PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa,

DPNT.401.41.2026

Pan
Dariusz Standerski
Sekretarz Stanu
w Ministerstwie Cyfryzacji

Szanowny Panie Ministrze,

w odpowiedzi na pismo z 6 lutego 2026 r. znak: DP.MC.0211.3.2026, działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1], art. 5 ust. 1 pkt 12 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[2] oraz art. 51 ustawy o ochronie danych osobowych[3], uprzejmie informuję, że do przedstawionego **projektu ustawy o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw (UC141)**, dalej: projekt, Prezes Urzędu Ochrony Danych Osobowych zgłasza następujące uwagi.

1. Uwagi ogólne.

Projektowane zmiany w ustawie o świadczeniu usług drogą elektroniczną[4] obejmują **dodanie rozdziału 2a**, który umożliwi stosowanie art. 9 rozporządzenia

[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.), dalej: rozporządzenie 2016/679.
[2] Ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206), dalej: ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.
[3] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).
[4] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2024 r. poz. 1513 ze zm.), dalej: ustawa o świadczeniu usług drogą elektroniczną.

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)[5]. Jak wskazuje się w uzasadnieniu do projektu, w prawie polskim nie istnieje szczególna podstawa prawna, która umożliwiałaby złożenie wniosku do sądu lub organu administracji publicznej o wydanie nakazu podjęcia działań przeciwko nielegalnym treściom udostępnianym w Internecie[6]. Należy zgodzić się z tezą projektodawcy, że „brak szczególnej procedury do wydawania nakazów w projekcie ustawy spowoduje, że ochrona prawna obywateli Rzeczypospolitej Polskiej będzie słabsza niż obywateli innych państw członkowskich Unii Europejskiej.”. Praktyka pokazuje, że **skuteczna ochrona prawna użytkowników, w tym obywateli przed nielegalnymi treściami w Internecie jest jednym z istotnych wyzwań naszego państwa**, deficytem w skutecznej ochronie praw podstawowych, a także problemem o skali globalnej.

Realizując swoje zadania Prezes Urzędu Ochrony Danych Osobowych (dalej: Prezes UODO) dostrzega szereg zjawisk związanych z przetwarzaniem danych osobowych w Internecie, które zagrażają osobom korzystającym z sieci. Należy się zgodzić z ekspertami, że do zagrożeń o największym ciężarze gatunkowym w cyberprzestrzeni należą te dotykające dzieci i młodzież, zwłaszcza polegające na wykorzystywaniu w kontekście seksualności oraz niegodziwym traktowaniu w celach seksualnych[7]. Korzystanie z Internetu i narzędzi cyfrowych przez małoletnich wiąże też z ryzykami wystąpienia uzależnień, w tym od pornografii[8] czy nawet hazardu internetowego[9]. Eksperci podkreślają także, iż samo używanie telefonów komórkowych i innych indywidualnych urządzeń cyfrowych przez dzieci może powodować uzależnienia i negatywny wpływ na ich zdrowie[10].

---

[5] 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) (Dz. Urz. UE L 277 z 27.10.2022, str. 1 oraz Dz. Urz. UE L 163 z 29.06.2023, str. 107), dalej: rozporządzenie 2022/2065.

[6] Do wyjątków należą:

a) art. 53 ustawy z dnia 12 lipca 2024 r. - Prawo komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1221 oraz z 2025 r. poz. 637 i 820),
b) art. 32c ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. 2025 r. poz. 902 i 1366 oraz z 2026 r. poz. 26) (wdrożenie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym),
c) ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1803);
d) art. 47t ustawy z dnia 29 grudnia 1992 r. o radiofonii i telewizji (Dz. U. z 2022 r. poz. 1722).

