



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

Analiza rozporządzenia Parlamentu Europejskiego i Rady (UE) 2026/1881 z dnia 24 lipca 2026 r. w sprawie tymczasowego odstępstwa od niektórych przepisów dyrektywy 2002/58/WE w odniesieniu do wykorzystywania technologii przez dostawców usług łączności interpersonalnej niewykorzystujących numerów do przetwarzania danych osobowych i innych danych do celów niegodziwego traktowania dzieci w celach seksualnych w internecie

Słowniczek pojęć

- **Chat Control 1.0** — potoczne określenie przejściowej regulacji unijnej przewidującej ograniczenie prywatności użytkowników różnych mediów i komunikatorów internetowych poprzez upoważnienie dostawców tych usług do dobrowolnego skanowania (zob. poniżej) treści postów i wiadomości pod kątem występowania materiałów CSAM (zob. poniżej) i nagabywania dzieci w celach seksualnych wprowadzonej rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/1232 z dnia 14 lipca 2021 r. w sprawie tymczasowego odstępstwa od niektórych przepisów dyrektywy 2002/58/WE w odniesieniu do wykorzystywania technologii przez dostawców usług łączności interpersonalnej niewykorzystujących numerów do przetwarzania danych osobowych i innych danych do celów zwalczania niegodziwego traktowania dzieci w celach seksualnych w internecie, obowiązującej od 2 sierpnia 2021 r. do 3 sierpnia 2024 r., a po przedłużeniu rozporządzeniem (UE) 2024/1307, do 3 kwietnia 2026 r.
- **Chat Control 2.0** — potoczne określenie projektowanej, stałej regulacji unijnej, która ma zastąpić obecne, tymczasowe rozwiązanie (Chat Control 1.0). Kluczowa różnica polega na tym, że o skanowaniu (zob. poniżej) wiadomości nie decydowałby już sam dostawca usługi, lecz niezależny organ krajowy, wydając w tej sprawie formalną decyzję, którą można by zaskarżyć do sądu. Nad projektem tej regulacji, przedstawionym przez Komisję Europejską w maju 2022 r., wciąż trwają prace, które jak dotąd nie zostały zakończone.
- **CSAM (ang. *child sexual abuse material*)** — materiały przedstawiające niegodziwe traktowanie dzieci w celach seksualnych w internecie, obejmujące zgodnie z art. 2 rozporządzenia zarówno pornografię dziecięcą, jak i przedstawienie pornograficzne w rozumieniu dyrektywy 2011/93/UE. Odrębną kategorię prawną stanowi nagabywanie dzieci w celach seksualnych, które również jest zakazane;



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

- **Dobrowolne skanowanie** — mechanizm umożliwiający dostawcy usługi na wgląd do rozmów użytkownika w ramach danej platformy (skrzynki mailowej, komunikatora internetowego) w celu weryfikacji, czy ich przedmiotem nie są materiały CSAM lub nagabywanie dzieci w celach seksualnych (art. 3 ust. 1 lit. a pkt (ii)) . Skanowanie jest dobrowolne, co oznacza, że dostawca może, ale nie musi wprowadzić takie rozwiązanie – jeśli się na nie zdecyduje, musi o tym powiadomić wszystkich użytkowników, że ich prywatna korespondencja może być przeglądana pod tym kątem.
- **Szyfrowanie end-to-end (E2EE)** — metoda ochrony komunikacji, w której wiadomość jest szyfrowana na urządzeniu nadawcy i odszyfrowywana dopiero na urządzeniu odbiorcy, tak że żaden podmiot pośredniczący, w tym dostawca usługi, nie ma technicznej możliwości zapoznania się z jej treścią. Metoda ta jest stosowana m.in. przez aplikacje Signal czy WhatsApp, w przeciwieństwie do Gmaila czy Outlooka. Rozporządzenie posługuje się w tym zakresie terminem „pełne szyfrowanie transmisji” (art. 1 ust. 3).
- **Haszowanie** — technologia polegająca na porównywaniu zdjęć i filmów z bazą danych zweryfikowanych, znanych materiałów.

