SEJM
RZECZYPOSPOLITEJ POLSKIEJ
X kadencja

Druk nr 728

Warszawa, 30 sierpnia 2024 r.

Pan
Szymon Hołownia
Marszałek Sejmu
Rzeczypospolitej Polskiej

Na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej i na podstawie art. 32 ust. 2 regulaminu Sejmu niżej podpisani posłowie wnoszą projekt ustawy:

- o zmianie ustawy - Kodeks postępowania cywilnego oraz niektórych innych ustaw.

Do reprezentowania wnioskodawców w pracach nad projektem ustawy upoważniamy pana posła Łukasza Osmalaka.

(-) Elżbieta Burkiewicz; (-) Żaneta Cwalina-Śliwowska; (-) Sławomir Ćwik; (-) Piotr Górnikiewicz; (-) Michał Gramatyka; (-) Rafał Kasprzyk; (-) Joanna Mucha; (-) Barbara Okuła; (-) Barbara Oliwiecka; (-) Łukasz Osmalak; (-) Ryszard Petru; (-) Piotr Paweł Strach; (-) Mirosław Suchoń; (-) Paweł Śliz; (-) Wioleta Tomczak; (-) Kamil Wnuk; (-) Paweł Zalewski; (-) Tomasz Zimoch.

Projekt

U S T A W A

z dnia ...

o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw[1)]

Art. 1. W ustawie z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2023 r. poz. 1550 z późn. zm.[2)]) w części pierwszej w księdze pierwszej w tytule VII dodaje się dział IX w brzmieniu:

„Dział IX

Postępowanie w sprawie ochrony dóbr osobistych przeciwko osobom o nieznanej tożsamości

Art. 505^{40}. § 1. Przepisy niniejszego działu stosuje się w sprawach o ochronę dóbr osobistych, jeżeli do ich naruszenia doszło drogą elektroniczną, a powód nie zna imienia i nazwiska albo nazwy lub adresu miejsca zamieszkania albo siedziby pozwanego, który naruszył jego dobra osobiste.

§ 2. Sprawy, o których mowa w § 1, rozpoznaje sąd okręgowy właściwy dla miejsca zamieszkania lub siedziby powoda na terytorium Rzeczypospolitej Polskiej.

§ 3. W sprawach, o których mowa w § 1, w pozwie zamiast imienia i nazwiska albo nazwy lub adresu pozwanego powód wskazuje jako pozwanego „osoba nieznana”.

Art. 505^{41}. § 1. Pozew, o którym mowa w art. 505^{40} § 3, powinien zawierać:

1) wniosek o zobowiązanie osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, która prowadząc, chociażby ubocznie, działalność zarobkową, zawodową lub pożytku publicznego świadczy usługi drogą elektroniczną, w tym również oferując usługi pośrednictwa internetowego w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1150 z dnia 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz. Urz. UE. L. 186 z 11.07.2019, str. 57) (usługodawca), za pośrednictwem, którego doszło do naruszenia dóbr osobistych powoda, do

---

1) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną i ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne

2) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2023 r. poz. 1429, 1606, 1615, 1667, 1860 i 2760 oraz z 2024 r. poz. 858, 859 i 863

wskazania danych pozwanego, określonych w art. 18 ust. 1 i 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344 oraz z 2024 r. poz. 1222 i ...) w oparciu o podane przez powoda informacje;

2) oznaczenie usługodawcy, za pośrednictwem którego drogą elektroniczną doszło do naruszenia dóbr osobistych powoda;
3) wskazanie w jaki sposób doszło do naruszenia dóbr osobistych powoda, w szczególności poprzez podanie publikacji naruszającej dobra osobiste powoda wraz z godziną i datą publikacji;
4) nazwę profilu lub login pozwanego, o ile wskazanie takich danych jest możliwe.

§ 2. Do pozwu należy dołączyć czytelne odwzorowanie publikacji, o której mowa w § 1 pkt 3, sporządzone w formie zapisu elektronicznego umieszczonego na nośniku danych oraz w formie wydruku przedstawiającego skopiowany obraz ekranu z widocznym adresem URL, o ile wskazanie adresu URL jest możliwe, oraz datą i godziną publikacji.

Art. $505^{42.}$ § 1. Sąd w terminie 7 dni od dnia złożenia pozwu, występuje z żądaniem do usługodawcy, za pośrednictwem którego doszło do naruszenia dóbr osobistych powoda, o nadesłanie wszystkich posiadanych danych pozwanego, o których mowa w art. 505^{41} § 1 pkt 1 oraz o wskazanie danych przedsiębiorcy telekomunikacyjnego w rozumieniu art. 2 pkt. 40 ustawy z dnia 12 lipca 2024 r. - Prawo komunikacji elektronicznej, będącego dostawcą systemu teleinformatycznego dla pozwanego wraz z pouczeniem o nałożeniu kary grzywny w przypadku nieprzekazania wszystkich posiadanych danych w wyznaczonym terminie.

§ 2. Usługodawca przekazuje wszystkie posiadane przez siebie dane, o których mowa w § 1, w terminie 7 dni od dnia doręczenia żądania sądu.

§ 3. Sąd w terminie 7 dni od dnia uzyskania danych przedsiębiorcy telekomunikacyjnego, o których mowa w § 1, występuje do przedsiębiorcy telekomunikacyjnego będącego dostawcą systemu teleinformatycznego dla pozwanego z żądaniem nadesłania wszystkich posiadanych danych pozwanego, o których mowa w art. 386 ust. 1 pkt. 1 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej wraz z pouczeniem o nałożeniu kary grzywny w przypadku nieprzekazania wszystkich posiadanych danych pozwanego w wyznaczonym terminie.

§ 4. Przedsiębiorca telekomunikacyjny przekazuje wszystkie posiadane przez siebie dane, o których mowa w § 3 w terminie 7 dni od dnia otrzymania żądania.

§ 5. Jeżeli usługodawca lub przedsiębiorca telekomunikacyjny o którym mowa w § 3 bez usprawiedliwionych powodów nie nadesłał wszystkich posiadanych danych, sąd nakłada karę grzywny w wysokości od stu tysięcy do miliona złotych.

Art. 505^{43}. Sąd rozpoznaje sprawę według przepisów ogólnych po uzyskaniu danych pozwanego.

Art. $505^{44.}$ Sąd umarza postępowanie, jeżeli usługodawca bądź przedsiębiorca telekomunikacyjny w rozumieniu art. 2 pkt 40 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej, nie wskazał wystarczających danych identyfikujących pozwanego bądź ich pozyskanie byłoby niemożliwe. Sąd z urzędu sporządza uzasadnienie postanowienia. Postanowienie z uzasadnieniem sąd z urzędu doręcza tylko powodowi, z pouczeniem o sposobie i terminie wniesienia środka zaskarżenia.”.

Art. 2. W ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344 oraz z 2024 r. poz. 1222) wprowadza się następujące zmiany:

1) w art. 18:
   a) w ust. 1:
      – wprowadzenie do wyliczenia otrzymuje brzmienie:
        "Osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, która prowadząc, chociażby ubocznie, działalność zarobkową, zawodową lub pożytku publicznego świadczy usługi drogą elektroniczną, w tym również oferując usługi pośrednictwa internetowego w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1150 z dnia 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz. Urz. UE L. 186 z 11.07.2019, str. 57) (usługodawca) może przetwarzać następujące dane osobowe usługobiorcy niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego między nimi:";
      – w pkt. 6 kropkę zastępuje się średnikiem i dodaje się pkt 7 w brzmieniu:
        "7) numer telefonu podany przez usługobiorcę.”;
   b) ust. 5 otrzymuje brzmienie:
      „5. Usługodawca ma prawo przetwarzać następujące dane charakteryzujące sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną (dane eksploatacyjne):

1) oznaczenia identyfikujące usługobiorcę nadawane na podstawie danych, o których mowa w ust. 1;
2) oznaczenia jednoznacznie identyfikujące zakończenie sieci telekomunikacyjnej lub zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221 i ...), z którego korzystał usługobiorca, w tym adres używany w sieci wykorzystującej protokół komunikacyjny IP (adres IP) wraz z portem źródłowym;
3) datę, godzinę, minutę i sekundę każdorazowego rozpoczęcia i zakończenia połączenia z systemem teleinformatycznym, do którego mają dostęp użytkownicy, w formacie (dd.mm.rr hh:mm:ss), zgodnie z czasem urzędowym w rozumieniu ustawy z dnia 10 grudnia 2003 r. o czasie urzędowym na obszarze Rzeczypospolitej Polskiej (Dz. U. z 2004 r. poz. 144), węzeł wyjścia tzw. „exit node" lub inne w zależności od zastosowanych technologii;
4) informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną;
5) informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną.";

3) po art. 18 dodaje się art. 18a i art. 18b w brzmieniu:

„Art. 18a. 1. Usługodawca jest obowiązany na własny koszt przechowywać dane, o których mowa w art. 18 ust. 1 i 5, generowane lub przetwarzane w trakcie prowadzonej przez niego działalności na terytorium Rzeczypospolitej Polskiej, przez okres 6 miesięcy, licząc od dnia wprowadzenia ich do systemu teleinformatycznego, do którego mają dostęp użytkownicy.

2. W przypadku danych osób dopuszczających się naruszenia dóbr osobistych użytkowników, usługodawca przechowuje i zabezpiecza dane, o których mowa w art. 18 ust. 1 i 5 oraz dane, o których mowa w art. 386 ust. 1 pkt 1 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej, przez okres nie krótszy niż 12 miesięcy od dnia ich wprowadzenia do systemu teleinformatycznego, do którego mają dostęp użytkownicy.

Art. 18b. Usługodawca jest obowiązany udostępnić dane, o których mowa w art. 18 ust. 1 i 5 oraz dane, o których mowa w art. 386 ust. 1 pkt 1 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej, na każdorazowe wezwanie sądu albo organu administracji publicznej na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz. Urz. UE L 277 z 27.10.2022, str. 1, z późn. zm[3)]).";

Art. 3. W ustawie z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221) wprowadza się następujące zmiany:

1) w art. 386 w ust. 1 pkt 1 otrzymuje brzmienie:

„1) dane dotyczące podmiotu korzystającego z publicznie dostępnej usługi telekomunikacyjnej lub żądającego świadczenia takiej usługi (użytkownika), w tym w szczególności: nazwisko i imiona użytkownika, numer ewidencyjny PESEL lub – gdy ten numer nie został nadany – numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość, adres zameldowania na pobyt stały, adres do korespondencji, jeżeli jest inny niż adres zameldowania na pobyt stały, dane służące do weryfikacji podpisu elektronicznego, adresy elektroniczne, numer telefonu;";

2) po art. 405 dodaje się art. 405a w brzmieniu:

„Art. 405a. Przedsiębiorca telekomunikacyjny udostępnia na żądanie sądu albo organu administracji publicznej, na podstawie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), dane osobowe użytkownika, o których mowa w art. 386 ust. 1 pkt 1.".

Art. 4. Ustawa wchodzi w życie po upływie 12 miesięcy od dnia ogłoszenia.

---

3) Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 163 z 29.06.2023, str. 107.

Uzasadnienie

Cel regulacji

W ostatnich latach, wraz z dynamicznym rozwojem technologii, naruszenia dóbr osobistych stały się poważnym problemem społecznym. Internet stał się przestrzenią, w której cyberprzemoc oraz hejt stały się powszechne. Poszkodowani, którzy padają ofiarą takich naruszeń, często zmagają się z poważnymi konsekwencjami psychicznymi. Publikacje na forach internetowych czy w mediach społecznościowych naruszają dobra osobiste osób nie tylko w sferze prywatnej, ale także mogą dotykać przedsiębiorców i stanowić zagrożenie dla prowadzonej przez nich działalności gospodarczej.

Jednym z najważniejszych problemów związanych z naruszeniami dóbr osobistych w Internecie jest trudność w identyfikacji sprawców. Osoby dokonujące tych naruszeń korzystają z anonimowości – jednej z kluczowych cech komunikacji w Internecie - którą zapewniają im media społecznościowe czy fora dyskusyjne. Odbiorca treści nie jest w stanie podać żadnej istotnej cechy identyfikującej jego nadawcę, jeśli nadawca sam się pod tą treścią nie podpisał.

W praktyce oznacza to, że poszkodowani mogą nie mieć możliwości ustalenia tożsamości sprawcy, co właściwie uniemożliwia im dochodzenie swoich praw na drodze sądowej i egzekwowanie odpowiedzialności za wyrządzone szkody.

Aktualny stan prawny w Polsce nie dostarcza wystarczających narzędzi do ochrony osób poszkodowanych naruszeniami dóbr osobistych w Internecie. Przepisy Kodeksu postępowania cywilnego nie nadążają za rozwojem technologii i pojawiającymi się problemami. W praktyce poszkodowani naruszeniem dóbr osobistych często rezygnują z dochodzenia swoich praw, z uwagi na brak możliwości skutecznego wniesienia pozwu, wobec braku możliwości ustalenia personaliów osoby dokonującej naruszeń. Na gruncie obecnie obowiązujących przepisów, powód, który chce dochodzić roszczenia w postępowaniu cywilnym, musi znać konkretne dane umożliwiające identyfikację pozwanego wskazane w art. 126 § 1 i 2 k.p.c. Jeżeli takich danych powód nie zna, to choćby dochodzone przez niego roszczenie byłoby w pełni uzasadnione, to w świetle obecnych regulacji nie ma możliwości uzyskania skutecznej ochrony sądowej. Złożony przez takie osoby pozew, wobec niewskazania danych pozwanego ujętych w art. 126 § 1 i 2 k.p.c., nie spełni wymagań formalnych pozwu.

Z perspektywy więc osoby, która nie zna danych osoby dopuszczającej się naruszenia jego dóbr osobistych w Internecie, wprowadzenie instytucji „ślepego pozwu” umożliwi skorzystanie z przewidzianego w art. 45 ust. 1 Konstytucji RP „prawa do sądu”.

W związku z powyższymi problemami, istnieje pilna potrzeba wprowadzenia rozwiązań legislacyjnych, które pozwolą ofiarom „anonimowego hejtu” skutecznie dochodzić swoich roszczeń przed sądem. Wprowadzenie instytucji "ślepego pozwu" stanowić będzie pierwszy istotny krok w walce z „anonimowym hejtem”. Takie rozwiązanie legislacyjne pozwoli na składanie pozwów bez konieczności wcześniejszego ustalenia tożsamości sprawcy przez osoby poszkodowane oraz zagwarantuje realną pomoc Państwa w identyfikacji sprawcy na potrzeby postępowania cywilnego. Wprowadzenie instytucji „ślepego pozwu” umożliwi osobom poszkodowanym sięgnięcie do mechanizmów odpowiedzialności cywilnoprawnej w celu zwalczania zniesławiających wpisów w Internecie.

Należy zwrócić również uwagę, że sam fakt istnienia instytucji umożliwiającej zidentyfikowanie osób dokonujących naruszenia dóbr osobistych w Internecie może spowodować też ograniczenie ilości takich zjawisk, pełnić funkcję odstraszającą i prewencyjną – obecnie istniejące regulacje prawne powodowały praktycznie całkowity brak odpowiedzialności za zniesławiające publikacje, o ile takie publikacje nie nosiły znamion przestępstwa, a tym samym całkowite poczucie bezkarności.

Proponowane rozwiązanie legislacyjne

Niniejszy projekt wprowadza nowy rodzaj cywilnego postępowania szczególnego tj. postępowanie o ochronę dóbr osobistych, jeżeli do ich naruszenia doszło drogą elektroniczną, a powód nie zna imienia i nazwiska albo nazwy lub adresu miejsca zamieszkania albo siedziby pozwanego, który naruszył jego dobra osobiste. Zaproponowane przepisy generalnie upoważniają sądy cywilne do występowania w imieniu powodów o konieczne do procedowania dane. Jest to znaczące ułatwienie szczególnie dla stron, których dobra osobiste zostały naruszone przez anonimowe wpisy, jak również dla osób niereprezentowanych przez profesjonalnych pełnomocników.

Wnosząc pozew o ochronę dóbr osobistych, jeżeli do ich naruszenia doszło drogą elektroniczną, powód w pozwie zamiast imienia i nazwiska albo nazwy lub adresu pozwanego wskazuje jako pozwanego „osobę nieznaną".

Właściwymi do rozpoznania niniejszej kategorii spraw będą sądy okręgowe miejsca zamieszkania lub siedziby powoda. Takie ukształtowanie właściwości sądu jest konieczne z uwagi na brak znajomości danych pozwanego, w tym miejsca jego zamieszkania w chwili wniesienia pozwu.

Art. 505^{41} proponowanych zmian do Kodeksu postępowania cywilnego zawiera szczegółowe wymagania dotyczące pozwu.

Powód będzie zobowiązany zawrzeć w pozwie wniosek o zobowiązanie osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, która prowadząc, chociażby ubocznie, działalność zarobkową, zawodową lub pożytku publicznego świadczy usługi drogą elektroniczną, w tym również oferując usługi pośrednictwa internetowego, za pośrednictwem którego doszło do naruszenia dóbr osobistych powoda, do wskazania wszystkich posiadanych danych pozwanego określonych w art. 18 ust. 1 i 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną oraz danych określonych w oparciu o podane przez powoda informacje.

Poza powyższymi dwoma wnioskami, powód będzie zobowiązany umieścić również w pozwie oznaczenie usługodawcy, za pośrednictwem którego drogą elektroniczną doszło do naruszenia dóbr osobistych powoda. Powód w pozwie będzie musiał wskazać, w jaki sposób doszło do naruszenia dóbr osobistych powoda, w szczególności podając publikacje naruszającą jego dobra osobiste – do pozwu należy załączyć czytelne odwzorowanie publikacji sporządzone w formie zapisu elektronicznego umieszczonego na nośniku danych oraz w formie wydruku przedstawiającego skopiowany obraz ekranu z widocznym adresem URL, o ile wskazanie adresu URL jest możliwe, oraz datą i godziną publikacji. Powód podaje informacje pozwalające ustalić osobę, która dopuściła się naruszenia - nazwę profilu lub login użytkownika.