[7] Zob. K. Staciwa, *Wykorzystywanie seksualne dzieci w cyberprzestrzeni*, Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy we współpracy z Instytutem Wymiaru Sprawiedliwości, Warszawa. 2023, s. 8, https://www.nask.pl/media/2024/10/Wykorzystywanie-seksualne-dzieci-raport.pdf

[8] Zob. Dezyderat nr 1/5 Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii oraz Komisji do Spraw Dzieci i Młodzieży do Rady Ministrów w sprawie podjęcia działań zmierzających do przeciwdziałania uzależnieniu dzieci i młodzieży od gier oferujących mechanizmy monetyzacji oraz od gier hazardowych w środowisku internetowym uchwalony na wspólnym posiedzeniu w dniu 18 grudnia 2025 r., https://orka.sejm.gov.pl/opinie10.nsf/nazwa/dim_d5/$file/dim_d5.pdf

[9] Zob. R. Lange (red) , M. Błażej, F. Kopczyński, A. Łada, *Nastolatki wobec pornografii cyfrowej. Trajektorie użytkowania, Raport z badań ogólnopolskich* , NASK-PIB, Warszawa, 2022, https://www.nask.pl/magazyn/nastolatki-wobec-pornografii-cyfrowej-trajektorie-uzytkowania-raport

[10] Zob. petycja „Ratuj dzieci!” Instytutu Spraw Obywatelskich stanowiąca apel wielu specjalistów z zakresu także psychologii i psychiatrii dotyczący ograniczeń w korzystaniu z urządzeń elektronicznych (https://instytutsprawobywatelskich.pl/ratuj-dzieci/).

W ostatnim czasie analizując zagrożenia dla osób fizycznych w sieci Prezes UODO ze szczególnym niepokojem monitoruje **zjawisko wykorzystania technologii deepfake**[11] jako przykład wykorzystania technologii zmierzających do naruszania prywatności oraz nielegalnego przetwarzania danych osób korzystających z Internetu. Przypadki nadużyć spowodowanych stosowaniem technologii deepfake zgłaszane do Prezesa Urzędu Ochrony Danych Osobowych, a także analiza aktualnych regulacji prawnych uwidoczniły braki w prawie krajowym, które w ocenie organu ochrony danych osobowych wymagają pilnego wypracowania i wdrożenia rozwiązań o charakterze systemowym, w tym przyjęcia regulacji przeciwdziałających szkodliwemu wykorzystaniu tej technologii.

W kontekście bezpieczeństwa państwa polskiego należy podkreślić, że deepfake'i przyczyniają się do szerzenia zjawiska dezinformacji, przeciwdziałanie której jest szczególnie istotne i potrzebne w czasach podejmowanych różnych form ataków ze strony podmiotów i państw wrogo do Polski nastawionych. Zagrożenia tego nie można więc oceniać jedynie przez pryzmat ochrony jednostki, ale również w świetle ochrony żywotnego interesu państwa polskiego.

Na wskazane ryzyka Prezes UODO wielokrotnie zwracał uwagę, zarówno opiniując akty prawne, jak i kierując wystąpienia w trybie przepisów o ochronie danych osobowych. W szczególności w wystąpieniu do Ministra Cyfryzacji przekazanym do wiadomości Ministra Sprawiedliwości organ ochrony danych osobowych zwrócił się o rozważenie wprowadzenia rozwiązań ustawowych, które zapewnią skuteczną ochronę, w szczególności osobom fizycznym, przed negatywnym wpływem deepfake'ów.[12] Ponadto Prezes UODO omówił te problemy na posiedzeniu Komisji do Spraw Dzieci i Młodzieży Sejmu RP, rozpatrującej informacje na temat technologii deepfake w kontekście bezpieczeństwa dzieci i młodzieży, ochrony wizerunku oraz danych osobowych[13].

Jak wynika z pisma Ministerstwa Sprawiedliwości[14], sygnalizowany przez Prezesa UODO problem braku skutecznych narzędzi do zwalczania deepfake'ów jest obecnie analizowany w tym resorcie, który zwrócił się dodatkowo do Komisji Kodyfikacyjnej Prawa Karnego „z prośbą o wydanie opinii, czy obecne przepisy prawnokarne w wystarczający sposób penalizują kwestie rozpowszechniania deepfake'ów przy użyciu sztucznej inteligencji (np. poprzez art. 190a § 2-3, art. 202 § 4b k.k.) i czy niezbędne jest spenalizowanie nowego typu przestępstwa, a jeśli tak - zaproponowanie jego brzmienia".