Wprowadzenie

Przedmiotem niniejszej analizy jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2026/1881 z dnia 24 lipca 2026 r. w sprawie tymczasowego odstępstwa od niektórych przepisów dyrektywy 2002/58/WE w odniesieniu do wykorzystywania technologii przez dostawców usług łączności interpersonalnej niewykorzystujących numerów do przetwarzania danych osobowych i innych danych do celów niegodziwego traktowania dzieci w celach seksualnych w internecie, (dalej: rozporządzenie)¹. Ten akt prawny UE ma na celu przywrócenie, z pewnymi zmianami, głównych założeń rozporządzenia (UE) 2021/1232 z 14 lipca 2021 roku² (dalej: rozporządzenie Chat Control 1.0.), które po przedłużeniu okresu jego

¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2026/1881 z dnia 24 lipca 2026 r. w sprawie tymczasowego odstępstwa od niektórych przepisów dyrektywy 2002/58/WE w odniesieniu do wykorzystywania technologii przez dostawców usług łączności interpersonalnej niewykorzystujących numerów do przetwarzania danych osobowych i innych danych do celów niegodziwego traktowania dzieci w celach seksualnych w internecie (Tekst mający znaczenie dla EOG); <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32026R1881>, dostęp: 12 sierpnia 2026.

² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1232 z dnia 14 lipca 2021 r. w sprawie tymczasowego odstępstwa od niektórych przepisów dyrektywy 2002/58/WE w odniesieniu do wykorzystywania technologii przez dostawców usług łączności interpersonalnej niewykorzystujących numerów do przetwarzania danych osobowych i innych danych do celów zwalczania niegodziwego traktowania dzieci w celach seksualnych w internecie (Tekst mający znaczenie dla EOG); <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32021R1232>, dostęp: 23 lipca 2026.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

stosowania rozporządzeniem (UE) 2024/1307³ do dnia 3 kwietnia 2026 roku wygaśło wraz z upływem tego terminu, jako że Parlamentowi Europejskiemu i Radzie nie udało się osiągnąć kolejnego porozumienia w tym względzie⁴.

Istotą omawianej regulacji jest umożliwienie dostawcom poczty elektronicznej i komunikatorów internetowych dobrowolnego skanowania korespondencji użytkowników w celu wykrywania materiałów przedstawiających seksualne wykorzystywanie dzieci⁵. Skanowanie to polega na automatycznym porównywaniu zdjęć i filmów z bazami znanych materiałów CSAM (*child sexual abuse material*, materiały przedstawiające niegodziwe traktowanie dzieci w celach seksualnych) za pomocą tzw. technologii haszowania, albo na analizie tekstu lub danych o ruchu przy użyciu klasyfikatorów i systemów sztucznej inteligencji w celu wykrywania nowych materiałów CSAM lub wzorców wskazujących na nagabywanie dzieci. Opisywane rozwiązanie, choć służy ochronie fundamentalnego dobra, budzi zarazem poważne wątpliwości co do zgodności z prawem do poszanowania życia prywatnego oraz ochrony danych osobowych, gwarantowanymi w art. 7 i art. 8 Karty praw podstawowych Unii Europejskiej⁶. Niniejsza analiza przedstawia charakter prawny i mechanizm działania regulacji, a następnie ocenia ją w świetle standardów wynikających z orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej oraz stanowisk organów ochrony danych, ważąc argumenty przemawiające za regulacją i przeciw niej. W kontekście problematyki poruszanej w niniejszej pracy warto jednocześnie zaznaczyć, iż aktualnie toczą się prace nad przyjęciem docelowej regulacji, określanej potocznie jako „Chat Control 2.0”⁷.

1. Charakter prawny i geneza regulacji

Analizowana regulacja przyjęła formę rozporządzenia w rozumieniu art. 288 TFUE⁸, a więc aktu wiążącego w całości i bezpośrednio stosowanego we wszystkich państwach członkowskich, niewymagającego transpozycji. Jej *ratio legis* jest przywrócenie, wraz ze zmianami, wygaśłego

³ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1307 z dnia 29 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) 2021/1232 w sprawie tymczasowego odstępstwa od niektórych przepisów dyrektywy 2002/58/WE w odniesieniu do wykorzystywania technologii przez dostawców usług łączności interpersonalnej niewykorzystujących numerów do przetwarzania danych osobowych i innych danych do celów zwalczania niegodziwego traktowania dzieci w celach seksualnych w internecie, Dz.Urz. UE L, 2024/1307 z 14.5.2024; <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R1307>, dostęp: 24 lipca 2026.