Powyższe wnioski i informacje przekazane już na początkowym etapie – w pozwie – umożliwią sądowi ustalenie personaliów pozwanego dokonującego naruszeń dóbr osobistych, poprzez

zwrócenie się o poszczególne informacje do usługodawcy, a następnie do przedsiębiorcy telekomunikacyjnego.

Pierwszym krokiem podejmowanym przez sąd po złożeniu pozwu przez powoda będzie ustalenie danych pozwanego. W tym celu sąd będzie występował do usługodawcy o nadesłanie danych identyfikujących pozwanego oraz o wskazanie danych przedsiębiorcy telekomunikacyjnego, będącego dostawcą systemu teleinformatycznego dla pozwanego wraz z pouczeniem o nałożeniu kary grzywny w przypadku nieprzekazania wszystkich posiadanych danych w wyznaczonym terminie.

Kolejnym krokiem będzie wystąpienie przez sąd do przedsiębiorcy telekomunikacyjnego będącego dostawcą systemu teleinformatycznego dla pozwanego z żądaniem nadesłania danych pozwanego, o których mowa w art. 386 ust. 1 pkt. 1 ustawy z dnia 12 lipca 2024 t. – Prawo komunikacji elektronicznej wraz z pouczeniem o nałożeniu kary grzywny w przypadku nieprzekazania wszystkich posiadanych danych w wyznaczonym terminie.

Termin, w jakim sąd ma obowiązek zwrócenia się do usługodawcy, a po uzyskaniu od niego informacji do przedsiębiorcy telekomunikacyjnego, zakreślono na 7 dni. Zakreślenie tak krótkiego terminu ma za zadanie przyśpieszyć postępowanie oraz przeciwdziałać sytuacjom, w których to uzyskanie danych od przedsiębiorców telekomunikacyjnych oraz usługodawców będzie niemożliwe z uwagi na przekroczenie obowiązkowego okresu retencji danych. Zaznaczyć należy, że w celu umożliwienia wywiązania się usługodawcy z powyższego obowiązku informacyjnego, wprowadzono do ustawy o świadczeniu usług drogą elektroniczną obowiązek retencji danych, w szczególności danych osobowych i eksploatacyjnych. Usługodawca oraz przedsiębiorca telekomunikacyjny w terminie 7 dni od dnia otrzymania żądania sądu przekazuje sądowi wszystkie posiadane przez siebie dane osobowe dotyczące pozwanego. Jeżeli usługodawca lub przedsiębiorca telekomunikacyjny bez usprawiedliwionych powodów nie nadesłał danych, sąd nakłada karę grzywny w wysokości od stu tysięcy do miliona złotych.

W niniejszym projekcie przewidziane zostały skutki prawne nieuzyskania danych od usługodawcy bądź przedsiębiorcy telekomunikacyjnego. Mianowicie, jeżeli usługodawca bądź przedsiębiorca telekomunikacyjny w rozumieniu art. 2 pkt 40 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej nie wskazał wystarczających danych identyfikujących

pozwanego bądź ich pozyskanie byłoby niemożliwe, postępowanie sądowe podlegać będzie umorzeniu. Sąd z urzędu jednak sporządza uzasadnienie postanowienia – postanowienie z uzasadnieniem sąd z urzędu doręcza tylko powodowi z pouczeniem o sposobie i terminie wniesienia środka zaskarżenia. W przypadku uzyskania przez sąd danych umożliwiających identyfikację pozwanego, sąd rozpoznaję sprawę według zasad ogólnych.

W art. 2 niniejszego projektu proponuje się wprowadzenie zmian w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. W art. 18 ust. 1 tej ustawy dodaje się numer telefonu jako kolejną daną osobową możliwą do przetwarzania przez usługodawcę. Zmiana art. 18 ust. 5 polega na uszczegółowieniu danych eksploatacyjnych przetwarzanych przez usługodawcę. Jednocześnie proponuje się dodanie dodatkowych danych eksploatacyjnych przetwarzanych przez usługodawcę. Zgodnie z proponowanym nowym brzmieniem art. 18 ust. 5, usługodawca będzie miał prawo przetwarzać następujące dane charakteryzujące sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną (dane eksploatacyjne):

1) oznaczenia identyfikujące usługobiorcę nadawane na podstawie danych, o których mowa w ust. 1;

2) oznaczenia jednoznacznie identyfikujące zakończenie sieci telekomunikacyjnej lub zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej, z którego korzystał usługobiorca, w tym adres używany w sieci wykorzystującej protokół komunikacyjny IP (adres IP) wraz z portem źródłowym;

3) datę, godzinę, minutę i sekundę każdorazowego rozpoczęcia i zakończenia połączenia z systemem teleinformatycznym, do którego mają dostęp użytkownicy, w formacie (dd.mm.rr hh:mm:ss), zgodnie z czasem urzędowym w rozumieniu ustawy z dnia 10 grudnia 2003 r. o czasie urzędowym na obszarze Rzeczypospolitej Polskiej (Dz. U. z 2004 r. poz. 144), węzeł wyjścia tzw. „exit node” lub inne w zależności od zastosowanych technologii;

4) informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną;

5) informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną.

W dodanym do ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną art. 18a proponuje się uregulowanie zagadnienia przechowywania danych niezbędnych do świadczenia usług. Zaproponowana zmiana poprzez dodanie do ustawy o świadczeniu usług drogą elektroniczną art. 18a wynika z okoliczności, że w obecnym brzmieniu tej ustawy brak jest przepisów normujących obowiązek retencji danych przez usługodawców. Nienałożenie na usługodawców obowiązku retencji danych sprawiłoby, że obowiązek wskazany w art. 18 ust. 6 ustawy o świadczeniu usług drogą elektroniczną obejmowałby wyłącznie te dane, które znajdują się w posiadaniu usługodawcy w dniu zgłoszenia przez organ takiego żądania, co tym samym mogłoby uniemożliwić faktyczne ustalenie pozwanego w ramach instytucji „ślepego pozwu".

W ustawie z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221) proponuje się wprowadzenie zmian w art. 386 w ust. 1 pkt 1 poprzez doprecyzowanie pojęcia danych użytkownika objętych tajemnicą komunikacji elektronicznej. Tajemnicą komunikacji elektronicznej będą więc objęte dane dotyczące podmiotu korzystającego z publicznie dostępnej usługi telekomunikacyjnej lub żądającego świadczenia takiej usługi (użytkownika), w tym w szczególności: nazwisko i imiona użytkownika, numer ewidencyjny PESEL lub – gdy ten numer nie został nadany – numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość, adres zameldowania na pobyt stały, adres do korespondencji, jeżeli jest inny niż adres zameldowania na pobyt stały, dane służące do weryfikacji podpisu elektronicznego, adresy elektroniczne, numer telefonu.

Zakłada się, że ustawa wejdzie w życie po 12 miesiącach od dnia ogłoszenia. Tak długi okres *vacatio legis* uzasadniony jest potrzebą zapewnienia usługodawcom i przedsiębiorcom telekomunikacyjnym odpowiedniego czasu do przystosowania się do norm wynikających z przedmiotowego projektu. Ponadto będzie to wystarczający czas, by sądy powszechne przygotowały się organizacyjnie do skutków nowelizacji, szczególnie w kontekście pierwszej części procesu dotyczącej ustalania tożsamości pozwanego.

Przedstawienie przewidywanych skutków społecznych i gospodarczych i finansowych

Ustawa będzie miała korzystne skutki społeczne. Poprawi sytuację wszystkich narażonych i dotkniętych skutkami anonimowego naruszania dóbr osobistych w Internecie. Poprawi bezpieczeństwo użytkowników Internetu.

W wymiarze gospodarczym wpłynie pozytywnie na wszystkich przedsiębiorców, którzy będą mogli skuteczniej dochodzić ochrony dóbr osobistych swoich firm.

Zostaną zwiększone obowiązki usługodawców w rozumieniu ustawy o świadczeniu usług drogą elektroniczną poprzez dodanie dodatkowych danych eksploatacyjnych przetwarzanych przez usługodawcę oraz obowiązek ich udostępniania. Nie ma innej możliwości realizacji celów ustawy. Dodawane obowiązki są niezbędne do skutecznego procedowania „ślepych pozwów". Z tego względu nie ma też możliwości korzystniejszego uregulowania sytuacji mikro-, małych i średnich przedsiębiorców.

Projekt nie zmieni zasad podejmowania, wykonywania lub zakończenia działalności gospodarczej (projektodawcy uznają, że skutki opisane w akapicie poprzedzającym nie zmieniają zasad wykonywania działalności gospodarczej, a tylko jej szczegółowe warunki).

Projekt ustawy może pociągać za sobą obciążenia budżetu państwa. Wejście w życie ustawy skutkować będzie zwiększeniem obciążenia sądów cywilnych. Ze względu na brak możliwości oszacowania, o ile więcej spraw o ochronę dóbr osobistych wpłynie do sądów po wejściu w życie nowelizacji (brak aktualnych, powszechnie dostępnych danych dotyczących liczby spraw o ochronę dóbr osobistych), nie jest możliwe precyzyjne oszacowanie skutków finansowych z tego tytułu. Przy mniejszej liczbie spraw ustawa nie wiąże się z potrzebą wsparcia kadrowego sądów powszechnych.

Projekt ustawy nie pociąga za sobą obciążenia budżetów jednostek samorządu terytorialnego

Dodatkowe informacje o spełnianiu przez projekt wymogów określonych przepisami

Projekt jest zgodny z prawem Unii Europejskiej.
Projekt nie zawiera przepisów regulacyjnych i przepisów określających wymogi dotyczące świadczenia usług transgranicznych w rozumieniu ustawy z dnia 22 grudnia 2015 r. o zasadach uznawania kwalifikacji zawodowych nabytych w państwach członkowskich Unii Europejskiej.
Projekt nie zawiera przepisów technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega procedurze notyfikacji.

SEJM RZECZYPOSPOLITEJ POLSKIEJ

BIURO EKSPERTYZ I OCENY SKUTKÓW REGULACJI
KANCELARII SEJMU

Warszawa, 10 września 2024 r.

BEOS-WPEiM-1898/24

Pan
Szymon Hołownia
Marszałek Sejmu
Rzeczypospolitej Polskiej

Opinia w sprawie zgodności z prawem Unii Europejskiej poselskiego projektu ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (przedstawiciel wnioskodawców: poseł Łukasz Osmalak)

Na podstawie art. 34 ust. 9 uchwały Sejmu Rzeczypospolitej Polskiej z dnia 30 lipca 1992 roku – Regulamin Sejmu Rzeczypospolitej Polskiej (Monitor Polski z 2022 r. poz. 990, ze zm.) sporządza się następującą opinię:

1. Przedmiot projektu ustawy

Projekt ustawy zmierza do nowelizacji ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego[1] (dalej: Kpc), ustawy z dnia 18 lipca 2022 r. o świadczeniu usług drogą elektroniczną[2] oraz ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej[3] (dalej: Pke).

Projektowane zmiany Kpc obejmują dodanie w części pierwszej w księdze pierwszej nowego działu IX zatytułowanego: Postępowanie w sprawie ochrony dóbr osobistych przeciwko osobom o nieznanej tożsamości. Przepisy te mają regulować zasady składania i rozpatrywania pozwu w sprawach o ochronę dóbr osobistych, jeżeli do ich naruszenia doszło droga elektroniczną, a powód nie zna imienia i nazwiska albo nazwy lub adresu miejsca zamieszkania albo siedziby pozwanego, który naruszył jego dobra osobiste.

Zmiany w ustawie o świadczeniu usług drogą elektroniczną przewidują poszerzenie zakresu danych usługobiorcy oraz zakresu danych charakteryzujących sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną, które usługodawca może przetwarzać. Projekt przewiduje także obciążenie usługodawców dwoma obowiązkami dotyczącymi tych danych: (1) obowiązkiem przechowywania przez okres 6 miesięcy (w przypadku osób dopuszczających się naruszenia dóbr osobistych użytkowników – 12 miesięcy) od dnia wprowadzenia danych do systemu teleinformatycznego, do którego mają dostęp użytkownicy, (2) obowiązkiem udostępniania na każdorazowe wezwanie

[1] Dz. U. z 2023 r. poz. 1550, ze zm.
[2] Dz. U. z 2020 r. poz. 344, ze zm.
[3] Dz. U. poz. 1221.

sądu albo organu administracji publicznej na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)[4] (dalej: rozporządzenie 2022/2065).

Zmiany w Pke przewidują doprecyzowanie zakresu danych dotyczących użytkownika objętych tajemnicą komunikacji elektronicznej. Ponadto projekt przewiduje dodanie nowego art. 405a, zgodnie z którym przedsiębiorca telekomunikacyjny udostępnia na żądanie sądu albo organu administracji publicznej, na podstawie rozporządzenia 2022/2065 dane osobowe użytkownika objęte tajemnicą komunikacji elektronicznej.

Projektowana ustawa ma wejść w życie po upływie 12 miesięcy od dnia ogłoszenia.

2. Stan prawa Unii Europejskiej w materii objętej projektem ustawy

2.1. Ze względu na przedmiot projektu ustawy należy przywołać następujące akty prawne Unii Europejskiej:

a) artykuł 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TfUE);
b) artykuł 7, art. 8, art. 51 i art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej[5] (dalej: Karta);
c) dyrektywę 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)[6] (dalej: dyrektywa 2000/31);
d) dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[7] (dalej: dyrektywa 2002/58);
e) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1150 z dnia 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego[8] (dalej: rozporządzenie 2019/1150);
f) rozporządzenie 2022/2065;
g) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu

[4] Dz. Urz. UE L 277 z 27.10.2022 r., s. 1, ze zm.
[5] Zgodnie z art. 6 ust. 1 Traktatu o Unii Europejskiej Karta praw podstawowych Unii Europejskiej ma taką samą moc prawną jak Traktaty.
[6] Dz. Urz. WE L 178 z 17.7.2000 r., s. 1, ze zm.
[7] Dz. Urz. UE L 201 z 31.7.2002 r., s. 37, ze zm.
[8] Dz. Urz. WE L 186 z 11.7.2019 r., s. 57.

takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[9] (dalej: RODO).

2.2. Artykuł 16 ust. 1 TfUE przyznaje każdej osobie prawo do ochrony danych osobowych jej dotyczących. Przepis ten ustanawia zasadę prawa UE ochrony danych osobowych, mającą ogólne zastosowanie, czyli dotyczącą przetwarzania danych w sektorze prywatnym i publicznym. Artykuł 16 ust. 1 TfUE wskazuje na potrzebę ochrony danych osobowych nie tylko w odniesieniu do przetwarzania ich przez instytucje UE, ale również w odniesieniu do przetwarzania ich przez państwa członkowskie.

Karta w art. 7 stanowi, że każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się. W art. 8 Karta stanowi, że każdy ma prawo do ochrony danych osobowych, które go dotyczą. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania. Przestrzeganie tych zasad podlega kontroli niezależnego organu. Artykuł 51 Karty stanowi, że postanowienia Karty mają zastosowanie do państw członkowskich wyłącznie w zakresie, w jakim stosują one prawo Unii. Z kolei, zgodnie z art. 52 ust. 1 Karty wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w Karcie muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

Dyrektywa 2002/58 przewiduje harmonizację przepisów krajowych wymaganych do zapewnienia równoważnego poziomu ochrony podstawowych praw i wolności, w szczególności prawa do prywatności i poufności, w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej oraz w celu zapewnienia swobodnego przepływu we Wspólnocie tego typu danych oraz urządzeń i usług łączności elektronicznej (art. 1 ust. 1).

W art. 5 dyrektywy 2002/58 uregulowano zagadnienia związane z poufnością komunikacji. Zgodnie z ustępem 1 tego przepisu państwa członkowskie zapewniają, poprzez ustawodawstwo krajowe, poufność komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. W szczególności zakazują słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników, z wyjątkiem upoważnienia zgodnego z art. 15 ust. 1. Artykuł 5 dyrektywy

[9] Dz. Urz. UE L 119 z 4.5.2016 r., s. 1, ze zm.

2002/58 nie zabrania technicznego przechowywania, które jest niezbędne do przekazania komunikatu bez uszczerbku dla zasady poufności.

Zgodnie z art. 6 ust. 1 dyrektywy 2002/58 dane o ruchu dotyczące abonentów i użytkowników przetwarzane i przechowywane przez dostawcę publicznej sieci łączności lub publicznie dostępnych usług łączności elektronicznej muszą zostać usunięte lub uczynione anonimowymi, gdy nie są już potrzebne do celów transmisji komunikatu, bez uszczerbku dla przepisów ust. 2, 3 i 5 niniejszego artykułu oraz art. 15 ust. 1.

Z kolei art. 15 ust. 1 dyrektywy 2002/58 stanowi, iż państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5 lub art. 6 (...) tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy 95/46/WE[10]. W tym celu, państwa członkowskie mogą, między innymi, uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie. Wszystkie środki muszą być zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 Traktatu o Unii Europejskiej[11].

RODO w art. 5 określa zasady przetwarzania danych osobowych, a w art. 6 określa, kiedy przetwarzanie danych jest zgodne z prawem. Zgodnie z art. 23 ust. 1 lit. i[12] RODO prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12-22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym ochronie osoby, której dane dotyczą, lub praw i wolności innych osób.

---

[10] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. 281 , 23/11/1995 s. 31; dalej: dyrektywa 95/46) została uchylona przez RODO. Odesłania do dyrektywy 95/46 należy traktować jako odesłania do RODO (zob. art. 94 RODO).