---

[11] Termin „deepfake" został zdefiniowany w art. 3 pkt 60 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji), (Dz.U.UE.L.2024.1689), dalej jako „akt w sprawie sztucznej inteligencji" i oznacza on „wygenerowane przez sztuczną inteligencję (dalej również jako SI) lub zmanipulowane przez SI obrazy, treści dźwiękowe lub treści wideo, które przypominają istniejące osoby, przedmioty, miejsca, podmioty lub zdarzenia, które odbiorca mógłby niesłusznie uznać za autentyczne lub prawdziwe".

[12] Zob. wystąpienie Prezesa UODO z 13 września 2025 r, DPNT.413.31.2025, dostępne na stronie internetowej: https://uodo.gov.pl/pl/138/3886

[13] Zob. zapis przebiegu posiedzenia Komisji do Spraw Dzieci i Młodzieży Sejmu RP która odbyła się 17 grudnia 2025 r. : https://www.sejm.gov.pl/sejm10.nsf/biuletyn.xsp?skrnr=DIM-47.

[14] Pismo Pana Arkadiusza Myrchy, Sekretarza Stanu w Ministerstwie Sprawiedliwości z 23 stycznia 2026 r., stanowiące odpowiedź na wystąpienie Prezesa UODO dotyczące problematyki deepfake skierowane do Ministerstra Cyfryzacji, a przekazane również do wiadomości Ministra Sprawiedliwości (Znak:DPK-I.40.4.2026).

Prezes UODO apeluje zatem by procedowane niniejszym projektem tworzone rozwiązania zostały zsynchronizowane z innymi projektowanymi rozwiązaniami, które mają się przyczynić się do zwalczania nielegalnych deepfake'ów.

Jednocześnie w ocenie Prezesa UODO nawet wypracowanie odpowiednich rozwiązań karnoprawnych w przepisach Kodeksu karnego[15], bez skutecznej procedury usuwania nielegalnych danych z Internetu, nie spełni jednego z podstawowych celów jakimi powinien kierować się polski ustawodawca, czyli **ochrony prawa do prywatności i dóbr osobistych osób dotkniętych deepfake'ami**. Z tego powodu – oprócz odpowiednich sankcji penalizujących czyny stanowiące zagrożenia dla prywatności oraz wiążące się z nielegalnym przetwarzaniem danych osobowych w Internecie – projektowane przepisy będą miały kluczowe znaczenie dla praktycznej i skutecznej ochrony przed takimi zagrożeniami wobec osób fizycznych, w tym przede wszystkim dzieci i młodzieży.

2. Test prywatności.

Analiza projektowanych przepisów wskazuje, że dla ich realizacji będą przetwarzane – w tym **z użyciem nowych technologii** (w związku z monitorowaniem Internetu) – w znacznej ilości oraz na ogromną skalę dane osobowe podmiotów danych będących osobami fizycznymi których dane będą przetwarzane w związku z procedurami kontroli i usuwania nielegalnych treści z Internetu.

Będą to zarówno tzw. **dane zwykłe**, mogące jednak dotyczyć **szczególnie wrażliwych dla prywatności i istotnej życiowo problematyki spraw w związku z postępowaniami prokuratorskimi i sprawami sądowymi**, jak i dane wprost w przepisach prawa określone jako **szczególne kategorie danych** objęte ochroną na postawie art. 9 ust. 1 rozporządzenia 2016/679[16], np. dane dotyczące poglądów politycznych, dane światopoglądowe, dane dotyczące zdrowia, dane biometryczne (dane pozyskane w ramach weryfikacji osób uczestniczących w rozpatrzeniu wniosków i wydawaniu decyzji w projektowanej procedurze, fotografie załączone do wniosków, dane ofiar przestępstw przetwarzane w projektowanej procedurze).