⁴ Motyw 12 dok. Rady ST-11703/26 (przyp. 2).

⁶ Karta praw podstawowych Unii Europejskiej, Dz.Urz. UE C 326 z 26.10.2012; <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:12012P/TXT>, dostęp: 23 lipca 2026.

⁷ Proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM/2022/209 final; <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0209>, dostęp: 13 sierpnia 2026.

⁸ Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana), Dz.Urz. UE C 202 z 7.6.2016; <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:12016E/TXT>, dostęp: 23 lipca 2026.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

odstępstwa od zasady poufności w komunikacji, ustanowionego wcześniej rozporządzeniem Chat Control 1.0. Nie stanowi ona jednak samodzielnej, ogólnej podstawy prawnej do przetwarzania danych osobowych w rozumieniu rozporządzenia o ochronie danych osobowych (RODO)⁹, lecz ustanawia wyłącznie czasowe i ściśle ograniczone odstępstwo od art. 5 ust. 1 i art. 6 ust. 1 tzw. dyrektywy ePrivacy¹⁰, chroniącej poufność komunikacji elektronicznej i danych o ruchu¹¹.

Szerszym tłem dla rozporządzenia 2021/1232, jak i aktualnego rozporządzenia, jest problem rozpowszechniania w internecie materiałów CSAM, a także nagabywania dzieci przez sprawców w celach seksualnych. Terminy te zdefiniowano w art. 2 pkt 2 rozporządzenia, odsyłając w tym zakresie do słowniczka legalnego dyrektywy 2011/93/UE¹². Materiały CSAM obejmują pojęcia „pornografii dziecięcej” (art. 2 lit. c dyrektywy) oraz „przedstawienia pornograficznego” (art. 2 lit. e dyrektywy): pierwsze z nich obejmuje wszelkie materiały ukazujące dziecko, lub osobę wyglądającą na dziecko, uczestniczące w rzeczywistych lub symulowanych zachowaniach o wyraźnie seksualnym charakterze, przedstawienia organów płciowych dziecka w celach głównie seksualnych, a także realistyczne obrazy o takim charakterze, nawet jeśli nie przedstawiają rzeczywistego dziecka; drugie natomiast odnosi się do skierowanego do publiczności ukazywania na żywo, w tym za pośrednictwem technologii informacyjno-komunikacyjnych, dziecka uczestniczącego w takim zachowaniu lub jego organów płciowych. Nagabywanie dzieci (*solicitation of children*) zdefiniowano z kolei przez odesłanie do art. 6 tej samej dyrektywy, który penalizuje dwa odrębne czyny: składanie dziecku, które nie osiągnęło wieku przyzwolenia, za pośrednictwem technologii informacyjno-komunikacyjnych, propozycji spotkania w celu popełnienia przestępstwa seksualnego, jeżeli propozycji tej towarzyszyły czynności zmierzające do takiego spotkania, oraz usiłowanie nagabywania takiego dziecka w celu uzyskania od niego pornografii dziecięcej przedstawiającej to samo dziecko.

⁹ 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, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016R0679>, dostęp: 27 lipca 2026.

¹⁰ Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.Urz. UE L 201 z 31.7.2002, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32002L0058>, dostęp: 27 lipca 2026.

¹¹ Zgodnie z art. 2 lit. b dyrektywy 2002/58/WE „dane o ruchu” oznaczają wszelkie dane przetwarzane do celów przekazywania komunikatu w sieci łączności elektronicznej lub naliczania opłat za te usługi.

¹² Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW; <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32011L0093>, dostęp: 12 sierpnia 2026.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

Samo zjawisko rozpowszechniania materiałów CSAM w sieci należy odczytywać w kontekście postępującej cyfryzacji życia społecznego, w ramach której wraz z globalizacją usług internetowych coraz większa część ludzkiej aktywności przenosi się do środowiska cyfrowego¹³. Rozwój komunikatorów internetowych, poczty elektronicznej i innych usług łączności online stworzył nowe możliwości popełniania przestępstw wobec dzieci, jednocześnie otwierając nowe, wcześniej niedostępne drogi ich wykrywania i zwalczania.

