
- 8) obowiązek przedsiębiorcy dostarczenia rzeczy bez wad;
- 9) gwarancje i usługi posprzedażne;
- 10) kodeks dobrych praktyk;
- 11) czas trwania umowy lub sposób i przesłanki jej wypowiedzenia;
- 12) minimalny czas trwania zobowiązań konsumenta wynikających z umowy;
- 13) wysokość i sposób złożenia kaucji lub udzielenia innych gwarancji finansowych;
- 14) funkcjonalności treści cyfrowych oraz techniczne środkach ich ochrony;
- 15) mające znaczenie interoperacyjności treści cyfrowych ze sprzętem komputerowym i oprogramowaniem;
- 16) możliwości skorzystania z pozasądowych sposobów rozpatrywania reklamacji.

W praktyce spełnienie tego obowiązku informacyjnego zazwyczaj następuje w obrębie jednego dokumentu, jakim jest regulamin świadczenia usług, z zastrzeżeniem, że regulamin ten zazwyczaj odsyła do pewnych informacji zamieszczonych poza nim, np. aktualne ceny usług.

RODO

Od wejścia w życie RODO przedsiębiorcy zaczęli zwracać większą uwagę na przetwarzanie przez nich danych osobowych konsumentów, w tym zwłaszcza na prawidłowe informowanie podmiotów danych o tym, w jaki sposób ich dane są wykorzystywane. Zakres obowiązku informacyjnego na gruncie prawa ochrony danych osobowych jest dość rozległy, ponieważ oprócz informacji o tożsamości i danych kontaktowych administratora danych osobowych i inspektora ochrony danych, obejmuje również następujące informacje:

- 1) cele przetwarzania danych osobowych;
- 2) podstawę prawną przetwarzania;

- 3) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f – prawnie uzasadnione interesy;
- 4) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
- 5) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- 6) prawa podmiotu danych;
- 7) jeżeli przetwarzanie odbywa się na podstawie zgody – prawo do jej cofnięcia w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
- 8) prawo wniesienia skargi do organu nadzorczego;
- 9) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym, lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- 10) zautomatyzowane podejmowanie decyzji, w tym profilowanie;
- 11) kategorie danych osobowych (w przypadku otrzymania ich z innego źródła niż podmiot danych);
- 12) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych (w przypadku otrzymania ich z innego źródła niż podmiot danych).

Zazwyczaj administratorzy danych osobowych udostępniają konsumentom politykę prywatności i politykę cookies lub klauzulę informacyjną. W praktyce polityki prywatności stron internetowych jako dokumenty kompleksowo informujące o przetwarzaniu danych osobowych zdają się być czytelniejszym rozwiązaniem niż klauzule informacyjne, które sprawdzają się w prostych przypadkach, a świadczenie usług drogą elektroniczną raczej stanowi bardziej skomplikowany sposób przetwarzania danych osobowych.

Samo przytoczenie zakresu szczegółowych informacji będących częścią obowiązków informacyjnych przedsiębiorcy zajmuje wiele miejsca i czasu, a każdy punkt z listy trzeba dodatkowo rozwinąć i opisać. Dlatego wobec tak dużej ilości treści kluczowy jest sposób przekazania tych informacji, bo nie tylko pominięcie wybranych elementów obowiązku, ale także niewłaściwe ich zakomunikowanie konsumentowi może rodzić negatywne konsekwencje dla przedsiębiorcy.

Wybrane konsekwencje niewłaściwego spełnienia obowiązku informacyjnego

Spełnienie obowiązku informacyjnego ocenia się w kategorii jego rzeczywistej przydatności dla konsumenta, a nie intencji przedsiębiorcy. Dlatego też tak ważne jest, aby

obowiązek ten spełnić w sposób właściwy, ponieważ ustawodawca zabezpieczył konsumentów, wprowadzając różne konsekwencje w postaci kar, których główny cel należy postrzegać w ich prewencyjnej funkcji. Wizja nałożenia na przedsiębiorcę grzywny lub administracyjnej kary finansowej jest wciąż skutecznym motywatorem do postępowania zgodnie z literą prawa.

Ustawa o świadczeniu usług drogą elektroniczną

Najczęściej przedsiębiorca narażony jest na karę, jeżeli nie podaje danych pozwalających na ustalenie jego tożsamości. I tak art. 23 ŚwUsłElekU wprowadza karę grzywny dla wszystkich, którzy wbrew obowiązkowi określonym w art. 5 nie podają danych, o których mowa w art. 5 ust. 2, 3 lub 5, albo podają dane nieprawdziwe lub niepełne. Choć ten przepis nie penalizuje podania informacji w sposób niewyraźny, niejednoznaczny i niedostępny bezpośrednio poprzez system teleinformatyczny, którym posługuje się usługobiorca¹⁸, a więc nie odnosi się do sposobu komunikacji z konsumentem, nie można uznać, że kwestia ta została całkowicie pominięta przez ustawodawcę. Część danych wskazanych w art. 5 pokrywa się z obowiązkami informacyjnymi wynikającymi z innych ustaw, które przewidują sankcje za niewłaściwą treść obowiązku informacyjnego i co ważne – sposób jego zrealizowania.

Ustawa o prawach konsumenta

Bardzo szczegółowe konsekwencje niedopełnienia obowiązku informacyjnego w relacjach z konsumentem przewiduje ustawa o prawach konsumenta. Mianowicie jeżeli przedsiębiorca nie spełnił obowiązków informacyjnych dotyczących opłat dodatkowych lub innych kosztów, o których mowa w art. 12 ust. 1 pkt 5, konsument nie ponosi tych opłat i kosztów (art. 23 PrKonsU). W sytuacji spornej to przedsiębiorca musi udowodnić, że obowiązek informacyjny spełnił i to właściwie, ponieważ przekazanie konsumentowi informacji w sposób niejasny i niezrozumiały również wywołuje skutek wskazany powyżej¹⁹. Przywołany przepis odnosi się jednak wyłącznie do informacji o cenie, wynagrodzeniu i innych opłatach czy kosztach, zatem skutków niepodania innych danych należy szukać w dalszych przepisach ustawy. I tak art. 29 PrKonsU wprowadza zmianę w terminie na odstąpienie od umowy na korzyść konsumenta w przypadku zaniechania przez przedsiębiorcę obowiązku przekazania

¹⁸ K. Chałubińska-Jentkiewicz, J. Taczkowska-Olszewska, Świadczenie usług drogą elektroniczną. Komentarz, Legalis/el. 2019.

¹⁹ K. Osajda (red. serii), P. Mikłaszewicz (red. tomu), Ustawa o prawach konsumenta. Komentarz, wyd. 4, Legalis/el. 2022.

informacji o prawie odstąpienia od umowy. Konsekwencją przewidzianą przez ustawodawcę w tej sytuacji jest wygaśnięcie prawa do odstąpienia od umowy po upływie 12 miesięcy od upływu 14-dniowego terminu wynikającego z art. 27 PrKonsU.

Gdyby zakończyć lekturę przepisów na samej ustawie o prawach konsumenta, to wydawać by się mogło, że konsekwencje niespełnienia obowiązku informacyjnego z art. 12 nie są aż tak dotkliwe. Jednak byłoby to złudne wrażenie, gdyż art. 139b Kodeksu wykroczeń stanowi, że kto w zakresie działalności swojego przedsiębiorstwa, zawierając umowę z konsumentem, nie spełnia wymagań dotyczących udzielenia informacji lub wydania dokumentu, przewidzianych w przepisach ustawy o prawach konsumenta, podlega karze grzywny. Zgodnie z art. 5 Kodeksu wykroczeń nie ma znaczenia, czy przedsiębiorca umyślnie czy nieumyślnie postąpił niezgodnie z przepisami prawa konsumenckiego.

Kodeks spółek handlowych

Kodeks spółek handlowych wprowadza podstawowy obowiązek informacyjny w zakresie tożsamości przedsiębiorcy i jednocześnie przepisy karne gwarantujące jego realizację. Otóż zgodnie z art. 595 KSH członek zarządu spółki kapitałowej, jeżeli dopuszcza do tego, że pisma i zamówienia handlowe oraz informacje, o których mowa w art. 206 § 1, art. 300⁶¹ § 1 i art. 374 § 1 KSH, nie zawierają danych określonych w tych przepisach albo, będąc komplementariuszem spółki komandytowo-akcyjnej uprawnionym do reprezentowania spółki, dopuszcza do tego, że pisma i zamówienia handlowe oraz informacje, o których mowa w art. 127 § 5 KSH, nie zawierają danych określonych w tym przepisie – podlega grzywnie do 5000 zł. Grzywna w tym wypadku pełni funkcję pozapenalnego środka prawnego przymusu²⁰, której celem jest przymuszenie przedsiębiorcy do stosowania właściwego oznaczenia.

Krajowy Rejestr Sądowy

Kolejna grzywna może zostać nałożona na przedsiębiorcę na podstawie art. 34 ustawy z 20.8.1997 r. o Krajowym Rejestrze Sądowym²¹, który stanowi, że podmioty wpisane do Krajowego Rejestru Sądowego są zobowiązane umieszczać w oświadczeniach pisemnych, skierowanych w zakresie swojej działalności do oznaczonych osób i organów, dane wskazane powyżej w tabeli oraz dodatkowo oznaczenie formy prawnej wykonywanej działalności. Sąd rejestrowy, który stwierdzi niedopełnienie powyższego obowiązku, może nałożyć grzywnę, nie wyższą niż 5000 zł na osoby odpowiedzialne za niewykonanie tej powinności. Grzywna nakładana jest według uznania sądu, pod warunkiem że przedsiębiorca nie wykonał obowiązków informacyjnych albo podawał niepełne

dane, albo podawał dane nieprawdziwe, w tym także nieaktualne czy wprowadzające w błąd²². Zatem to od sądu zależy, czy grzywna zostanie nałożona, a jeśli tak, to w jakiej wysokości. Sąd posiadając w tym zakresie pewien luz decyzyjny ocenia stopień naruszenia przepisów, więc przedsiębiorca, który omyłkowo nie zaktualizuje danych, z pewnością zostanie potraktowany łagodniej niż przedsiębiorca, który całkowicie i świadomie zaniechał umieszczenia właściwego oznaczenia.

RODO

Kompleksową regulację w zakresie kar administracyjnych i odpowiedzialności cywilnej za naruszenie przepisów wprowadza RODO. Przede wszystkim art. 83 ust. 5 lit. b stanowi, że naruszenia przepisów dotyczących realizacji obowiązku informacyjnego (art. 12, 13 lub 14) podlegają administracyjnej karze pieniężnej w wysokości do 20 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. Uszczegółowienie zasad wymierzania kary znajduje się w przepisach ustawy z 10.5.2018 r. o ochronie danych osobowych²³, gdzie można znaleźć m.in. przepisy regulujące zasady przeliczania kwot euro na polską walutę, przeznaczenie uiszczonych kar administracyjnych czy kwestie terminów płatności. Kara za niespełnienie obowiązku informacyjnego obejmuje nie tylko nieprzekazanie informacji wskazanych w art. 13 lub 14, ale także niewłaściwe ich przekazanie, tj. naruszenie art. 12²⁴. Oczywiście kara administracyjna powinna być niższa w przypadku poinformowania konsumenta o wszystkich aspektach przetwarzania jego danych w sposób rozwlekły, nieprzejrzysty, niezrozumiały, w trudno dostępnej formie czy też niejasnym i skomplikowanym językiem niż w przypadku nieprzekazania żadnych informacji. Kary administracyjne w Polsce w praktyce są dosyć dotkliwe, bo np. PUODO dwa lata temu nałożył karę w wysokości 943 470,00 zł na podstawie art. 83 ust. 5 lit. b oraz nakazał spełnienie obowiązku informacyjnego wobec 682 439 osób, których dane ukarana spółka pobrała z ogólnodostępnych baz danych²⁵. Urząd Ochrony Danych Osobowych stoi zatem na straży postępowania przez przedsiębiorców zgodnie z przepisami prawa ochrony danych osobowych, choć nie wszystkie decyzje zostały utrzymane w mocy po zaskarżeniu ich do wojewódzkich sądów administracyjnych. Widoczne jednak

²⁰ J. Bieniak, M. Bieniak, G. Nita-Jagielski, Kodeks spółek handlowych. Komentarz, wyd. 8, Legalis/el. 2022.

²¹ T.j. Dz.U. z 2022 r. poz. 1683 ze zm.

²² K. Osajda (red.), Ustawa o Krajowym Rejestrze Sądowym. Komentarz, wyd. 7, Legalis/el. 2022.

²³ T.j. Dz.U. z 2019 r. poz. 1781 ze zm.

²⁴ P. Litwiński (red.), Rozporządzenie Parlamentu Europejskiego i Rady..., Legalis/el. 2021.

²⁵ Decyzja Prezesa UODO numer ZSPR.421.3.2018.

jest przykładanie dużej uwagi do samego obowiązku informacyjnego, który właściwie umożliwia podmiotom danych realizację praw. Wiele decyzji Prezesa UODO wskazuje na naruszenie przepisów odnoszących się do obowiązku informacyjnego, także w sferze samej chociażby przejrzystości²⁶. Jako że RODO stosowane jest horyzontalnie, a celem jego ustanowienia było zapewnienie pełnej realizacji jednego z podstawowych praw człowieka, jakim jest prawo do ochrony danych osobowych²⁷, wśród przepisów tego aktu prawnego można znaleźć również prawo do odszkodowania w art. 82 RODO. Otóż każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia RODO, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. W doktrynie przyjmuje się, że konstrukcja tej odpowiedzialności odszkodowawczej jest zbliżona do odpowiedzialności odszkodowawczej za czyny niedozwolone²⁸. Roszczenie podmiotu danych jest niezależne od innych uprawnień i możliwe do dochodzenia w przypadku wykazania, że szkoda powstała wskutek naruszenia przepisów z zakresu ochrony danych osobowych.

Nie sposób w tym opracowaniu wymienić wszystkich przepisów, które mogłyby mieć zastosowanie do sytuacji wynikających z nieodpowiedniego spełnienia obowiązków informacyjnych powstających przy świadczeniu usług drogą elektroniczną. Dla przykładu jedynie można wskazać tutaj również art. 5 ustawy z 23.8.2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym²⁹ czy nawet art. 286 KK. Choć przedsiębiorcy często nie są świadomi grożącej im odpowiedzialności z powodu niewłaściwego spełnienia obowiązków informacyjnych i często bagatelizują znaczenie regulaminów, polityk prywatności, klauzul informacyjnych czy nawet treści umieszczanych na stronach internetowych, to powyższa analiza przepisów prawa uzasadnia przyłożenie dużej uwagi do informacji przekazywanych konsumentowi.

Information overkill

Spełnienie obowiązku informacyjnego to nie tylko samo przekazanie informacji, ale także użyta forma. Zjawisko zarzucenia konsumenta różnorodnymi informacjami o przedsiębiorcy i świadczonych usługach stało się ostatnio tak powszechne, że doczekało się swojej nazwy – *information overkill*³⁰. Rozbudowane obowiązki informacyjne wynikające z różnych aktów prawnych coraz częściej przynoszą odwrotny skutek niż zamierzony. Informacje stają się nieczytelne przez to, że jest ich zbyt dużo w jednym miejscu. Z jednej strony doktryna wskazuje, że spełnianie obowiązku informacyjnego ma następować w taki sposób, aby konsument nie musiał wykonywać żadnych czynności, aby zapoznać się z jego treścią³¹. Jednak taka interpretacja przepisów prowadziła by do zupełnie niepraktycznych rozwiązań, przedsiębiorca musiałby bowiem często przy pierwszym wejściu na jego

stronę internetową wyświetlać wszystkie informacje w postaci ciągłego tekstu, np. jako powiadomienie typu „pop-up”. Wówczas wątpliwe byłoby spełnienie przez przedsiębiorcę wymogu przejrzystego tekstu, a zatem konsument mógłby powoływać się na niewłaściwe spełnienie obowiązku informacyjnego w sytuacji spornej ze względu właśnie na nieczytelność komunikatu. Na szczęście istnieje również przeciwnie stanowisko doktryny, które nie tylko pozwala na umieszczenie części obowiązku informacyjnego w innym miejscu, ale wręcz stanowczo opowiada się za umieszczaniem informacji na kolejnych podstronach³². Za słuszością takiej wykładni opowiada się także Europejska Rada Ochrony Danych, która m.in. wskazuje to rozwiązanie jako szczególnie pomocne dla użytkowników urządzeń mobilnych z niewielkimi wyświetlaczami³³. Stosując w praktyce takie podejście do obowiązku informacyjnego, należy pamiętać, że podzielenie treści musi być czytelne, a hiperłącza muszą być właściwie i zrozumiale opisane. Zatem trzeba mieć cały czas na względzie to, że takie rozwiązanie ma ułatwić konsumentowi zapoznanie się z informacjami, a nie utrudnić. Przykładem niewłaściwego spełnienia obowiązku informacyjnego mogą być tzw. cookie walls. Przedsiębiorcy czasami wyświetlają komunikat o plikach cookies (element obowiązku informacyjnego z RODO) blokujący dostęp do strony internetowej i wymuszający wyrażenie zgody na przetwarzanie tych metadanych. Taka forma poinformowania konsumenta jest nieefektywna, ponieważ po pierwsze konsument musi wyrazić zgodę, która w efekcie jest nieważna³⁴, a po drugie komunikat ten jest nieczytelny i często nawet nie zawiera podstawowych danych identyfikujących przedsiębiorcę, natomiast zawiera wiele ogólnych informacji o RODO czy przetwarzaniu danych.

²⁶ Zob. motyw 58 RODO. Ustawodawca unijny wskazuje, że jego celem jest nie tylko wymuszenie od przedsiębiorcy podania wskazanych danych, ale także zastosowanie odpowiedniej formy, w tym także dostosowanej do dzieci. Pewną nowością w porównaniu do innych ustaw tworzących obowiązki prawne jest wskazanie na wizualne formy przekazania treści. Warto zatem rozważyć stosowanie infografik, które w interesujący sposób mogą przekazać dość skomplikowane i obszerne treści informacji o przetwarzaniu danych osobowych.

