Do druku nr 728

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, *24-11-2024*

DOL.401.350.2024.WL.PM

Pan
Dariusz Salamończyk
Zastępca Szefa Kancelarii Sejmu RP

ul. Wiejska 4/6/8
00-902 Warszawa
elektroniczna skrzynka podawcza
/KSRP/SkrytkaESP

Szanowny Panie Ministrze,

w odpowiedzi na pismo z 5 września 2024 r. znak: SPS-WP.020.211.5.2024, działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1] oraz art. 51 ustawy o ochronie danych osobowych[2], uprzejmie informuję, że do przedstawionego poselskiego projektu **ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (przedstawiciel wnioskodawców: poseł Łukasz Osmalak),** Prezes UODO, jako organ nadzorczy, zgłasza następujące uwagi.

Celem projektowanej ustawy jest zmiana zasad dochodzenia roszczeń z tytułu naruszenia drogą elektroniczną dóbr osobistych przeciwko osobom o nieznanej tożsamości. **Pomysł wprowadzenia do polskiego systemu prawnego podstawy umożliwiającej nakazanie ujawnienia danych osoby-naruszyciela publikującego treści dyfamacyjne organ nadzorczy ocenia jako zabieg trafny**. Jak wskazał lakonicznie projektodawca, „Nie ma innej możliwości realizacji celów ustawy" (s. 14 uzasadnienia). Stan taki rzeczywiście aktualnie istnieje, z uwagi na brak w rozporządzeniu 2016/679 oraz w polskiej ustawie o ochronie danych osobowych

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.).
[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

Urząd Ochrony
Danych Osobowych
ul. Stawki 2
00-193 Warszawa

tel. 22 531-07-20

www.uodo.gov.pl

przepisów upoważniających Prezesa UODO do nakazania udostępnienia danych osobowych osoby trzeciej (zob. np. wyrok WSA w Warszawie z dnia 18 grudnia 2020 r., sygn. akt II SA/Wa 989/20). Podobnych podstaw prawnych brakuje w innych odrębnych przepisach, gdy chodzi o możliwość dochodzenia praw przez osobę, której dobra osobiste (także dane osobowe) zostały naruszone przez podmiot anonimowy, publikujący różnego rodzaju bezprawne treści.

Organ nadzorczy wskazuje, że stworzenie regulacji prawnej umożliwiającej nakazania ujawnienia danych osobowych użytkownika publikującego treści dyfamacyjne, jest krokiem pożądanym także w zakresie ewentualnej odpowiedzialności państwa za możliwe naruszenia art. 10 Europejskiej Konwencji o Ochronie Praw Człowieka. Potwierdził to w jednym z wyroków ETPCz, wskazując, że wprawdzie istnienie takiej procedury może nie być koniecznym elementem dochodzenia odpowiedzialności przez ofiary naruszeń, to jednak umożliwienie nakazania identyfikacji danych użytkowników publikujących zniesławiające komentarze może być uzasadnione, zwłaszcza gdy chodzi o konieczność identyfikacji i ścigania sprawców, (zob. pkt 149-151 uzasadnienia wyroku Wielkiej Izby ETPCz z 16 czerwca 2015, sprawa DELFI AS przeciwko Estonii, skarga nr 64569/09). Należy jednak pamiętać o proporcjonalności w zakresie ujawnianych danych a także takiego ukształtowania przepisów, które nie spowoduje powstania tzw. efektu mrożącego, tzn. skutkiem ich nie może być obawa przed publikacją opinii. Dlatego zabieg, by to sądy decydowały o zobowiązaniu do ujawnienia danych jest – zdaniem organu nadzorczego – rozwiązaniem prawidłowym. Zasadnicze wątpliwości, jakie jednak organ w tym miejscu sygnalizuje, dotyczą umiejscowienia poszczególnych przepisów, a także szczegółowych rozwiązań.