[11] Zgodnie z art. 6 ust. 1 akapit pierwszy TUE Unia uznaje prawa, wolności i zasady określone w Karcie praw podstawowych Unii Europejskiej z 7 grudnia 2000 roku, w brzmieniu dostosowanym 12 grudnia 2007 roku w Strasburgu, która ma taką samą moc prawną jak Traktaty.

[12] Art. 23 ust. 1 RODO jest odpowiednikiem 13 ust. 1 dyrektywy 95/46, do której odwołuje się art. 15 ust. 1 dyrektywy 2002/58.

Rozporządzenie 2022/2065 ma na celu przyczynienie się do właściwego funkcjonowania rynku wewnętrznego usług pośrednich poprzez ustanowienie zharmonizowanych przepisów dotyczących bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego, które ułatwia innowacje i w którym skutecznie chronione są prawa podstawowe zapisane w Karcie praw podstawowych Unii Europejskiej, w tym zasada ochrony konsumentów (art. 1 ust. 1). W art. 10 rozporządzenia 2022/2065 uregulowano udzielanie, na podstawie żądania odpowiedniego krajowego organu sądowego lub administracyjnego, przez dostawców usług pośrednich[13] informacji o określonych indywidualnych odbiorcach usług[14]. Regulacja ta pozostaje bez uszczerbku dla krajowego prawa cywilnego procesowego i krajowego prawa karnego procesowego (ust. 6).

Dyrektywa 2000/31 [15] ma na celu przyczynienie się do właściwego funkcjonowania rynku wewnętrznego przez zapewnienie swobodnego przepływu usług społeczeństwa informacyjnego między państwami członkowskimi. Dyrektywa 2000/31 zbliża, w zakresie potrzebnym do osiągnięcia swojego celu, niektóre przepisy krajowe w sprawie usług społeczeństwa informacyjnego odnoszące się do rynku wewnętrznego, siedzib usługodawców, informacji handlowych, umów zawieranych drogą elektroniczną, odpowiedzialności pośredników, kodeksów postępowania, pozasądowych dróg rozstrzygania sporów, dochodzenia praw przed sądem oraz współpracy między państwami członkowskimi (art. 1 ust. 1 i 2).

Rozporządzenie 2019/1150 ma na celu przyczynianie się do właściwego funkcjonowania rynku wewnętrznego poprzez ustanowienie przepisów w celu zapewnienia, aby użytkownikom biznesowym korzystającym z usług pośrednictwa internetowego i użytkownikom korzystającym ze strony internetowej w celach biznesowych w odniesieniu do wyszukiwarek internetowych zapewniono odpowiednią przejrzystość, sprawiedliwość i możliwości skutecznego dochodzenia roszczeń. Rozporządzenie ma zastosowanie do usług pośrednictwa internetowego [16] i wyszukiwarek internetowych, które są dostarczane lub których dostarczenie jest oferowane, odpowiednio, użytkownikom biznesowym i użytkownikom korzystającym ze strony internetowej w celach biznesowych, mającym siedzibę lub miejsce pobytu w Unii, którzy poprzez te usługi pośrednictwa internetowego lub wyszukiwarki internetowe oferują towary lub usługi konsumentom znajdującym się w Unii, niezależnie od siedziby lub miejsca pobytu dostawców tych usług oraz niezależnie od innych mających zastosowanie przepisów (art. 1 ust. 1 i 2).

---

[13] Definicja usługi pośredniej znajduje się w art. 3 lit. g rozporządzenia 2022/2065.

[14] Definicja odbiorcy usługi znajduje się w art. 3 lit. b rozporządzenia 2022/2065.

[15] Dyrektywa 2000/31 została implementowana do prawa polskiego ustawą o świadczeniu usług drogą elektroniczną, której nowelizację przewiduje opiniowany projekt ustawy.

[16] Usługi pośrednictwa internetowego zdefiniowane są w art. 2 pkt 2 rozporządzenia 2019/1150.

3. Analiza przepisów projektu ustawy pod kątem ustalonego stanu prawa Unii Europejskiej

Przewidziana w art. 1 projektu ustawy nowelizacja Kpc polegająca na ustanowieniu postępowania w sprawie ochrony dóbr osobistych przeciwko osobom o nieznanej tożsamości nie jest – co do zasady – objęta zakresem prawa Unii Europejskiej. Przewidziane w projektowanym art. 505^{42} Kpc prawo żądania przez sąd określonych danych dotyczących pozwanego nie jest sprzeczne z art. z art. 10 rozporządzenia 2022/2065 w związku z art. 5 i art. 15 ust. 1 dyrektywy 2002/58 oraz w związku z art. 23 ust. 1 lit. i RODO.

Zmiana art. 18 ust. 1 ustawy o świadczeniu usług drogą elektroniczną, polegająca na zmianie (na użytek tego przepisu) definicji usługodawcy[17] oraz rozszerzeniu katalogu danych osobowych usługobiorcy, które usługodawca może przetwarzać, a które są niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego między nimi, nie narusza art. 5 i art. 6 RODO.

Zmiana art. 18 ust. 5 ustawy o świadczeniu usług drogą elektroniczną, polegająca na poszerzeniu katalogu danych eksploatacyjnych, charakteryzujących sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną, które usługodawca może przetwarzać nie narusza art. 5 i art. 6 RODO.

Projektowany art. 18a ustawy o świadczeniu usług drogą elektroniczną przewiduje nałożenie na usługodawców obowiązku przechowywania na własny koszt danych osobowych usługobiorców, określonych w art. 18 ust. 1 i 5 tej ustawy, generowanych lub przetwarzanych przez niego w trakcie prowadzonej przez niego działalności na terytorium RP. Okres przechowywania miałby wynosić 6 miesięcy, a w przypadku danych osób dopuszczających się naruszenia dóbr osobistych użytkowników – 12 miesięcy. Z kolei proponowany art. 18b ustawy o świadczeniu usług drogą elektroniczną nakłada na usługodawcę obowiązek udostępniania gromadzonych danych osobowych usługobiorców, w tym danych objętych tajemnicą komunikacji elektronicznej, na wezwanie sądu albo organu administracji publicznej na podstawie rozporządzenia 2022/2065. Kwestia przechowywania danych uregulowana jest także w art. 180a-180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne [18] . Prawo telekomunikacyjne ma zostać zastąpione przez Pke, która w art. 47-50 powtarza regulację Prawa telekomunikacyjnego dotyczącą przechowywania danych.

Należy zwrócić uwagę, że przywołane przepisy Prawa telekomunikacyjnego implementowały – w zakresie swojej regulacji – dyrektywę Parlamentu Europejskiego i Rady 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci

[17] Należy wskazać, że w ustawie znajduje się już jedna definicja usługodawcy – art. 2 pkt 6. Projekt jej nie zmienia, lecz wprowadza drugą.

[18] Dz. U. z 2024 r. poz. 34, ze zm.

łączności oraz zmieniającej dyrektywę 2002/58/WE [19] (dalej: dyrektywa 2006/24). Trybunał Sprawiedliwości UE[20] (dalej: TSUE) stwierdził nieważność dyrektywy 2006/24, ze względu na to, że przyjęte w niej rozwiązania zbyt głęboko ingerowały w prawo do poszanowania życia prywatnego i rodzinnego (art. 7 Karty) oraz prawo do ochrony danych osobowych (art. 8 Karty). TSUE wskazał na szereg wymogów, jakie powinny spełniać przepisy przewidujące retencję danych telekomunikacyjnych[21].

W oparciu o przytoczony wyrok TSUE można stwierdzić, że projektowane art. 18a i art. 18b ustawy o świadczeniu usług drogą elektroniczną stanowią ingerencję w prawa przewidziane w art. 7 i art. 8 Karty w związku z art. 52 ust. 1 Karty i art. 16 ust. 1 TfUE. Projektowana regulacja może być uznana za odpowiadającą jej celowi w postaci interesu ogólnego, jakim jest zwalczanie naruszania praw osób trzecich (projekt zapewnia dostępność danych dla dochodzenia praw innych osób) i odpowiednią dla realizacji zakładanego celu. Mimo to proponowaną regulację można uznać za nieproporcjonalną do zamierzonego celu. Obejmuje ona wszystkich usługobiorców korzystających z usług świadczonych drogą elektroniczną, których dane są zatrzymywane, nawet wtedy, gdy nie ma wobec nich podstaw, nawet pośrednich, do wszczęcia postępowania w sprawie naruszenia praw osób trzecich. Proponowana regulacja ma zastosowanie nawet do usługobiorców, co do których brak jest dowodów mogących sugerować, że ich zachowanie może mieć związek, nawet pośredni, z naruszeniem praw osób trzecich. Ponadto projektowana regulacja nie przewiduje wyjątków, a więc stosować się ją będzie także wobec usługobiorców, których komunikacja na gruncie prawa polskiego objęta jest tajemnicą zawodową. Projektowane przepisy nie wymagają związku między danymi, które mają być przechowywane przez usługodawców, a naruszeniem praw osób trzecich[22].

Artykuł 386 ust. 1 Pke określa zakres tajemnicy komunikacji elektronicznej. Punkt pierwszy tego przepisu wskazuje, że tajemnica obejmuje dane dotyczące użytkownika. Projekt przewiduje dodanie przykładowego wyliczenia tych danych (art. 3 pkt. 1 projektu ustawy). Zmiana ta nie jest sprzeczna z art. 5 dyrektywy 2002/58.

Projektowany art. 405a Pke przewiduje, że przedsiębiorca telekomunikacyjny będzie udostępniał na żądanie sądu albo organu administracji publicznej, na podstawie rozporządzenia 2022/2065 dane osobowe użytkownika, o których mowa w art. 386 ust. 1 pkt 1 Pke. Proponowany przepis należy uznać

---

[19] Dz. Urz. UE L 105 z 13.4.2006 r., s. 54.

[20] Wyrok z dnia 8 kwietnia 2014 r. w połączonych sprawach C-293/12 i C 594/12, *Digital Rights Ireland i in.*

[21] Zob. dołączoną do projektu ustawy – Prawo komunikacji elektronicznej opinię ministra właściwego do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej z 15 maja 2024 r. o zgodności z prawem Unii Europejskiej projektu ustawy (druk nr 423).

[22] Por. wyrok TSUE z dnia 8 kwietnia 2014 r. w połączonych sprawach C-293/12 i C 594/12 *Digital Rights Ireland i in.*, pkt. 58 i 59.

za niesprzeczny z art. 10 rozporządzenia 2022/2065 w związku z art. 5 i art. 15 ust. 1 dyrektywy 2002/58.

4. Konkluzje

Poselski projekt ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw jest objęty zakresem prawa Unii Europejskiej.

Projekt w zakresie, w jakim przewiduje dodanie art. 18a i art. 18b w ustawie o świadczeniu usług drogą elektroniczną, może być uznany za niezgodny z art. 7 i art. 8 w związku z art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej oraz art. 16 TfUE.

W pozostałym zakresie projekt nie jest sprzeczny z prawem Unii Europejskiej.

Autor:
Bartosz Pawłowski
ekspert ds. legislacji
w Biurze Ekspertyz
i Oceny Skutków Regulacji

Akceptował:
Wicedyrektor
Biura Ekspertyz
i Oceny Skutków Regulacji
Piotr Chybalski

SEJM RZECZYPOSPOLITEJ POLSKIEJ

BIURO EKSPERTYZ I OCENY SKUTKÓW REGULACJI
KANCELARII SEJMU

Warszawa, 10 września 2024 r.

BEOS-WPEiM-1899/24

Pan
Szymon Hołownia
Marszałek Sejmu
Rzeczypospolitej Polskiej

Opinia w sprawie stwierdzenia, czy poselski projekt ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (przedstawiciel wnioskodawców: poseł Łukasz Osmalak) jest projektem ustawy wykonującej prawo Unii Europejskiej w rozumieniu art. 95a regulaminu Sejmu

Projekt ustawy zmierza do nowelizacji ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego[1] (dalej: Kpc), ustawy z dnia 18 lipca 2022 r. o świadczeniu usług drogą elektroniczną[2] oraz ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej[3] (dalej: Pke).

Projektowane zmiany Kpc obejmują dodanie w części pierwszej w księdze pierwszej nowego działu IX zatytułowanego: Postępowanie w sprawie ochrony dóbr osobistych przeciwko osobom o nieznanej tożsamości. Przepisy te mają regulować zasady składania i rozpatrywania pozwu w sprawach o ochronę dóbr osobistych, jeżeli do ich naruszenia doszło droga elektroniczną, a powód nie zna imienia i nazwiska albo nazwy lub adresu miejsca zamieszkania albo siedziby pozwanego, który naruszył jego dobra osobiste.

Zmiany w ustawie o świadczeniu usług drogą elektroniczną przewidują poszerzenie zakresu danych usługobiorcy oraz zakresu danych charakteryzujących sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną, które usługodawca może przetwarzać. Projekt przewiduje także obciążenie usługodawców dwoma obowiązkami dotyczącymi tych danych: (1) obowiązkiem przechowywania przez okres 6 miesięcy (w przypadku osób dopuszczających się naruszenia dóbr osobistych użytkowników – 12 miesięcy) od dnia wprowadzenia danych do systemu teleinformatycznego, do którego mają dostęp użytkownicy, (2) obowiązkiem udostępniania na każdorazowe wezwanie sądu albo organu administracji publicznej na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku

[1] Dz. U. z 2023 r. poz. 1550, ze zm.
[2] Dz. U. z 2020 r. poz. 344, ze zm.
[3] Dz. U. poz. 1221.

usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)[4] (dalej: rozporządzenie 2022/2065).

Zmiany w Pke przewidują doprecyzowanie zakresu danych dotyczących użytkownika objętych tajemnicą komunikacji elektronicznej. Ponadto projekt przewiduje dodanie nowego art. 405a, zgodnie z którym przedsiębiorca telekomunikacyjny udostępnia na żądanie sądu albo organu administracji publicznej, na podstawie rozporządzenia 2022/2065 dane osobowe użytkownika objęte tajemnicą komunikacji elektronicznej.

Projekt nie zawiera przepisów mających na celu wykonanie prawa Unii Europejskiej.

Poselski projekt ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw **nie jest projektem ustawy wykonującej prawo Unii Europejskiej** w rozumieniu art. 95a regulaminu Sejmu.

Autor:
Bartosz Pawłowski
ekspert ds. legislacji
Biurze Ekspertyz
i Oceny Skutków Regulacji

Akceptował:
Wicedyrektor
Biura Ekspertyz
i Oceny Skutków Regulacji
Piotr Chybalski
Piotr Chybalski

[4] Dz. Urz. UE L 277 z 27.10.2022 r., s. 1, ze zm.

SEJM RZECZYPOSPOLITEJ POLSKIEJ

BIURO EKSPERTYZ I OCENY SKUTKÓW REGULACJI
KANCELARII SEJMU

Warszawa, 18 września 2024 r.

BEOS-WP/WOSR-1900/24

Pan Minister
Dariusz Salamończyk
Zastępca Szefa Kancelarii Sejmu

Ocena skutków regulacji
zawartej w poselskim projekcie ustawy
o zmianie ustawy– Kodeks postępowania cywilnego
oraz niektórych innych ustaw
(przed nadaniem numeru druku)[1]

I. Jaki problem jest rozwiązywany?

1. Projekt ustawy przewiduje nowelizację ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego[2], ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[3] oraz oczekującej na wejście w życie ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej[4].

2. Jak podkreślono w uzasadnieniu projektu, w ostatnich latach doszło do nasilenia się zjawiska naruszania dóbr osobistych w Internecie. Zamieszczane na forach internetowych, czy też w mediach społecznościowych publikacje „naruszają dobra osobiste osób nie tylko w sferze prywatnej, ale także mogą dotykać przedsiębiorców i stanowić zagrożenie dla prowadzonej przez nich działalności gospodarczej". Przy czym, jak zauważają projektodawcy, dokonujący naruszeń „korzystają z anonimowości – jednej z kluczowych cech komunikacji w Internecie", co skutkuje tym, iż „poszkodowani mogą nie mieć możliwości ustalenia tożsamości sprawcy". To zaś „właściwie uniemożliwia im dochodzenie swoich praw na drodze

[1] Projekt ustawy znajduje się w wykazie projektów wniesionych, którym nie został jeszcze nadany numer druku sejmowego. Numer w wykazie: SH-020-207/24. Przedstawiciel wnioskodawcy: pos. Łukasz Osmalak.
[2] Dz. U. z 2023 r. poz. 1550, ze zm.; dalej: kodeks postępowania cywilnego lub k.p.c.
[3] Dz. U. z 2020 r. poz. 344; dalej: ustawa o świadczeniu usług drogą elektroniczną lub u.ś.u.e.
[4] Dz. U. z 2024 r. poz. 1221; dalej: p.k.e.

sądowej i egzekwowanie odpowiedzialności za wyrządzone szkody", gdyż w obowiązującym stanie prawnym warunkiem wniesienia pozwu jest uprzednie ustalenie przez powoda danych osobowych pozwanego. Skutkiem takiego stanu rzeczy jest zaś „praktycznie całkowity brak odpowiedzialności za zniesławiające publikacje, o ile takie publikacje nie nosiły znamion przestępstwa, a tym samym całkowite poczucie bezkarności".

W związku z tym proponuje się wprowadzenie instytucji tzw. ślepego pozwu, która „pozwoli na składanie pozwów bez konieczności wcześniejszego ustalenia tożsamości sprawcy przez osoby poszkodowane oraz zagwarantuje realną pomoc Państwa w identyfikacji sprawcy na potrzeby postępowania cywilnego", co „umożliwi osobom poszkodowanym sięgnięcie do mechanizmów odpowiedzialności cywilnoprawnej w celu zwalczania zniesławiających wpisów w Internecie". Projektodawcy wskazują przy tym, iż „sam fakt istnienia instytucji umożliwiającej zidentyfikowanie osób dokonujących naruszenia dóbr osobistych w Internecie może spowodować też ograniczenie ilości takich zjawisk, pełnić funkcję odstraszającą i prewencyjną".