²⁷ M. Sakowska-Baryła (red.), Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, Warszawa 2018.

²⁸ P. Fajgielski, Ogólne rozporządzenie o Ochronie Danych. Ustawa o ochronie danych. Komentarz, Warszawa 2018.

²⁹ T.j. Dz.U. z 2017 r. poz. 2070 ze zm.

³⁰ M. Stec (red.), Prawo umów handlowych. System Prawa Handlowego, Tom 5C, wyd. 1, Legalis/el. 2020.

³¹ M. Węgiński, Charakterystyka prawna umów zawieranych drogą elektroniczną, Legalis/el. 2020.

³² P. Litwiński, [w:] P. Podrecki (red.), Prawo Internetu, Lex/el. 2004.

³³ European Data Protection Board, Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, Wersja 1.1, przyjęta 4.5.2020 r.

³⁴ Zgoda wyrażona w tej sytuacji nie jest dobrowolna, gdyż od jej udzielenia zależy możliwość wejścia na stronę internetową przedsiębiorcy, a zatem świadczenie usług następuje pod warunkiem udzielenia zgody (zob. European Data Protection Board, Wytyczne 05/2020...).

Proponowane rozwiązania problemu *information overkill*

Problem tzw. *information overkill* można postrzegać w dwóch płaszczyznach: pierwsza z nich to objętość tekstu przekraczająca możliwości zapoznania się z nim przeciętnego konsumenta, a druga to sposób komunikacji.

W zakresie pierwszej płaszczyzny niewiele przedsiębiorca może zrobić, gdyż obowiązki informacyjne jako przepisy semiimperatywne nie mogą być stosowane przez przedsiębiorców w zakresie węższym niż wyznaczonym przez akt prawa. Skoro nie można zmniejszyć ilości informacji przekazywanych konsumentowi, to pozostaje jedynie zmienić formę przekazu. Najmniej skuteczną formą jest tzw. ściana tekstu, czyli umieszczenie wszystkich informacji w jednym miejscu i wyświetlanie ich jednocześnie konsumentowi. Dlatego też coraz częściej jako rozwiązanie nieczytelności informacji spotyka się warstwowe informowanie konsumenta. Grupa Robocza Art. 29³⁵ zalecała unikanie przeładowania informacyjnego właśnie poprzez stosowanie warstwowego obowiązku informacyjnego³⁶. Rozwiązanie to sprawia, że treści stają się bardziej przystępne, a jednocześnie dostępne dla konsumenta.

Kolejny sposób na złagodzenie skutków rzetelnego wypełniania przez przedsiębiorców nałożonych na nich obowiązków to odformalizowanie języka, czyli stosowanie prostego języka (ang. *plain language*). Aby zrozumieć koncepcję stosowania *plain language* przez prawników, należy zacząć od wyjaśnienia, na czym ona polega. Jako że nie jest to pojęcie języka prawniczego, a z zakresu językoznawstwa, słuszne wydaje się zatem odwołanie do definicji sformułowanej przez samych językoznawców. Otóż na podstawie badań naukowych nad tym zjawiskiem udało im się sformułować następującą definicję: „Prosty język (*plain language*) – sposób organizacji tekstu, który zapewnia przeciętnemu obywatelowi szybki dostęp do zawartych w nim informacji, lepsze ich zrozumienie oraz – jeśli trzeba – skuteczne działanie na ich podstawie”³⁷, którą należy uznać za wyczerpującą i prawidłowo opisującą zjawisko będące przedmiotem niniejszego artykułu. O tym, że język prawniczy jest trudny, świadczą badania naukowe polegające np. na mierzeniu stopnia trudności regulaminów świadczenia usług podmiotów z branży telekomunikacyjnej³⁸ za pomocą dedykowanych do tego narzędzi, takich jak np. FOG³⁹. Istnieje zatem obiektywna potrzeba zmiany podejścia do języka stosowanego przez prawników. O wyższej skuteczności komunikacji zbudowanej na bazie koncepcji *plain language* w relacji przedsiębiorca – konsument świadczą liczne badania empiryczne. Jedne z nich zasługują na szczególnej uwadze, gdyż odnoszą się do przywołanej powyżej ustawy o prawach konsumenta⁴⁰. Otóż po uproszczeniu języka ustawy okazało się, że stała się ona o wiele bardziej przystępna i zrozumiała dla osób bez wykształcenia prawniczego. Wystarczyło dodać stronę tytułową, streszczenie, spis treści, za-

mienić wyrażenia takie jak „umowa zawierana na odległość, przy użyciu środków komunikacji elektronicznej” na „umowa zawierana przez internet”, dodać infografiki, aby treść stała się bardziej przystępna. Okazało się, że nie tylko osoby bez wykształcenia prawniczego, ale także te z tytułem magistra prawa o wiele częściej odpowiadały poprawnie na pytania dotyczące treści aktu, mając do dyspozycji ustawę o prawach klienta, czyli ustawę o prawach konsumenta zmienioną zgodnie z ideą *plain language*. Zatem koncepcja ta może pochwalić się niepodważalnymi argumentami za jej stosowaniem. Uproszczenie komunikacji nie tylko pozytywnie wpływa na skuteczność realizacji obowiązków informacyjnych, ale także może pozytywnie zmienić wizerunek przedsiębiorcy jako podmiotu, który w przeciwieństwie do konkurentów nie tworzy sztucznej bariery w relacji z klientami.

Podsumowanie

Z jednej strony istniejące obowiązki informacyjne przedsiębiorcy wobec konsumenta w zamyśle ustawodawcy mają go chronić przed wykorzystywaniem przez przedsiębiorcę przewagi w relacji przedsiębiorca – konsument, a z drugiej strony poziom ich szczegółowości negatywnie wpływa na czytelność przekazu.

W związku z tym wśród prawników zajmujących się prawem nowych technologii pojawiło się innowacyjne podejście do sposobu spełniania obowiązków informacyjnych, które w założeniu ma ułatwić konsumentowi przyswojenie informacji o samym przedsiębiorcy, świadczonych usługach czy przysługujących uprawnieniach. Sam zamysł zmiany hermetycznego języka prawniczego na zrozumiały język jest jak najbardziej słuszny, jednak należy z pewną dozą ostrożności

³⁵ Grupa Robocza Artykułu 29 to niezależna europejska grupa robocza o charakterze doradczym, która zajmowała się kwestiami związanymi z ochroną prywatności i danych osobowych do dnia wejścia w życie Ogólnego Rozporządzenia o Ochronie Danych Osobowych (25.5.2018 r.) na podstawie art. 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

³⁶ Grupa Robocza Art. 29, Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679, przyjęte 29.11.2017 r., ostatnio zmienione i przyjęte 11.4.2018 r., 17/PL GR260 rev.01, <https://uodo.gov.pl/pl/file/1430> (dostęp z 25.4.2022 r.).

³⁷ T. Piekot, G. Zarzeczny, E. Moroń, Standard plain language w polskiej sferze publicznej, [w:] M. Zaśko-Zielińska, K. Kredens (red.), *Lingwistyka kryminalistyczna. Teoria i praktyka*, Wrocław 2019, s. 197–214, http://ppp.uni.wroc.pl/pliki/standard_plain_language_w_polskiej_sferze_publicznej.pdf (dostęp z 25.4.2022 r.).

³⁸ Badania naukowe na ten temat prowadzili studenci filologii polskiej w ramach działalności Pracowni Prostej Półszczyzny Uniwersytetu Wrocławskiego. Więcej o badaniach zob.: <http://www.ppp.uni.wroc.pl/pliki/styl-plain-language-i-przystepnosc-jezyka-publicznego-jako-nowy-kierunek-w-polskiej-polityce-jezykowej.pdf> (dostęp z 25.4.2022 r.).

³⁹ Więcej o narzędziach do mierzenia trudności treści: W. Gruszczynski, M. Ogrodniczuk (red.), *Jasnopis, czyli mierzenie zrozumiałości polskich tekstów użytkowych*, Wydawnictwo Asra, Warszawa 2015.

⁴⁰ N. Zych, *Uproszczenie ustawy o prawach konsumenta – Plain legal language a język prawny*, *Oblicza Komunikacji* 2019, Nr 1.

podchodzić do upraszczania komunikatów. Przede wszystkim *plain language* nie może zamienić się w upraszczanie tekstu, nie chodzi bowiem o ingerencję w treść, a w stylistykę⁴¹. Często nieumiejętne zabiegi stylistyczne prawników opracowujących obowiązki informacyjne prowadzą do utraty istoty obowiązku informacyjnego, gdyż stosują oni język potoczny zamiast prostego. W konsekwencji konsument otrzymuje informacje, z których niewiele wynika, i choć wie, że przysługuje mu konkretne prawo, wciąż nie wie, w jakim zakresie i w jaki sposób może je zrealizować. Kolejne zagrożenie niesie za sobą traktowanie odbiorcy obowiązku informacyjnego jako osoby słabo wykształconej⁴². Takie podejście może stwarzać ryzyko infantylności tekstu i wywołania efektu urażenia konsumenta, który czytając obowiązki informacyjne, odczuwa, że tekst został napisany w sposób umniejszający jego wiedzy i inteligencji. Często prawnicy uważają, że idea *plain language* jest dostosowanie treści do osób z niższym wykształceniem lub bez wykształcenia prawniczego, choć prawidłowym rozumieniem celu stosowania takich zabiegów stylistycznych powinno być po prostu unikanie tworzenia sztucznej trudności i niezrozumiałości języka. Przecież zazwyczaj treści obowiązków informacyjnych są kierowane do szerokiego grona odbiorców, wśród których mogą znajdować się zarówno osoby z wykształceniem średnim lub wyższym, ale nieprawniczym, jak i sami prawnicy czy osoby ze stopniami naukowymi.

Dużo mniejsze problemy w stosowaniu rodzi warstwowe informowanie konsumenta, które należy generalnie ocenić pozytywnie, z zastrzeżeniem jednak, że nie może ono służyć

Słowa kluczowe: świadczenie usług drogą elektroniczną, obowiązek informacyjny, przedsiębiorca, konsument, dane osobowe, RODO, *information overkill*, *plain language*.

ukrywaniu pewnych informacji. Celem wprowadzenia takiego rozwiązania jest ułatwienie konsumentowi zapoznania się z poszczególnymi informacjami, a nie utrudnianie dostępu do nich. Jeżeli warstwowe informowanie powoduje, że konsument ma problem w odnalezieniu informacji lub dotarcie do nich wymaga poświęcenia większej ilości czasu niż odnalezienie jej w tekście ciągłym, to znaczy, że nie tylko nie doszło do uproszczenia, ale wręcz do utrudnienia i skomplikowania procesu informowania.

Umiejętne i przemyślane rozwiązania z pewnością przyczynią się do zwiększenia czytelności i przejrzystości obowiązków informacyjnych. Należy jednak pamiętać, że wymaga to odpowiedniej wiedzy i umiejętności językowych, gdyż nie każda próba zastosowania *plain language* kończy się sukcesem. Wobec tego wydaje się, że konieczna jest gruntowna zmiana w sposobie nauczania prawa podczas studiów i dalszej aplikacji, gdzie obecnie kładzie się duży nacisk na formalizm i używanie języka prawniczego, który staje się podstawowym językiem w późniejszej pracy prawników. Tak wykształceni prawnicy mogą później nie zauważać tego, że przygotowywane przez nich obowiązki informacyjne nie są czytelne dla adresatów.

⁴¹ T. Piekot, G. Zarzeczny, E. Moroń, Standard plain language...

⁴² T. Piekot, M. Maziarski, Styl „plain language” i przystępność języka publicznego jako nowy kierunek w polskiej polityce językowej [w:] Acta Universitatis Wratislaviensis, No 3588, Język a Kultura, tom 24, Wrocław 2014 <http://www.ppp.uni.wroc.pl/pliki/styl-plain-language-i-przystepnosc-jezyka-publicznego-jako-nowy-kierunek-w-polskiej-polityce-jezykowej.pdf> (dostęp z 25.4.2022 r.).

Entrepreneurs' information obligations characteristic to the electronic provision of services to the consumer and plain language and layered information obligations as a proposed solution to the so-called information overkill problem

The electronic provision of services regarding the entrepreneur-consumer relationship is characterized by the lack of parties' simultaneous presence that affects mutual trust. By introducing various information obligations, the legislator tries to compensate this lack of trust and protect the consumer. Therefore, the consumer is consequently overwhelmed with a huge amount of information, which is usually also incomprehensible and unclear. On the other hand, failure to provide the consumer with information has many negative consequences for the entrepreneur. The phenomenon of inadequate fulfilment of information obligations has become so common that it is now known as "information overkill". Thus, entrepreneurs are trying to meet legal requirements and are looking for various ways for consumers to better understand their statements. In the first part of the article the author analyses legal provisions in terms of information obligations of entrepreneurs providing services electronically, and then she presents the consequences of inadequate informing of the consumer. In the final part the author presents two selected tools that can solve the problem of the so-called information overkill.

Key words: provision of services by electronic means, information obligation, entrepreneur, consumer, personal data, GDPR, information overkill, plain language.

Ochrona konsumenta zawierającego umowy elektroniczne

Marlena Sobczak¹

Celem niniejszego opracowania jest przybliżenie mechanizmów ochronnych, jakimi ustawodawca objął konsumenta, noszącego miano słabszej strony zawieranych umów, w szczególności za pośrednictwem środków komunikacji elektronicznej. W związku z powyższym, zadaniem niniejszej pracy jest przedstawienie definicji pojęcia konsumenta, zarysowanie obowiązków przedsiębiorcy ukonstytuowanym na gruncie przepisów o prawach konsumentów oraz nakreślenie obowiązujących regulacji związanych z niedozwolonymi klauzulami umownymi. Powyższe zagadnienia zostaną przedstawione w odniesieniu do wyodrębnionej przez ustawodawcę kategorii umów zawieranych przez strony online, tj. umów elektronicznych.

Uwagi wstępne

Z każdym kolejnym rokiem Internet staje się coraz popularniejszym narzędziem szeroko rozumianego codziennego życia. Dobitnie świadczą o tym dane zawarte w raporcie „Digital 2021”, który został opracowany przez We Are Social i Hottsuite. W Polsce żyje prawie 38 mln ludzi, niemal 32 mln zaś korzysta z Internetu, co stanowi 84,5% populacji kraju². Liczba korzystających z możliwości Internetu i tym samym szybko rozwijające się techniki elektronicznej komunikacji stały się asumptem do wyróżnienia i opisanie nowej kategorii umów elektronicznych. W procesie zawierania umów elektronicznych Internet staje się środkiem komunikowania oraz przesyłania oświadczeń woli pomiędzy stronami zawieranej umowy³. Cechą charakterystyczną umów elektronicznych jest zatem brak wspólności czasu i obecności obu stron podczas zawierania umowy⁴. Umowy elektroniczne mogą być zawierane online, ale wykonywane offline bądź też zawierane i wykonywane online⁵. Z punktu widzenia prawa istotne jest również to, jak należy kwalifikować strony umowy, tj. czy umowa elektroniczna zawierana jest pomiędzy konsumentami, pomiędzy przedsiębiorcami czy też stronami umowy jest zarówno konsument, jak i przedsiębiorca⁶. W sytuacji zatem gdy jedną ze stron zawieranej umowy jest konsument, drugą przedsiębiorca zaś, konieczne jest wdrożenie przez ustawodawcę odpowiednich mechanizmów obronnych, chroniących przed niekorzystnymi skutkami funkcjonowania rynku. Konsument jako podmiot mający własną pozycję na rynku, musi posiadać konkretne, oparte na bezwzględnie obowiązujących przepisach prawa, narzędzia, które w konsekwencji pozwolą mu przezwyciężyć bierność będącą skutkiem niezajomości rynku oraz praktyk biznesowych⁷.

Definicja pojęcia konsument

W celu zdefiniowania pojęcia „konsument” należy odnieść się do przepisów ukonstytuowanych na gruncie Ko-

deku cywilnego. W art. 221 KC ustawodawca podkreślił, iż konsumentem jest osoba fizyczna, która dokonuje z przedsiębiorcą czynności prawnej niezwiązanej bezpośrednio z jej działalnością gospodarczą lub zawodową. Zatem aby daną stroną umowy elektronicznej zakwalifikować jako konsumenta, w pierwszej kolejności należy dokonać oceny, czy dana strona umowy jest osobą fizyczną, dokonuje czynności prawnej, adresatem oświadczenia woli jest przedsiębiorca, a ponadto czy przedmiot dokonywanej czynności pozostaje bez związku z działalnością gospodarczą lub zawodową tej osoby⁸. Kwalifikacja konsumenta nie będzie zaś przysługiwać tak osobom prawnym, jak i jednostkom organizacyjnym niebędącym osobami prawnymi, którym ustawa przyznaje zdolność prawną. Dokonując natomiast interpretacji pojęcia czynność prawna, należy przywołać stanowisko dominujące w polskiej nauce prawa, w myśl którego na czynność prawną składa się co najmniej oświadczenie woli nakierowane na wywołanie określonych skutków prawnych w postaci ustanowienia, zmiany lub zniesienia stosunku cywilnoprawnego⁹. Zatem *a contrario* należy uznać, iż działania podejmowane przez osoby fizyczne, których elementem nie jest oświadczenie woli, nie będą zakwalifikowane jako umowy zawierane przez konsumenta¹⁰. Ustawowa definicja konsumenta

¹ ORCID: 0000-0002-8200-6902.

² Digital in Poland: All the Statistics You Need in 2021 – DataReportal – Global Digital Insights.

³ P. Podrecki, Prawo Internetu, Warszawa 2004, s. 40.