Przede wszystkim zauważyć należy, że wprowadzenie zmian do Kodeksu postępowania cywilnego (k.p.c.) o proponowanym tytule Działu IX, tj. Postępowanie w sprawie ochrony dóbr osobistych przeciwko osobom o nieznanej tożsamości, nie zostało precyzyjnie ujęte. Tytuł nie jest zgodny z zakresem zmian, opisanych w art. 505^{40} k.p.c. Tytuł sugeruje bowiem, że chodzi o każde naruszenie dóbr osobistych przez osobę o nieznanej tożsamości, a zatem dotyczy każdego, a nie tylko naruszenia dokonanego „drogą elektroniczną". Tymczasem z treści art. 505^{40} k.p.c. wynika, że chodzi o ustanowienie kognicji sądu jedynie w zakresie tych ostatnich naruszeń, pozostawiając naruszenia dokonane w inny sposób poza tym zakresem. Projektodawcy natomiast nie wyjaśniają, dlaczego postępowanie, którego zasadniczym celem jest stworzenie poszkodowanym naruszeniem dóbr osobistych w Internecie możliwości skierowania tzw. ślepego pozwu, a więc zasadniczo postępowania zmierzającego do ustalenia personaliów osoby dokonującej naruszeń, miałoby być jednym z postępowań odrębnych. W projekcie brak uzasadnienia dla powyższej decyzji. Skoro celem postępowania jest stworzenie rozwiązania legislacyjnego pozwalającego „na składanie pozwów bez konieczności wcześniejszego ustalenia tożsamości sprawcy przez osoby poszkodowane", co „zagwarantuje realną pomoc Państwa w identyfikacji sprawcy na potrzeby postępowania cywilnego", przepisy te winny zostać umiejscowione w przepisach ogólnych k.p.c. regulujących doręczenia, ewentualnie można zastanawiać się nad umiejscowieniem ich w ramach postępowania zabezpieczającego.

Przypomnieć należy, że skuteczne doręczenie pozwu tworzy tzw. zawisłość sporu i warunkuje dopiero możliwość prowadzenia postępowania, które w razie np. zbędności wydania wyroku może zostać umorzone. Jak słusznie podkreśla się w doktrynie, „Prawidłowe doręczenie pozwala na przyjęcie, że pozwanemu znana jest treść pozwu i ma on możliwość podjęcia właściwych czynności w celu wyrażenia swego stanowiska w sprawie. Pozew skierowany przeciwko osobie nieżyjącej, podobnie jak pozew, w którym w ogóle nie wyznaczono pozwanego, nie powoduje wszczęcia postępowania sądowego ani nie wywołuje skutków objętych zawisłością sporu, które ustawa wiąże dopiero z doręczeniem pozwu (uzasadnienie postanowienia SN z 5.11.1970 r., sygn. akt II CZ 186/70, OSNCP 1971/6, poz. 111, i uzasadnienie wyroku SN z 9.12.1999 r., sygn. akt I PKN 430/99, OSNAPiUS 2001/9, poz. 309, zob. też T. Żyznowski [w:] *Kodeks postępowania cywilnego. Komentarz. Tom I. Artykuły 1–366*, red. T. Wiśniewski, Warszawa 2021, art. 192, uwaga nr 1). W konsekwencji niezrozumiała jest także treść proponowanego art. 505^{44} k.p.c., zgodnie z którym 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. Nie wiadomo jakie postępowanie sąd ma umarzać, skoro skuteczne doręczenie pozwu w świetle aktualnych przepisów warunkuje dopiero jego rozpoczęcie. Aktualnie zatem nieoznaczenie pozwanego oznacza odrzucenie pozwu, z uwagi na niedopuszczalność drogi sądowej.

Zgodnie z proponowanym brzmieniem art. 505^{41} § 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. Zdaniem organu nadzorczego tak swobodnie ujęty wymóg formalny, może oznaczać dołączanie screenów, kopii, wydruków, które w żaden sposób nie są weryfikowane. Aktualnie nie mogą one stanowić dowodu z dokumentu. Sąd powinien przeprowadzić postępowanie w kierunku ustalenia prawdziwości danych, które stanowią przedmiot takiego dokumentu. Tymczasem, w proponowanej wersji projektu ustawy wystarczy jakakolwiek kopia, niepoświadczona nawet przez notariusza, by sąd miał podstawę, by kierować do wskazanego podmiotu żądanie ujawnienia danych użytkownika. Organ nadzorczy zwraca uwagę, że w dobie funkcjonowania różnego rodzaju aplikacji, czy programów umożliwiających tworzenie treści nieprawdziwych, istnieje zagrożenie ujawnienia danych użytkownika, który nie ma nic wspólnego z treściami zamieszczonymi w określonej przestrzeni. Jednak nie jest to kwestia weryfikacji przez sąd tych danych na początkowym etapie formalnej kontroli pozwu. Dlatego ważne jest by dane, o które występuje sąd, zawierały jedynie minimalne informacje o użytkowniku, pozwalające na skuteczne doręczenie mu pozwu. Wystarczy zatem imię, nazwisko i adres. Reszta danych, które miałyby być przekazywane na tym etapie, nie są konieczne. Podmiot pozwany bowiem musi mieć możliwość obrony i przedstawienia na etapie postępowania