Geneza rozporządzenia 2021/1232 sięga 2020 roku, kiedy nowa unijna dyrektywa, ustanawiająca Europejski kodeks łączności elektronicznej¹⁴, rozszerzyła definicję pojęcia „usługi łączności elektronicznej” tak, by objęła ona również komunikatory internetowe i pocztę elektroniczną, poddając je tym samym zasadom poufności i danych o ruchu¹⁵ wynikającym z art. 5 ust. 1 i art. 6 ust. 1 dyrektywy 2002/58/WE¹⁶, które wcześniej dotyczyły wyłącznie „usługi łączności elektronicznej” z dyrektywy ramowej 2002/21/WE¹⁷, w praktyce ograniczoną do usług polegających głównie na przekazywaniu sygnałów w sieciach telekomunikacyjnych. Rozstrzygnęło to trwający od lat spór o to, jak klasyfikować takie usługi, do którego odniósł się TSUE w sprawach Skype i Gmail¹⁸ ale jednocześnie pozbawiło dostawców dotychczasowej podstawy do dobrowolnego skanowania korespondencji w poszukiwaniu materiałów CSAM, opartej dotąd na ogólnych przepisach RODO. W odpowiedzi Parlament Europejski i Rada przyjęły 14 lipca 2021 r. rozporządzenie (UE) 2021/1232, pomyślane od początku jako rozwiązanie tymczasowe, mające obowiązywać do 3 sierpnia 2024 roku¹⁹. Termin jego stosowania przedłużono następnie do 3 kwietnia 2026 r., a kolejna próba przedłużenia, zgłoszona przez Komisję Europejską w grudniu 2025 r., nie została uzgodniona na czas, więc rozporządzenie po prostu wygasło²⁰. Ten sam wniosek Komisji był następnie procedowany w Parlamencie Europejskim, który 26 marca 2026 roku zamknął pierwsze czytanie, przyjmując

¹³ M. Rojszczak, Preventing the dissemination of child sexual abuse material (CSAM) with surveillance technologies: The case of EU Regulation 2021/1232 (2025) Computer Law & Security Review 56 2025, s. 1.

¹⁴ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/172 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona), Dz.Urz. UE L 321 z 17.12.2018; <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32018L172>, dostęp: 27 lipca 2026.

¹⁵ Zgodnie z art. 2 lit. b dyrektywy 2002/58/WE „dane o ruchu” oznaczają wszelkie dane przetwarzane do celów przekazywania komunikatu w sieci łączności elektronicznej lub naliczania opłat za te usługi.

¹⁶ Dyrektywa 2002/58/WE parlamentu europejskiego i rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej); <https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=celex:32002L0058>; dostęp: 12 sierpnia 2026.

¹⁷ Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa); <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32002L0021>, dostęp: 12 sierpnia 2026.

¹⁸ TSUE, wyrok z 5.06.2019, C-142/18, Skype Communications oraz TSUE, wyrok z 13.06.2019, C-193/18, Google (Gmail)

¹⁹ Art. 10 rozporządzenia 2021/1232.

²⁰ Motyw 12 dok. Rady ST-11703/26.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

stanowisko odrzucające go w całości.²¹ Rada przyjęła jednak własne stanowisko w pierwszym czytaniu 2 lipca 2026 roku, które zostało uzupełnione poprawkami Parlamentu Europejskiego w drugim czytaniu 9 lipca, co ukształtowało tekst rozporządzenia będącego przedmiotem niniejszej analizy..

W kontekście problematyki poruszanej w niniejszej analizie warto również pamiętać, że równolegle, od 2022 roku trwają prace nad docelową, stałą regulacją, określaną jako Chat Control 2.0²². Negocjacje międzyinstytucjonalne nad tym aktem toczą się od listopada 2023 roku, kiedy komisja LIBE przyjęła mandat do rozmów trójstronnych, zatwierdzony przez plenum 22 listopada tego roku²³. Według rejestru procedur legislacyjnych PE nadal oczekują one na formalne stanowisko Parlamentu w pierwszym czytaniu²⁴.