⁴ W. Kilian, [w:] J. Gołaczyński (red.), Prawne i ekonomiczne aspekty komunikacji elektronicznej, Warszawa 2003, s. 221.

⁵ J. Gołaczyński, Sporządzanie umów elektronicznych. Komentarz praktyczny, wzory umów, orzecznictwo, Warszawa 2017, s. 13.

⁶ *Ibidem*.

⁷ M. Jagielska, Ewolucja ochrony konsumenta w prawie kolizyjnym Unii Europejskiej w zakresie zobowiązań umownych, Legalis/el. 2010.

⁸ M. Gutowski, Kodeks cywilny. Komentarz do art. 1–352, Legalis/el. 2021.

⁹ Z. Radwański, [w:] A. Olejniczak, Z. Radwański (red.), System Prawa Prywatnego, podane za: K. Osajda, [w:], K. Osajda, W. Borysiak (red.), Kodeks cywilny. Komentarz, Legalis/el. 2021

¹⁰ K. Osajda, [w:] K. Osajda, W. Borysiak (red.), Kodeks cywilny..., Legalis/el. 2021.

znajduje również zastosowanie do jednostronnych czynności prawnych¹¹. Co istotne, status osoby fizycznej jako konsumenta powinien być oceniany właśnie na chwilę dokonywania czynności prawnej¹². Zaprzestanie prowadzenia działalności gospodarczej lub zawodowej nie oznacza, że osoba fizyczna powinna być uważana za konsumenta, gdy w chwili dokonywania czynności prawnej statusu takiego nie miała¹³. Odnosząc się do kolejnej przesłanki zawartej w ustawowej definicji konsumenta, podkreślić należy, iż przedsiębiorca, z którym osoba fizyczna dokonuje czynności prawnej, musi być definiowany zgodnie z art. 431 KC, tj. musi prowadzić we własnym imieniu działalność gospodarczą lub zawodową. Bez znaczenia jest natomiast, czy jest to osoba fizyczna, prawna czy jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną¹⁴. Ostatnią przesłanką pozwalającą na zakwalifikowanie danej strony umowy jako konsumenta jest brak bezpośredniego związku czynności prawnej tej osoby z działalnością gospodarczą lub zawodową. Wyrażonego podkreślenia wymaga jednak fakt, że dla ustalenia statusu konsumenta znaczenie ma brak bezpośredniego związku czynności z działalnością gospodarczą lub zawodową, nie zaś prowadzenie działalności w ogóle¹⁵. Istnienie pośredniego związku nie wyklucza zatem uznania danej osoby za konsumenta¹⁶. W praktyce stwierdzenie braku bezpośredniego związku czynności prawnej z działalnością gospodarczą lub zawodową napotyka wiele trudności, w związku z czym przedstawiciele doktryny zaproponowali, aby badając ww. związek, odnosić się do stwierdzenia, czy dokonywana czynność prawna jest typowa ze względu na rodzaj prowadzonej przez daną stronę umowy działalności¹⁷. Ponadto w doktrynie wskazuje się, iż oceniając pozycję danej osoby w stosunku cywilnoprawnym, należy odnieść się do kryteriów obiektywnych, tj. typu i rodzaju czynności prawnej, przedmiotu tej czynności, charakteru, ilości, przeznaczenia nabytego towaru oraz okoliczności towarzyszących transakcji, a także kryteriów subiektywnych, a więc woli stron oraz celu zawarcia danej umowy¹⁸. Natomiast w wyroku z 23.8.2011 r. SA w Warszawie wskazał na kontrowersyjny charakter zagadnienia kwalifikowania do grona przedsiębiorców osób wykonujących tzw. wolne zawody, jednocześnie podkreślając, iż faktycznie czynność prawna podjęta przez przedstawiciela wolnego zawodu (adwokat, radca prawny, notariusz) dokonana w bezpośrednim związku z działalnością zawodową nie będzie kwalifikowana jako podjęta przez konsumenta¹⁹. Co istotne, w orzecznictwie TS wypracowano wzorzec konsumenta, który jest właściwie poinformowany, dostatecznie uważny i rozsądny, co uzasadnia nałożenie na niego powinności wykazania aktywności i dbałości o własne interesy²⁰. Przywołany model konsumenta został powołany m.in. w wyroku z 6.7.1995 r. wydanym w sprawie *Verein gegen Uriwesen in Handel und Gewerbe Koln e.V. v. Mars GmbH*, kiedy to TS rozstrzygał kwestie dotyczące swobodnego prze-

plywu towarów, stosowania środków równoważnych przez państwa członkowskie UE, jak również zakazu ograniczeń ilościowych²¹. Wzorzec konsumenta rozsądnego, który dba o własne interesy, został również odzwierciedlony w wyroku SN z 13.6.2012 r.²². Mimo wypracowania ww. wzorca w orzecznictwie podkreśla się jednak, iż znacznie silniejsza pozycja ekonomiczna oraz społeczna i organizacyjna przedsiębiorcy wymaga zapewnienia konsumentowi równorzędności materialnej, rzeczywistej, dającej mu niezbędne „wyprzedzenie” (handicap) w relacjach z przedsiębiorcą²³. Takie stanowisko motywowane jest natomiast obowiązaniem art. 76 Konstytucji RP, z którego to wynika obowiązek władz publicznych ochrony konsumentów, m.in. przed nieuczciwymi praktykami rynkowymi²⁴.

Spełnienie przesłanek umożliwiających identyfikację danej strony umowy jako konsumenta staje się podstawą wdrożenia wzmożonej ochrony jej interesów przez ustawodawcę. Istotność powyższych uregulowań nabiera znaczenia, zwłaszcza w kontekście umów elektronicznych, które to zawierane są bez jednoczesnej obecności stron i tym samym możliwości oceny przedmiotu danej umowy. Należy zatem zaryzykować stwierdzenie, iż przypisanie danej stronie umowy elektronicznej kwalifikacji konsumenta stanowi pierwszy i podstawowy mechanizm obronny, którego konsekwencją jest wyrównanie pozycji kontraktowej stron danej umowy.

Ochrona konsumenta

Odnosząc się do zagadnienia dotyczącego ochrony konsumenta zawierającego umowy elektroniczne, w pierwszej kolejności, konkretnych uregulowań prawnych, należy poszukiwać w ustawie z 30.5.2014 r. o prawach konsumenta²⁵. Jako że cechą charakterystyczną umów elektronicznych jest brak wspólności czasu i obecności obu stron podczas zawierania umowy, umowy elektroniczne można interpretować jako umowy zawierane na odległość. Zgodnie z definicją przyjętą

¹¹ *Ibidem*.

¹² Wyrok SA w Gdańsku z 9.2.2012 r., V ACa 96/12, Legalis.

¹³ *Ibidem*.

¹⁴ R. Strugała, [w:] E. Gniewek, P. Machnikowski (red.), Kodeks cywilny. Komentarz, Legalis/el. 2021.

¹⁵ K. Osajda, [w:] K. Osajda, W. Borysiak (red.), Kodeks cywilny..., Legalis/el. 2021.

¹⁶ *Ibidem*.

¹⁷ S. Koraluk, [w:] J. Strzebińczak, E. Gniewek (red.), Kodeks cywilny. Komentarz, podane za: K. Osajda, [w:] K. Osajda, W. Borysiak (red.), Kodeks cywilny..., Legalis/el. 2021.

¹⁸ J. Gołaczyński, Sporządzanie umów..., s. 87.

¹⁹ VI Aca 262/11, Legalis.

²⁰ M. Gutowski, Kodeks cywilny..., Legalis/el. 2021.

²¹ C-470/93, Legalis.

²² II CSK 515/11, Legalis.

²³ Zob. wyrok SA w Warszawie z 28.4.2015 r., VI ACA 775/14, Legalis.

²⁴ *Ibidem*.

²⁵ Tj. Dz.U. z 2020 r. poz. 287 ze zm.; dalej jako: PrKonsU.

na gruncie ww. ustawy, umowa zawarta na odległość jest taką umową, którą zawiera konsument w ramach zorganizowanego systemu zawierania umów na odległość, bez jednoczesnej fizycznej obecności stron, z wyłącznym wykorzystaniem jednego lub większej liczby środków porozumiewania się na odległość do chwili zawarcia umowy włącznie. Zatem aby zakwalifikować daną umowę jako umowę zawieraną na odległość, łącznie muszą wystąpić cztery cechy, tj. dana umowa musi zostać zawarta pomiędzy konsumentem a przedsiębiorcą, brak jest jednoczesnej obecności stron, do zawarcia umowy strony wykorzystują jedną lub większą ilość środków porozumiewania się na odległość, przedsiębiorca będący stroną umowy działa w sposób zorganizowany²⁶. Samo wykorzystanie środka porozumiewania się na odległość nie jest jednak wystarczające do zakwalifikowania danej umowy jako zawartej na odległość²⁷. W sytuacji gdy strony zawierają umowę za pośrednictwem środków porozumienia się na odległość, jednakże znajdują się fizycznie w tym samym miejscu w momencie zawierania umowy, nie można przyjąć, iż umowa została zawarta na odległość²⁸. W literaturze podnosi się również, że jednoczesną fizyczną obecność stron umowy w tym samym czasie bez świadomości tego faktu można uznać za spełnienie przesłanki braku jednoczesnej fizycznej obecności stron, o której ustawodawca stanowi w art. 2 pkt 1 PrKonsU²⁹. Natomiast nie ma znaczenia, czy strony używają różnych środków porozumiewania się na odległość bądź też czy zmieniają ww. środki w procesie zawierania umowy, jak również sposób zawarcia umowy, a więc m.in. czy umowa została zawarta poprzez ofertę czy też negocjację³⁰. B. Kaczmarek-Templin broni również tezy, iż za umowę zawieraną na odległość należy uznać taką umowę, której warunki były negocjowane przy jednoczesnej fizycznej obecności stron, ale zawarcie umowy nastąpiło z wykorzystaniem środków porozumiewania się na odległość.

Próbując natomiast zinterpretować zakres pojęciowy środków porozumiewania się na odległość, należy odnieść się do podziału zaproponowanego przez E. Łętowską, która wskazuje na trzy kategorie środków porozumiewania się na odległość, tj. media drukowane (np. formularze, listy seryjne, katalogi reklamowe) oraz środki komunikacji telefonicznej (np. telefon, telefaks), środki komunikacji radiowej i telewizyjnej (radio, telewizja, videotekst), a także Internet, w tym poczta elektroniczna³¹. Warto podkreślić również, że poza kategorią umów zawieranych na odległość pozostaje okazjonalne zawieranie umów, a więc umowy zawierane na odległość, ale przy braku zorganizowanego po stronie przedsiębiorcy takiego sposobu zawierania umów³². Ustawodawca wymienia również umowy, które wyłączone są spod regulacji ustawy o prawach konsumenta, wskazując m.in. na umowy dotyczące gier hazardowych, przewozu osób czy też dotyczących usług socjalnych, mieszkań socjalnych, opieki nad dziećmi,

wsparcia dla rodzin i osób znajdujących się stale lub czasowo w potrzebie, w tym opieki długoterminowej.

Ochrona konsumenta zawierającego umowy elektroniczne zaproponowana przez ustawodawcę opiera się głównie na obowiązkach informacyjnych przedsiębiorcy, które to obowiązki stanowią narzędzie służące realizacji polityki „ochrony konsumenta przez informację”³³. Celem obowiązków informacyjnych nałożonych na przedsiębiorcę jest prewencyjna ochrona konsumenta oraz zapobieżenie nieprawidłowemu czy nieświadomemu zawarciu umowy przez konsumenta³⁴. To również akcesorium stworzenia równych warunków kontraktowania pomiędzy konsumentem a przedsiębiorcą, jak również kształtowania świadomości konsumenta będącego czynnym uczestnikiem rynku i w konsekwencji nadawania rynkowi cech przejrzystego, transparentnego³⁵.

Trybunał Sprawiedliwości Unii Europejskiej wielokrotnie podkreślał istotność uzyskania przez konsumenta informacji na etapie przedkontraktowym o skutkach, jakie wywoła zawarta umowa. W wyroku z 30.4.2014 r. (sprawa *Árpád Kásler Hajnalka Káslerné Rábai v. OTP Jelzálogbank Zrt*) TS zaznaczył, że: „informacja, przed zawarciem umowy, o warunkach umownych i skutkach owego zawarcia ma fundamentalne znaczenie dla konsumenta. To w szczególności na podstawie tej informacji ten ostatni podejmuje decyzję, czy zamierza związać się warunkami sformułowanymi uprzednio przez przedsiębiorcę”³⁶. Niniejsze stanowisko TS potwierdził również w wyroku z 7.9.2016 r. w sprawie *Vincent Deroo-Blanquart v. Sony Europe Limited*³⁷. Niemniej, idąc za E. Macierzyńską-Franaszczyk, zapewnienie właściwego standardu informacji przekazywanych konsumentowi jest wymagane na każdym etapie kontraktowania³⁸.

Przedsiębiorca przede wszystkim jest zobowiązany do uzyskania zgody konsumenta na wszelkie dodatkowe płatności, jak również niepobieranie od konsumenta, który kontaktuje się z przedsiębiorcą w sprawach zawartej umowy, korzystając z przeznaczonego przez przedsiębiorcę do

²⁶ J. Gołaczyński, *Sporządzanie umów...*, s. 91.

²⁷ B. Kaczmarek-Templin, [w:] B. Kaczmarek-Templin, P. Stec, D. Szostek (red.), *Ustawa o prawach konsumenta. Kodeks cywilny. Komentarz*, Warszawa 2004, s. 11.

²⁸ *Ibidem*.

²⁹ *Ibidem*.

³⁰ *Ibidem*.

³¹ E. Łętowska, *Prawo umów konsumenckich*, Warszawa 1999, s. 733–734.

³² B. Kaczmarek-Templin, [w:] B. Kaczmarek-Templin, P. Stec, D. Szostek (red.), *Ustawa o prawach...*, s. 13.

³³ E. Macierzyńska-Franaszczyk, [w:] M. Jagielska, K. Podgórski, E. Śluga-Krupa, M. Frasa (red.), *Prawa konsumenta w teorii i praktyce*, Warszawa 2018, s. 126.

³⁴ J. Gołaczyński, *Sporządzanie umów...*, s. 95.

³⁵ E. Macierzyńska-Franaszczyk, [w:] M. Jagielska, K. Podgórski, E. Śluga-Krupa, M. Frasa (red.), *Prawa konsumenta...*, s. 126.

³⁶ C-26/13, *Legalis*.

³⁷ C-310/15, *Legalis*.

³⁸ E. Macierzyńska-Franaszczyk, [w:] M. Jagielska, K. Podgórski, E. Śluga-Krupa, M. Frasa (red.), *Prawa konsumenta...*, s. 133.

tego celu numeru telefonu, opłat wyższych niż za zwykle połączenie telefoniczne³⁹. Niniejsze obowiązki powinny być spełniane w przypadku zawierania wszystkich umów konsumenckich. Natomiast dodatkowe obowiązki informacyjne zostały ukonstytuowane na gruncie art. 12 PrKonsU. Formułując katalog informacji, które muszą zostać udzielone konsumentowi, ustawodawca określa jedynie ich minimalny charakter, pozostawiając przedsiębiorcy możliwość rozszerzenia zaproponowanego katalogu obowiązków. Ponadto ustawodawca kładzie nacisk na jasne i zrozumiałe przekazywanie informacji konsumentowi. W literaturze wskazuje się, iż wymóg transparentności oznacza przekazywanie informacji w sposób czytelny, a więc informacje muszą zostać przekazane za pomocą odpowiedniego języka. Przekazywane informacje powinny być w taki sposób zredagowane, aby forma, w której są podawane, była przystępna⁴⁰. Powyższe potwierdza SIKIK w wyroku z 22.7.2009 r., zgodnie z którym: „Informacje udzielone konsumentowi powinny być wyraźne i bezpośrednie, gdyż dzięki temu konsument ma możliwość dokonania świadomej decyzji przy nabywaniu towarów i usług. Niedostarczenie konsumentowi istotnych informacji o oferowanym produkcie lub usłudze prowadzi do wypaczenia ich decyzji rynkowych”⁴¹. Także TS w wyroku z 17.12.2015 r. (w sprawie *Neptune Distribution SNC v. Ministre de l'Économie et des Finances*), odnosząc potrzebę przekazania informacji w sposób przejrzysty do względów zdrowia ludzkiego, podkreślił, iż „potrzeba zapewnienia konsumentom możliwie najdokładniejszych i najbardziej przejrzystych informacji dotyczących właściwości produktu pozostaje zaś w ścisłym związku z ochroną zdrowia ludzkiego i stanowi kwestię interesu ogólnego, który może uzasadniać ograniczenia wolności wypowiedzi przedsiębiorcy i udzielenia przez niego informacji oraz jego wolności prowadzenia działalności gospodarczej”⁴². Tym samym TS wyraźnie wyeksponował konieczność zagwarantowania konsumentowi, iż otrzyma właściwą i przejrzystą informację. Podając obowiązkowe informacje, przedsiębiorca musi również uwzględnić potrzeby szczególnie wrażliwych konsumentów wynikające m.in. z niepełnosprawności, wieku, braku wykształcenia czy też mniejszego stopnia zaradności życiowej⁴³. Powyższe potwierdza ustawodawca europejski, wskazując w dyrektywie Parlamentu Europejskiego i Rady 2011/83/UE z 25.10.2011 r. w sprawie praw konsumentów, zmieniającej dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylającej dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady, iż: „udzielając takich informacji, przedsiębiorca powinien uwzględniać szczególne potrzeby szczególnie wrażliwych konsumentów, z uwagi na ich niepełnosprawność umysłową, fizyczną lub psychiczną, wiek lub łatwowierność, w sposób, który powinien być, racjonalnie oczekując, przewidzieć”. Co istotne, uwzględnienie tego rodzaju szczególnych potrzeb

nie powinno jednak prowadzić do zróżnicowania poziomów ochrony konsumentów. G. Bar podkreśla jednak, iż obowiązkiem przedsiębiorcy jest zapewnienie konsumentom warunków do zapoznania się z przekazanymi informacjami, nie ma natomiast znaczenia, czy konsument faktycznie się z nimi zapozna. Odnosząc się do sposobu przekazania informacji, w zakresie umów zawieranych na odległość, przedsiębiorca winien użyć takiej metody, która odpowiada rodzajowi użytego środka porozumiewania się na odległość. Obowiązek informacyjny musi zostać spełniony przez przedsiębiorcę najpóźniej w chwili wyrażenia przez konsumenta woli związania się umową.