II. Rekomendowane rozwiązanie (w tym planowane narzędzia interwencji) i oczekiwany efekt

1. Artykuł 1 projektu zakłada nowelizację kodeksu postępowania cywilnego poprzez dodanie w jego części pierwszej, księdze pierwszej, tytule VII, działu IX „Postępowanie w sprawie ochrony dóbr osobistych przeciwko osobom o nieznanej tożsamości" (art. 505^{40}–505^{44}).

Przedłożone rozwiązania normatywne nawiązują do wnoszonych już wcześniej propozycji legislacyjnych[5], dlatego zasadnym jest odwołanie się do zgłaszanych w związku z nimi uwag.

Proponowana nowelizacja kodeksu postępowania cywilnego zakłada wprowadzenie nowego rodzaju postępowania odrębnego w ramach trybu procesowego. Zabieg ten rodzi dwojakiego rodzaju wątpliwości.

[5] Por. np. poselski projekt ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz ustawy – Prawo telekomunikacyjne, druk sejmowy nr 1715/VIII kad. oraz poselski projekt ustawy o zmianie ustaw – Kodeks postępowania cywilnego oraz ustawy – Prawo telekomunikacyjne (projektowi ustawy nie został nadany numer druku sejmowego, znajduje się on w wykazie projektów wniesionych w IX kadencji. Numer w wykazie: EW-020-388/21).

Po pierwsze, pojawia się pytanie o zasadność tworzenia kolejnego rodzaju postępowania odrębnego[6]. Jak zauważa się w doktrynie postępowania cywilnego, w obecnym stanie prawnym postępowania odrębne nie funkcjonują już na zasadzie wyjątku od zwykłego postępowania procesowego, „lecz stały się równoległym a czasem nawet konkurującym z nim, rodzajem postępowania procesowego"[7]. Wiąże się to z tendencją do fragmentarycznego reformowania procedury cywilnej, która budzi zastrzeżenia nauki prawa. Wskazuje się mianowicie, iż kolejne postępowania odrębne wprowadzane są jako wybiórcza reakcja ustawodawcy na roszczenia, które zyskują w danym czasie na znaczeniu społecznym, gospodarczym lub politycznym. Przy czym, dla zapewnienia owym roszczeniom – a także innym, nieznajdującym się w danym momencie w centrum uwagi prawodawcy – odpowiedniej ochrony należałoby przede wszystkim zadbać o sprawność postępowania procesowego prowadzonego na zasadach ogólnych[8]. Dodatkowo, zauważyć trzeba, iż wprowadzenie postępowania odrębnego umożliwiać ma rozpatrywanie spraw odznaczających się szczególnymi cechami (specyfiką, swoistością), które powodują, że rozpoznanie sprawy w postępowaniu zwykłym byłoby nieefektywne[9]. Proponowane postępowanie w sprawie ochrony dóbr osobistych przeciwko osobom o nieznanej tożsamości ma zaś być prowadzone na zasadach ogólnych (zob. projektowany art. 505^{43} k.p.c.), a jego odrębność sprowadza się do obowiązku ustalenia przez sąd tożsamości osoby mającej być pozwanym w procesie. Nie wydaje się zatem, by można było mówić o dostatecznej swoistości rozpatrywanych spraw uzasadniającej wprowadzenie kolejnego postępowania odrębnego. Przepisy dotyczące ustalania tożsamości pozwanego *in spe*, jak zauważono w dyskusjach nad analizowaną instytucją, mogłyby zostać umiejscowione wśród regulacji dotyczących wymogów formalnych pozwu[10].

Po drugie, przy pominięciu wyrażonych powyżej wątpliwości, zastrzeżenia budzi umiejscowienie projektowanego postępowania odrębnego w ramach struktury procesu cywilnego[11]. Wskazuje się w tym kontekście, iż fakt naruszenia dóbr

---

[6] Por. D. Wybrańczyk, *Ocena skutków prawych regulacji poselskiego projektu ustawy o zmianie ustaw – Kodeks postępowania cywilnego oraz ustawy – Prawo telekomunikacyjne*, BAS-WAP-160/21, s. 7–8.

[7] A. Machnikowska [w:] *System Postępowania Cywilnego*, t. 6, *Postępowania odrębne*, red. A. Machnikowska, Warszawa 2022, s. 27 (nb 55).

[8] Tamże, s. 11 (nb 15).

[9] Por. np. tamże, s. 16 (nb 30).

[10] Por. P. Szymaniak, *Koniec bezkarnego hejtu w sieci? Jest projekt o "ślepych" pozwach.*, https://www.rp.pl/dobra-osobiste/art41061011-koniec-bezkarnego-hejtu-w-sieci-jest-projekt-o-slepych-pozwach.

[11] Na temat znaczenia tego zagadnienia oraz powiązaniach pomiędzy rodzajami postępowań w procesie cywilnym patrz np. S. Cieślak, *Powiązania wewnątrzsystemowe w postępowaniu cywilnym*, Warszawa 2013.

osobistych drogą elektroniczną nie wydaje się wystarczający do tego, by uznać proponowane postępowanie za elektroniczne – w takim znaczeniu, w jakim odnosi się to do elektronicznego postępowania upominawczego – co uzasadniałoby umieszczenie projektowanego działu po dziale dotyczącym postępowania elektronicznego[12].

Zgodnie z projektowanym art. 505^{40} § 1 k.p.c. przepisy wprowadzanego działu IX znajdą zastosowanie w przypadku gdy do naruszenia dóbr osobistych doszło drogą elektroniczną, a powód nie zna imienia i nazwiska albo nazwy lub adresu miejsca zamieszkania albo siedziby pozwanego, który naruszył jego dobra osobiste. W tym kontekście aktualność zachowuje wątpliwość co do zasadności określania jako „pozwanego" podmiotu identyfikowanego na tym etapie, co najwyżej, poprzez nazwę, jakiej używa w Internecie (zob. projektowany art. 505^{41} § 1 pkt 4 k.p.c.), którego tożsamość ma dopiero zostać ustalona, dzięki czemu możliwe będzie doręczenie mu pozwu[13].

Wspomnianego ustalenia, zgodnie z założeniami projektu, miałby dokonywać, właściwy ze względu na miejsce zamieszkania albo siedziby powoda, sąd okręgowy, do którego wniesiono pozew (zob. projektowany art. 505^{40} § 2 k.p.c.). W kontekście rozwiązań obligujących sąd do ustalenia tożsamości osoby, która stać się ma stroną pozwaną, podnosi się, iż godzą one w regułę konstrukcyjną postępowania cywilnego wymagającą dla skuteczności wniesienia pozwu oznaczenia przez powoda stron postępowania[14]. Dodatkowo zauważa się, że reguła ta powiązana jest z zasadą dyspozycyjności zakładającą swobodę stron w korzystaniu z przysługujących im uprawnień oraz środków ochrony prawnej, co jak się podkreśla, wyłącza dopuszczalność nałożenia na sąd obowiązku wskazywania stron postępowania[15]. Obowiązek ustalenia przez sąd danych osoby, przeciwko której skierowany ma zostać pozew, jak się także podnosi, budzi wątpliwości również w kontekście przyjętej w procedurze cywilnej zasady kontradyktoryjności[16], zgodnie z którą „przygotowanie, gromadzenie i dostarczenie materiału procesowego należy do stron procesowych,

---

[12] Por. D. Wybrańczyk, *Ocena skutków prawych…*, s. 8.
[13] Por. *Opinia Prokuratorii Generalnej Rzeczypospolitej Polskiej do poselskiego projektu ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz ustawy – Prawo telekomunikacyjne (druk nr 1715)* z 28 lipca 2017 r., znak: KR-51-597/17/MSĘ, s. 9–10. https://orka.sejm.gov.pl/Druki8ka.nsf/0/DDA724FDC4D2EB1FC125817100394523/%24File/1715-003.pdf.
[14] Por. tamże, s. 5.
[15] Por. tamże oraz wskazane tam orzecznictwo.
[16] Por. D. Wybrańczyk, *Ocena skutków prawych…*, s. 11–12.

a do sądu należy jedynie ocena tego materiału i wydanie na jego podstawie rozstrzygnięcia"[17].

Zauważa się także, iż nałożenie na sąd obowiązku ustalenia strony pozwanej w połączeniu z przyjętym w kodeksie cywilnym [18] domniemaniem bezprawności naruszenia dobra osobistego [19], skutkującym koniecznością wykazania przez pozwanego, że jego zachowanie nie było bezprawne, prowadzi do sytuacji, w której powód może ograniczyć się jedynie do wniesienia pozwu[20].

W kontekście „ślepego pozwu" sygnalizowano już także problem potencjalnego wykorzystania tej instytucji jako formy szykany wobec osoby, której zachowanie w istocie nie naruszyło dóbr osobistych powoda, czy też formułowania żądania celem obejścia przepisów o ochronie danych osobowych[21]. W takim bowiem przypadkach mogłoby dojść do ujawnienia danych osobowych „bezpodstawnie i niepotrzebnie"[22]. Problem takiego „bezpodstawnego i niepotrzebnego" ujawnienia danych osobowych nabiera dodatkowego znaczenia z uwagi na to, iż w świetle proponowanych regulacji wskazany ma zostać podmiot korzystający z publicznie dostępnej usługi telekomunikacyjnej lub żądający świadczenia takiej usługi – (zob. projektowany art. 505^{42} § 4 k.p.c. w zw. z art. 386 ust. 1 pkt. 1 p.k.e. w brzmieniu proponowanym w art. 3 pkt 1 omawianego projektu), któremu dostarczony zostanie pozew. Nie musi być on jednak osobą, która zachowała się w sposób potencjalnie naruszający dobra osobiste powoda. Przykładowo, wpis, który powód uznał za naruszający jego dobre imię, mógł zostać zamieszczony przez pracownika osoby będącej „użytkownikiem" w powyższym rozumieniu, czy też jego domownika, gościa albo osobę mu nieznaną w przypadku braku zabezpieczenia sieci [23]. W tym kontekście zwraca się uwagę, iż błędne określenie tożsamości pozwanego przez sąd stanowić może podstawę do formułowania roszczeń odszkodowawczych względem Skarbu Państwa[24]. Powstaje także pytanie o konsekwencje wykazania przez osobę określoną jako pozwany, że to nie ona dopuściła się zachowania mającego naruszać dobra osobiste powoda[25].

---

[17] Tak W. Siedlecki [w:] *Postępowanie cywilne. Zarys wykładu*, W. Siedlecki, Z. Świeboda, Warszawa 2004, s. 56.
[18] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny, t.j. Dz. U. z 2024 r. poz. 1061, ze zm.
[19] Por. np. J. Panowicz-Lipska [w:] *Kodeks cywilny. Komentarz*, t. 1, *Art. 1–352*, red. M. Gutowski, Warszawa 2021, komentarz do art. 24, nb 7 oraz wskazaną tam literaturę i orzecznictwo, Legalis.
[20] Por. D. Wybrańczyk, *Ocena skutków prawych…*, s. 12.
[21] Por. tamże, s. 10, 14.
[22] Tamże, s. 10.
[23] Por. np. tamże, s. 11; *Opinia Prokuratorii Generalnej…*, s. 8–9; O. Rudak, *„Ślepy pozew" jako ochrona przed anonimowym hejtem* – https://czasopismo.legeartis.org/2017/06/slepy-pozew-ochrona-przed-anonimowym-hejtem/ (dostęp: 09.09.2024 r.).
[24] *Opinia Prokuratorii Generalnej…*, s. 9.
[25] Por. tamże.

Jako problematyczne określa się także posłużenie się zwrotem „adres URL" (zob. projektowany art. 505^{41} § 2 k.p.c.) z uwagi na brak zdefiniowania go w kodeksie postępowania cywilnego, co potencjalnie może utrudniać stosowanie proponowanych regulacji [26]. Dodatkowo podnosi się, iż odwołanie się do adresu URL, charakterystycznego dla sieci Internet, nie jest uzasadnione w sytuacji, gdy intencją projektodawcy jest objęcie proponowanymi regulacjami spraw wynikłych w związku z wykorzystaniem także innych systemów łączności komputerowej[27]. Zgodnie zaś z projektowanym art. 505^{40} § 1 k.p.c., proponowane regulacje mają znaleźć zastosowanie w przypadku naruszenia dóbr osobistych drogą elektroniczną, co sugeruje objęcie nimi także sytuacji, gdy do zarzucanego naruszenia doszło nie tylko poprzez zamieszczenie danych treści na posiadającej adres URL stronie internetowej, ale także np. w drodze korespondencji elektronicznej.

Podnoszona jest także wątpliwość co do obowiązku wskazania daty i godziny zamieszczenia treści, która, w ocenie powoda, narusza jego dobra osobiste (zob. projektowany art. 505^{41} § 1 pkt 3 oraz § 2 *in fine*) z uwagi na fakt, iż dane te nie muszą być uwidocznione[28].

Zauważa się również, że potencjalne naruszenie dóbr osobistych drogą elektroniczną zaistnieć może w związku z działalnością prasy. Pojawia się zatem kwestia relacji proponowanych rozwiązań normatywnych do regulacji ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe[29]. Ustawa ta statuuje m.in. prawo autora materiału prasowego do zachowania anonimowości oraz zakaz ujawniania przez dziennikarzy oraz pozostałych pracowników redakcji, wydawnictwa, czy też innej prasowej jednostki organizacyjnej: a) danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze oraz danych innych osób udzielających informacji opublikowanych albo przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych; b) wszelkich informacji, których ujawnienie mogłoby naruszać chronione prawem interesy osób trzecich (zob. art. 15 pr. pras.). Projektowane przepisy nie odnoszą się do tego zagadnienia[30].

---

[26] Por. D. Wybrańczyk, *Ocena skutków prawych…*, s. 7; *Opinia Krajowej Rady Sądownictwa z dnia 27 lipca 2017 r. w przedmiocie projektu ustawy o zmianie ustawy - Kodeks postępowania cywilnego oraz ustawy – Prawo telekomunikacyjne*, znak: WO-020-71/17, s. 2. https://orka.sejm.gov.pl/Druki8ka.nsf/0/50565BBD49140525C125817100403A8F/%24File/1715-004.pdf.

[27] Por. *Opinia Krajowej Rady Sądownictwa…*, s. 2.

[28] Por. tamże.

[29] Dz. U. z 2018 r. poz.1914; dalej: pr. pras.

[30] Por. D. Wybrańczyk, *Ocena skutków prawych…*, s. 10.

Wątpliwości wzbudza również zakreślenie siedmiodniowego terminu na wystąpienie przez sąd o potrzebne dane oraz przekazanie tychże danych przez właściwe podmioty. Termin ten, jak się podkreśla, jest w zasadzie niemożliwy do dotrzymania przez sądy z uwagi na obciążenie rozpatrywanymi sprawami oraz problematyczny z punktu widzenia dostawcy usług elektronicznych, zwłaszcza gdy nie jest to duży podmiot gospodarczy[31].

2. Artykuł 2 projektu zakłada nowelizację ustawy o świadczeniu usług drogą elektroniczną poprzez zmianę treści art. 18 ust 1 i 5 oraz dodanie art. 18a i art. 18b.

W świetle projektowanej zmiany art. 18 ust. 1 modyfikacji ulegnie wprowadzenie do zawartego w tym przepisie wyliczenia, dodany ma także zostać punkt siódmy wskazujący jako daną osobową, która podlega przetwarzaniu numer telefonu podany przez usługobiorcę. We wprowadzeniu do wyliczenia zawarta jest definicja usługodawcy ujęta inaczej niż definicja wprowadzona w słowniczku ustawowym (art. 2 pkt 6 u.ś.u.e.). Nowelizacja art. 18 ust. 5 u.ś.u.e. zakłada poszerzenie katalogu danych charakteryzujących sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną, które usługodawca może przetwarzać, a niejako w konsekwencji zobowiązany jest przechowywać oraz udostępniać na żądanie organów państwa (o czym niżej).

Projektowany art. 18a u.ś.u.e. zobowiązuje usługodawcę do przechowywania, na własny koszt, danych wskazanych w art. 18 ust. 1 i 5 u.ś.u.e. generowanych lub przetwarzanych w trakcie prowadzonej przez niego działalności na terytorium Rzeczypospolitej Polskiej, przez okres 6 miesięcy, licząc od dnia wprowadzenia ich do systemu teleinformatycznego, do którego mają dostęp użytkownicy (art. 18a ust. 1 u.ś.u.e.). Przy czym, w odniesieniu do osób dopuszczających się naruszenia dóbr osobistych użytkowników, usługodawca przechowuje i zabezpiecza dane, o których mowa w art. 18 ust. 1 i 5 u.ś.u.e., oraz dane, o których mowa w art. 386 ust. 1 pkt 1 p.k.e. (w brzmieniu nadanym w omawianym projekcie), przez okres nie krótszy niż 12 miesięcy od dnia ich wprowadzenia do systemu teleinformatycznego, do którego mają dostęp użytkownicy (art. 18a ust. 2 u.ś.u.e.). W związku z zaproponowanym kształtem art. 18 ust. 2 u.ś.u.e. powstaje pytanie, od kogo i w jakim trybie usługodawca miałby powziąć informację, że dany użytkownik dopuszcza się naruszenia dóbr osobistych. Zagadnienie to wymaga odnotowania zwłaszcza ze względu na fakt, iż analizowany przepis powiązany jest z regulacjami wprowadzającymi „ślepe pozwy". W założeniu

[31] Por. P. Szymaniak, *Koniec bezkarnego hejtu…*

więc dotyczy sytuacji sprzed wszczęcia postępowania cywilnego, w toku którego sąd ustala, czy w danym przypadku doszło do naruszenia dobra osobistego powoda. Poza tym w świetle art. 15 u.ś.u.e., jak podkreśla się w doktrynie, wyłączona jest możliwość nałożenia generalnego obowiązku monitorowania danych na podmioty świadczące usługi tzw *mere conduit*, *cachingu* oraz *hostingu*[32]. Problematycznym jest także wskazanie jedynie minimalnego okresu, przez jaki usługodawca ma przechowywać dane „osób dopuszczających się naruszeń dóbr osobistych". Rozwiązanie to umożliwia bowiem retencję podlegających ochronie konstytucyjnej danych[33] przez potencjalnie nieograniczony czas, co budzi wątpliwości w zakresie proporcjonalności ingerencji w prawa jednostki gwarantowane przez ustawę zasadniczą. Wskazać także należy, iż zgodnie z art. 5 ust. 1 lit. e) zdanie 1 RODO[34] dane w formie umożliwiającej identyfikację osoby mogą być, co do zasady, przechowywane przez okres nie dłuższy, niż jest to niezbędne dla osiągniecia celu, w którym dane te są przetwarzane. Regulacja ta, jak wskazuje się w piśmiennictwie, ma zapobiegać właśnie przetwarzaniu danych osobowych „w nieskończoność"[35].