Projektowane zmiany – w związku z przetwarzaniem w procedurze danych potencjalnych sprawców przestępstw – z samej swojej istoty mogą wiązać się z przetwarzaniem na ogromną skale informacji dotyczących danych podlegających wzmocnionemu reżimowi ochrony w rozumieniu art. 10 rozporządzenia 2016/679[17]. Będą to dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych

[15] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2025 r. poz. 383 ze zm.).

[16] Zgodnie z art. 9 ust. 1 rozporządzenia 2016/679 zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

[17] Zgodnie z art. 10 rozporządzenia 2016/679 przetwarzania danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

środków bezpieczeństwa. Jednocześnie oprócz ww. danych, na podstawie projektowanej ustawy będą przetwarzane także **dane objęte tajemnicami prawnie chronionymi**, których przetwarzanie podlega wzmocnionej ochronie prawnej.

To oznacza, że przetwarzanie danych powinno być nie tylko **zgodne ze standardami i zasadami dotyczącymi przetwarzania danych osobowych ukształtowanymi mocą art. 5 rozporządzenia 2016/679**[18], ale i **objęte testem prywatności wraz z oceną skutków dla ochrony danych** (art. 25 [19] oraz art. 35 ust. 1 rozporządzenia 2016/679[20]). Pozwoliłoby to m.in. zbadać, czy projektowane przepisy – zgodnie z art. 6 ust. 3 z rozporządzenia 2016/679 – są proporcjonalne i zawierają gwarancje odpowiednie do *ratio legis* projektu. Istotne jest zatem, aby projektowane przepisy zapewniły stosowanie norm ogólnego rozporządzenia o ochronie danych dla realizacji proponowanych rozwiązań i były przeanalizowane z uwzględnieniem ryzyk towarzyszących operacjom przetwarzania takich danych osobowych, bez obniżenia

[18] Zgodnie z art. 5 ust. 1 rozporządzenia 2016/679 dane osobowe muszą być: a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość"); b) 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 ("ograniczenie celu"); c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych"); d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość"); e) 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 ("ograniczenie przechowywania"); f) 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 ("integralność i poufność"). Zgodnie z art. 5 ust. 2 rozporządzenia 2016/679 Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność").

[19] Ust. 1 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 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.
2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych. 3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42.

[20] 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.

standardów wynikających z ogólnego rozporządzenia, a tym samym zapewniały gwarancje wynikające z przepisów dotyczących przetwarzania danych osobowych, m.in. co do realizacji praw i wolności osób, których dane dotyczą (podmiotów danych). Szczególną uwagą projektodawcy powinien być objęty sposób przetwarzania danych osobowych w ramach tworzonej procedury wydania nakazu podjęcia działań przeciwko nielegalnym treściom udostępnianym w Internecie oraz sposób kontroli osób zaangażowanych w proces rozpatrywania wniosków w tych sprawach co do ich bezstronności. Projektodawca powinien bowiem ocenić czy projektowane rozwiązania ustawy nie powinny zostać rozbudowane tak, by w pełni realizowały zasady ochrony danych osobowych (art. 5 rozporządzenia 2016/679), a także zawierały rozwiązania gwarantujące środki ochrony praw i wolności osób, których dane dotyczą zgodnie z przepisami tego aktu.

3. Zakres czynów zabronionych objętych możliwością nakazu podjęcia działań przeciwko nielegalnym treściom polegającego na uniemożliwieniu dostępu do nielegalnych treści.