Formułując katalog danych, które przedsiębiorca obowiązany jest przekazać konsumentowi, ustawodawca rozpoczyna ich wyliczenie od nałożenia na przedsiębiorcę powinności przekazania informacji o głównych cechach świadczenia z uwzględnieniem przedmiotu świadczenia oraz sposobu porozumiewania się z konsumentem. Prawidłowe oznaczenie przedmiotu świadczenia dotyczy zarówno wskazania cech danego przedmiotu, jak i określeniu sposobu uzyskania do niego dostępu⁴⁴. Istotą wprowadzenia do katalogu danych ww. informacji jest fakt, iż konsument musi posiadać wiedzę o przedmiocie umowy oraz jakie są istotne cechy świadczenia, które wpływają na sposób korzystania z niego⁴⁵. W konsekwencji takie uregulowanie wpływa na możliwość podejmowania przez konsumenta świadomych i racjonalnych decyzji. J. Gołaczyński podkreśla również, iż w przypadku wystąpienia świadczenia polegającego na wykonaniu pewnej usługi, określając przedmiot, przedsiębiorca ma obowiązek dokładnie wskazać, na czym owo świadczenie z jego strony ma polegać⁴⁶. Co istotne, w wyroku z 19.9.2006 r. (sprawa *Lidl Belgium GmbH and Co KG v. Etablissements Franz Colruyt NV*) TS zaznaczył również, iż przedsiębiorca, czyniąc zadość obowiązkowi informacyjnym w zakresie istotnych cech produktu lub świadczenia, powinien dokładniej przedstawić właściwości charakterystyczne dla oferowanych grup produktów lub świadczeń, dzięki czemu konsument może dokonać ich porównania⁴⁷.

Kolejnym rodzajem obowiązkowych informacji są te, które dotyczą danych identyfikujących przedsiębiorcę, tj. dane o firmie, organie, który zarejestrował działalność gospodarczą, a także numerze, pod którym został zarejestrowany, adres

³⁹ B. Bar, [w:] B. Kaczmarek-Templin, P. Stec, D. Szostek (red.), Ustawa o prawach..., s. 96.

⁴⁰ *Ibidem*.

⁴¹ XVII Ama 26/09, Legalis.

⁴² C-157/14, Legalis.

⁴³ *Ibidem*.

⁴⁴ J. Gołaczyński, *Sporządzanie umów...*, s. 101.

⁴⁵ G. Bar, [w:] B. Kaczmarek-Templin, P. Stec, D. Szostek (red.), Ustawa o prawach..., s. 99.

⁴⁶ J. Gołaczyński, *Sporządzanie umów...*, s. 101.

⁴⁷ C-356/04, Legalis.

przedsiębiorcy, adres poczty elektronicznej, numer telefonu oraz faksu, jeżeli są dostępne, jak i adres, pod którym konsument może składać reklamacje. Przedsiębiorca ma obowiązek posługiwać się w obrocie prawnym i gospodarczym numerem identyfikacji podatkowej (NIP) oraz numerem rejestracji w KRS. Celem przekazania ww. danych jest zatem możliwość uzyskania przez konsumenta wiedzy, z jakim dokładnie podmiotem zawiera umowę, a nadto umożliwienie konsumentowi szybkiego kontaktu z przedsiębiorcą, zarówno drogą elektroniczną, jak również w sposób tradycyjny⁴⁸.

Ustawodawca nakazuje również przedsiębiorcy, aby poinformował konsumenta o cenie lub wynagrodzeniu. W zakresie ww. informacji wchodzi wszystkie składniki ceny lub wynagrodzenia, co w konsekwencji oznacza, że przedsiębiorca powinien wskazać kwotę należną jemu samemu, kwotę podatku, opłat za transport, kwotę opłat za dostarczenie towaru, usługi pocztowe, jak również inne koszty, które poniósł⁴⁹. W przypadku niemożności określenia wysokości ww. kosztów konsument musi zostać poinformowany o obowiązku ich uiszczenia⁵⁰. W razie zawarcia natomiast umowy na czas nieoznaczony lub umowy obejmującej prenumeratę, przedsiębiorca ma obowiązek podania łącznej ceny lub wynagrodzenia obejmującego wszystkie płatności za okres rozliczeniowy, a gdy umowa przewiduje stałą stawkę – także łącznych miesięcznych płatności. Obowiązek informacyjny spoczywa na przedsiębiorcy także w przypadku, gdy koszty korzystania ze środka porozumiewania się na odległość w celu zawarcia umowy są wyższe niż stosowane zwykle za korzystanie z tego środka porozumiewania się. Pojęcia środków zwykle stosowanych należy odnosić do cen lub wynagrodzenia rynkowego. Przedsiębiorca nie może również zaniechać poinformowania konsumenta o sposobie i terminie zapłaty, sposobie i terminie spełnienia świadczenia, jak również procedurze rozpatrywania reklamacji. W praktyce wykorzystywane są różne formy zapłaty, które zależą od uznania przedsiębiorcy. Konsument może dokonać zapłaty m.in. w formie bezgotówkowej, jak również przy wykorzystaniu wciąż popularnej formy, tj. płatności za pobraniem. To właśnie przedsiębiorca określa katalog możliwych form płatności, mając na uwadze oczekiwania i komfort konsumenta. Termin zapłaty może zostać natomiast oznaczony w dniach, tygodniach, miesiącach, poprzez wskazania konkretnej daty kalendarzowej bądź też w sposób opisowy. Z kolei spełnienie świadczenia zamówionego przez konsumenta, które może mieć charakter jednorazowy lub też ciągły, odbywa się jednorazowo, częściami bądź też okresowo⁵¹. Istnieje możliwość spełnienia świadczenia przez samego przedsiębiorcę bądź też osoby trzecie posługujące przy prowadzeniu działalności gospodarczej⁵². Ponadto sposób spełnienia świadczenia określany jest również przez miejsce jego spełnienia. Informacje o procedurze reklamacyjnej obejmują natomiast miejsce składania reklamacji, sposób składania reklamacji, sposób dostarczania towaru do miejsca

wskazanego przez przedsiębiorcę wraz ze wskazaniem kosztów dostarczenia towaru, dane, które winny zostać wskazane przez konsumenta w procedurze reklamacyjnej, jak również wskazanie terminu i sposobu rozpatrywania zgłoszeń reklamacyjnych przez przedsiębiorcę, a także procedurę uzupełniania ewentualnych jego braków⁵³.

Przedsiębiorca ma również prawny obowiązek udzielenia konsumentowi informacji o sposobie i terminie wykonania prawa do odstąpienia od umowy, kosztach zwrotu rzeczy w przypadku odstąpienia od umowy, które ponosi konsument w odniesieniu do umów zawieranych na odległość – kosztach zwrotu rzeczy, jeżeli ze względu na swój charakter rzeczy te nie mogą zostać w zwykłym trybie odesłane pocztą, a także braku prawa odstąpienia od umowy na podstawie art. 38 PrKonsU. Konsument może zatem odstąpić od umowy elektronicznej, którą zawarł w terminie 14 dni bez podawania przyczyny i ponoszenia kosztów. W tym zakresie możliwe jest skorzystanie z gotowego wzorca odstąpienia od umowy, jednakże do skutecznego wykonania przysługującego prawa wystarczy, aby konsument wyraził swoją wolę w ustawowym terminie. Z ogólnych zasad wykonywania zobowiązań wynika natomiast obowiązek przedsiębiorcy dostarczenia rzeczy wolnej od wad, a więc odpowiadającej umowie stron oraz poinformowania o tym konsumenta. Obowiązek informacyjny przedsiębiorcy to również konieczność przekazania informacji drugiej stronie umowy o gwarancji lub usługach posprzedażowych, jeżeli na zakupiony towar ma być udzielona gwarancja bądź też oferowane są tzw. usług posprzedażowe, które to informacje obejmują wiadomości o odpowiedzialności gwaranta, uprawnieniach przysługujących konsumentowi i sposobie ich realizacji⁵⁴.

Ustawodawca nakazuje także, aby przedsiębiorca poinformował konsumenta o kodeksie dobrych praktyk, a więc o zbiorze zasad postępowania, a w szczególności norm etycznych i zawodowych przedsiębiorców, którzy zobowiązali się do ich przestrzegania w odniesieniu do jednej lub większej ilości praktyk rynkowych, czasie trwania umowy i jej wypowiedzenia, minimalnym czasie trwania zobowiązań konsumenta wynikających z umowy, kaucji lub innych gwarancji finansowych, a także treściach cyfrowych i technicznych środkach ich ochrony, tj. o funkcjonalności treści cyfrowych oraz interoperacyjności tych treści ze sprzętem komputerowym i oprogramowaniem. Ponadto przedsiębiorca ma obowiązek poinformować konsumenta o pozasądowych

⁴⁸ G. Bar, [w:] B. Kaczmarek-Templin, P. Stec, D. Szostek (red.), Ustawa o prawach..., s. 99.

⁴⁹ J. Gołaczyński, Sporządzanie umów..., s. 103.

⁵⁰ *Ibidem*.

⁵¹ G. Bar, [w:] B. Kaczmarek-Templin, P. Stec, D. Szostek (red.), Ustawa o prawach..., s. 101.

⁵² *Ibidem*.

⁵³ *Ibidem*.

⁵⁴ *Ibidem*.

sposobach rozstrzygnięcia sporu, a więc tzw. alternatywnych metodach rozwiązania sporów w sprawach konsumenckich. W ramach pozasądowych sposobów rozstrzygnięcia sporu, znaczenie mogą mieć również sposoby rozstrzygnięcia sporów online, za pośrednictwem środków komunikacji elektronicznej, który to sposób funkcjonuje jako europejska platforma ORD mająca ułatwiać niezależne, bezstronne, przejrzyste, szybkie i sprawiedliwie rozwiązanie sporu przez Internet pomiędzy konsumentem a przedsiębiorcą. Co istotne, jeżeli umowa jest zawierana w imieniu innego przedsiębiorcy, należy podać dane umożliwiające identyfikację przedsiębiorcy, tj. dane o firmie, organie, który zarejestrował działalność gospodarczą, a także numerze, pod którym został zarejestrowany, adres przedsiębiorcy, adres poczty elektronicznej, numer telefonu oraz faksu, jeżeli są dostępne, jak również adres, pod którym konsument może składać reklamacje.

Niewykonanie obowiązków informacyjnych pociąga za sobą utratę przez przedsiębiorcę części jego uprawnień, ewentualnie poszerzenia uprawnień konsumenta⁵⁵. W sytuacji gdy przedsiębiorca nie spełni obowiązków informacyjnych dotyczących opłat dodatkowych lub innych kosztów, jak też kosztów zwrotu rzeczy, konsument nie może ponosić tych opłat i kosztów. Jeżeli konsument nie został poinformowany przez przedsiębiorcę o prawie odstąpienia od umowy, prawo to wygasa po upływie 12 miesięcy od dnia upływu 14-dniowego terminu. Brak wypełnienia nałożonych obowiązków wpływa również na ewentualną odpowiedzialność konsumenta za zmniejszenie wartości rzeczy będące wynikiem korzystania z niej w sposób wykraczający poza konieczny do stwierdzenia charakteru, cech i funkcjonowania rzeczy, chyba że przedsiębiorca nie poinformował konsumenta o prawie odstąpienia od umowy. Ponadto zaniechanie wykonania obowiązków może zostać uznane za nieuczciwą praktykę rynkową, naruszającą zbiorowe interesy konsumentów, delikt przedsiębiorcy bądź może zostać uznane za wykroczenie zagrożone karą grzywny.

Szczególną regulacją, która znajduje zastosowanie w umowach elektronicznych nakładających na konsumenta obowiązek zapłaty, jest konieczność udzielenia przez przedsiębiorcę, w jasny i widoczny sposób, bezpośrednio przez złożeniem zamówienia, informacji o głównych cechach świadczenia z uwzględnieniem przedmiotu świadczenia oraz sposobu porozumiewania się z konsumentem, łącznej cenie lub wynagrodzeniu za świadczenie wraz z podatkami, a gdy charakter przedmiotu świadczenia nie pozwala, rozsądnie oceniając, na wcześniejsze obliczenie ich wysokości – sposobie, w jaki będą one obliczane, a także opłatach za transport, dostarczenie, usługi pocztowe oraz innych kosztach, a gdy nie można ustalić wysokości tych opłat – o obowiązku ich uiszczenia (w razie zawarcia umowy na czas nieoznaczony lub umowy obejmującej prenumeratę przedsiębiorca ma obowiązek podania łącznej ceny lub wynagrodzenia obejmującego wszyst-

kie płatności za okres rozliczeniowy, a gdy umowa przewiduje stałą stawkę – także łącznych miesięcznych płatności), czasie trwania umowy lub o sposobie i przesłankach wypowiedzenia umowy – jeżeli umowa jest zawarta na czas nieoznaczony lub jeżeli ma ulegać automatycznemu przedłużeniu oraz minimalnym czasie trwania zobowiązań konsumenta wynikających z umowy. Dodatkowo przedsiębiorca musi zapewnić, aby konsument w momencie składania zamówienia wyraźnie potwierdził, że wie, że zamówienie pociąga za sobą obowiązek zapłaty. W przypadku gdy do składania zamówienia używa się przycisku lub podobnej funkcji, muszą być one oznaczone w łatwo czytelny sposób słowami „zamówienie z obowiązkiem zapłaty” lub innego równoważnego jednoznacznego sformułowania. Momentem wypełnienia ww. obowiązku przez przedsiębiorcę jest natomiast moment składania zamówienia. Analizując natomiast relację pomiędzy obowiązkami informacyjnymi zawartymi w art. 12 i 17 PrKonsU, w literaturze podnosi się, iż przedsiębiorca ma możliwość wywiązania się z nałożonych obowiązków równocześnie, co w konsekwencji powoduje, iż udzielenie wszystkich informacji zawartych w art. 12 ww. ustawy może nastąpić już bezpośrednio przed złożeniem zamówienia przez konsumenta⁵⁶.

Mając na celu ochronę konsumentów, ustawodawca ustanawia mechanizmy ochrony nie tylko na etapie przedkontraktowym. W art. 22 PrKonsU ustawodawca stanowi, iż informacje z katalogu, o którym mowa w art. 12, stanowią integralną część umowy zawieranej na odległość albo poza lokalem przedsiębiorstwa i mogą być zmienione jedynie za wyraźnym porozumieniem stron. Pojęcie integralności, idąc za B. Kaczmarek-Templin, należy zatem rozumieć w ten sposób, że wymienione informacje stanowią część umowy w sensie prawnym, cywilistycznym, a umowa nie może funkcjonować bez tych informacji⁵⁷. Informacje wraz z umową tworzą jeden stosunek cywilnoprawny pomiędzy konsumentem a przedsiębiorcą, wyznaczając ich wzajemne prawa i obowiązki⁵⁸. Natomiast w sensie technicznym ww. informacje nie muszą być częścią umowy, co oznacza, iż nie muszą być załączone do umowy lub też utrwalone na tym samym nośniku⁵⁹.

Mechanizm ochrony został również wzmocniony poprzez regulację zawartą w art. 21 PrKonsU, który stanowi, iż przedsiębiorca ma obowiązek przekazać konsumentowi potwierdzenie zawarcia umowy na odległość na trwałym nośniku w rozsądnym czasie po jej zawarciu, najpóźniej w chwili dostarczenia rzeczy lub przed rozpoczęciem świadczenia usługi. Ma to istotne znaczenie dla ewentualnego wstąpienia

⁵⁵ G. Bar, [w:] B. Kaczmarek-Templin, P. Stec, D. Szostek (red.), Ustawa o prawach..., s. 106.

⁵⁶ *Ibidem*.

⁵⁷ B. Kaczmarek-Templin, [w:] B. Kaczmarek-Templin, P. Stec, D. Szostek (red.), Ustawa o prawach..., s. 140.

⁵⁸ *Ibidem*.

⁵⁹ *Ibidem*.

przez konsumenta na drogę sądową celem uzyskania ochrony prawnej⁶⁰.

Ochrona praw konsumenta a niedozwolone klauzule umowne

Podjmując temat ochrony konsumenta zawierającego umowy elektroniczne, nie sposób również pominąć zagadnienia niedozwolonych klauzul umownych, które rozumiane są jako postanowienia umowy zawieranej z konsumentem niezgodnione indywidualnie. Jeśli kształtują jego prawa i obowiązki w sposób sprzeczny z dobrymi obyczajami, rażąco naruszając jego interesy, nie wiążą konsumenta. W praktyce najczęściej występującymi klauzulami niedozwolonymi są te, które ograniczają możliwość odstąpienia od umowy oraz zwrotu towaru bądź też uzależniają niniejsze prawo od wystąpienia określonych okoliczności, które nakładają na konsumenta obowiązek zachowania określonej formy lub też wymagają dokonania wraz ze złożeniem oświadczenia o odstąpieniu innej czynności, jak również te, które warunkują przyjęcie zwróconego towaru od tego, czy pozostaje on oryginalnie zapakowany, a nadto od dostarczenia dowodu zawarcia umowy w określonej postaci⁶¹.