Zgodnie z projektowanym art. 18b u.ś.u.e. usługodawca jest obowiązany udostępnić dane, o których mowa w art. 18 ust. 1 i 5 u.ś.u.e., oraz dane, o których mowa w art. 386 ust. 1 pkt 1 p.k.e. (w projektowanym brzmieniu) na każdorazowe wezwanie sądu albo organu administracji publicznej na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)[36]. W tym kontekście należy zwrócić uwagę na kontrowersje co do statusu art. 18 ust. 1 u.ś.u.e. W piśmiennictwie wskazuje się, że w związku z wejściem w życie ogólnego rozporządzenia o ochronie danych oraz brakiem, pierwotnie zakładanego, uchylenia art. 18 ust. 1-4 u.ś.u.e. powstają „poważne

---

[32] Por. np. W. Chomiczewski [w:] *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, red. D. Lubasz, M. Namysłowska, Warszawa 2011, komentarz do art. 15 ustawy o świadczeniu usług drogą elektroniczną, teza 1, LEX.

[33] Por. wyrok TK z 30 lipca 2014 r., sygn. akt K 23/11.

[34] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, s. 1.); dalej także: ogólne rozporządzenie o ochronie danych.

[35] Por. np. P. Barta, M. Kawecki, P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021, komentarz do art. 5 ogólnego rozporządzenia o ochronie danych osobowych, nb 20, Legalis; A. Nerka [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, komentarz do art. 5, nb 8, Legalis.

[36] Dz. Urz. UE L 277 z 27.10.2022, str. 1, ze zm., ELI: http://data.europa.eu/eli/reg/2022/2065/oj; dalej: akt o usługach cyfrowych.

wątpliwości interpretacyjne w zakresie możliwości wskazywania adekwatnych podstaw prawnych przetwarzania danych usługobiorcy"[37]. Formułowana jest także dalej idąca teza o derogacji art. 18 ust. 1–4 u.ś.u.e. w miejsce których winien być stosowany art. 6 ust. 1 RODO[38]. Niejasnym jest także sformułowanie mówiące o wystosowanym przez sąd lub organ administracji publicznej wezwaniu do udostępnienia danych na podstawie aktu o usługach cyfrowych. Artykuł 10 aktu o usługach cyfrowych odnosi się do nakazu udzielenia informacji na temat indywidualnego odbiorcy usługi, który jednak wydany ma zostać w oparciu o mające zastosowanie prawo Unii Europejskiej lub mające zastosowanie prawo krajowe zgodne z prawem Unii. Regulacja ta, jak wskazuje się w doktrynie, nie statuuje „nowego typu nakazu, lecz harmonizuje elementy, jakie nakazy powinny posiadać, oraz nakłada związane z tym obowiązki informacyjne na usługodawców, organy wydające nakaz oraz koordynatorów ds. usług cyfrowych"[39].

3. Artykuł 3 projektu zakłada nowelizację prawa komunikacji elektronicznej poprzez zmianę treści art. 386 ust. 1 pkt 1 oraz dodanie art. 405a.

Planowana nowelizacja dotyczy ustawy, która nie weszła jeszcze w życie. Wspomnieć w związku z tym należy, iż zmiana przepisów w okresie *vacatio legis* nie jest uznawana za „właściwą praktykę ustawodawczą", jako że okres spoczywania ustawy służy przede wszystkim adresatom danych norm prawnych dając im czas na zapoznanie się z tymi normami i dostosowanie swoich zachowań do nowej regulacji[40]. Niemniej jednak praktyka ta nie jest bezwzględnie wykluczona, gdyż *vacatio legis* „to również okres, w którym prawodawca ma sposobność korygowania dostrzeżonych już po uchwaleniu aktu normatywnego błędów, sprzeczności wewnętrznych, czy też rozwiązań prowadzących do powstania sprzeczności w systemie prawa, bądź zapobieżenia negatywnym skutkom wejścia w życie uchwalonych, a jeszcze nie obowiązujących regulacji" [41]. Za okoliczność uzasadniającą nowelizację przepisów, które nie weszły jeszcze w życie, można uznać włączenie ich w ramy szerszego rozwiązania normatywnego, co wymaga zapewnienia spójności wszystkich relewantnych uregulowań.

---

[37] A. Krzyżak [w:] *Ogólne rozporządzenie...*, red. P. Litwiński, komentarz do art. 18 ustawy o świadczeniu usług drogą elektroniczną, nb 1.
[38] Por. K. Chałubińska-Jentkiewicz, J. Taczkowska-Olszewska, *Świadczenie usług drogą elektroniczną. Komentarz*, Warszawa 2019, komentarz do art. 18, nb 1, Legalis.
[39] K. Garstka [w:] *Akt o usługach cyfrowych. Komentarz*, red. J. Gołaczyński, R. Skibicki, Warszawa 2024, komentarz do art. 10, teza 1, LEX.
[40] Por. np. wyrok TK z 18 lutego 2004 r., sygn. akt K 12/03.
[41] Tamże. Por. także M. Zubik, *Prawo konstytucyjne współczesnej Polski*, Warszawa 2020, s. 61 (nb 70).

Zgodnie z projektowanym art. 386 ust. 1 pkt 1 p.k.e. tajemnica komunikowania się w sieciach telekomunikacyjnych ma obejmować dane dotyczące podmiotu korzystającego z publicznie dostępnej usługi telekomunikacyjnej lub żądającego świadczenia takiej usługi (użytkownika), w szczególności jego: nazwisko i imiona, numer PESEL lub numer paszportu – w przypadku braku nadania numeru PESEL, numer dowodu osobistego lub innego dokumentu potwierdzającego tożsamość, adres zameldowania na pobyt stały, adres do korespondencji – jeżeli jest inny niż adres zameldowania na pobyt stały, dane służące do weryfikacji podpisu elektronicznego, adresy elektroniczne oraz numer telefonu.

Proponowana zmiana normatywna polega na wskazaniu przykładowego katalogu danych[42] objętych tajemnicą komunikacji elektronicznej, które mogą być przetwarzane jedynie w przypadkach wskazanych w ustawie (zob. art. 386 ust. 3 p.k.e.). Wprowadza ona także do art. 386 ust. 1 pkt 1 p.k.e. definicję użytkownika ujętą inaczej niż ta zawarta w art. 2 pkt 85 p.k.e.

W świetle projektowanego art. 405a p.k.e. przedsiębiorca telekomunikacyjny zobowiązany jest do udostępnienia danych osobowych użytkownika wskazanych w art. 386 ust. 1 pkt 1 p.k.e, na wydane na podstawie aktu o usługach cyfrowych żądanie sądu lub organu administracji publicznej. Skutkuje to powstaniem problemu analogicznego do tego wskazanego powyżej przy analizie projektowanego art. 18b u.ś.u.e.

4. Projekt ustawy był przedmiotem analiz Biura Ekspertyz i Oceny Skutków Regulacji Kancelarii Sejmu dotyczących zgodności z prawem Unii Europejskiej[43]. Omawiany projekt był także przedmiotem analizy BEOS w trybie art. 95a ust. 3 regulaminu Sejmu[44].

---

[42] Wskazuje na to użycie zwrotu „w szczególności', który zgodnie z § 153 ust. 3 załącznika do rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie Zasad techniki prawodawczej (Dz. U. z 2016 r. poz. 283), stosowany jest dla wyraźnego zaznaczenia przykładowego charakteru wyliczenia objaśniającego znaczenie danego określenia w sytuacji gdy niemożliwe jest sformułowanie definicji zakresowej – szerzej patrz np. M. Zieliński [w:] *Komentarz do Zasad techniki prawodawczej z dnia 20 czerwca 2002 r.*, S. Wronkowska, M. Zieliński, Warszawa 2021, komentarz do § 153, s. 253–254.

[43] *Opinia w sprawie zgodności z prawem Unii Europejskiej poselskiego projektu ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (przedstawiciel wnioskodawców: poseł Łukasz Osmalak)*, opinia z 10 września 2024 r., BEOS-WPEiM-1898/24.

[44] *Opinia w sprawie stwierdzenia, czy poselski projekt ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (przedstawiciel wnioskodawców: poseł Łukasz Osmalak) jest projektem ustawy wykonującej prawo Unii Europejskiej w rozumieniu art. 95a regulaminu Sejmu*, opinia z 10 września 2024 r., BEOS-WPEiM-1899/24.

III. Jak problem został rozwiązany w innych państwach, w szczególności państwach członkowskich OECD/UE?

Rozwiązanie przewidujące możliwość wniesienia do sądu cywilnego pozwu bez określania podmiotu pozwanego zidentyfikowano w prawie procesowym Stanów Zjednoczonych [45]. Konstrukcja *John Doe lawsuit* umożliwia wniesienie pozwu przeciwko osobie początkowo nieznanej co do tożsamości, której dane identyfikujące – już po wniesieniu pozwu – zostają ustalone przez powoda przy pomocy sądu[46]. Możliwość wniesienia *John Doe lawsuit* jest potwierdzona orzeczeniami precedensowymi, które w amerykańskim systemie prawnym mają charakter źródła prawa powszechnie obowiązującego[47]. Samo wniesienie pozwu nie jest jeszcze wystarczające. Powód musi od razu wskazać działania, które zamierza podjąć, aby ustalić tożsamość pozwanego (funkcją *John Doe lawsuit* nie jest bowiem umożliwienie prowadzenia i zakończenia procesu bez działania pozwanego, ale jedynie umożliwienie jego wszczęcia celem ustalenia tożsamości adresata żądania i dalszego jego prowadzenia już z zachowaniem ogólnej regulacji)[48]. W precedensowej sprawie *Dendrite International, Inc. v. Doe, No. 3* (2001) Wyższy Sąd New Jersey sformułował następujące zasady dopuszczalności ujawnienia tożsamości autora wypowiedzi dokonanej w przestrzeni internetowej: 1) powód powinien wykazać, że podjął próbę powiadomienia anonimowego autora wypowiedzi o ewentualnym procesie oraz zapewnił mu możliwość udzielenia odpowiedzi; próba ta może polegać na zawiadomieniu zamieszczonym na stronie internetowej, na której umieszczona była wypowiedź anonimowego autora; 2) powód musi dokładnie przytoczyć wypowiedzi, których dotyczy zarzut procesowy; 3) roszczenie powoda jest na tyle umotywowane, że jest w stanie „przetrwać" próbę obalenia go przez pozwanego już na wstępnym etapie sprawy; powód zobowiązany jest przedstawić dowody na poparcie każdego elementu roszczenia[49]. Wykluczony jest automatyzm w korzystaniu z tego narzędzia prawnego – nawet spełnienie przez powoda wszystkich powyższych wymogów nie

---

[45] Wystąpienie Rzecznika Praw Obywatelskich do Ministra Sprawiedliwości ws. zwalczania mowy nienawiści w internecie, 17.05.2016, s. 3; https://bip.brpo.gov.pl/sites/default/files/Wystapienie%20do%20Ministra%20Sprawiedliwosci%20ws%20zwalczania%20mowy%20nienawisci%20w%20internecie%2017.05.2016.pdf.

[46] Winczura M.: *Anonimowość pozwanego – aktualnie dostępne środki prawne oraz postulat wprowadzenia ślepego pozwu do Kodeksu postępowania cywilnego*, rozprawa doktorska M. Winczura, 9.04.2024, s. 259, https://uwedupl.bip.gov.pl/doktoraty-udostepnione-na-stronie-bip-zgodnie-z-art-188-ust-1-i-2-ustawy-z-dnia-3-lipca-2018-r-prawo-o-szkolnictwie-wyzszym/mateusz-winczura.html.

[47] Ibidem, s. 225.

[48] Ibidem, s. 234.

[49] Wystąpienie Rzecznika Praw Obywatelskich..., s. 6.

obliguje sądu do ujawnienia tożsamości anonimowego autora wypowiedzi: sąd waży interes powoda w ujawnieniu tożsamości pozwanego i interes pozwanego w zachowaniu anonimowości, w ramach korzystania z wolności (także anonimowej) wypowiedzi.

IV. Podmioty, na które oddziałuje projekt

Proponowane rozwiązanie potencjalnie będzie oddziaływało na podmioty uczestniczące w utrzymywaniu i korzystaniu z przestrzeni cyfrowej, prowadzące działalność telekomunikacyjną, usługową oraz korzystające z e-usług w przypadku, gdy do tej przestrzeni zostaną wprowadzone informacje uznawane za naruszające dobra osobiste. Będą to:

- podmioty korzystające z usług w przestrzeni cyfrowej będące nadawcami oraz odbiorcami informacji. Dane wynikające z corocznych badań GUS pozwalają zobrazować skalę i dynamikę wzrostu liczby nadawców i odbiorców informacji w sieciowym środowisku informacyjnym, które sukcesywnie staje się podstawowym środowiskiem komunikacyjnym. Według najnowszych dostępnych danych, w 2023 r., w Polsce co najmniej raz w tygodniu korzystało z internetu 85,3% osób w wieku 16–74 lata. Odsetek osób, które łączyły się z internetem codziennie lub prawie codziennie wyniósł 92,0%, korzystanie z komunikatorów zadeklarowało 64,5%, a z serwisów społecznościowych 62,3%[50].
- usługodawcy usług w przestrzeni cyfrowej – osoby fizyczne, osoby prawne albo jednostki organizacyjne nieposiadające osobowości prawnej, które prowadzą (również ubocznie) działalność zarobkową, zawodową lub pożytku publicznego, świadczące usługi drogą elektroniczną, w tym również oferujące usługi pośrednictwa internetowego (tj. portale internetowe, aplikacje mobilne, wyszukiwarki internetowe albo inne usługi online, które umożliwiają sprzedawanie bądź promowanie produktów lub usług)[51]. W Polsce taką

[50] GUS *Społeczeństwo informacyjne w Polsce w 2023 r.*, Warszawa–Szczecin, 2023, s. 119, 124 https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/1/17/1/spoleczenstwo_informacyjne_w_polsce_w_2023.pdf.

[51] Przykładami są: Facebook, LinkedIn, Instagram, eBay, Allegro, Ceneo, Booking, Google Play, Apple App Store, wyszukiwarki internetowe i płatne reklamy (Google Ads).

działalność, sklasyfikowaną w sekcji J, w dziale 63 Polskiej Klasyfikacji Działalności[52], prowadzi około 22 tysiące podmiotów[53].

- przedsiębiorców telekomunikacyjnych – liczba operatorów sieci i dostawców usług telekomunikacyjnych w Polsce wynosi 3672[54]. Usługę stacjonarnego dostępu do internetu świadczy ponad 2200 przedsiębiorców (dla 9,5 mln klientów, co stanowi 65,5% gospodarstw domowych), usługę dostępu mobilnego ponad 100 przedsiębiorców (dla 8,9 mln klientów). Z usług wiązanych korzysta 14,2 mln użytkowników[55]. Należy zauważyć, że działalność niegospodarczą z zakresu telekomunikacji prowadzą również jednostki samorządu terytorialnego (w szczególności polegającą na dostarczaniu sieci telekomunikacyjnej i świadczeniu usług telekomunikacyjnych z wykorzystaniem własnej sieci i infrastruktury)[56] – i one również powinny być objęte obowiązkiem udzielania informacji. Do rejestru prowadzonego przez Prezesa UKE wpisanych jest 575 takich jednostek[57].
- sądy okręgowe w liczbie 47 – przez przekazanie do ich właściwości spraw o ochronę dóbr osobistych (w przypadkach gdy do naruszenia doszło drogą elektroniczną, a powód nie zna danych identyfikujących pozwanego) i nałożenie obowiązków organizacyjno-procesowych związanych z pozyskiwaniem informacji od usługodawców i przedsiębiorców telekomunikacyjnych na potrzeby toczącego się postępowania.

V. Informacje o zakresie, czasie trwania i wynikach konsultacji

Projekt ustawy nie zawiera informacji na temat poddania go konsultacjom społecznym.

---

[52] Rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD) (Dz.U. z 2007,nr 251, poz.1885 ze zm.).
[53] GUS, Miesięczna informacja o podmiotach gospodarki narodowej w rejestrze REGON, sierpień 2024, https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5504/4/88/1/tablice_internet_sierpien_2024.xls.
[54] https://bip.uke.gov.pl/rpt/, stan na dzień 30 sierpnia 2024 r.
[55] UKE *Raport o stanie rynku telekomunikacyjnego w 2023 roku,* Warszawa 2024 r., s. 5–6 i 8, 11, 26– 28 stan na dzień 31 grudnia 2023 r. https://www.uke.gov.pl/download/gfx/uke/pl/defaultaktualnosci/36/545/9/uke_raport_tele_2023_net_small_3.pdf.
[56] Art. 3 ust. 1 i art. 5 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz.U. z 2024, poz. 604 ze zm.).
[57] Zob. https://bip.uke.gov.pl/rjst, stan na dzień 30 sierpnia 2024 r.

