**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. 50541 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.