M. Jagielska wskazuje również na regulacje rozporządzenia Rzym I, która dopuszcza w umowach konsumenckich zawieranych w handlu elektronicznym, wybór prawa, jeśli konsument nie będzie gorzej chroniony niż w miejscu swojego zwykłego pobytu⁶². W braku wyboru prawa w niniejszych umowach, umowa konsumencka powinna podlegać prawu państwa, w którym konsument ma miejsce zwykłego pobytu. Mając na uwadze powyższą regulację, w wyroku z 17.9.2014 r. SN uznał, iż zamieszczenie we wzorcu umowy konsumenckiej postanowienia przewidującego zastosowanie prawa obcego dla konsumenta, właściwego zaś dla twórcy wzorca, stanowi klauzulę niedozwoloną w rozumieniu art. 3851 § 1 KC⁶³. Oceniając stanowisko zaprezentowane przez SN, *M. Jagielska* podkreśla, iż w praktyce wyłączono możliwość dokonania przez przedsiębiorcę wyboru prawa przez zamieszczenie stosownej klauzuli w regulaminie, jednakże rozwiązanie to nie chroni konsumentów⁶⁴. Autorka zaznacza, iż wyłączenie dopuszczalności wyboru prawa może w konsekwencji spowodować ograniczenie dostępu polskich konsumentów do towarów i usług oferowanych przez zagranicznych przedsiębiorców⁶⁵.

Ostrzeżenie konsumenckie

Coraz częściej w doktrynie podnosi się, iż sankcje braku związania umową zawieraną na odległość, przy użyciu środków komunikacji elektronicznej, o których mowa w art. 17 ust. 4 PrKonsU, w rzeczywistości nie stanowią skutecznego mechanizmu chroniącego konsumentów przed nieuczciwy-

mi praktykami rynkowymi⁶⁶. Z tego też powodu ustawodawca tworzy nowe prewencyjne rozwiązania, sięgając po najskuteczniejsze środki, za które uznać należy medialne nagłaśnianie zastanych nadużyć ze strony przedsiębiorców, które to w konsekwencji przestrzegają konsumentów przez zawieraniem z nimi stosunków kontraktowych⁶⁷.

Kompetencje w zakresie zamieszczania tzw. ostrzeżeń konsumenckich, na mocy art. 73a ustawy z 16.2.2007 r. o ochronie konkurencji i konsumentów⁶⁸, przyznane zostały Prezesowi Urzędu Ochrony Konkurencji i Konsumentów (UOKiK). Jeśli zatem z informacji zgromadzonych w toku postępowania w sprawie praktyk naruszających zbiorowe interesy konsumentów wynika, że istnieje szczególnie uzasadnione podejrzenie, że przedsiębiorca dopuszcza się praktyki naruszającej zbiorowe interesy konsumentów, która może spowodować znaczne straty lub niekorzystne skutki dla szerokiego kręgu konsumentów, Prezes Urzędu podaje do publicznej wiadomości, w tym na stronie internetowej Urzędu, zgromadzone w toku postępowania informacje o tym zachowaniu i jego prawdopodobnych skutkach. Co istotne, możliwość publikacji ostrzeżenia konsumenckiego aktualizuje się dopiero wówczas, gdy toczy się postępowania przed Prezesem UOKiK-u, jednakże z wyłączeniem takich sytuacji, gdy toczy się jedynie postępowanie wyjaśniające bądź informacje dotyczące nadużyć konkretnych przedsiębiorców, zostały powzięte w wyniku prowadzenia postępowania, np. antymonopolowego⁶⁹. Dokonując natomiast interpretacji pojęcia „szczególnie uzasadnionego podejrzenia, podkreślić należy, idąc za stanowiskiem zaprezentowanym w doktrynie, iż jest to sytuacja, w której Prezes UOKiK, przeprowadzając kwalifikację, ma pewność w świetle zgromadzonych w postępowaniu informacji, iż dany przedsiębiorca dopuszcza się praktyki naruszającej zbiorowe interesy konsumentów, a więc w sytuacji, gdy przedsiębiorca dopuszcza się bezprawnego działania, godząc w zbiorowe interesy konsumentów oraz zagrażając interesowi publicznemu⁷⁰. Posługiwanie się wykładnią rozszerzającą jest niedozwolone.

⁶⁰ J. Gołaczyński, *Sporządzanie umów...*, s. 115.

⁶¹ *Ibidem*.

⁶² *M. Jagielska, A. Kunkiel-Kryńska*, Wybór prawa jako klauzula abuzywna w umowach konsumenckich zawieranych przez Internet, *Kwartalnik Antymonopolowy i Regulacyjny* 2016, zeszyt 3(5), Legalis.

⁶³ I CSK 555/13, Legalis.

⁶⁴ *M. Jagielska, A. Kunkiel-Kryńska*, Wybór prawa..., Legalis.

⁶⁵ *Ibidem*.

⁶⁶ *M. Dąbroś*, [w:] *M. Jagielski, E. Sługocka-Krupa, K. Podgórski* (red.) *Ochrona konsumenta na rynku usług*, Warszawa 2017, s. 335.

⁶⁷ *Ibidem*.

⁶⁸ Tj. Dz.U. z 2021 r. poz. 275 ze zm.

⁶⁹ *Ibidem*.

⁷⁰ *A. Piszcz*, [w:] *T. Skoczny* (red.), *Ustawa o ochronie konkurencji i konsumentów. Komentarz*, Warszawa 2014, s. 1002.

Po stwierdzeniu przez Prezesa UOKiK zaistnienia ustawowych przesłanek ostrzeżenie konsumenckie publikowane jest niezwłocznie. W realiach konkretnego przypadku musi wystąpić również następstwo w postaci możliwości spowodowania przez przedsiębiorcę znacznych strat lub niekorzystnego skutku dla szerokiego kręgu konsumentów. Prezes UOKiK może publikować ostrzeżenie konsumenckie wielokrotnie, dopóki przedsiębiorca podejmuje działania niezgodne z prawem.

Podsumowanie

Mając na uwadze liczbę osób korzystających z możliwości Internetu, jego inkluzywny charakter, a także szybko rozwijające się techniki elektronicznej komunikacji, ustawodawca nie tylko wyróżnił specyficzną kategorię umów elektronicznych, a także wprowadził stosowne mechanizmy ochronne

adresowane do słabszej strony umów, jaką jest konsument. Już samo uznanie danej strony umowy za konsumenta jawi się jako silny mechanizm ochronny, który umożliwia wdrożenie w konkretnej sytuacji określonych uprawnień. Nałożenie na przedsiębiorcę licznych obowiązków informacyjnych i tym samym położenie nacisku na transparentność dokonywanych działań, zarówno na etapie przedkontraktowym, jak i w treści samej umowy, a nadto wprowadzenie regulacji dotyczących niedozwolonych klauzul umownych i instytucji ostrzeżenia konsumenckiego, spowodowało, iż konsument został wyposażony w narzędzia umożliwiające dostateczne rozpoznania rynku, a także podmiotów na nim występujących, co pozytywnie wpływa nie tylko na relacje pomiędzy stronami umowy i szeroko rozumiane dobre praktyki rynkowe, ale także na podejmowanie przez konsumenta świadomych decyzji przy nabywaniu oferowanych towarów i usług.

Słowa kluczowe: umowy elektroniczne, konsument, ochrona praw konsumenta, umowy zawierane na odległość.

Protecting consumers who enter into electronic contracts

The purpose of this study is to present the protection mechanisms used by the legislator to protect the consumer, who is the weaker party to contracts concluded, in particular, by means of electronic communication. Therefore, the task of this paper is to present a definition of the concept of a consumer, outline the obligations of an entrepreneur constituted on the grounds of the provisions on consumer rights, and outline the applicable regulations relating to prohibited contractual clauses. The above issues will be presented in relation to a category of contracts, differentiated by the legislator, concluded online, i.e. electronic contracts.

Key words: electronic contracts, consumer, consumer protection, distance contracts.

Prekursorskie opracowanie
dotyczące prawnych
aspektów problematyki
InsurTech



ksiegarnia.beck.pl

Zadzwoni: 81 46 13 300

E-mail: kontakt@beck.pl



Odpowiedzialność cywilnoprawna *host providera*

Wiktor Żochowski¹

Dobra osobiste przysługujące każdej osobie fizycznej oraz osobie prawnej stanowią bardzo liczną grupę uprawnień, której katalog otwarty prawodawca umieścił w art. 23 KC. Wraz z rozwojem technologii ochrona szeroko rozumianych dóbr osobistych uległa poszerzeniu na płaszczyznę cyfrową. Niniejszy artykuł omawia proces wdrażania wspomnianych regulacji do prawa polskiego, skupiając się przede wszystkim na opracowaniu tytułowej odpowiedzialności cywilnoprawnej *host providera*.

Uwagi wstępne

Wobec dynamicznego rozwoju nowoczesnych technologii konieczne jest ustawiczne wprowadzanie przez prawodawcę nowych regulacji prawnych celem dostosowania obowiązujących przepisów do zmieniającej się rzeczywistości. Co oczywiste, dobór odpowiednich narzędzi prawnych wiąże się z licznymi trudnościami. W tym kontekście jedną z kluczowych dla obrotu prawnego kwestii jest odpowiednie ukształtowanie odpowiedzialności podmiotu świadczącego usługę przechowywania danych, czyli tzw. *host providera*.

Host provider udostępnia zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę, pełni zatem funkcję tzw. podmiotu pasywnego. Rola usługodawcy sprowadza się zatem do bycia pośrednikiem między dostawcą treści a użytkownikami je przeglądającymi. Stąd też nie dokonuje on weryfikacji zamieszczanych treści pod kątem bezprawności. Funkcję *host providera* pełnią m.in. portale społecznościowe (np. w odniesieniu do treści dostarczanych przez ich użytkowników, blogerów względem komentarzy dodawanych przez użytkowników czy osoby prowadzące fora internetowe²).

Kwalifikacja prawna odpowiedzialności *host providera* na gruncie przepisów krajowych

Na wstępie podkreślić należy, że podmiot świadczący usługę hostingu może odpowiadać zarówno z tytułu odpowiedzialności deliktowej, jak i kontraktowej. Co do zasady brak jest *de lege lata* przepisów szczegółowo normujących odpowiedzialność *host providera*, wobec czego zastosowanie znajdują przepisy ogólne³. Co więcej, odpowiedzialność *host providera* jest oparta na zasadzie ryzyka i zależy od uprzedniego naruszenia dokonanego przez osobę trzecią. Jest jednakże odpowiedzialnością za własne działanie, które polega m.in. na nieusunięciu danych naruszających dobra osobiste osoby trzeciej, pomimo posiadania informacji o ich umieszczeniu na platformie⁴.

Pojawia się pytanie, czy cel omawianego przepisu, którym było zrównoważenie interesów *host providerów* oraz poszkodowanych ewentualnymi naruszeniami, został w pełni zrealizowany. Kwestia ta została dostrzeżona przez judykaturę. Sądownictwo często przyjmuje szerszą interpretację przepisów, z korzyścią dla poszkodowanych bezprawnym wpisem⁵. Można zaobserwować, że sądy często uwzględniają podnoszone zarzuty przeciwko *host providerom*, które dotyczą przede wszystkim ich biernej postawy wobec naruszeń innych użytkowników. Oprócz tego, w debacie publicznej pojawiały się głosy nowelizacji ustawy w duchu unijnym. Jedną z propozycji było wprowadzenie dodatkowego przepisu do art. 14 ustawy z 18.7.2002 r. o świadczeniu usług drogą elektroniczną⁶, który dokładnie regulowałby odpowiedzialność odszkodowawczą podmiotu świadczącego usługę przechowywania danych⁷. Nowelizacja polegałaby m.in. na poszerzeniu możliwości usługobiorcy co do zawiadamiania o nielegalności treści czy wyznaczeniu konkretnych procedur zawiadamiania o naruszeniach innych użytkowników⁸. Póki co propozycje te pozostają jedynie w sferze dyskusji.

¹ Uniwersytet Mikołaja Kopernika w Toruniu. ORCID: 0000-0002-6304-2991.

² J. Sieńczyło-Chlabicz, M. Rutkowska-Sowa, Z. Zawadzka, M. Nowikowska, Prawo własności intelektualnej, s. 326; R. Markiewicz, A. Matlak, Prawo autorskie w społeczeństwie informacyjnym, [w:] J. Barta (red.), Prawo autorskie. System Prawa Prywatnego. Tom 13, Legalis/el. 2017; M. Kępiński, J. Kępiński, K. Klafkowska-Waśniowska, Wyłączenia odpowiedzialności *host providerów* – w poszukiwaniu równowagi pomiędzy dobrami prawnie chronionymi, [w:] M. Kępiński (red.), Własność intelektualna w obrocie elektronicznym. Tom V, Legalis/el. 2015.

³ Zob. szerzej G. Karaszewski, [w:] J. Ciszewski, P. Nazaruk (red.), Kodeks cywilny. Komentarz aktualizowany, Lex/el. 2022, komentarz do art. 41; G. Stojek, [w:] M. Fras, M. Habdas (red.), Kodeks cywilny. Komentarz. Tom III. Zobowiązania. Część ogólna (art. 353–534), Warszawa 2018, komentarz do art. 471.

⁴ P.F. Piesiewicz, Zarys problematyki odpowiedzialności cywilnej za naruszenie dóbr osobistych w postaci wpisów umieszczanych na forach internetowych, PiP 2019, Nr 10, s. 91–104.

⁵ Zob. np. wyroki: SN z 14.1.2015 r., II CSK 747/13, Legalis; z 30.9.2016 r., I CSK 598/15, Legalis.

⁶ T.j. Dz.U. z 2020 r. poz. 344 ze zm.; dalej jako: ŚwUsiElekU.

⁷ K. Chałubińska-Jentkiewicz, J. Taczkowska-Olszewska, Ustawa o świadczeniu usług drogą elektroniczną. Komentarz, Warszawa 2019, *passim*.

⁸ *Ibidem*.

Zasadniczo, odpowiedzialność cywilnoprawna dostawcy hostingu aktualizuje się wobec osoby, której dobra osobiste zostały naruszone, w momencie pozyskania informacji o bezprawnym wpisie, co wynika z treści art. 14 ust. 1 ŚwUsłElekU. Usługodawca bowiem powinien zareagować na bezprawne działanie usługobiorcy poprzez usunięcie takiego wpisu, a niezrobienie tego powoduje powstanie odpowiedzialności *host providera*. Jednocześnie, powstanie odpowiedzialności usługodawcy nie wyłącza odpowiedzialności autora komentarza. Fakt ten zwiększa jedynie liczbę podmiotów odpowiadających z tytułu odpowiedzialności cywilnej za treść komentarza⁹.

Ponadto ustawodawca w treści art. 14 ŚwUsłElekU przewidział dwie sytuacje, w których podmiot świadczący usługę hostingu ponosi odpowiedzialność za działania osób trzecich. Pierwsza dotyczy posiadania wiedzy o bezprawnym charakterze udostępnionych za jego pośrednictwem danych. Przykładowo może ona wynikać z urzędowego powiadomienia *host providera* przez organ władzy publicznej o bezprawności danego komentarza. Natomiast druga odnosi się do braku reakcji na urzędowe zawiadomienie lub wiarygodną wiadomość o bezprawnym charakterze udostępnionych danych, w postaci zablokowania dostępu do tych danych¹⁰. W tym wypadku odpowiedzialność dotyczy zachowania usługodawcy, który przyjmuje bierną postawę pomimo otrzymania informacji o bezprawnym wpisie. Zaniechanie administratora powoduje powstanie odpowiedzialności cywilnoprawnej. Jest to wynikiem niedopełnienia ciążącego na nim obowiązku usuwania komentarzy naruszających dobra osobiste osób trzecich¹¹.

Powstaje także kwestia odpowiedzialności *host providera* za działania lub zaniechania osób trzecich. Jest to szczególnie istotne z tego względu, że czynności podejmowane przez *host providera* w praktyce obrotu prawnego mogą powstać w szczególności w sytuacji publikacji przez osobę trzecią treści w sposób niezgodny z przepisami prawa. Przedstawione sytuacje spełniają przesłanki określone w art. 422 KC i przewidzianą w nim odpowiedzialność za pomocnictwo. Warunkiem jej przypisania jest stwierdzenie winy umyślnej, zatem co do zasady *host provider* musi mieć świadomość o działaniach bezprawnych¹².

W zakresie analizy dotyczącej *host providera* pojawia się także zagadnienie jego odpowiedzialności za naruszenie dóbr osobistych osób trzecich przez usługobiorców, w związku z zamieszczonymi przez nich komentarzami. Należałoby spoznać, że zasadniczo za komentarz bądź inny wpis naruszający dobra osobiste w Internecie odpowiada przede wszystkim jego autor będący usługobiorcą na podstawie art. 24 KC. Odpowiedzialność za naruszenie dóbr osobistych osób trzecich może jednak, w ustawowo określonych przypadkach, rozszerzyć się również na administratora będącego dostawcą hostingu. Podstawy dla takiego rozszerzenia odpowiedzialności

należałoby upatrywać w treści art. 14 ust. 1 ŚwUsłElekU, zgodnie z którym usługodawca może odpowiadać za treść wpisów użytkowników, jeżeli posiada wiedzę o ich bezprawnym charakterze.

W jednym z budzących pewne wątpliwości wyroków SN orzekł, że za bezprawne wpisy anonimowych internautów administrator portalu internetowego świadczącego usługi hostingu może odpowiadać na podstawie art. 24 § 1 KC¹³. Jednocześnie sąd stwierdził istnienie pozytywnego obowiązku działania administratora, który polega na stałym monitorowaniu sieci. Ponadto w przypadku sporu sądowego SN orzekł o rozkładzie ciężaru dowodu na poszkodowanego i administratora polegającym na obowiązku udowodnienia przez administratora, że nie wiedział i nie mógł wiedzieć o pojawieniu się takich komentarzy¹⁴. Ostatecznie sąd w wyroku oparł się przede wszystkim na treści art. 24 § 1 KC. Całość orzeczenia wraz z przytoczoną argumentacją SN stała się tematem gorliwej dyskusji w doktrynie, a nawet orzecznictwie¹⁵.