Zgodnie z informacjami z Systemu Informacyjnego Sejmu, w dniu 4 września 2024 r. Marszałek Sejmu skierował projekt do konsultacji (SN, KRS, NRA, KRRP, PG, PGRP, KIG, RDS, RMiŚP, UODO i KRBR).

VI. Wpływ na sektor finansów publicznych

Według projektowanych przepisów w przypadku niewywiązania się przez usługodawców i przedsiębiorców z obowiązku udzielania informacji kary grzywny mogą wynosić od 100 tysięcy zł do miliona zł. Tym samym rozwiązania potencjalnie mogą zwiększyć dochody budżetu państwa klasyfikowane w paragrafach 0570 i 0580 „wpływy z tytułu grzywien, mandatów i innych kar pieniężnych"[58] w części 15 Sądy powszechne.

Proponowane przepisy zwiększą obciążenie organizacyjno-proceduralne sądów w skali, której nie da się wyprzedzająco oszacować. Obciążenie będzie polegać na przygotowaniu i obsłudze korespondencji prowadzonej z usługodawcami i przedsiębiorcami telekomunikacyjnymi w celu pozyskania danych pozwalających ustalić dane pozwanego. Dostępne dane pozwalają jedynie w sposób ilustracyjny zobrazować liczbę przypadków, w których osoby poszkodowane na podstawie obecnie obowiązujących przepisów decydują się na uruchomienie postępowania przed sądem. Postępowania cywilne w sprawie ochrony dóbr osobistych – bez wyszczególnienia, o jakie dobro i w jaki sposób zagrożone chodzi – są corocznie sprawozdawane, jednakże nie ma dostępnych danych zbiorczych[59]. Przejrzenie kilkunastu sprawozdań za 2023 r. losowo wybranych sądów rejonowych (na sumaryczną liczbę wszystkich 319) prowadzi do wniosku, że coroczna liczba takich postępowań może wynosić od 0 do 10 w mniejszych ośrodkach miejskich, około 20-30 w większych ośrodkach, a w dużych około 50-70.

VII. Wpływ na konkurencyjność gospodarki i przedsiębiorczość oraz na rodzinę, obywateli i gospodarstwa domowe

Projekt ustawy ze względu na swój charakter nie będzie miał wpływu na konkurencyjność gospodarki i przedsiębiorczość, ponieważ nie określa zasad podejmowania, wykonywania lub zakończenia działalności gospodarczej.

---

[58] Rozporządzenie Ministra Finansów z dnia 2 marca 2010 r. w sprawie szczegółowej klasyfikacji dochodów, wydatków, przychodów i rozchodów oraz środków pochodzących ze źródeł zagranicznych (Dz. U. z 2022 r. poz. 513, ze zm.).

[59] Coroczne sprawozdania statystyczne dotyczące działalności sądu sporządzane w ramach programu badań statystycznych MS-S1r dla Ministerstwa Sprawiedliwości umieszczane są w Biuletynach Informacji Publicznej poszczególnych sądów.

Proponowana regulacja będzie jednak mieć wpływ na funkcjonowanie podmiotów prowadzących działalność usługową w przestrzeni cyfrowej przez wprowadzenie obowiązku przechowywania na własny koszt danych ułatwiających zidentyfikowanie osób korzystających z usług w powiązaniu z ich aktywnością przez okres 6 miesięcy, a w przypadku osób dopuszczających się naruszenia dóbr osobistych – przez okres 12 miesięcy. Koszt archiwizacji zależny będzie od skali działania, wykorzystywanych nośników pamięci oraz kosztów aplikacji obsługujących wykonanie obowiązku przechowywania danych. Wydaje się, że długi okres *vacatio legis* – 12 miesięcy – pozwoli na przygotowanie adekwatnych rozwiązań. Podanie szacunkowych kosztów tego obciążenia nie jest możliwe z powodu wielości i rozmaitości rozwiązań dostępnych na rynku oraz różnych sposobów działania usługodawców.

Kolejnym obciążeniem organizacyjnym wprowadzanym przez projektowaną ustawę jest obowiązek udzielenia sądowi odpowiedzi przez usługodawcę i przez przedsiębiorcę telekomunikacyjnego w terminie 7 dni od otrzymania wezwania[60].

Naruszanie dóbr osobistych w sieci jest zbadanym i dobrze udokumentowanym problemem społecznym[61], mającym negatywny wpływ na dobrostan psychiczny ludzi, w szczególności dzieci i młodzieży. Projektowane rozwiązanie ma potencjał w ograniczeniu tego problemu, ponieważ znacząco ułatwi wszczynanie postępowań przed sądem i skorzystanie ze cywilnoprawnej ochrony dóbr osobistych przez osoby poszkodowane. Może też mieć wpływ prewencyjny, powstrzymując od naruszania dóbr osobistych osób fizycznych, czy podmiotów, w szczególności gospodarczych, z obawy o dotkliwe konsekwencje finansowe (w efekcie orzeczenia sądu – koszty usuwania skutków naruszenia, wypłaty odszkodowania czy zadośćuczynienia na rzecz podmiotu, którego dobro naruszono).

Należy podkreślić, że proponowane rozwiązanie nie we wszystkich wypadkach naruszenia dóbr osobistych w przestrzeni cyfrowej będzie efektywne. Projekt będzie oddziaływać wyłącznie na podmioty uczestniczące w przestrzeni cyfrowej prowadzące

---

[60] Termin ten jest oceniany jako zbyt krótki. Zob. np. opinię A. Wiercińskiej – https://www.rp.pl/dobra-osobiste/art41061011-koniec-bezkarnego-hejtu-w-sieci-jest-projekt-o-slepych-pozwach.

[61] Zob. np.: Urząd Komunikacji Elektronicznej *Analiza funkcjonowania rynku usług telekomunikacyjnych w Polsce oraz ocena preferencji konsumentów. 2022 rok. Badania dzieci i rodziców*, Warszawa, 2022, https://cik.uke.gov.pl/gfx/cik/userfiles/_public/badania_dzieci_i_rodzicow_2022.pdf; NASK – Państwowy Instytut Badawczy *Nastolatki 3.0 Raport z ogólnopolskiego badania uczniów i rodziców,* Warszawa 2023 r.; Instytut Polska Przyszłości *Raport z projektu ogarnij hejt,* 2022, https://instytutlema.pl/wp-content/uploads/2022/04/Raport-Ogarnij-Hejt-2022.pdf, S. Spurek, *Raport. Cyberprzemoc wobec kobiet w Polsce,* 2024, https://sylwiaspurek.pl/wp-content/uploads/2024/06/raport-cyberprzemoc-10-online.pdf.

działalność usługową jak również tworzące i utrzymujące tę przestrzeń[62], od których będzie można pozyskać dane. Natomiast sieć może być tworzona, utrzymywana i wykorzystywana przez podmioty również z takich państw, które nie są związane umowami międzynarodowymi z Unią Europejską czy Rzeczpospolitą Polską pozwalającymi na pozyskiwanie potrzebnych danych[63]. Kolejnymi ograniczeniami efektywności są kwestie dowodowe (dane osobowe abonenta IP nie są automatycznie danymi sprawcy; konsekwencje używanego standardu IPv4[64]), kwestie techniczne (precyzja ograniczona do „sekundy" nie będzie wystarczająca dla hostingu dużych usługodawców[65]) oraz kompetencje osób naruszających dobra osobiste pozwalające na ukrycie tożsamości (używanie otwartych hotspotów, niezabezpieczonych routerów, VPN, TOR[66]).

VIII. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

Wejście w życie opiniowanego projektu skutkować będzie nałożeniem dodatkowych obowiązków na sądy, które zostaną zobowiązane do podjęcia próby ustalenia, w przewidzianej projektem procedurze, danych anonimowej osoby, która w ocenie powoda naruszyła jego dobra osobiste drogą elektroniczną. Proponowane regulacje wpłyną także na obowiązki podmiotów świadczących usługi w zakresie komunikacji elektronicznej, które zobligowane zostaną do przechowywania oraz udostępniania organom państwa zwiększonej liczby danych o swoich usługobiorcach.

---

[62] W przestrzeni cyfrowej granicami stają się fizyczne i logiczne punkty połączeń sieci operatorów infrastruktury łączności (zob. art. 2 pkt 36 ustawy z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz.U. z 2024, poz. 1221).Ustawa ta wejdzie w życie dnia 10 listopada br. zastępując ustawę z dnia z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2024, poz. 34 ze zm.).

[63] Wyczerpujące omówienie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2020/1784 z dnia 25 listopada 2020 r. dotyczącego doręczania w państwach członkowskich dokumentów sądowych i pozasądowych w sprawach cywilnych lub handlowych (Dz.Urz.UE.L.2020.405.40), Konwencji o doręczaniu za granicą dokumentów sądowych i pozasądowych w sprawach cywilnych lub handlowych, sporządzonej w Hadze dnia 15 listopada 1965 r. (Dz. U. z 2000 r. Nr. 50, poz. 582) oraz umów międzynarodowych dwustronnych i wielostronnych których RP jest stroną: S. Jastrzemska, *Praktyczny przewodnik w zakresie międzynarodowej pomocy prawnej w sprawach cywilnych,* KSSIP, Lublin, 2023, https://www.kssip.gov.pl/sites/default/files/praktyczny_przewodnik_w_zakresie_miedzynarodowej_pomocy_prawnej_w_sprawach_cywilnych_-_sylwia_jastrzemska.pdf.

[64] IPv4 (ang. *Internet Protocol version 4*) czwarta wersja protokołu komunikacyjnego IP dla internetu, mająca pojemność adresów ograniczoną do ok. 4 mld oraz jej niekompatybilność z pojemniejszą IPv6.

[65] Np. takich jak Cloudflare https://www.cloudflare.com/pl-pl/what-is-cloudflare.

[66] VPN (ang. Virtual Private Network) pol. Wirtualna Sieć Prywatna – technologia, która pozwala na stworzenie szyfrowanego tunelu pomiędzy urządzeniem użytkownika a siecią, dzięki czemu może on zabezpieczyć przesyłane dane oraz chronić swoją prywatność. TOR (ang.The Onion Router) – oprogramowanie, które pozwala na prawie anonimowe przeglądanie internetu i udostępnianie usług Zob. https://bezpiecznyvpn.pl/tor-vs-vpn.

IX. Wpływ na rynek pracy

Projekt ustawy nie będzie miał wpływu na rynek pracy.

X. Wpływ na pozostałe obszary

Projekt ustawy nie będzie miał wpływu na pozostałe obszary.

XI. Planowane wykonanie przepisów aktu prawnego

Zgodnie z art. 4 projektu ustawa wchodzi w życie po upływie 12 miesięcy od dnia ogłoszenia.

XII. W jaki sposób i kiedy nastąpi ewaluacja projektu oraz jakie mierniki zostaną zastosowane?

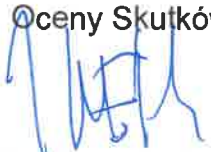
Projekt ustawy nie zawiera informacji na temat planowanej ewaluacji.

Autorzy:
dr Bartłomiej Oszkinis (pkt I, II, V, VIII, XI, XII)
ekspert ds. legislacji
w Biurze Ekspertyz
i Oceny Skutków Regulacji

Kamilla Kurczewska (pkt IV, VI, VII, IX, X)
specjalista ds. systemu gospodarczego
w Biurze Ekspertyz
i Oceny Skutków Regulacji

Angelina Tazuszel (pkt III)
specjalista w Wydziale Oceny Skutków Regulacji
w Biurze Ekspertyz
i Oceny Skutków Regulacji

Akceptował:
Wicedyrektor Biura Ekspertyz
i Oceny Skutków Regulacji



Ziemowit Cieślik

Polska 2050
Trzecia Droga

Klub Parlamentarny
Polska 2050 – Trzecia Droga
ul. Wiejska 4/6/8
00-489 Warszawa
tel. 226942912
e-mail: kp-polska2050@kluby.sejm.pl
REGON:526953069
NIP: 7011174948

Warszawa, dn. 10.10.2024 r.

Łukasz Osmalak
Poseł na Sejm RP

SEKRETARIAT MARSZAŁKA SEJMU WPŁYNĘŁO
10. 10. 2024
SH. 020.207/2/2024

Pan
Szymon Hołownia
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku

W uzupełnieniu pisma z dnia 25. września 2024 r. (znak. SPS-WP.020.211.9.2024) imieniu posłów wnioskodawców uprzejmie przedstawiam uzupełnienie uzasadnienia projektu ustawy nr SH-020-207/24 o zmianie ustawy - Kodeks postępowania cywilnego oraz niektórych innych ustaw zgodnie z wymogiem określonym w art. 34 ust. 2 pkt 4 Regulaminu Sejmu.

Z upoważnienia

Łukasz Osmalak

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU
L.dz. SPS-WP.020.211.10.2024
Data wpływu 10.10.2024

Uzupełnienie uzasadnienia projektu ustawy

Zgodnie z proponowanymi rozwiązaniami, skutki ekonomiczne dla usługodawców, w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną będą związane z wprowadzoną obowiązkową retencją danych.

Zgodnie z dodanym art. 18a i 18b w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344 oraz z 2024 r. poz. 1222) każdy usługodawca będzie obowiązany na własny koszt przechowywać dane, o których mowa w art. 18 ust. 1 i 5, generowane lub przetwarzane w trakcie prowadzonej przez niego działalności, przez okres 6 miesięcy, licząc od dnia wprowadzenia ich do systemu teleinformatycznego, do którego mają dostęp użytkownicy. Dodatkowo, w przypadku danych osób dopuszczających się naruszenia dóbr osobistych użytkowników, usługodawca ma przechowywać dane przez okres nie krótszy niż 12 miesięcy od dnia ich wprowadzenia do systemu teleinformatycznego, do którego mają dostęp użytkownicy.

Powyższe zapisy – wprowadzenie obowiązku retencji danych – mogą wprowadzić pewne finansowe obciążenie usługodawców, w stopniu jednak znikomym biorąc pod uwagę charakter oraz uciążliwość planowanych obowiązków.

W zakresie obowiązkowej retencji danych, podkreślić należy, że w obecnym stanie prawnym każdy dostawca usług świadczonych drogą elektroniczną samodzielnie określa jakie dane osobowe i eksploatacyjne swoich użytkowników chce zbierać i jak długo chce przechowywać (przetwarzać) tak zebrane dane, nie istnieje prawny obowiązek ich przechowywania. Praktyka wskazuje jednak, że przeważająca większość usługodawców gromadzi i przechowuje dane osobowe i eksploatacyjne swoich użytkowników – w celach komercyjnych.

Długość retencji danych i zakresu danych przechowywanych dobrowolnie przez usługodawców determinowana jest obecnie charakterem świadczonej usługi, a nie nałożonym na usługodawców obowiązkiem ze strony państwa.

Projektowana ustawa i wprowadzony obowiązek retencji danych zmieni obecny stan prawny, bo w miejscu swobodnego decydowania przez usługodawców, jakie dane i przez jaki okres mają być przechowywane, wprowadza obowiązek ich przechowywania przez okres odpowiednio 6 i 12 miesięcy.

Innymi słowy, usługodawcy nie będą mogli już swobodnie decydować o tym, przez jaki okres i jakie dane będą przechowywać. Nie istnieje inna możliwość realizacji celów ustawy, a dodawane obowiązki są niezbędne do skutecznego procedowania „ślepych pozwów".

Wprowadzenie obowiązku retencji, jak również obowiązku udostępnienia danych może wiązać się z koniecznością wymiany urządzeń, zapewnienia infrastruktury czy też serwerów o odpowiedniej pojemności lub wykupienia odpowiedniej usługi, jak również w przypadku największych podmiotów, takich jak popularne serwisy społecznościowe – zatrudnieniem dedykowanych pracowników do obsługi zapytań ze strony sądu. Należy jednak zwrócić uwagę, że jak wyżej wskazano, przeważająca część usługodawców dokonuje dobrowolnej retencji danych, stąd w większości przypadków usługodawcy będą posiadać już odpowiednią infrastrukturę przystosowaną do nowo nałożonego na nich obowiązku i nie będzie istniała po ich stronie konieczność ponoszenia dodatkowych kosztów związanych z nową regulacją.

Dodatkowo długość okresu przechowywania danych nie będzie miała wpływu na koszty ponoszone przez usługodawców.

Osobną kwestią pozostaje kwestia kosztów związanych z udzieleniem odpowiedzi na żądanie sądu o udostępnienie danych.

Przy założeniu, że łączna roczna ilość zapytań ze strony sądów do usługodawców będzie wahała się w granicach dziesięciu tysięcy (bądź też mniej, biorąc pod uwagę funkcję odstraszającą i prewencyjną ustawy), zaś koszt obsługi – odpowiedzi na zapytanie sądu – będzie wynosić statystycznie około 50 zł za jedną odpowiedź (zaangażowanie czasowe pracownika, koszt korespondencji, koszt materiałów, koszt wydruków danych) – łączne szacunkowe roczne koszty odpowiedzi na żądanie sądu o przekazanie danych leżące po stronie usługodawców wynosić będą około 500.000,00 zł. Koszty te obciążać będą w całości usługodawców, nie planuje się ponoszenia tych kosztów przez budżet państwa.