dowodowego dowodów świadczących o braku jego/jej aktywności w sieci w zakresie stawianych zarzutów. Katalog danych określonych art. 18 ust. 1 i 5 ustawy o świadczeniu usług drogą elektroniczną (dalej: UŚUDE) został ukształtowany w celu prawidłowego świadczenia usług na rzecz użytkowników, są to to dane „niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego między nim" (zarówno w obecnym, jak i proponowanym brzmieniu tych przepisów). Dodatkowo UŚUDE posługuje się terminem „może przetwarzać", co wskazuje na brak obowiązku prawnego przetwarzania danych po stronie usługodawcy. Przyjęcie więc proponowanych zmian w Kodeksie postępowania cywilnego spowoduje, że samo złożenie pozwu (niezależnie od jego zasadności) będzie prowadziło do udostępnienia sądowi – a co za tym idzie powodowi – całego szeregu informacji o użytkowniku, którymi nie dysponowałby, gdyby pozew składany był na warunkach ogólnych. Będą to m.in. dane służące do weryfikacji podpisu elektronicznego usługobiorcy, adresy elektroniczne usługobiorcy, numer telefonu podany przez usługobiorcę oraz szereg danych związanych z daną usługą świadczoną drogą elektroniczną (art. 18 ust. 8 UŚUDE). Powstaje więc pytanie, czy biorąc pod uwagę cele przetwarzania danych określone w art. 18 ust. 1 UŚUDE oraz ogólne warunki składania pozwu z k.p.c., proponowane zasady ustalania tożsamości osoby naruszającej czyjeś dobra osobiste są adekwatne z punktu widzenia zasady zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a rozporządzenia 2016/679[3]), zasady ograniczenia celu (art. 5 ust. 1 lit. b rozporządzenia 2016/679[4]), zasady minimalizacji danych (art. 5 ust. 1 lit. c rozporządzenia 2016/679[5]), zasady ograniczenia przechowywania (art. 5 ust. 1 lit. e rozporządzenia 2016/679[6]), zasady integralności i poufności (art. 5 ust. 1 lit. f rozporządzenia 2016/679[7]) oraz zasady rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679[8]) – do formalnie poprawnego pozwu w opisie pozwanego wystarczą wszak takie dane jak imię i nazwisko (nazwa) i adres (art. 126 i 187 k.p.c.).

Zgodnie z art. 1 projektu ustawy dodającym nowy art. 505^{41} k.p.c. w ustawie z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2023 r. poz. 1550 ze zm.): Wniosek o zobowiązanie osoby fizycznej, osoby prawnej albo jednostki

---

[3] Zgodnie z zasadą zgodności z prawem, rzetelności i przejrzystości dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

[4] Zgodnie z zasadą ograniczenia celu dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami.

[5] Zgodnie z zasadą minimalizacji danych dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

[6] Zgodnie z zasadą ograniczenia przechowywania dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą.

[7] Zgodnie z zasadą integralności i poufności dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

[8] Zgodnie z zasadą rozliczalności administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie.

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 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) w oparciu o podane przez powoda informacje". Wątpliwości budzi proponowana definicja usługodawcy, wobec którego sąd kieruje żądanie zobowiązania do ujawnienia danych. Według projektodawcy jest nim, jak wskazano wyżej, 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 (usługodawca). Z perspektywy organu nadzorczego prawidłowość przetwarzania danych osobowych użytkowników istnieją wątpliwości co do zakresu podmiotowego podmiotów zobowiązanych do przekazania danych. Początkowa część przepisu stanowi powtórzenie definicji usługodawcy zawartej w art. 2 pkt 6 UŚUDE, druga część z kolei korzysta z definicji usług pośrednictwa internetowego w rozumieniu art. 2 pkt 3 rozporządzenia 2019/1150. Proponowane hybrydowe ujęcie podmiotów, do których kierowany jest obowiązek ujawnienia danych, budzi zastrzeżenia z powodu niejasności jego zakresu. Po pierwsze, wskazanie bez odwołania się do art. 2 pkt 6 UŚUDE rodzi pytanie o autonomiczny charakter pojęcia usługodawcy w proponowanej zmianie. Wskazać bowiem należy na niedookreśloność zwrotu „prowadząc chociażby ubocznie działalność". Nie wiadomo jak interpretować ten zwrot i czy np. prowadzenie bloga, vloga przez osobę fizyczną nieprowadzącą w ogóle działalności gospodarczej, zawodowej, ale publikującej reklamy (niekoniecznie za wynagrodzeniem) jest w ujęciu projektodawcy takim usługodawcą. Projektodawca pisze że chodzi tu o usługodawców w rozumieniu ustawy o świadczeniu usług drogą elektroniczną", a jednocześnie w definicji wprowadza jeszcze usługi pośrednictwa, których cytowana ustawa w analizowanym pojęciu nie wprowadza. W opinii organu nadzorczego definicję tę należy przemyśleć i uzasadnić jej charakter i zakres podmiotowy. Po drugie, nie wiadomo czy w razie skierowania żądania zobowiązania ujawnienia danych użytkowania sąd, w razie wskazania administratora strony i operatora przeglądarki, ma skierować żądanie do obydwu podmiotów, do jednego, a jeżeli tak to do którego.