W piśmiennictwie panuje stanowisko, że *host provider* jest zobowiązany do zachowania należytej staranności¹⁶. Takie przekonanie przystaje do omawianego wyroku SN¹⁷. Jest tak, ponieważ SN w uzasadnieniu podniósł konieczność wykazania przez administratora, że nie posiadał on wiedzy o bezprawnych komentarzach internautów. Wynika to z regulacji dotyczącej rozkładu ciężaru dowodu przewidzianej w art. 24 KC. Wobec tego termin „zachowanie należytej staranności” może być interpretowany w sposób oznaczający konieczność starannego monitorowania sieci i dbania o treści, które się w niej pojawiają.

Z kolei w innym orzeczeniu SN wskazał, że pomimo nałożonego na usługodawcę obowiązku usuwania wpisów naruszających dobra osób trzecich nie ma on obowiązku monitorowania sieci¹⁸. W doktrynie dotychczas podkreśla-

⁹ Ł. Kierznowski, P. Szorc, Odpowiedzialność cywilna administratora portalu internetowego za wpisy internautów, Forum Prawnicze 1(63) 2021, https://forumprawnicze.eu/attachments/article/421/Kierznowski_Szorc%2024-36.pdf. (dostęp z 20.3.2022 r.).

¹⁰ Zob. art. 14 ŚwUsłElekU.

¹¹ Szerzej zob. M. Świerczyński, [w:] J. Gołaczyński (red.), Ustawa o świadczeniu usług drogą elektroniczną. Komentarz, Warszawa 2009, komentarz do art. 14; W. Chomiczewski, Komentarz do ustawy o świadczeniu usług drogą elektroniczną, [w:] D. Lubasz, M. Namysłowska (red.), Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw, Warszawa 2011, komentarz do art. 14.

¹² K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Media elektroniczne. Współczesne problemy prawne, Warszawa 2016.

¹³ Zob. wyrok SN z 30.9.2016 r., I CSK 598/15, Legalis.

¹⁴ *Ibidem* – zob. fragmenty tezy wyroku.

¹⁵ Szerzej zob. B. Janiszewska, [w:] J. Gudowski (red.), Kodeks cywilny. Komentarz. Tom I. Część ogólna, cz. 1 (art. 1–55(4)), Warszawa 2021, komentarz do art. 24; zob. wyrok SA w Warszawie z 11.6.2019 r., V ACA 475/18, Legalis.

¹⁶ G.J. Pacek, Wybrane zagadnienia związane z odpowiedzialnością dostawców usług hostingowych, PME 2007, Nr 6, *passim*.

¹⁷ Zob. wyrok SN z 30.9.2016 r., I CSK 598/16, Legalis.

¹⁸ Zob. wyrok SN z 14.1.2015 r., II CSK 747/13, Legalis.

no głównie wymóg posiadania wiedzy przez usługodawcę o bezprawnym charakterze zamieszczanych danych. Jednak to nie możliwość uzyskania wiedzy, lecz jej faktyczne posiadanie, było przesłanką do poniesienia odpowiedzialności przez usługodawcę¹⁹. Był to utrwalony pogląd aprobowany w literaturze przedmiotu oraz orzecznictwie. Jednakże, od momentu przytoczonego wyżej wyroku²⁰, nastąpił przełom, a wypracowane stanowisko uległo zachwianiu i obecnie zdają się orzeczenia podążające za argumentacją SN²¹.

Jako wiedzę administratora o inkryminowanych komentarzach internautów w rozumieniu art. 14 ust. 1 ŚwUsłElekU należy zakwalifikować sytuację, kiedy administrator w związku z doświadczeniem z dotychczasowej działalności na polu świadczenia usług hostingu liczy się z realną możliwością dokonywania przez internautów wpisów o treści naruszającej dobra osobiste konkretnych osób. Może to wynikać m.in. z treści kontrowersyjnego artykułu prasowego zamieszczonego na stronie. Innym przykładem może być brak systemu automatycznej filtracji lub świadomość, że system ten nie jest skuteczny, i pozostawanie wobec tego faktu biernym²².

Z perspektywy wielu lat od uprawomocnienia się omawianego wyroku można przyjąć, że nie doprowadził on do wypracowania jednolitej linii orzeczniczej. Wręcz przeciwnie – ze względu na swoje kontrowersyjne stanowisko stał się przyczyną jeszcze zacieklejszych dyskusji i sporów. Chociaż część doktryny i orzecznictwa przyjmuje te same założenia, to nie brakuje licznych głosów krytycznych²³.

Krytycy przedstawionego orzeczenia podnoszą przede wszystkim, że nie należy interpretować rozszerzająco zasad odpowiedzialności *host providera* poprzez wychodzenie poza reżim ustawy o świadczeniu usług drogą elektroniczną i opierania się przede wszystkim na przepisach Kodeksu cywilnego. Do czasu spornego orzeczenia w sądownictwie przyjmowano przede wszystkim odpowiedzialność usługodawcy na podstawie przepisów ustawy o świadczeniu usług drogą elektroniczną. Oznaczało to, że *host provider* odpowiadał za naruszenie dóbr osobistych dopiero wówczas, gdy swoim zachowaniem umożliwił osobie trzeciej ich naruszenie lub nie usunął bezprawnych treści, mając świadomość ich istnienia. Zdaniem zwolenników poglądu krytycznego nie ma obowiązku stałego moderowania forum i usuwania nielegalnych wpisów na bieżąco²⁴.

Podstawowym zarzutem wobec argumentacji przyjętej przez SN w omawianym wyroku jest uzasadnienie prawne oparte przede wszystkim na gruncie art. 24 KC. Przed tym orzeczeniem za podstawę rozstrzygnięć w podobnych sprawach przyjmowano art. 14 ŚwUsłElekU. Miało to szczególne znaczenie przy ustalaniu kręgów odpowiedzialności za bezprawne wpisy. Sąd Najwyższy natomiast, wbrew dotychczasowemu pogładowi większościowemu, uznał za podstawę odpowiedzialności usługodawcy art. 24 KC²⁵.

Innym skutkiem, który również podnoszą krytycy orzeczenia SN²⁶, jest wywołanie tzw. efektu mrożącego na usługodawcach. Efekt mrozący polega na zaprzestaniu lub zahamowaniu działalności usługodawcy ze względu na zagrożenie konsekwencjami prawnymi²⁷. Efekt ten ma szczególne znaczenie w przypadku *host providerów* prowadzących portal internetowy stanowiący np. prasę. Niejednokrotnie administratorzy nie posiadają środków pozwalających na stałe kontrolowanie treści wprowadzanych przez innych Internautów. Orzeczenie to może doprowadzić do unikania przez usługodawców publikacji tematów kontrowersyjnych, wzbudzających emocje opinii publicznej²⁸. Niosłoby to bowiem ryzyko umieszczenia niestosownych, obraźliwych komentarzy przez usługobiorców, za które odpowiedzialność mógłby ponieść również usługodawca.

Należy przychylić się do strony stojącej w opozycji do omawianego wyroku Sądu Najwyższego. Chociaż zamiar orzekania w duchu dyrektywy unijnej jest słuszną praktyką, to wydaje się, że obecnie brakuje mechanizmów umożliwiających prawidłowe wydanie takiego orzeczenia. Przepisy implementujące dyrektywę o handlu elektronicznym zostały wdrożone przez polskiego ustawodawcę z pominięciem celów, którymi kierowało się prawodawstwo unijne. Niemniej jednak to rolę ustawodawcy, a nie sądu, powinno być dostosowywanie i kształtowanie prawa w sposób przystający do jego pierwotnych założeń. Rozwiązaniem problemu powstałego na gruncie przytaczanego wielokrotnie wyroku SN powinno być przede wszystkim przekształcenie obowiązujących regulacji w polskim systemie prawa i dostosowanie ich do celów dyrektywy poprzez m.in. rozszerzenie odpowiedzialności *host providera*. Chociaż założenia SN zasługują na pochwałę,

¹⁹ J. Sieńczyło-Chlabicz, M. Rutkowska-Sowa, Z. Zawadzka, M. Nowikowska, Prawo własności intelektualnej, Warszawa 2018.

²⁰ Zob. przypis Nr 15.

²¹ Zob. np. wyroki SA w Warszawie: z 21.6.2018 r., I ACa 204/17, Legalis; z 11.6.2019 r., V ACa 475/18, Legalis; zob. też wyrok SN z 24.11.2017 r., I CSK 73/17, Legalis.

²² Zob. przypis Nr 17.

²³ Zob. Ł. Wydra, Ustalenie odpowiedzialności hosting providera. Glosa do wyroku SN z 30.9.2016 r., I CSK 598/15, Glosa 2017, Nr 4, s. 91–98; A. Burda, P. Modrzejewski, Odpowiedzialność administratorów stron internetowych za naruszenie dóbr osobistych. Glosa do wyroku SN z 24.11.2017 r., I CSK 73/17, Glosa 2018, Nr 4, s. 69–78.

²⁴ Zob. szerzej Ł. Wydra, Ustalenie odpowiedzialności hosting providera. Glosa krytyczna do wyroku Sądu Najwyższego z 30.9.2016 r., I CSK 598/15, Glosa 2017, Nr 4, s. 91–98; M. Kępiński, J. Kępiński, K. Kłafkowska-Waśniewska, R. Sikorski (red.), Własność intelektualna w obrocie elektronicznym. Tom V, Warszawa 2015, Legalis.

²⁵ *Ibidem*.

²⁶ Zob. przypis Nr 17.

²⁷ E. Łętowska, Legal harassment, contempt of court, chilling effect – jakby kto nie wiedział..., <https://konstytucyjny.pl/legal-harassment-contempt-of-court-chilling-efect-jakby-kto-nie-wiedzial/> (dostęp z 11.9.2022 r.).

²⁸ Ł. Kierznowski, P. Szorc, Odpowiedzialność cywilna administratora portalu internetowego za wpisy internautów, Forum Prawnicze 1(63) 2021, https://forumprawnicze.eu/attachments/article/421/Kierznowski_Szorc%2024-36.pdf (dostęp z 20.3.2022 r.).

opieranie swojego orzeczenia przede wszystkim na przepisach Kodeksu cywilnego regulujących kwestię dóbr osobistych, na dalszym planie pozostawiając ustawę o świadczeniu usług drogą elektroniczną stanowiącą *lex specialis* wobec odpowiedzialności usługodawcy, nie powinno być pożądaną praktyką w judykaturze.

Znaczenie implementacji dyrektywy o handlu elektronicznym dla kształtowania się odpowiedzialności *host providera* w polskim porządku prawnym

Na zasadniczy kształt normatywnej regulacji odnoszącej się do kwestii odpowiedzialności *host providera* ważki wpływ miało prawodawstwo unijne. Regulacje dotyczące tej odpowiedzialności stanowią implementację art. 14 dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z 8.6.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego²⁹. Pierwotne brzmienie art. 14 ust. 1 lit. a dyrektywy stanowiło, że odpowiedzialność usługodawcy za przechowywane informacje jest wyłączona, gdy nie ma on wiarygodnych wiadomości o bezprawnym charakterze działalności lub informacji. Z kolei w odniesieniu do roszczeń odszkodowawczych zgodnie ze wskazanym przepisem nie przysługują, gdy *host provider* nie wie o stanie faktycznym lub okolicznościach, które w sposób oczywisty świadczą o bezprawności treści zamieszczanych przez usługobiorców³⁰.

Polski ustawodawca w toku implementacji wprowadził regulacje prawne przewidujące szerszy zakres wyłączenia odpowiedzialności *hosting providera*, niż zostało to założone we wspomnianej dyrektywie. Różnica w zakresie wyłączeń dotyczy cywilnoprawnych roszczeń odszkodowawczych. Dyrektywa unijna przewiduje, że *host provider* może ponosić odpowiedzialność cywilną z tytułu naruszeń dóbr osobistych osoby trzeciej za wpisy innych użytkowników. Natomiast polski ustawodawca wyłączył odpowiedzialność administratora w większym stopniu, niż było to celem ustawodawcy europejskiego³¹.

W przyjętym w polskim porządku prawnym modelu prawnej odpowiedzialności *host providera* nie ma zawężenia wyłączającego odpowiedzialność odszkodowawczą administratora do wiedzy o stanie faktycznym lub okolicznościach, które w sposób oczywisty świadczą o bezprawnym charakterze działalności lub informacji przechowywanych w ramach usługi hostingu³².

Warto zaznaczyć, że część doktryny opowiada się za stanowiskiem, iż jest to nieprawidłowy sposób implementacji unijnej dyrektywy³³. Wynika to z faktu stawiania poszko-

dowanych w gorszej pozycji, niż jest to przewidziane w dyrektywie. Artykuł 14 ust. 1 lit. a dyrektywy unijnej stanowi, że odpowiedzialność usługodawcy za przechowywane informacje jest wyłączona, gdy nie ma on wiarygodnych wiadomości o bezprawnym charakterze działalności lub informacji, a w odniesieniu do roszczeń odszkodowawczych nie wie o stanie faktycznym lub okolicznościach, które w sposób oczywisty świadczą o tej bezprawności. Zestawienie przepisu dyrektywy 2000/31/WE z art. 14 ust. 1 ŚwUsłElekU prowadzi do wniosku, że polski prawodawca wprowadził szersze wyłączenie odpowiedzialności *hosting providera*, niż zostało to założone w dyrektywie o handlu elektronicznym. Różnica w zakresie wyłączenia dotyczy roszczeń odszkodowawczych, czyli odpowiedzialności opartej na przepisach prawa cywilnego³⁴.

Pośrednią przyczyną wskazanej krytyki są przepisy dyrektywy o handlu elektronicznym. Krytycy omawianej dyrektywy podnoszą, że obowiązujący reżim odpowiedzialności z dyrektywy 2000/31/WE nie przystaje do obecnej rzeczywistości i wymaga radykalnej zmiany. Istniejące dokumenty o charakterze niewiążącym nie są wystarczająco skuteczne i niestety wiele z promowanych działań jest niezgodnych z przepisami dyrektywy 2000/31/WE.

Wskazany problem został zauważony na gruncie europejskim. Przewodnicząca Komisji Europejskiej wskazała, że konieczna jest analiza dotychczasowych rozwiązań, w tym dyrektywy o handlu elektronicznym, by stwierdzić, czy pozwalają one na efektywne zwalczanie nielegalnych treści zamieszczanych w Internecie. Po analizie dokumentów i aktów prawnych UE³⁵, zarówno o charakterze wiążącym, jak i niewiążącym, nasuwa się myśl o braku zdecydowanej inicjatywy ze strony Komisji Europejskiej. Istnieje tendencja do zostawiania platformom internetowym szerszej swobody w zakresie regulacji odpowiednich narzędzi do przestrzegania aktów unijnych. Jednocześnie powoduje to powstawanie coraz większych oczekiwań wobec administratorów i witryn internetowych. Nie jest to zjawiskiem pożądanym, ponieważ

²⁹ Dz.Urz. UE L Nr 178, s. 1.

³⁰ D. Lubasz, M. Namysłowska, K. Klafkowska-Waśniowska, Ustawa o świadczeniu usług drogą elektroniczną. Komentarz, Warszawa 2011.

³¹ W. Chomiczewski, Wybrane problemy odpowiedzialności *host providera* w Internecie według prawa polskiego. <https://portalprawait.com/entry/wybrane-problemy-odpowiedzialnosci-host-providera-w-internecie-wedlug-prawa-polskiego/> (dostęp z 27.3.2022 r.).

³² *Ibidem*.

³³ Zob. np. W. Chomiczewski, Komentarz do ustawy o świadczeniu usług drogą elektroniczną, [w:] D. Lubasz, M. Namysłowska (red.), Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw, Warszawa 2011, komentarz do art. 14.

³⁴ *Ibidem*.

³⁵ Aktami regulującymi kwestię odpowiedzialności administratora są m.in. Dyrektywa o handlu elektronicznym, Strategia jednolitego rynku cyfrowego dla Europy, Komunikat w sprawie realizacji jednolitego rynku cyfrowego, Zalecenie w sprawie nielegalnych treści, Komunikat o platformach internetowych i inne.

doprowadza to dla wielu niepewnych sytuacji dla podmiotów rynkowych w zakresie stosowania regulacji unijnych. Komisja Europejska zawarła w zaleceniu w sprawie nielegalnych treści postulat wskazujący, że w razie braku satysfakcjonujących rezultatów owych dobrowolnych działań UE ustanowi wiążące akty prawne w tym obszarze³⁶. Mając na uwadze, że już teraz omawianą materię reguluje zarówno tzw. *soft law*, jak i *hard law*, istnieją pewne obawy, czy wprowadzenie kolejnych aktów o wiążącym charakterze rozwiązałyby problem konkretnej regulacji odpowiedzialności *host providera*.

Praktyczny przykład problemów, które mogą powstać na skutek implementacji dyrektywy w sposób nieuwzględniający jej głównych założeń możemy zaobserwować w polskim obrocie prawnym. Od wielu lat trwa konflikt opisany we wcześniejszym fragmencie niniejszej pracy, dotyczący tego, czy odpowiedzialność administratora mieści się wyłącznie na gruncie ŚwUsłElekU, czy należy sięgnąć również do przepisów KC. Być może zdecydowana inicjatywa Komisji Europejskiej w zakresie opracowania regulacji dotyczących zwalczania nielegalnych treści w Internecie stanowiłaby rozwiązanie problemu dotyczącego zakresu odpowiedzialności *host providera*. Nie wiadomo jednak, czy do tego dojdzie. Od wielu lat KE nie podejmuje dalszych inicjatyw dotyczących unormowania *host providerów* i wiele kwestii pozostawia do rozwiązania samemu rynkowi, w szczególności platformom internetowym³⁷.