W zakresie zapytań ze strony sądu o nadesłanie danych kierowanych do przedsiębiorców telekomunikacyjnych, to należy zauważyć, że zgodnie z obowiązującymi przepisami, na przedsiębiorcach telekomunikacyjnych ciąży już obowiązek retencji danych, stąd są w posiadaniu infrastruktury, która umożliwi im odpowiedź na żądanie sądów, zgodnie z projektowanymi zmianami.

Biorąc pod uwagę znaczną ilość kierowanych do przedsiębiorców telekomunikacyjnych zapytań ze strony organów ścigania i sądów na podstawie odrębnych przepisów, przewidziany w ustawie obowiązek udostępnienia danych w sprawach o ochronę dóbr osobistych przeciwko osobom o nieznanej tożsamości nie wpłynie znacząco na obciążenie finansowe przedsiębiorców telekomunikacyjnych, ponieważ będzie jedynie niewielkim promilem spraw, w których to przedsiębiorca telekomunikacyjny ma obowiązek udostępnić dane.

Projekt ustawy będzie pociągać za sobą obciążenie budżetu państwa. Wejście w życie ustawy skutkować będzie zwiększeniem obciążenia sądów cywilnych – wzrost ten będzie prawdopodobnie stopniowy z uwagi na upowszechnianie się wśród obywateli wiedzy o możliwości występowania z roszczeniami o ochronę dóbr osobistych, jeżeli do ich naruszania doszło drogą elektroniczną i przy braku znajomości danych osobowych osoby dopuszczającej się naruszenia.

Biorąc pod uwagę funkcję odstraszającą i prewencyjną – sam fakt powstania instytucji umożliwiającej zidentyfikowanie osób do tej pory anonimowych w Internecie może spowodować ograniczenie ilości zniesławiających wpisów w Internecie, a tym samym ograniczenia liczby naruszeń i związanych z tym postępowań sądowych.

Z uwagi na planowane zwiększenie zatrudnienia w sądownictwie powszechnym, planowane w rządowym projekcie ustawie budżetowej na rok 2025 r., dalsze prognozowane wsparcie kadrowe nie będzie elementem niezbędnym. Ewentualny wzrost wydatków z tym związanych zostanie sfinansowany częściowo przez strony procesu stosownie do przepisów ustawy z dnia 28 lipca 2005 r. o kosztach sądowych w sprawach cywilnych.

Planuje się przygotowanie ogólnopolskich szkoleń dla sędziów, referendarzy, asystentów i pracowników sądownictwa powszechnego ze stosowania projektowanej ustawy – szacunkowy koszt ich przeprowadzenia szacuje się na 10.000.000,00 złotych.

SĄD NAJWYŻSZY
Pierwszy Prezes Sądu Najwyższego

Warszawa, 9 października 2024 r.

BSA I.021.34.2024

Pan
Dariusz Salamończyk

Zastępca Szefa Kancelarii Sejmu

Szanowny Panie Ministrze,

w odpowiedzi na pismo z dnia 5 września 2024 r., znak: SPS-WP.020.211.5.2024, mając na uwadze treść art. 1 pkt 4 ustawy z dnia 8 grudnia 2017 r. o Sądzie Najwyższym (tekst jednolity: Dz.U. z 2024 r. poz. 622), w załączeniu uprzejmie przesyłam uwagi Sądu Najwyższego do ***poselskiego projektu ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw.***

Z poważaniem,

dr hab. Małgorzata Manowska
/podpisano kwalifikowanym podpisem elektronicznym/

SEKRETARIAT PIERWSZEGO ZASTĘPCY
L. dz. DS. 1804.411.2024
Data wpływu 15.10.2024

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU
L. dz. SPS-WP.020.211.12.2024
Data wpływu 15.10.2024 r.

Biuro Studiów i Analiz Sądu Najwyższego

Warszawa, dnia 9 października 2024 r.

BSA I.021.34.2024

Opinia

do projektu ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw

Przedmiotem opinii jest projekt ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw[1] (dalej jako „Projekt"), którym proponuje się wprowadzenie tzw. ślepego pozwu, tj. nowego rodzaju cywilnego postępowania szczególnego w postaci postępowania o ochronę dóbr osobistych, jeżeli do ich naruszenia doszło drogą elektroniczną, a powód nie zna imienia i nazwiska albo nazwy lub adresu miejsca zamieszkania albo siedziby pozwanego, który naruszył jego dobra osobiste.

Zgodnie z art. 1 pkt 4 ustawy z dnia 8 grudnia 2017 r. o Sądzie Najwyższym[2], opinia dotyczy zawartych w Projekcie przepisów, na podstawie których orzekają i funkcjonują sądy, jak również tych, które mogą mieć wpływ na sprawy należące do właściwości Sądu Najwyższego.

Uwagi wstępne

Problem braku znajomości przez powoda danych identyfikujących pozwanego występuje w kontekście zróżnicowanych stosunków prawnych, zarówno w związku z działalnością prowadzoną w Internecie, jak i w sferach tradycyjnych, to jest niezwiązanych z rzeczywistością cyfrową. Projekt odnosi się wyłącznie do pierwszej sytuacji, wyposaża osoby, których dobra osobiste są naruszane anonimowo, w instrument umożliwiający lub ułatwiający skuteczne dochodzenie roszczeń przed sądem. Wprowadzenie instytucji umożliwiającej zidentyfikowanie osób dokonujących naruszenia dóbr osobistych w sieci należy co do zasady ocenić pozytywnie, może on zadziałać prewencyjnie i ograniczyć liczbę i skalę cyberprzemocy oraz hejtu w Internecie.

Wzorcem dla projektowanej regulacji wydaje się przyjęta w praktyce sądów anglosaskich (amerykańskich) procesowa instytucja *John Doe lawsuit*, która umożliwiaj powodowi – już po wniesieniu pozwu – w ramach tzw. *expedited discovery* ustalenie danych identyfikujących pozwanego przez podejmowanie czynności odpowiednich do stanu faktycznego konkretnej sprawy, w tym przede wszystkim przez zobowiązanie podmiotów trzecich do udzielenia niezbędnych informacji. Przy zaangażowaniu sądu powód zyskuje możliwość ustalenia danych pozwanego, którymi nie dysponował przed wszczęciem postępowania.

---

[1] Projektowaną ustawą zmienia się ustawy: ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną i ustawę z dnia 16 lipa 2004 r. – Prawo telekomunikacyjne.

[2] Tekst jedn. Dz.U. z 2024, poz. 622 ze zm.

Należy zaznaczyć, że przedłożony Projekt stanowi już trzecią próbę uregulowania w prawie polskim instytucji tzw. ślepego pozwu – zob. projekt z 2017 r. (projekt ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz ustawy – Prawo telekomunikacyjne, Druk Sejmowy Sejmu RP VIII kadencji, nr 1715) oraz z 2022 r. (projekt ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych, numer z wykazu UD293 (legislacja.rcl.gov.pl).

Uwagi dot. ukształtowania postępowania w sprawie ochrony dóbr osobistych przeciwko osobom o nieznanej tożsamości

Zgodnie z Projektem regulacja dot. postępowania w sprawie ochrony dóbr osobistych przeciwko osobom o nieznanej tożsamości ma zostać umieszczona w części pierwszej w księdze pierwszej w tytule VII (postępowania odrębne) w nowotworzonym dziale IX Kodeksu postępowania cywilnego. Wykładnia systemowa wskazuje, że postępowanie to ma być kolejnym postępowaniem odrębnym. Nasuwa się zatem wątpliwość, czy konieczne jest kreowanie kolejnego postępowania o tym charakterze. Refleksji projektodawcy wymaga, czy proponowany kształt postępowania o ochronę dóbr osobistych przeciwko osobom o nieznanej tożsamości (art. 505^{40} – art. 505^{44} k.p.c.) zawierać ma aż tyle istotnych odstępstw od zwykłego procesu, by uzasadniały nadanie mu charakteru postępowania odrębnego.

Należy przede wszystkim mieć na względzie, że multiplikowanie postępowań odrębnych, a także mnożenie odrębności postępowania w określonych sprawach, są zjawiskami niebezpiecznymi dla systemowej spójności prawa procesowego[3]. Efektem tego jest widoczna komplikacja powiązań wewnątrzsystemowych[4], a stosowanie przepisów Kodeksu postępowania cywilnego – choćby ze względu na możliwość jednoczesnego stosowania przepisów o kilku postępowaniach odrębnych – napotyka coraz większe trudności, co znacząco utrudnia dochodzenie praw przed sądem.

Projektodawca przyjął założenie, że po uzyskaniu danych pozwanego sąd ma rozpoznawać sprawę według przepisów ogólnych. Takie rozwiązanie może wywołać wątpliwości odnośnie do relacji między wprowadzanym kolejnym postępowaniem odrębnym a zastosowaniem w tym wypadku przepisów o postępowaniu w sprawach własności intelektualnej, do którego należą m.in. sprawy o ochronę dóbr osobistych w zakresie, w jakim dotyczy ona wykorzystania dobra osobistego w celu indywidualizacji, reklamy lub promocji towarów lub usług (art. 479^{89} § 2 pkt 2 k.p.c.)[5]. Do takiego naruszenia może dojść za pośrednictwem usługi świadczonej drogą

[3] Zob. T. Ereciński, Postępowania odrębne de lege lata i de lege ferenda [w:] Ewolucja polskiego postępowania cywilnego wobec przemian politycznych, społecznych i gospodarczych. Materiały konferencyjne Ogólnopolskiego Zjazdu Katedr Postępowania Cywilnego Szczecin-Niechorze 28-30.09.2007 r., red. H. Dolecki, K. Flaga-Gieruszyńska, Warszawa 2009, s. 3 i n.; P. Grzegorczyk, Postępowania odrębne w świetle projektowanych zmian Kodeksu postępowania cywilnego [w:] Reforma postępowania cywilnego w świetle projektów Komisji Kodyfikacyjnej, K. Markiewicz (red.), Warszawa 2011, s. 72 i n.

[4] Szerzej zob. S. Cieślak, Powiązania wewnątrzsystemowe w postępowaniu cywilnym, Warszawa 2013, s. 132 i n. Por. także M. Osowska-Grzelak, Wzajemna relacja postępowań odrębnych występujących w procesie cywilnym w ujęciu ogólnym, cz. 1, MoP 2008/13, s. 695 i n.

[5] Ponadto, w myśl art. 479^{89} § 2 pkt 3 k.p.c., w postępowaniu odrębnym w sprawach własności intelektualnej są rozpoznawane sprawy o ochronę dóbr osobistych w związku z działalnością naukową lub wynalazczą. W tych przypadkach

elektroniczną. W razie zaś ewentualnego zbiegu postępowania w sprawie ochrony dóbr osobistych przeciwko osobom o nieznanej tożsamości z postępowaniem w sprawach własności intelektualnej, jak się wydaje, będą miały zastosowanie przepisy tego ostatniego, co wynika z art. 479^{91} k.p.c.

Należy przy tym zwrócić uwagę, że określenie nowego postępowania wprowadzanego do Kodeksu postępowania cywilnego mieniem postępowania „w sprawie ochrony dóbr osobistych przeciwko osobom o nieznanej tożsamości" jest nieadekwatne (szersze) w stosunku do jego przedmiotu. Zaproponowane określenie (nazwa) nowego postępowania może sugerować, że będzie ono dotyczyć wszelkich spraw o ochronę dóbr osobistych przeciwko osobom o nieznanej tożsamości, nie zaś jedynie dotyczących naruszeń, do których doszło drogą elektroniczną, o czym stanowi projektowany art. 505^{40} k.p.c.

Reasumując, pod rozwagę można poddać ukształtowanie instytucji ślepego pozwu jako postępowania pomocniczego, tj. samodzielnego postępowania toczącego się poza ramami sprawy głównej, ale pozostającym z nim w związku, który uzasadnia jego istnienie. Zawarte w Projekcie odrębności odnoszą się w rzeczywistości do etapu wstępnego postępowania. Można zatem także rozważyć ich umiejscowienie – zamiast konstrukcji kolejnego postępowania odrębnego - wśród przepisów o warunkach formalnych pozwu. Przepisy odnoszące się do czynności służących pozyskiwaniu danych pozwanego można umieścić wśród regulacji Tytułu VI Działu I Rozdziału 1 (pisma procesowe).

Art. 505^{40} – uwagi ogólne

W art. 505^{40} k.c. przewidziano wprowadzenie instytucji tzw. ślepego pozwu, umożliwiającego wszczęcie postępowania nawet w sytuacji, gdy powód nie zna podstawowych danych pozwanego, który naruszył jego dobra osobiste w Internecie. W takim wypadku powód nie musi oznaczać strony pozwanej w sposób tradycyjny, lecz może ograniczyć się do wskazania jako pozwanego „osoby nieznanej" – zamiast imienia i nazwiska albo nazwy lub adresu pozwanego. Ustalenia tożsamości pozwanego przez nadesłanie wszystkich posiadanych danych pozwanego ma dokonywać – w wykonaniu zobowiązania sądu – usługodawca, za pośrednictwem którego doszło do naruszenia dóbr osobistych powoda, a także przedsiębiorca telekomunikacyjny będący dostawcą systemu teleinformatycznego. Po dostarczeniu niezbędnych danych sprawa ma być rozpoznawana według w ogólnych reguł.

Należy zgodzić się z projektodawcą, że wprowadzenie instytucji tzw. ślepego pozwu wymaga wprowadzenia wyraźnego przepisu, jak bowiem przyjął Sąd Najwyższy w uzasadnieniu uchwały z dnia 20 sierpnia 2020 r., III CZP 78/19[6], 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.

---

sprawca naruszenia wydaje się jednak możliwy do ustalenia przez samego powoda. To samo dotyczy przewidzianego w art. 479^{89} § 2 pkt 2 k.p.c. wykorzystania dobra osobistego w celu indywidualizacji przedsiębiorcy.

[6] OSNC 2021/2 poz. 7.

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 Sąd Najwyższy przyjął dopuszczalność żądania od podmiotu związanego tajemnicą telekomunikacyjną informacji pozwalających zweryfikować twierdzenie powoda[7], że czynu naruszającego dobra osobiste dopuścił się pozwany w sprawie, na podstawie art. 159 ust. 2 pkt 4 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[8]. *De lege lata* jednak powód musi w pozwie oznaczyć pozwanego.

Potrzeba uregulowania instytucji ślepego pozwu i związanego z nią postępowania przed sądem wynika z pozwu, że ograniczenia w zakresie ochrony praw naruszonych w Internecie wynikają z przepisów RODO, które nie przyznają potencjalnemu powodowi prawa żądania przekazania niezbędnych informacji do wytoczenia powództwa o ochronę dóbr osobistych ze względu na to, że takie udostępnienie nie mieści się w pojęciu uzasadnionego interesu. Brakuje także regulacji prawnych umożliwiających Prezesowi Urzędu Ochrony Danych Osobowych nakazanie usługodawcom udostępnienia danych osobom, które zamierzają na drodze sądowej chronić dobra osobiste. W praktyce Prezes UODO nie ma możliwości uwzględnienia kierowanych do niego wniosków o udostępnienie danych osób naruszających i zobligowany jest umarzać tego rodzaju postępowania ze względu na ich bezprzedmiotowość.

Uwagi do art. 505^{40} § 2 k.p.c.

Projektowany art. 505^{40} § 2 k.c. ma przewidywać, że sprawy, o których mowa w § 1 – a zatem takie, w których wniesiono tzw. ślepy pozew o ochronę dóbr osobistych – będzie rozpoznał sąd okręgowy właściwy dla miejsca zamieszkania lub siedziby powoda na terytorium Rzeczypospolitej Polskiej. Uregulowanie to będzie, przynajmniej w pewnym zakresie, powielać rozwiązania obowiązujące już w Kodeksie postępowania cywilnego.

Zgodnie z art. 17 pkt 1 k.p.c., sprawy o prawa niemajątkowe (m.in. o ochronę dóbr osobistych)[9] i łącznie z nimi dochodzone roszczenia majątkowe należą do właściwości sądów okręgowych. Do właściwości tego sądu należą również sprawy o roszczenia wynikające z Prawa prasowego (art. 17 pkt 3 k.p.c.)[10]. W tej sytuacji może budzić wątpliwości, czy konieczna jest dodatkowa regulacja, że sprawy określone w art. 505^{40} § 1 k.p.c., wprost określone jako „sprawy o ochronę dóbr osobistych", rozpoznawane są w pierwszej instancji przez sąd okręgowy.

W myśl zaś art. 35^{1} k.p.c., powództwo o ochronę dóbr osobistych naruszonych przy wykorzystaniu środków masowego przekazu można wytoczyć przed sąd właściwy dla miejsca

[7] W sprawie powód oznaczył z imienia i nazwiska pozwanego, a ustalenie danych przez abonenta domeny i dostawcę Internetu miało służyć potwierdzeniu roszczeń.

[8] Ustawa z 16.07.2004 r. Prawo telekomunikacyjne (tekst jedn. Dz.U. z 2021 r., poz. 576 ze zm.).

[9] Zob. J. Gudowski [w:] Kodeks postępowania cywilnego. Komentarz. Tom I. Postępowanie rozpoznawcze, red. T. Ereciński, Warszawa 2016, s. 266 i n.

[10] Por. uchwałę Sądu Najwyższego z dnia 10 lipca 2015 r., III CZP 36/15 (OSNC 2016/6 poz. 70, z glosą J. Misztal-Koneckiej, OSP 2016/7-8 poz. 65), w której stwierdzono, że sprawy o zadośćuczynienie za krzywdę wyrządzoną naruszeniem dóbr osobistych przez opublikowanie materiału prasowego należą do właściwości sądu okręgowego (art. 17 pkt 3 k.p.c.).

zamieszkania albo siedziby powoda, przy czym naruszenia praw, do których odnoszą się projektowane regulacje, maja miejsce przy wykorzystaniu środków masowego przekazu, do których Internet zalicza się obok prasy, radia czy telewizji[11]. Przepis ten przewiduje właściwość przemienną, a zatem rozwiązanie przewidziane w projektowanym art. 505^{40} § 2 k.p.c. jest zatem dalej idące, ponieważ przewiduje jedynie właściwość sądu miejsca zamieszkania lub siedziby powoda[12]. Rozwiązanie takie jest jednak nieuniknione, skoro Projekt dopuszcza wniesienie pozwu bez oznaczenia pozwanego.