Projekt ustawy uprawnia prokuratora, Policję, organ Krajowej Administracji Skarbowej, Straż Graniczną w zakresie przestępstwa określonego w art. 189a Kodeksu karnego (handel ludźmi), usługobiorcę oraz zaufany podmiot sygnalizujący do złożenia wniosku o wydanie nakazu podjęcia działań przeciwko nielegalnym treściom polegającego na uniemożliwieniu dostępu do nielegalnych treści występujących w usłudze świadczonej przez dostawcę usług pośrednich, których rozpowszechnianie może wyczerpywać znamiona czynu zabronionego, a także pochwalających lub nawołujących do popełnienia czynu zabronionego. W projektowanym **art. 11a** ustawy o świadczeniu usług drogą elektroniczną enumeratywnie wymienione zostały czyny zabronione, których ma dotyczyć procedura nakazowa. Jak podkreślono w uzasadnieniu projektu, kryteria, które zostały przyjęte przy odesłaniu do konkretnych czynów zabronionych są trzy:

1) zakwalifikowanie danego przestępstwa jako przestępstwa internetowego rozumianego jako przestępstwo związane z internetem według sposobu działania (modus operandi) sprawcy;
2) związek przestępstwa z rozpowszechnianiem treści;
3) brak negatywnych skutków dla dyskursu obywatelskiego i procesów wyborczych z powodu pozbawienia dostępu do treści.

Nie kwestionując przyjętych przez projektodawcę założeń, Prezes UODO zwraca uwagę na **poważną lukę** jaką jest brak w projektowanym katalogu czynów zabronionych w postaci przestępstwa nielegalnego przetwarzanie danych osobowych (art. 107 ustawy o ochronie danych osobowych[21]) oraz przestępstwa niedopuszczalnego lub

[21] Zgodnie z art. 107 ustawy o ochronie danych osobowych, „1.Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.
2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby

nieuprawnionego przetwarzania danych osobowych (art. 54 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[22]). Oba te czyny mogą wiązać się z poważnym ryzykiem wykorzystania przez sprawcę pozyskanych danych osoby fizycznej i dalszego ich nielegalnego przetwarzania, w tym upublicznienia lub przesyłania tych danych za pośrednictwem Internetu.

W ocenie organu nadzorczego w przypadku prowadzenia postepowań na podstawie wskazanych przepisów karnych organy ścigania powinny mieć możliwość wykorzystania projektowanego mechanizmu umożliwiającego uruchomienie procedury zastosowania nakazu podjęcia działań przeciwko nielegalnym treściom polegającego na uniemożliwieniu dostępu do nielegalnych treści – co w sposób zasadniczy zwiększyłoby skuteczną ochronę ofiar przestępstwa.

Przykładem obrazującym konieczność podejmowania takich działań w przypadku nielegalnego przetwarzania danych osobowych za pośrednictwem Internetu może być sprawa dotycząca wygenerowania przez uczniów szkoły podstawowej fałszywego zdjęcia nagiej koleżanki oraz zachęcania innych osób do jego „zamawiania" na platformie Instagram. W tej sprawie Prezes UODO zawiadomił organy ścigania o możliwości popełnienia przestępstwa[23].

Biorąc pod uwagę powyższe, **Prezes UODO wnosi o rozszerzenie wskazanego w art. 11a ustawy o świadczeniu usług drogą elektroniczną katalogu czynów zabronionych objętych możliwością nakazu podjęcia działań przeciwko nielegalnym treściom polegającego na uniemożliwieniu dostępu do nielegalnych treści o art. 107 ustawy o ochronie danych osobowych i art. 54 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.**

Jednocześnie Prezes UODO ponownie sygnalizuje konieczność zapewnienia zgodności przepisów projektu z innymi tworzonymi w ramach projektowanych aktów prawnych rozwiązań, mających chronić prywatność i dane osobowe w sieci internetowej, w szczególności mającymi przyczynić się do zwalczania nielegalnych deepfake'ów.

---

fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.".

[22] Zgodnie z art. 54 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości „1. Kto przetwarza dane osobowe, o których mowa w przepisach o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

2. Jeżeli czyn określony w ust. 1 dotyczy danych wrażliwych, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.".

[23] Zob. Komunikat UODO dot. tej sprawy dostępny jest pod linkiem: https://uodo.gov.pl/pl/138/4041.