Wyłączenia odpowiedzialności podmiotu świadczącego usługę przechowywania danych

Należy odnotować, że odpowiedzialność *host providerów* według prawa polskiego jest wyłączona, gdy usługodawca nie wie o bezprawnej działalności usługobiorcy, a w razie gdy dowie się o niej w sposób urzędowy lub inny wiarygodny, gdy niezwłocznie uniemożliwi dostęp do tych danych (art. 14 ust. 1 ŚwUsłElekU)³⁸. W przeciwnym razie wyłączenie odpowiedzialności przestaje mieć zastosowanie. Innymi słowy, na podmiot świadczący usługę przechowywania danych nałożony jest tzw. pozytywny obowiązek działania. Polega on na konieczności reakcji wobec wiarygodnych wiadomości informujących o wpisach naruszających cudze dobra osobiste, a także usuwaniu treści, co do których istnieje przekonanie o ich nielegalności.

Pomimo tzw. obowiązku pozytywnego działania *host provider* nie jest zobowiązany do przeprowadzenia szczegółowego postępowania wyjaśniającego w zakresie ustalenia, czy wiadomość o bezprawym charakterze treści zamieszczonych przez użytkowników jest wiarygodna. Oznacza to, że na osobie żądającej uniemożliwienia dostępu do danych bądź żądającej usunięcia wpisu spoczywa dostarczenie rzetelnych

informacji *host providerowi* o ich bezprawym charakterze (art. 14 ust. 1 ŚwUsłElekU)³⁹.

W zakresie odpowiedzialności usługodawcy istnieje wciąż wiele sprzeczności oraz problemów z uwagi na brak sprecyzowanych informacji w ustawie o świadczeniu usług drogą elektroniczną, co powoduje konieczność odwołania się do doktryny oraz orzecznictwa. Mając na uwadze rozważania podjęte przez SN w omawianym wcześniej wyroku, można mieć pewne wątpliwości co do wspomnianego wyłączenia odpowiedzialności *host providera*. Pomimo ustawowej regulacji SN w przytaczanym wielokrotnie orzeczeniu⁴⁰, orzekając w duchu założeń dyrektywy o handlu elektronicznym, wskazał pewne wyjątki od wyłączeń wskazanych w ustawie o świadczeniu usług drogą elektroniczną, rozszerzając odpowiedzialność *host providerów*⁴¹.

Zbyt wąskie rozumienie wskazanego przepisu ustawy o świadczeniu usług drogą elektroniczną spowoduje, że *host provider* uzyska wiedzę o bezprawym charakterze danych, lecz w literalnym rozumieniu art. 14 ust. 1 ŚwUsłElekU nie będzie to wiedza istotna dla jego zastosowania, ponieważ nie będzie nabyta ani w drodze urzędowego zawiadomienia, ani wiarygodnej wiadomości. W efekcie podmiot, którego dobra osobiste zostały naruszone, pozostanie wówczas bez realnych możliwości wywarcia wpływu na *host providera*, by ten uniemożliwił dostęp do danych. Taka interpretacja art. 14 ust. 1 ŚwUsłElekU prowadzi do tego, że pasywność usługodawcy w procesie ustalania stanu faktycznego sugerującego bezprawność wpisów innych użytkowników nie będzie sankcjonowana. Należy dążyć do tego, by wyłączenie odpowiedzialności *host providera* wynikało ze spełnienia cięższych na administratorze obowiązków ustawowych, polegających na zapoznaniu się z wpisem i usunięciu go, w przypadku stwierdzenia bezprawności⁴².

Ponadto warto zaznaczyć, że przepisy ustawy o świadczeniu usług drogą elektroniczną przewidują wyłączenie odpowiedzialności kontraktowej dostawcy usługi hostingu za niewykonanie lub nienależyte wykonanie umowy hostingu. Przy czym kwestia wyłączenia odpowiedzialności kształtuje się odmiennie w zależności od tego, czy podstawą uniemoż-

³⁶ K. Flaga-Gieruszyńska, J. Gołaczyński, *Prawo nowych technologii*. Warszawa 2021, *passim*.

³⁷ E. Galewska, *Ocena kierunków działań Unii Europejskiej w zakresie zwalczania nielegalnych treści internetowych*, [w:] K. Flaga-Gieruszyńska, J. Gołaczyński (red.), *Prawo nowych technologii*, Warszawa 2021.

³⁸ Szerzej zob. np. wyrok SN z 24.11.2017 r., I CSK 73/17, *Legalis*; K. Chabubińska-Jentkiewicz, J. Taczowska-Olszewska, *Ustawa o świadczeniu usług drogą elektroniczną. Komentarz*, Warszawa 2018, komentarz do art. 14; K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, *Media elektroniczne. Współczesne problemy prawne*, Warszawa 2016, *Legalis*.

³⁹ Zob. wyrok SA w Warszawie z 18.4.2017 r., I ACa 55/16, *Legalis*.

⁴⁰ Zob. przypis Nr 15.

⁴¹ Więcej o wyjątkach od wyłączeń ustawowych autor wskazuje w podrozdziale drugim artykułu, przy okazji omawiania wyroku.

⁴² M. Kepiński, K. Klafkowska-Waśniowska, R. Sikorski, *Własność intelektualna w obrocie elektronicznym*. Tom V, Warszawa 2015.

liwienia dostępu do danych jest urzędowe zawiadomienie (art. 14 ust. 2 ŚwUsłElekU) czy wiarygodna informacja (art. 14 ust. 3 ŚwUsłElekU).

Odnosnie do regulacji ujętej w treści przepisu art. 14 ust. 2 ŚwUsłElekU trzeba odnotować, że dla wyłączenia odpowiedzialności kontraktowej *host providera* wystarczy samo uniemożliwienie przez administratora dostępu do danych na skutek otrzymania urzędowego zawiadomienia. Niekiedy przyjmuje się, że *host provider* po otrzymaniu urzędowego zawiadomienia ma trzydniowy termin na reakcję⁴³. Termin ten stanowi jednak wyłącznie postulat przedstawiony w doktrynie, ponieważ ustawodawca nie dookreślił go w przepisach ustawy. Natomiast w świetle art. 14 ust. 3 ŚwUsłElekU należałoby przyjąć, że usługodawca, w przypadku otrzymania wiarygodnej informacji o zamieszczeniu niezgodnego z prawem komentarza, musi niezwłocznie zawiadomić usługobiorcę o zamiarze uniemożliwienia dostępu do danych, które wskazanego komentarza dotyczą. Zawiadomienie to musi nastąpić przed usunięciem danych. Skierowanie takiej informacji *ex post* usunięciu komentarza spowoduje brak wyłączenia odpowiedzialności kontraktowej dostawcy usługi hostingu, co wyraźnie wynika z treści art. 14 ust. 3 ŚwUsłElekU⁴⁴.

Warto nadmienić, że wyłączenie odpowiedzialności *host providera* nie obejmuje sytuacji, kiedy posiada on uprawnienia kontrolne w stosunku do usługobiorcy zamieszczającego bezprawne informacje. Kontrola sprowadza się w tym przypadku do przejścia kontroli nad czynnościami dostawcy danych. Nie chodzi więc o kontrolę samych informacji⁴⁵. Przejście kontroli musi nastąpić w rozumieniu przepisów ustawy o ochronie konkurencji i konsumentów⁴⁶, o czym świadczy art. 14 ust. 4 ŚwUsłElekU. Oznacza to, że przez przejście kontroli należy rozumieć wszelkie formy bezpośredniego lub pośredniego uzyskania przez przedsiębiorcę uprawnień, które osobno albo łącznie, przy uwzględnieniu wszystkich okoliczności prawnych lub faktycznych, umożliwiają wywieranie decydującego wpływu na innego przedsiębiorcę lub przedsiębiorców⁴⁷. Innymi słowy, w sytuacji gdy *host provider* miał decydujący wpływ na pojawienie się bezprawnego wpisu, co jest jednoznaczne z możliwością zapobieżenia tego, ponosi on odpowiedzialność z chwilą pojawienia się wpisu.

Podsumowanie

Pomimo funkcjonowania pojęcia *host providera* w polskim systemie prawnym od wielu lat pozostaje on kwestią otwartą, a liczne spory prowadzone przed sądami są praktycznym dowodem na potwierdzenie owej tezy. Przełomowy w tej materii wyrok SN⁴⁸ do tej pory jest przedmiotem dyskusji, a w doktrynie pojawiają się liczne głosy krytyczne. Jedną z głównych przyczyn takiego stanu rzeczy jest to, że sporny wyrok stanowi niejako wyłom w dotychczasowej praktyce

sądowniczej w zakresie odpowiedzialności cywilnoprawnej usługodawców.

Prowadzi to do przeświadczenia, że konieczne jest zawarcie konsensusu łączącego poglądy obu stron. Obecne spory w doktrynie i orzecznictwie prowadzą do przyjmowania różnych rozstrzygnięć przez sądy, w zależności od poglądów sędziego rozpatrującego daną sprawę. Jest to bardzo niekorzystne z punktu widzenia pewności prawa, przede wszystkim wobec *host providerów*.

Z jednej strony, prawodawca zapewnił usługodawcom szeroką ochronę na mocy ustawy o świadczeniu usług drogą elektroniczną, z drugiej strony, SN z kolei zainicjował szeroką interpretację tych przepisów i ich powiązanie z Kodeksu cywilnego, by lepiej chronić pokrzywdzonego. Mając to na uwadze, wypracowanie konsensusu byłoby przełomowym rozwiązaniem stabilizującym niepewność związaną z odpowiedzialnością cywilnoprawną *host providera*.

Niewątpliwie obie strony konfliktu dysponują uzasadnioną argumentacją, tłumaczącą ich stanowiska. Należy przychylić się jednak do strony krytykującej pogląd przedstawiony przez przytoczony wielokrotnie wyrok SN. Tak szeroka wykładnia art. 24 KC wraz z art. 14 i 15 ŚwUsłElekU może doprowadzić do wielu negatywnych konsekwencji. Rozszerzenie odpowiedzialności administratora w tak znaczący sposób przypuszczalnie doprowadzi do upadku mniejszych, niezależnych stron i czasopism. Te natomiast, które będą dalej funkcjonować, mogą zaprzestać publikowania treści o wydzźwięku emocjonalnym, by uniknąć negatywnych komentarzy usługobiorców. Niweczyłoby to podstawowe wartości i cele prawa prasowego⁴⁹ oraz prasy jako takiej.

Przy tak dynamicznym tempie rozwoju technologii należy wziąć pod uwagę, że wielu autorów przyjmuje szeroką definicję hostingu. Część przedstawicieli doktryny przyjmuje, że hosting nie polega już na całkowitej bierności usługodawcy lub braku technicznej kontroli nad treściami. Zgodnie z szerokim rozumieniem pojęcia hostingu, usługa ta polega nie tylko na udostępnianiu i przechowywaniu treści zamieszczanych przez użytkowników, ale również na kontroli i wpływniu na przekaz danych⁵⁰. Niezwykle istotne jest zatem, aby

⁴³ W. Chomiczewski, Komentarz do ustawy o świadczeniu usług drogą elektroniczną, [w:] D. Lubasz, M. Namysłowska (red.), Świadczenie..., komentarz do art. 14.

⁴⁴ *Ibidem*.

⁴⁵ M. Świerczyński, [w:] J. Gołaczyński (red.), Ustawa o świadczeniu usług drogą elektroniczną. Komentarz, Warszawa 2009, komentarz do art. 14.

⁴⁶ Ustawa z 16.2.2007 r. o ochronie konkurencji i konsumentów, t.j. Dz.U. z 2021 r. poz. 275 ze zm.

⁴⁷ *Ibidem*.

⁴⁸ Zob. przypis Nr 15.

⁴⁹ Ustawa z 26.1.1986 r. – Prawo prasowe, t.j. Dz.U. z 2018 r. poz. 1914 ze zm.

⁵⁰ J. Gołaczyński, Recenzja: M. Piech, Pośrednicy internetowi w prawie Unii Europejskiej. Rola i obowiązki wobec treści użytkowników, Warszawa 2019, PiP 2021, Nr 2.

ustawodawca wysłuchał argumentów prezentowanych przez obie strony sporu, ponieważ niezaprzeczalne jest, że dysponują one racjonalnym uzasadnieniem dla swoich poglądów.

Głównym założeniem SN była konieczność zwiększenia ochrony poszkodowanego. Jest to słuszny cel, do którego niewątpliwie należy dążyć. Jednakże obecne przepisy dają możliwość wystąpienia do administratora z prośbą o usunięcie takich treści. Jednocześnie brak reakcji *host providera* powoduje powstanie wobec niego odpowiedzialności cywilnoprawnej. Wobec tego można przyjąć, że jest

to prawidłowe założenie, które nakłada na administratora obowiązek pod rygorem powstania odpowiedzialności cywilnoprawnej.

W konkluzji należy wskazać, że wobec trwającego sporu nie sposób wskazać daty jego zakończenia. Wydaje się, że dopiero kolejny wyrok SN uwzględniający uwagi krytyków bądź reakcja samego ustawodawcy może doprowadzić do jego ustania. Niewątpliwie jego rozwiązanie byłoby rozwiązaniem korzystnym dla wszystkich, a ujednoczenie linii orzeczniczej skutkiem pożądanym dla każdej ze stron.

Słowa kluczowe: odpowiedzialność prawna, *host provider*, technologia, Internet, usługodawcy, usługobiorcy.

Civil liability of the hosting provider

Personal rights of every natural person and legal person constitute a very large group of permissions, of which the open catalogue was placed by the legislator in Article 23 of the Civil Code. Along with the development of technology, the protection of personal rights has been extended to the digital plane. This article discusses the process of implementing the abovementioned regulations into Polish law, focusing primarily on the development of the civil liability of the hosting provider from the title.

Key words: liability, hosting provider, technology, Internet, service providers, recipients.

100 istotnych pojęć
i instytucji normatywnych
z zakresu technologii
informatycznych



ksiegarnia.beck.pl

Zadzwoń: 81 46 13 300

E-mail: kontakt@beck.pl

Charakter prawny umowy *Software as a Service* w polskim systemie prawnym

Stanisław Małkowski¹

Z jednej strony we francuskiej literaturze prawniczej wydaje się przeważać stanowisko, że umowa o korzystanie z oprogramowania w modelu SaaS powinna być kwalifikowana jako umowa licencyjna. Z drugiej strony literatura niemiecka prezentuje pogląd odmawiający umowie o korzystanie z oprogramowania w modelu SaaS charakteru umowy prawnoutorskiej. Stanowisko pośrednie pomiędzy dwoma powyższymi prezentowane jest natomiast w literaturze szwajcarskiej². W polskiej doktrynie prawniczej zdania na powyższy temat są zróżnicowane. Celem niniejszego opracowania jest ustalenie, która kwalifikacja prawna umów na korzystanie z oprogramowania w modelu SaaS obecnie przeważa w literaturze.

Uwagi wstępne

Oprogramowanie jako usługa (*Software as a Service*, dalej jako: SaaS) to obecnie jeden z najpopularniejszych modeli cloud computing. Do dziś nie udało się jednak wypracować jednolitej koncepcji kwalifikacji powyższej umowy. Wydawałoby się, iż sama nazwa modelu SaaS (oprogramowanie jako usługa) wskazuje na kwalifikację takiej umowy jako umowy o świadczeniu usług. Zarówno jednak w polskiej literaturze, jak i w doktrynie zagranicznej kwalifikacja ta nie jest taka oczywista. Oceny nie ułatwia fakt, iż do dnia dzisiejszego brak jest orzeczeń sądów, które rozstrzygałyby jednoznacznie powyższą kwestię.

Na wstępie warto przywołać podstawowe definicje dotyczące niniejszego tematu, tj. cloud computing oraz model SaaS (nie wchodząc przy tym w szczegółowe zagadnienia dotyczące chmury obliczeniowej). Jak wskazuje *M. Siwicki*, chmura obliczeniowa (ang. *cloud computing*) to, ogólnie ujmując, platforma umożliwiająca korzystanie w różnych formach z różnorodnych zasobów technologii informacyjnych, obejmująca m.in. usługi związane z dostarczaniem infrastruktury fizycznej i wirtualnej na żądanie użytkownika, które może on dynamicznie dostosowywać do własnych potrzeb biznesowych³. Natomiast SaaS to model chmury obliczeniowej, za pomocą której świadczy się usługi związane z dostarczaniem oprogramowania. Dzięki tej usłudze użytkownik nie potrzebuje instalować ani uruchamiać oprogramowania na swoim komputerze, ponieważ zarządzaniem, aktualizowaniem czy pomocą techniczną zajmuje się dostawca⁴.

Umowa w modelu SaaS a licencja

Wydaje się, iż w polskiej judykaturze przeważa pogląd przeciwny zakwalifikowaniu umowy w modelu SaaS jako umowy licencyjnej. Zwolennicy powyższego poglądu wskazują, że w modelu tym użytkownik jedynie korzysta z oprogramowania zainstalowanego na serwerach dostawcy, nie dokonując jego zwielokrotnienia na dysku twardym własne-

go komputera. W procesie korzystania z oprogramowania w modelu SaaS może co najwyżej dochodzić do wyświetlania efektów prac programu komputerowego na komputerze użytkownika, co jednakże samo w sobie nie stanowi ingerencji w sferę autorskich praw majątkowych do głównego oprogramowania będącego przedmiotem umowy. Jednocześnie podkreśla się, iż sama instalacja we własnym środowisku informatycznym określonych programów pomocniczych lub interfejsów nie powinna determinować modelu prawnego korzystania z zasadniczego oprogramowania znajdującego się na serwerach dostawcy, mają one bowiem znaczenie drugorzędne z punktu widzenia celu umowy⁵.