Projektowane rozwiązanie odnośnie do określenia właściwości miejscowej sądu pogorsza sytuację procesową pozwanego, który – gdy jego dane identyfikacyjne zostaną już oznaczone – będzie zmuszony bronić się przed roszczeniami w niekiedy odległym sądzie, który nie jest dla niego sądem właściwym, tylko dlatego, że powód na wstępnym etapie nie miał dostatecznej wiedzy o nim. Jeżeli docelowo okaże się, że sąd rozpoznający sprawę jest sądem niewłaściwym według przepisów ustawy, pozwany powinien mieć możliwość podniesienia zarzut braku właściwości miejscowej sądu (art. 200 § 1^2 k.p.c.) lub – jeżeli uzna, że jego prawa nie doznają ograniczenia przez konieczność obrony przed roszczeniami przed sądem niewłaściwym - wdania się w spór i tym samym ustanowienia właściwości danego sądu. Można wyrazić postulat, aby w przypadku ślepego pozwu ewentualne badanie właściwości miejscowej sądu zostało odroczone w czasie do momentu po doręczeniu pozwu i być dokonywane na zarzut pozwanego.

Za dyskusyjne rozwiązanie może być także uznane przyznanie kompetencji do oceny ślepych pozwów *de facto* wszystkim sądom okręgowym, w zależności od miejsca zamieszkania lub siedziby powoda. Rozważyć można ukształtowanie mechanizmu właściwości sądu w sposób, który skierowałby postępowanie w przedmiotowym zakresie do właściwości sądów własności intelektualnej – pięć profilowanych wydziałów SO w Gdańsku, w Katowicach, w Lublinie, w Poznaniu oraz w Warszawie. Pod rozwagę można poddać celowość utworzenia jednego wyspecjalizowanego sądu, który zajmowałby się wszystkimi sprawami o naruszenie dóbr osobistych w Internecie.

Uwagi do art. 505^{41} § 1 i § 2 k.p.c.

Projektowany art. 505^{41} k.p.c. zawiera dodatkowe wymagania formalne pozwu ślepego. W pozwie wnoszonym w postępowaniu o ochronę dóbr osobistych przeciwko „osobie nieznanej" powód będzie miał obowiązek złożyć wniosek o zobowiązanie usługodawcy[13] za pośrednictwem którego doszło do naruszenia dóbr osobistych powoda do wskazania – w oparciu o podane przez

[11] Zob. T. Wiśniewski [w:] Kodeks postępowania cywilnego. Komentarz. Tom I. Artykuły 1- 366, red. T. Wiśniewski, Warszawa 2021, teza 8 do art. 35^1.

[12] Projektowane uregulowanie art. art. 505^{40} § 2 k.c. odwraca zatem wynikającą z art. 27-30 k.p.c. zasadę *„actor sequitur forum rei"*.

[13] Osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, która prowadząc, chociażby ubocznie, działalność zarobkową, zawodową lub pożytku publicznego świadczy usługi drogą elektroniczną, w tym również oferując usługi pośrednictwa internetowego w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UW) 2019/1150 z dnia 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz.Urz UE. L. 186 z 11.07.2019)

powoda informacje – przekazania danych pozwanego[14], określonych w art. 18 ust. 1 i 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[15]. Powód powinien oznaczyć usługodawcę, za pośrednictwem którego drogą elektroniczną doszło do naruszenia dóbr osobistych. Obowiązkiem powoda ma być także wskazanie, w jaki sposób doszło do naruszenia dóbr osobistych, w szczególności poprzez podanie publikacji naruszającej dobra osobiste powoda wraz z godziną i datą publikacji, a ponadto nazwę profilu lub loginu pozwanego, o ile ich wskazanie jest możliwe. Zgodnie z art. 505[41] § 2 k.p.c. do pozwu należy dołączyć czytelne odwzorowanie ww. publikacji, sporządzone w formie zapisu elektronicznego umieszczonego na nośniku danych oraz w formie wydruku przedstawiającego skopiowany obraz ekranu z widocznym adresem URL[16] oraz datą i godziną publikacji.

Należy mieć na względzie, że powód posiada zdecydowanie szerszą wiedzę niż sąd o okolicznościach sprawy, a zatem z większym prawdopodobieństwem może wskazać odpowiednie działania, które mogą przyczynić się do osiągnięcia celu ślepego pozwu. Takiej możliwości nie przewidziano w Projekcie. Na etapie wymagań formalnych dyskusyjne wydaje się odgórnie ograniczanie rodzaju i liczby możliwych do przeprowadzenia czynności, gdyż zagadnienie ich proporcjonalności może być badane już na etapie merytorycznego wstępnego badania powództwa.

Powód powinien mieć również możliwość składania wniosków w sposób kaskadowy – a więc przykładowo uzyskanie niektórych informacji powinno móc być wykorzystane przy przeprowadzeniu kolejnej czynności. Można także brać pod uwagę możliwość modyfikowania wniosków powoda w toku procedury ustalania danych identyfikujących pozwanego, zwłaszcza w świetle nowopoznanych informacji.

Można rozważyć zobligowanie powoda do zawarcia w pozwie oświadczenie o działaniach podjętych w kierunku samodzielnego pozyskania danych pozwanego. Funkcją takiego wymagania byłoby ograniczenie zastosowania ślepego pozwu wyłącznie do sytuacji, w których powód – mimo dochowania należytej staranności – nie był w stanie ustalić danych identyfikujących pozwanego. Wymaganie to pozwoliłoby poczynić oszczędności w zakresie zasobów wymiaru sprawiedliwości, co przyczyniłoby się do przyspieszenia rozpoznania tych spraw, które rzeczywiście wymagają określonych we wnioskach powoda poszukiwań.

Projekt zakłada automatyzm podjęcia przez sąd ustalenia personaliów pozwanego dokonującego naruszenia dóbr osobistych poprzez zwrócenie się o poszczególne informacje najpierw do usługodawcy, następnie do przedsiębiorcy telekomunikacyjnego. Wydaje się, że powództwo powinno podlegać wstępnemu badaniu pod kątem uprawdopodobnienia jego przesłanek, proporcjonalności wagi roszczenia materialnoprawnego powoda do naruszenia praw

[14] W tym dane osobowe usługobiorcy niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego z usługodawcą: 1) nazwisko i imiona usługobiorcy; 2) numer ewidencyjny PESEL lub - gdy ten numer nie został nadany - numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość; 3) adres zameldowania na pobyt stały; 4) adres do korespondencji, jeżeli jest inny niż adres, o którym mowa w pkt 3; 5) dane służące do weryfikacji podpisu elektronicznego usługobiorcy; 6) adresy elektroniczne usługobiorcy.

[15] Tekst jedn. Dz.U. z 2020 r., poz. 344 ze zm.

[16] O ile wskazanie adresu URL jest możliwe.

pozwanego oraz podjęcia przez pozwanego uzasadnionych prób ustalenia danych identyfikujących pozwanego przed skorzystaniem ze ślepego pozwu.

Wydaje się, że ślepy pozew powinien podlegać badaniu pod kątem spełnienia wymagań formalnych (innych niż wskazanie danych identyfikujących pozwanego) oraz fiskalnych. Nie jest jasne, jak nowe wymaganie pozwu (dodatkowe w stosunku do wymagań określonych w art. 187 § 1 k.p.c.) należy traktować z perspektywy określonego w art. 130 § 1 k.p.c. mechanizmu naprawczego w postaci wezwania powoda do usunięcia braków formalnych pod rygorem zwrotu pozwu. Powstaje pytanie, czy przesłanka do zastosowania tego przepisu (w postaci niemożności nadania pozwowi prawidłowego biegu) będzie zachodzić jedynie w razie niepodania przez powoda jakichkolwiek danych wskazanych w treści projektowanego art. 505^{41} § 1 oraz 2 k.p.c., czy także w wypadku podania danych niepełnych. Należy mieć na względzie, że w wielu wypadkach weryfikacja tego elementu we wstępnej fazie postępowania może być utrudniona, a nawet niemożliwa.

Uwagi do art. 505^{42} § 1-4 k.p.c.

Zgodnie z projektowanym art. 505^{42} § 1 k.p.c. sąd w terminie 7 dni od dnia złożenia pozwu ma występować z żądaniem do usługodawcy, za pośrednictwem którego doszło do naruszenia dóbr osobistych powoda, o nadesłanie wszystkich posiadanych danych pozwanego, o których mowa w art. 505^{41} § 1 pkt 1 k.p.c. oraz o wskazanie danych przedsiębiorcy telekomunikacyjnego[17] będącego dostawcą systemu teleinformatycznego dla pozwanego. Na usługodawcę nałożono obowiązek przekazania powyższych danych w terminie 7 dni od dnia doręczenia żądania pozwu. Analogiczne rozwiązanie przewidziano w art. 505^{42} § 3 k.p.c. wobec przedsiębiorcy telekomunikacyjnego, na którym również miałby spoczywać obowiązek przekazania posiadanych przez siebie danych – w tym wypadku danych pozwanego, o których mowa w art. 386 ust. 1 pkt 1 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej[18] - w terminie 7 dni od dnia otrzymania żądania.

Należy wyrazić zasadniczą wątpliwości, że zaproponowane w Projekcie krótkie terminy (7 dni), zarówno w odniesieniu do sądów, jak i przedsiębiorców (usługodawca, przedsiębiorca telekomunikacyjny) mogą się okazać nierealne. Siedmiodniowy termin na odpowiedź wydaje się zbyt krótki. Pod rozwagę należy poddać zastosowanie konstrukcji terminu sądowego, tj. wyznaczanego ad casu przez sąd. Zaletą takiego rozwiązania jest także możliwość zastosowania normy z art. 166 k.p.c., która umożliwiłaby z ważnej przyczyny przedłużenie terminu na wniosek zgłoszony przed jego upływem. Należy mieć ponadto na względzie, że z punktu widzenia tzw. cyfrowych gigantów nawet maksymalna sankcja z art. 505^{42} § 5 k.p.c. (do miliona złotych) może mieć zupełnie inne znaczenie niż w wypadku niewielkiego dostawcy usług, dla którego szybkie udostępnienie danych może sprawiać poważne trudności.

[17] W rozumieniu art. 2 pkt 40 ustawy z dnia 12 lipca 2024 r. – Prawo telekomunikacji elektroniczne.
[18] Tj. danych dotyczących użytkownika.

Siedmiodniowy termin zakreślony dla sądu, w którym ma on obowiązek dokonania analizy pozwu oraz oceny istnienia prawdopodobieństwa naruszenia dobra osobistego, czego efektem ma być zwrócenie się do dostawcy usług o przekazanie danych, wydaje się umiarkowanie realny.

Uwagi do art. 505^{42} § 5 k.p.c.

Wezwanie do wskazania danych, o których mowa w art. 505^{42} § 5 k.p.c., ma być powiązane z nałożeniem kary grzywny na usługodawcę lub przedsiębiorcę telekomunikacyjnego w sytuacji, w której nie nadesłaliby oni wszystkich posiadanych danych bez usprawiedliwionych powodów. Przewidziano sankcję grzywny w wysokości od stu tysięcy do miliona złotych. Określenie powyższych granic wydaje się wątpliwe. Choć wprowadzenie dolnej granicy w wysokości stu tysięcy złotych może mieć charakter mobilizujący usługodawcę lub przedsiębiorcę do podjęcia wszelkich możliwych działań, to warto rozważyć ukształtowanie mechanizmu sankcjonującego na wzór ogólnego mechanizmu grzywny z art. 163 § 1 k.p.c., zgodnie z którym „grzywnę wymierza się w kwocie do (...)". Projektowana regulacja pozbawia sąd możliwości miarkowania grzywny w sytuacji, w której w ocenie sądu byłaby ona w wysokości stu tysięcy złotych nieadekwatna.

Wydaje się, że odnośnie do skazania na grzywnę należy stosować ogólne reguły o zażaleniu, przy założeniu, że usługodawca oraz przedsiębiorca telekomunikacyjny będą traktowani jako osoba trzecia. W takim wypadku zgodnie z art. 394^{1a} § 1 pkt 5 k.p.c. zażalenie przysługuje do innego składu sądu pierwszej instancji (zażalenie poziome).

Uwagi do art. 505^{44} k.p.c.

Projekt zakłada umorzenie postępowania w sytuacji, w której usługodawca bądź przedsiębiorca telekomunikacyjny nie wskaże wystarczających danych identyfikujących pozwanego bądź ich pozyskanie byłoby niemożliwe.

Do oceny sądu należy zweryfikowanie, czy przekazane dane identyfikujące pozwanego są wystarczające. Nie jest jasne, czy do umorzenia postępowania musi dojść, gdy usługodawca podał tylko niektóre dane pozwanego – np. tylko imię i nazwisko, bez adresu. W razie uznania, że podanie niewystarczających danych prowadzi do umorzenia postępowania, należałoby rozważyć wprowadzenie mechanizmu przekazywania tych niekompletnych danych powodowi, co może mu ułatwić wytoczenie powództwa na zasadach ogólnych. Nie ulega wątpliwości, że umorzenie postępowania nie pozbawia powoda prawa ponownego wytoczenia powództwa, jeżeli w inny sposób uda mu się ustalić dane identyfikujące stronę pozwaną.

W zależności od tego, z jakich przyczyn albo na jakim etapie postępowania dochodzi do umorzenia postępowania, ustawa może różnicować jego konsekwencje[19]. Mając na względzie, że umorzenie postępowania na podstawie art. 505^{44} k.p.c. ma następować z powodu czynników zasadniczo niezależnych od powoda, wyjaśnienia wymaga, czy – mimo umorzenia postępowania – ślepy pozew, na tle którego nie udało się ustalić wystarczających danych identyfikujących

[19] Zob. P. Grzegorczyk [w:] Kodeks postępowania cywilnego. Komentarz. Tom I. Postępowanie rozpoznawcze, red. T. Ereciński, Warszawa 2016, s. 1027 i n.

pozwanego, będzie wywoływał skutki, które ustawa wiąże z wytoczeniem powództwa. Może mieć to znaczenie zwłaszcza z perspektywy przedawnienia roszczenia – w razie ponownego (po umorzeniu postępowania toczącego na skutek ślepego pozwu) wytoczenia w określonym czasie kolejnego powództwa przeciwko podmiotowi, którego dane identyfikujące zostały następczo ustalone.

Wątpliwości w tym zakresie może pogłębiać to, że w zawartych w Projekcie przepisach o postępowaniu o ochronę dóbr osobistych przeciwko osobom o nieznanej tożsamości nie przewidziano odpowiednika art. 505^{37} § 2 k.p.c., z którego wynika, że „jeżeli w terminie trzech miesięcy od dnia wydania postanowienia o umorzeniu elektronicznego postępowania upominawczego powód wniesie pozew przeciwko pozwanemu o to samo roszczenie w postępowaniu innym niż elektroniczne postępowanie upominawcze, skutki prawne, które ustawa wiąże z wytoczeniem powództwa, następują z dniem wniesienia pozwu w elektronicznym postępowaniu upominawczym. Na żądanie stron sąd, rozpoznając sprawę, uwzględni koszty poniesione przez strony w elektronicznym postępowaniu upominawczym"[20].

Wymaga zatem wyjaśnienia, jakie mają być konsekwencje umorzenia postępowania na podstawie art. 505^{44} k.p.c., zwłaszcza gdy chodzi o skutki związane z wytoczeniem powództwa w postępowaniu w sprawie dóbr osobistych przeciwko osobom o nieznanej tożsamości.

Można wyrazić obawę, że stosowanie projektowanego rozwiązania w praktyce przyniesie zamierzone efekty, tj. pozwalać będzie na ustalanie imienia i nazwiska albo nazwy lub adresu miejsca zamieszkania albo siedziby pozwanego. Wynika to z faktu, że w wielu wypadkach zwłaszcza przedsiębiorcy telekomunikacyjni nie będą dysponować danymi identyfikującymi pozwanego. Ponadto portale i serwisy społecznościowe z reguły nie prowadzą bieżącej weryfikacji prawdziwości danych podawanych podczas procesu rejestracji profilu (w tym nawet imienia i nazwiska). Jednocześnie obowiązek takiej weryfikacji nie wynika z przepisów prawa. Warto mieć na względzie, że skala zjawiska profili, o których dane osobowe nie odpowiadają rzeczywistości jest, jak przyznają sami usługodawcy, ogromna. Dla przykładu w pierwszym kwartale 2021 r. Facebook na całym świecie dezaktywował 1,3 miliarda fałszywych kont, zaś w drugim kwartale – 1,7 miliarda[21].

W świetle powyższego należy wyrazić obawę, że skuteczność pozyskiwania od wskazanych w projekcie podmiotów danych niezbędnych do zapewnienia prawidłowego toku postępowania sądowego pozostanie w przypadku części informacji praktycznie ograniczona (lub wątpliwa ze względu na brak możliwości weryfikacji ich prawdziwości). W takich wypadkach postępowania będą podlegały umorzeniu na zasadach wskazanych w art. 505^{44} k.p.c. Powyższe nie podważa jednak zasadności wprowadzenia do Kodeksu postępowania cywilnego instytucji tzw. ślepego pozwu.

[20] Por. na ten temat A. Gołąb, Umorzenie postępowania w procesie cywilnym, Warszawa 2019, s. 390 i n.
[21] https://transparency.fb.com/data/community-standards-enforcement/fake-accounts/facebook/