Zgodnie z **art. 2** projektu ustawy, zmieniającym **art. 18 ust. 1** UŚUDE, „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: (...)". Biorąc pod uwagę, fakt, że dane, o których mowa w art. 18 ust. 1 UŚUDE, zgodnie z art. 1 projektu ustawy wprowadzającym art. 505^{41} do k.p.c., będą musiały być obligatoryjnie udostępniane na żądanie sądu, art. 18 ust. 1 UŚUDE musiałby zostać tak ukształtowany, żeby wynikał z niego obowiązek prawny gromadzenia danych. Ponownej analizie powinien zostać również poddany katalog danych, o którym mowa w art. 18 ust. 1 UŚUDE, jeżeli zmianie ulegnie cel ich gromadzenia. Należy również zauważyć, że **art. 2 tiret drugie** projektu ustawy zakłada dodanie nowego **pkt 7** w art. 18 ust. 1 UŚUDE dopuszczającego przetwarzanie numeru telefonu usługodawcy. Zważywszy na fakt, że nie jest to dana niezbędna „do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego" jej wprowadzenie nie odpowiada wymogom zasady zgodności z prawem, rzetelności i przejrzystości, zasady ograniczenia celu oraz zasady minimalizacji danych.

Zgodnie z **art. 2 pkt 3** projektu ustawy, dodającym **art. 18a** UŚUDE, „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". W pierwszej kolejności należy zwrócić uwagę, że zasada ograniczenia przechowywania (art. 5 ust. 1 lit. e rozporządzenia 2016/679[9]) wymaga, aby górna granica okresu przechowywania danych była wyraźnie określona. W omawianym przypadku, w szczególności – jeśli chodzi o art. 18a ust. 2 UŚUDE, gdzie jest mowa „o okresie nie krótszym niż 12 miesięcy" – granica ta nie jest w ogóle ustalona. Dodatkowo, powstaje pytanie w jaki sposób dostawca usług będzie klasyfikował danego użytkownika jako dopuszczającego się naruszenia dóbr osobistych i – co za tym idzie – stosował wobec niego inne niż w przypadku pozostałych użytkowników zasady przechowywania danych. Wyjaśnienie tej kwestii jest konieczne z punktu widzenia poszanowania zasady

[9] Zgodnie z zasadą ograniczenia przechowywania dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą.

zgodności z prawem, rzetelności i przejrzystości, zasady ograniczenia celu oraz zasady minimalizacji danych.

Zgodnie z **art. 2 pkt 3** projektu ustawy, dodającym **art. 18b** w UŚUDE, „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).". Należy podkreślić, że rozporządzenie 2022/2065 reguluje m.in. kwestie postępowania z nielegalnymi treściami w Internecie oraz udział krajowych organów administracji publicznej w tym procesie (art. 9 rozporządzenia 2022/2065). Jeżeli intencją projektodawcy jest odwołanie się do tego trybu, to powinno to wyraźnie wynikać z projektowanej ustawy. Przy konstruowaniu tego typu przepisów konieczne jest wskazanie przesłanek udostępnienia danych, sposobu tego udostępnienia, jak również doprecyzowanie jakim konkretnie organom publicznym i dla realizacji jakich celów dane mają być udostępniane. Odpowiadałoby to zasadzie zgodności z prawem, rzetelności i przejrzystości, zasadzie ograniczenia celu oraz zasadzie minimalizacji danych oraz regulacji art. 6 ust. 3 rozporządzenia 2016/679.

Uwaga odnosi się analogicznie do **art. 3 pkt 2** projektu ustawy dodającego nowy **art. 405a** w ustawie z dnia 12 lipca 2024 r. - Prawo komunikacji elektronicznej (Dz. U. poz. 1221).