W ocenie *M. Modrzejewskiego* za bardziej przekonujące należy uznać argumenty, w świetle których korzystanie z oprogramowania komputerowego w modelu SaaS nie wiąże się ze zwielokrotnianiem utworu (programu) w infrastrukturze użytkownika, a tym samym w wkroczeniem w zakres autorskich praw majątkowych. Zatem, co do zasady, korzystanie z oprogramowania komputerowego w modelu SaaS powinno odbywać się na podstawie umowy niebędącej umową licencyjną⁶.

W podobnym tonie wypowiada się *K. Żok*. Jego zdaniem umowa o korzystanie z programu komputerowego w modelu SaaS nie przybiera, co do zasady, postaci umowy licencji. Jak wskazuje powyższy autor, w przypadku modelu SaaS użytkownik nie ma bezpośredniego dostępu do oprogramowania,

¹ Absolwent kierunku Prawo na Wydziale Prawa, administracji i Ekonomii Uniwersytetu Wrocławskiego.

² *K. Żok*, Kwalifikacja umowy o korzystanie z programu komputerowego jako usługi (Software as a service, SaaS) – uwagi na tle prawa polskiego i wybranych zagranicznych systemów prawnych, *Zeszyty Naukowe Uniwersytetu Jagiellońskiego, Prace z Prawa Własności Intelektualnej* 2015, z. 129, s. 21–22.

³ *M. Siwicki*, Prawnoautorska ochrona konstrukcji chmury obliczeniowej, *Przegląd Sądowy* 2016, Nr 3, s. 81.

⁴ *Ibidem*, s. 82.

⁵ *M. Modrzejewski*, Podatkowe aspekty korzystania z oprogramowania komputerowego w modelu SaaS (Software as a Service), *Przegląd Podatkowy* 2016, Nr 8, s. 17.

⁶ *Ibidem*, s. 18.

a zatem nie może go również reprodukować. Zwielokrotnienia tego utworu dokonuje natomiast dostawca w ramach zaciągniętego zobowiązania. W istocie bowiem przekazuje on jedynie swojemu kontrahentowi wyniki pracy programu komputerowego. Dynamika wymiany informacji stwarza natomiast iluzję bezpośredniego korzystania z głównego oprogramowania przez użytkownika⁷.

W tym miejscu warto przywołać także pogląd Ł. Pirożka. W jego ocenie korzystanie przez użytkownika z programu komputerowego udostępnionego w modelu SaaS nie ingeruje w zakres uprawnień prawnoautorskich, a w procesie świadczenia usług w tym modelu nie dochodzi do zwielokrotnienia programu komputerowego. Udostępniany program komputerowy nie jest reprodukowany w jakikolwiek sposób w pamięci stałej komputera ani też w pamięci czasowej komputera. W pamięci czasowej komputera, w trakcie korzystania z usługi w modelu SaaS zapisywane są jedynie dane interfejsu użytkownika, np. przeglądarki internetowej, a nie dane udostępnianego programu komputerowego. Co więcej, w pamięci czasowej komputera nie jest zapisywany jakikolwiek element kodu źródłowego programu komputerowego⁸.

W związku z powyższym przywołany autor przyjmuje, że co do zasady do świadczenia usług w modelu SaaS na rzecz użytkownika nie jest wymagane zawarcie umowy licencyjnej. Jako wyjątek Ł. Pirożek wskazuje sytuację, w której dochodzi do zwielokrotnienia całości lub części oprogramowania w pamięci stałej komputera z możliwością dostępu przez użytkownika do kodów źródłowych⁹.

Analogiczne stanowiska wydają się zajmować autorzy komentarzy do ustawy z 24.2.1994 r. o prawie autorskim i prawach pokrewnych¹⁰. Dla przykładu warto przywołać jedno z nowszych stanowisk doktryny. W komentarzu pod redakcją A. Michalaka wskazuje się, że w przypadku korzystania z oprogramowania komputerowego pojawiają się również formy korzystania z software (tzw. SaaS – Software as a Service), które nie mają charakteru licencji – nie dochodzi bowiem do korzystania z samego oprogramowania przez zamawiającego usługę (jego zwielokrotnienia dokonuje bowiem podmiot świadczący usługę), ale do uzyskania efektu działania tegoż programu. Do takich umów stosuje się art. 750 i n. KC¹¹.

Podobnie w komentarzu pod redakcją E. Ferenc-Szydelko podkreśla się, że nie wszystkie umowy dotyczące korzystania z programu komputerowego będą umowami licencyjnymi. W przypadku korzystania z oprogramowania w modelu SaaS użytkownik nie dokonuje zwielokrotnienia programu komputerowego; zwielokrotnienia dokonuje dostawca usługi, użytkownik zaś otrzymuje jedynie wyniki pracy programu komputerowego. Dlatego tego rodzaju umowy, zdaniem doktryny, nie są umowami licencji, lecz umowami o świadczenie usług, do których należy stosować art. 750 KC¹².

W piśmiennictwie można zaobserwować spór dotyczący tego, czy definicja „zwielokrotniania” obejmuje także takie czynności, które łączą się jedynie z czasowym wprowadzeniem programu komputerowego (lub jego części) do tzw. roboczej lub operacyjnej (RAM) pamięci danego urządzenia (komputera, tabletu czy smartfona) w celu wyświetlenia wyników jego pracy za pomocą przeglądarki internetowej, a więc dokładnie z takim działaniem, z jakim mamy do czynienia na gruncie modelu SaaS. Powyższe rozbieżności zostały szczegółowo omówione przez Z. Drzewieckiego oraz S. Kubsik¹³.

Aby móc ocenić zaprezentowane tam stanowiska, powyżsi autorzy odwołali się do podstawowych zasad funkcjonowania pamięci operacyjnej komputera oraz rodzaju danych, jakie są w nim zapisywane. W tym celu wymienili oni dwie kategorie danych, które przetwarza komputer. Pierwsze, które potrzebne są komputerowi „na stałe”, to m.in. wszystkie pliki instalacyjne oprogramowania, a także dokumenty (zdjęcia, pliki muzyczne, tekstowe, arkusze kalkulacyjne itd.). Drugie to takie, które są potrzebne tylko tymczasowo – na okres, w którym są przetwarzane. Tymczasowym zapisem danych tej drugiej kategorii zajmuje się pamięć operacyjna (RAM – Random Access Memory, czyli w wolnym tłumaczeniu „pamięć o dostępie swobodnym”), która pełni funkcję swobodnego łącznika, bez którego na monitorze komputera nie zostałyby wyświetlone to, co chcemy otworzyć/zobaczyć¹⁴.

W związku z powyższym zdaniem autorów, dopóki w ramach wykonywania umowy SaaS nie dochodzi do powielenia oprogramowania na sprzęcie użytkownika, na przykład na pamięci stałej komputera (czyli, w uproszczeniu, nie dochodzi do jego instalacji), użytkownik nie wkracza w zakres pól eksploatacji wymienionych w art. 74 ust. 4 PrAutU, a w konsekwencji nie potrzebuje on licencji autora (dostawcy) danego oprogramowania na korzystanie z niego¹⁵.

Podobnego zdania jest M. Modrzejewski, który wskazuje, iż wyświetlanie efektów prac programu komputerowego na komputerze użytkownika samo w sobie nie stanowi inge-

⁷ K. Żok, Kwalifikacja umowy..., s. 24.

⁸ Ł. Pirożek, Prawne aspekty świadczenia usług w modelu SaaS przez przedsiębiorcę telekomunikacyjnego, Internetowy Kwartalnik Antymonopolowy i Regulacyjny 2015, Nr 6, s. 81.

⁹ *Ibidem*, s. 82.

¹⁰ T.j. Dz.U. z 2022 r. poz. 2509 ze zm.; dalej jako: PrAutU.

¹¹ M. Kubiak, [w:] A. Michalak (red.), Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, Legalis/el. 2019, komentarz do art. 67, nb. 2.

¹² J. Szyjewska-Bagińska, [w:] E. Ferenc-Szydelko (red.), Ustawa o prawie autorskim i prawach pokrewnych. Komentarz, Legalis 2021/el., komentarz do art. 67, nb. 27.

¹³ Z. Drzewiecki, S. Kubsik, Umowy na korzystanie z oprogramowania oparte na modelu Software as a Service – ich kwalifikacja prawna oraz kwestię z tym związane, [w:] M. Dumkiewicz (red.), K. Kopaczynska-Pieczniak (red.), J. Szczotka (red), Sto lat polskiego prawa handlowego. Księga jubileuszowa dedykowana Profesorowi Andrzejowi Kidybie. Tom II, Lex/el. 2020, pkt 2.1.

¹⁴ *Ibidem*, pkt 2.1.

¹⁵ *Ibidem*.

rencji w sferę autorskich praw majątkowych do głównego oprogramowania będącego przedmiotem umowy¹⁶. Pogląd ten aprobuje także E. Molenda-Kropelnicka. Autorka ta opowiada się także za poglądem, iż w przypadku modelu SaaS co do zasady zawarcie umowy licencyjnej nie jest konieczne, ponieważ samo używanie nie będzie wkraczało w domenę autorskich praw majątkowych twórcy¹⁷.

Podsumowując powyższe rozważania, wskazać należy, że obecnie w doktrynie wydaje się przeważać stanowisko, iż w modelu SaaS nie dochodzi do zwielokrotnienia programu komputerowego, a tym samym nie jest konieczne zawarcie umowy licencyjnej. Jednocześnie podnosi się jednak, iż w niektórych przypadkach taka konieczność może zająć.

Dla przykładu K. Żok wskazuje, że wyjątek w tej mierze może dotyczyć reprodukcji interfejsów głównego oprogramowania, jeżeli korzystają one z ochrony prawnoautorskiej. Jak wskazuje ten autor, jest to jednak przypadek graniczny, który wydaje się pozbawiony szerszego znaczenia w praktyce¹⁸. E. Molenda-Kropelnicka wskazuje także, iż konieczność zawarcia licencji zachodzi także w sytuacji, kiedy uruchomienie danej aplikacji wymaga zainstalowania jej komponentów, np. w postaci tzw. wtyczek (ang. *plug-in*) na komputerze¹⁹. Odmienny pogląd wyraził natomiast Ł. Pirożek. Jego zdaniem takie elementy oprogramowania jak wtyczki stanowią bowiem jedynie narzędzie do korzystania z programu komputerowego znajdującego się w zasobach dostawcy i nie są one „głównym” oprogramowaniem udostępnianym przez dostawcę²⁰.

Charakter prawny umowy w modelu SaaS

Wykluczenie zatem kwalifikacji omawianego kontraktu w modelu SaaS jako umowy prawnoautorskiej prowadzi w konsekwencji do pytania o to, jak należy go oceniać z perspektywy Kodeksu cywilnego. W tej kwestii w piśmiennictwie przyjmuje się, co do zasady (co można już było zauważyć w przywołanych stanowiskach doktryny), że umowa o korzystanie z programu komputerowego w modelu SaaS stanowi umowę o świadczenie usług, do której na mocy art. 750 KC odpowiednio znajdują zastosowanie przepisy o umowie zlecenia. W takim ujęciu zobowiązanie dostawcy polega na zachowaniu odpowiedniego poziomu wykonywanej usługi, określonego w stosownym porozumieniu. Oprócz przywołanych autorów komentarzy pogląd ten aprobuje także K. Żok oraz Ł. Pirożek²¹.

Jak podnoszą Z. Drzewiecki oraz S. Kubsik, w świetle prawa polskiego umowy SaaS są umowami o charakterze mieszanym, które nie są uregulowane ustawowo. Co więcej, trudno jest wskazać na dominujący (uniwersalny) model takiej umowy i często wymieszane są elementy różnych umów, co dodatkowo komplikuje ich kwalifikację prawną. W związku

z powyższym podstawowym wspólnym mianownikiem tych umów jest często jedynie ich cel, czyli umożliwienie użytkownikowi korzystania z oprogramowania zainstalowanego na serwerach dostawcy. Cel ten z kolei umowę SaaS najbardziej zbliża do umów o świadczenie usług w rozumieniu art. 750 KC²².

Powyższe stanowisko odpowiada także orzecznictwu SN dotyczącemu kwalifikacji umów nienazwanych, zgodnie z którym jeżeli w umowie mieszanej wyraźnie przeważa pewien rodzaj świadczenia, a jedynie świadczenia uboczne mają inny charakter, wówczas za trafne uznaje się zastosowanie przepisów dotyczących umowy nazwanej głównego typu (tak m.in. wyrok SN z 14.1.2010 r.²³; uchwała SN z 9.12.2010 r.²⁴).

Jak już zostało wspomniane, w dotychczasowym orzecznictwie sądów powszechnych brak jest judykatów dotyczących niniejszego zagadnienia. Warto jednak wskazać, że kwalifikację umowy w modelu SaaS pojawiają się często w interpretacjach organów podatkowych. Jest to związane z tym, iż powyższe zagadnienie prawne rzutuje w sposób bezpośredni na kwestie podatkowe, takie jak zasady ujmowania wydatków na oprogramowanie do kosztów uzyskania przychodów, możliwość korzystania z ulgi na nabycie nowych technologii, a także konieczność poboru zryczałtowanego podatku dochodowego u źródła.

Przykładowo w interpretacji indywidualnej z 22.11.2013 r. IBPP3/443-1049/13/AZ Izby Skargowej w Katowicach wskazano, że „*software as a service* (w skrócie SaaS, z ang. oprogramowanie jako usługa) to jeden z modeli chmury obliczeniowej, polegający na dystrybucji oprogramowania, gdzie aplikacja jest przechowywana i udostępniana przez producenta użytkownikom, poprzez Internet. Eliminuje to potrzebę instalacji i uruchamiania programu na komputerze klienta. Model SaaS przerzuca obowiązki zarządzania, aktualizacji, pomocy technicznej z konsumenta na dostawcę. W efekcie użytkownik oddaje kontrolę nad oprogramowaniem dostawcy i obowiązek zapewnienia jego ciągłości działania. W tym modelu klient otrzymuje konkretne, potrzebne mu funkcjonalności danego oprogramowania, a nie program. Programy działają na serwerze dostawcy, koszty ich utrzymania obciążają dostawcę – w tym wypadku Wnioskodawcę. Klient nie jest zmuszony nabywać na nie licencji. Dystrybucja programu

¹⁶ M. Modrzejewski, Podatkowe aspekty..., s. 17.

¹⁷ E. Molenda-Kropelnicka, Cloud Computing – zagadnienia prawne, Zeszyty Naukowe Uniwersytetu Jagiellońskiego Prace z Prawa Własności 2013, z. 119, s. 131.

¹⁸ K. Żok, Kwalifikacja umowy..., s. 27.

¹⁹ E. Kropelnicka-Molenda, Cloud Computing..., s. 132.

²⁰ Ł. Pirożek, Prawne aspekty..., s. 81.

²¹ K. Żok, Kwalifikacja umowy..., s. 27 i n.; Ł. Pirożek, Prawne aspekty..., s. 81.

²² Z. Drzewiecki, S. Kubsik, Umowy na korzystanie..., pkt 3.

²³ IV CSK 319/09, Legalis.

²⁴ III CZP 104/10, OSNC 2011, Nr 7–8, poz. 79.

w modelu SaaS nie wiąże się z koniecznością zawierania umowy licencyjnej, gdyż jego użytkownik nie wkracza najczęściej w zakres praw autorskich (art. 74 ust. 4 pkt 1 PrAutU). Spółka więc nie przekazuje klientom licencji na użytkowanie produktu, a jedynie umożliwia czasowy dostęp do opisanej wyżej usługi. Klient płaci jedynie za użycie platformy (każdorazowo, w formie abonamentu bądź w dowolnym udostępnionym przez usługodawcę trybie), a dostęp do niej uzyskuje na żądanie. Dostęp do platformy jest więc usługą”.

Podsumowanie

Podsumowując powyższe rozważania, nie ulega wątpliwości, iż kwalifikacja prawna umów w modelu SaaS stanowi kwestię sporną w literaturze prawniczej. Brak jest jednolitego stanowiska co do powyższej kwestii. Jest to związane także z tym, iż umowy w modelu SaaS potrafią różnić się od siebie

i mogą być „nasycone” elementami różnych umów nazwanych. Co do zasady jednak w doktrynie przeważa stanowisko, iż umowa o korzystanie z programu komputerowego w modelu SaaS stanowi umowę o świadczenie usług, do której na mocy art. 750 KC odpowiednio znajdują zastosowanie przepisy o umowie zlecenia. Jednocześnie wydaje się dominować pogląd, że w przypadku modelu SaaS nie dochodzi do zwielokrotnienia programu komputerowego, a tym samym nie jest konieczne zawarcie umowy licencyjnej. Należy jednak pamiętać, iż konieczność taka może zająć np. w przypadku, kiedy uruchomienie danej aplikacji wymaga zainstalowania jej komponentów, np. w postaci tzw. wtyczek (ang. *plug-in*) na komputerze. W związku z powyższym brak jest możliwości jednoznacznego i generalnego zakwalifikowania umowy w modelu SaaS jako umowy licencyjnej bądź też umowy o świadczenie usług. W konsekwencji treść każdej z tych umów powinna być rozpatrywana indywidualnie.

Słowa kluczowe: usługa, oprogramowanie jako usługa, licencja.

Legal nature of a Software as a Service contract in the Polish legal system

On the one hand, it seems that in French legal literature there is a strong position that contracts connected with using software in a SaaS model should be qualified as a licence agreement. On the other hand, German literature presents a view that denies such a contract its copyright nature. However, the middle ground between the abovementioned examples is presented in Swiss literature. In the Polish legal doctrine the opinions on the matter are varied. The purpose of the present article is to determine which legal qualification of a contract to use software in a SaaS model is currently dominating in literature.

Key words: service, software as a service, licence.



Prawo nowych technologii



C.H. BECK

ksiegarnia.beck.pl

Zadzwoni: 81 46 13 300

E-mail: kontakt@beck.pl