4. **Przetwarzanie danych osób uczestniczących w rozpatrzeniu wniosków w procedurze wydania nakazu podjęcia działań przeciwko nielegalnym treściom.**

Zgodnie z projektowanym **art. 11c** ustawy o świadczeniu usług drogą elektroniczną, „Osoby uczestniczące w rozpatrzeniu wniosków, o których mowa w art. 11a ust. 1 i 2, w szczególności poprzez wydawanie w imieniu właściwego organu na podstawie upoważnienia decyzji nie mogą należeć do partii politycznej, publicznie manifestować poglądów politycznych, ani prowadzić działalności publicznej niedającej się pogodzić z zasadami bezstronności, rzetelności i politycznej neutralności.”.

Prezes UODO nie kwestionuje celu przedmiotowego przepisu, który ma gwarantować bezstronność, rzetelność i polityczną neutralność wydawania nakazów podjęcia działań przeciwko nielegalnym treściom. Należy jednak zwrócić uwagę, że z projektowanych rozwiązań nie wynika w jaki sposób i w jakim zakresie, a także kto konkretnie będzie badany na okoliczność przynależności do partii politycznej czy manifestowania lub prowadzenia działalności niedających się pogodzić z wskazanymi w przepisie zasadami. Przedmiotowe informacje w istocie stanowią dane osobowe ujawniające poglądy polityczne i światopoglądowe i jako takie stanowią **szczególne kategorie danych** objęte szczególnym reżimem przetwarzania, w tym ochroną na postawie art. 9 rozporządzenia 2016/679. Przetwarzanie takich danych musi się więc odbywać w sposób proporcjonalny do wyznaczonego celu, nie naruszając istoty prawa do ochrony danych. Przepisy, na podstawie których takie dane będą przetwarzane muszą przewidywać odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Biorąc pod uwagę powyższe w świetle zasady zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a rozporządzenia 2016/679) projektodawca powinien rozbudować projektowany art. 11c ustawy o świadczeniu usług drogą elektroniczną tak, by z przepisu tego wynikało w jaki konkretny sposób będą przetwarzane dane osób uczestniczących w rozpatrzeniu wniosków w procedurze wydania nakazu podjęcia działań przeciwko nielegalnym treściom na okoliczność spełnienia wymagań określonych w tym przepisie (przy uregulowaniu w tym przepisie konkretnych środków ochrony praw podstawowych i interesów tych osób).

5. **Decyzja w procedurze wydania nakazu podjęcia działań przeciwko nielegalnym treściom w Internecie.**

5.1. W projektowanym **art. 11m ust. 3** ustawy o świadczeniu usług drogą elektroniczną wskazano, że „Właściwy organ publikuje na stronie internetowej urzędu obsługującego ten organ w całości treść decyzji, o której mowa w ust. 1, z tym że publikacja uzasadnienia nie obejmuje informacji prawnie chronionych. Publikacja opatrzona jest informacją, czy decyzja jest prawomocna.”.

Prezes UODO, kierując się zasadą zgodności z prawem, rzetelności i przejrzystości, wnosi o uzupełnienie przedmiotowego przepisu o jednoznaczne wskazanie, że w publikowanej decyzji nie będą zamieszczane dane osób fizycznych. Jeżeli jednak celowe

jest by w opublikowanej na stronie internetowej urzędu decyzji znajdowały się także dane osobowe projektodawca powinien rozbudować art. 11m ust. 3 ustawy o świadczeniu usług drogą elektroniczną i wskazać jakie dane osób fizycznych będą zamieszczane na stronie internetowej urzędu. Zgodnie z zasadami ograniczenia celu (art. 5 ust. 1 lit. b) i minimalizacji danych (art. 5 ust. 1 lit. c rozporządzenia 2016/679) dane te muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których będą przetwarzane. W świetle zasady ograniczenia przechowania (art. 5 ust. 1 lit. e rozporządzenia 2016/679) przepis powinien również wskazywać retencję danych, w tym okres, po którym dane te będą usuwane.