Zgodnie z **art. 3 pkt 1** projektu ustawy, zmieniającym **art. 386 ust. 1 pkt 1** w ustawie - Prawo komunikacji elektronicznej, zmianie ulegnie zakres danych dotyczących użytkownika objętych tajemnicą komunikacji elektronicznej. W obecnym brzmieniu przepisu tajemnicą komunikacji elektronicznej objęte są „dane dotyczące użytkownika", proponuje się natomiast następujące brzmienie przepisu: „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". W ocenie organu nadzorczego użycie określenia „w szczególności" stworzy otwarty katalog informacji o użytkownikach, co może spowodować obniżenie standardu ochrony danych osobowych. Taka konstrukcja nie odpowiada zatem zasadzie zgodności z prawem, rzetelności i przejrzystości, zasadzie ograniczenia celu oraz zasadzie minimalizacji danych.

Kolejne wątpliwości które dostrzega organ nadzorczy w związku z projektowanymi zmianami, łączą się z brzmieniem proponowanego art. 505^{42} § 5 k.p.c., zgodnie z którym 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.

Mając na uwadze powyższe, wskazać należy, że projektodawca nie wskazał co rozumie przez nie nadesłanie bez usprawiedliwionych powodów żądanych danych. Brak identyfikacji sytuacji (chociażby w uzasadnieniu projektu) i powiązanie tego zachowania z obligatoryjnym nałożeniem przez sąd grzywny nakazuje jednak bliższe określenie i doprecyzowanie treści przepisu, bądź jego rozumienia. Wątpliwości dotyczą na przykład takich sytuacji, jak umożliwianie przez podmiot publikacji treści osobom anonimowym, a zatem oznacza to, że nie będzie on w stanie podać imienia i nazwiska użytkownika, bądź mogą się one okazać fałszywe. Powstaje wątpliwość, czy wówczas jest to przesądzające o usprawiedliwionych okolicznościach, a także czy wystarczy jedynie podanie danych operatora telekomunikacyjnego.

Brak w uzasadnieniu odniesienia się przez projektodawców do wysokości nakładanej grzywny nie pozwala na zrozumienie skąd wzięły się proponowane stawki kar, tj. od wysokości 100.000 do miliona złotych. Przypomnieć jedynie należy, że k.p.c. co do zasady w art. 163 § 1 w przypadkach nałożenia grzywny aczkolwiek bez określenia jej wysokości, wskazuje na grzywnę, którą wymierza się w kwocie do trzech tysięcy złotych. W innych przepisach k.p.c. odnaleźć można doprecyzowane kwoty grzywny, jednak nigdzie nie ma tak wysokich kwot i to w odniesieniu do odmowy przekazania informacji (np. art. 762 § 1 za nieuzasadnioną odmowę udzielenia wyjaśnień – 2.000 zł, art. 1050 § 4 za brak publikacji oświadczenia – 15.000 zł, art. 886 § 1 – uprawnienie komornika do wymierzenia grzywny do 5.000 zł, czy art. 764 – do 1000 zł).

Organ nadzorczy, rozumiejąc doniosłość społecznego problemu jakim jest dochodzenie roszczeń wobec nieznanego sprawcy naruszenia, pragnie wskazać, że projektowane zmiany będą miały istotny wpływ na zasady ochrony tajemnicy komunikacji elektronicznej i tym samym na wszystkich użytkowników komunikacji elektronicznej. Charakter proponowanych rozwiązań prawnych i projektowanych zmian wskazuje zatem na konieczność przeprowadzenia przez projektodawcę **testu prywatności** w procesie tworzenia prawa, w tym **oceny skutków dla ochrony danych** – art. 25 ust. 1 [10] rozporządzenia 2016/679, tj. przy określaniu sposobów przetwarzania, jak i art. 35 (w

[10] Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

szczególności ust. 1 [11] i ust. 10 [12]), tj. w związku z przyjmowaniem podstawy prawnej przetwarzania.

Jednocześnie pragnę podkreślić, że uwagi organu nadzorczego przedstawiane w toku prac legislacyjnych mają charakter eksperckich wskazówek dla projektodawcy, który podejmuje decyzję co do ostatecznego kształtu przyjmowanych przepisów i odpowiada za zapewnienie ich zgodności z przepisami o ochronie danych osobowych.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych

/ - dokument w postaci elektronicznej podpisany kwalifikowanym podpisem elektronicznym/

[11] Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

[12] Ust. 1–7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.