5.2. Zgodnie z projektowanym **art. 11n** ustawy o świadczeniu usług drogą elektroniczną „decyzji, o której mowa w art. 11m ust. 1, nie nadaje się rygoru natychmiastowej wykonalności.”. Jak wskazuje projektodawca w uzasadnieniu: „Decyzji nie można nadać rygoru natychmiastowej wykonalności. Brak możliwości zastosowania rygoru natychmiastowej wykonalności w przypadku wydania nakazu uniemożliwienia dostępu do nielegalnej treści jest uzasadniony zapewnieniem skuteczniejszej kontroli sądowej decyzji podejmowanych przez Prezesa UKE lub Przewodniczącego Krajowej Rady Radiofonii i Telewizji. Takie rozwiązanie jest korzystne dla autora zakwestionowanej treści, daje bowiem czas na wniesienie sprzeciwu do sądu powszechnego, bez ponoszenia negatywnych konsekwencji związanych z wykonaniem decyzji administracyjnej. Analogicznie do wydanej decyzji w zakresie usunięcia ograniczeń nałożonych przez dostawcę usług pośrednich na usługobiorcę, proponowany przepis umożliwi wniesienie sprzeciwu od decyzji bez konieczności wykonania jej przed rozstrzygnięciem sądu.”.

Prezes UODO zwraca także uwagę, że w przypadku niektórych czynów zabronionych określonych w projektowanym **art. 11a** ustawy o świadczeniu usług drogą elektroniczną skutki nadużyć związanych z ujawnieniem w Internecie określonych informacji są niezwykle dotkliwe i natychmiastowe (zwłaszcza gdy ofiarami są osoby małoletnie czy nieporadne). Zaproponowana w projekcie kontrola sądowa decyzji podejmowanych przez Prezesa UKE lub Przewodniczącego Krajowej Rady Radiofonii i Telewizji przy braku rygoru natychmiastowej wykonalności ma oczywiście swoje uzasadnienie, jednakże w praktyce może znacznie wydłużać procedury dotyczące usuwania skutków naruszenia prawa. W wielu sytuacjach może to prowadzić do nieodwracalnych konsekwencji dla ofiary przestępstwa (w tym nawet do poważnych kryzysów psychicznych i suicydalnych osób, których dane są ujawniane przez przestępców, np. dokonywanych przez dzieci, których wyłudzone lub spreparowane technologią deepfake’ nagie zdjęcia zostaną rozpowszechnione przez Internet i media społecznościowe).

Z tego powodu Prezes UODO poddaje pod rozwagę, by w przypadku zagrożeń o największym ciężarze gatunkowym w cyberprzestrzeni, do których należą te dotykające dzieci i młodzież, zwłaszcza polegających na wykorzystywaniu w kontekście seksualności oraz niegodziwym traktowaniu w celach seksualnych, projektodawca rozważył wprowadzenie odrębnego trybu postępowania w tworzonej procedurze i możliwości niezwłocznego blokowania nielegalnych treści. Pod rozwagę projektodawcy organ

nadzorczy poddaje zatem, czy w ramach proponowanego trybu usuwania treści z Internetu, w wybranych wyjątkowych kategoriach spraw decyzje Prezesa UKE lub Przewodniczącego Krajowej Rady Radiofonii i Telewizji nie powinny uzyskiwać jednak rygoru natychmiastowej wykonalności i podlegać wówczas następczej, a nie uprzedniej, kontroli sądowej.

Uwagi Prezesa UODO 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. Wyrażam nadzieję, że uwzględnienie powyższych wskazówek będzie pomocne w tym procesie i przyczyni się do podwyższenia poziomu ochrony danych osobowych w projektowanych przepisach.

Łączę wyrazy szacunku,

Mirosław Wróblewski

Prezes Urzędu Ochrony Danych Osobowych