Rozporządzenie w pigułce:

- Wprowadza tymczasowe, fakultatywne odstępstwo od art. 5 ust. 1 i art. 6 ust. 1 dyrektywy 2002/58/WE, chroniących poufność komunikacji elektronicznej i danych o ruchu, pozwalając dostawcom na dobrowolne skanowanie korespondencji użytkowników, choć samo rozporządzenie nie nakłada na nich obowiązku takiego działania.
- Obejmuje dostawców poczty elektronicznej i komunikatorów internetowych, czyli tzw. usług łączności interpersonalnej niewykorzystujących numerów.
- Służy wykrywaniu materiałów CSAM oraz nagabywania dzieci i zgłaszaniu takich przypadków organom ścigania lub organizacjom działającym w interesie publicznym.
- Opiera się na dwóch rodzajach technologii: haszowaniu, czyli prostym porównywaniu zdjęć i filmów ze znaną bazą materiałów oraz klasyfikatorach sztucznej inteligencji, służących do analizy tekstu i danych o ruchu w poszukiwaniu nowych materiałów lub wzorców wskazujących na nagabywanie.
- Nie obejmuje komunikacji szyfrowanej metodą end-to-end, a więc komunikacji tekstowej i multimedialnej zabezpieczonej pełnym szyfrowaniem transmisji, takiej jak

²¹ *European Parliament, Child sexual abuse online: voluntary detection measures will not be extended*, <https://www.europarl.europa.eu/news/en/press-room/20260325IPR39207/child-sexual-abuse-online-voluntary-detection-measures-will-not-be-extended>,

²² Proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM/2022/209 final; <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0209>, dostęp: 27 lipca 2026.

²³ European Parliament, Legislative Observatory, Procedure File: 2022/0155(COD) – Combating child sexual abuse online, sekcja „Key events”; [https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2022/0155\(COD\)](https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2022/0155(COD)), dostęp: 27 lipca 2026.

²⁴ Tamże, sekcja „Basic information” (status: „Awaiting Parliament's position in 1st reading”), dostęp: 27 lipca 2026.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

np. tryb Secret Chats w aplikacji Telegram, ani komunikacji głosowej, a więc połączeń głosowych realizowanych za pośrednictwem komunikatorów internetowych, niezależnie od zastosowanego szyfrowania. Przewiduje zabezpieczenia w postaci nadzoru ludzkiego, mechanizmów odwoławczych, uprzedniej oceny skutków dla ochrony danych, ograniczenia przechowywania danych do 12 miesięcy czy obowiązku corocznej sprawozdawczości.

- Ma charakter tymczasowy i obowiązuje do 3 kwietnia 2028 roku, w oczekiwaniu na docelową i stałą regulację, określaną mianem Chat Control 2.0.

2. Zakres i warunki odstępowstwa

Rozporządzenie nie nakłada na dostawców poczty elektronicznej i komunikatorów internetowych obowiązku wdrożenia mechanizmów wykrywania materiałów CSAM i innych przejawów niegodziwego traktowania dzieci w internecie, lecz ustanawia jedynie fakultatywne i czasowe odstępowstwo od art. 5 ust. 1 i art. 6 ust. 1 dyrektywy 2002/58/WE, chroniących poufność komunikacji i danych o ruchu. Przywoływane przepisy zakazują, co do zasady, osobom innym niż użytkownicy słuchania, przechwytywania, przechowywania oraz stosowania innych form ingerencji w treść komunikacji, a także nakazują usuwanie lub anonimizację danych o ruchu, gdy nie są już potrzebne do przekazania komunikatu²⁵. Zgodnie z przedmiotową propozycją legislacyjną, z odstępowstwa będzie mógł skorzystać dostawca usługi łączności interpersonalnej niewykorzystującej numerów²⁶ (np. komunikatory internetowe), o ile spełni kumulatywnie warunki określone w art. 3 ust. 1 rozporządzenia: przetwarzanie musi być bezwzględnie konieczne wyłącznie do wykrywania i zgłaszania materiałów CSAM oraz nagabywania dzieci, proporcjonalne i ograniczone do technologii służących temu celowi, ograniczone do danych treści i powiązanych danych o ruchu oraz do tego, co bezwzględnie konieczne; zastosowana technologia ma odpowiadać aktualnemu stanowi wiedzy technicznej i być najmniej ingerująca w prywatność, a w zakresie skanowania tekstu — niepozwalająca na odtworzenie treści komunikatu, lecz jedynie na wykrycie wzorców; dostawca ma przeprowadzić uprzednią ocenę skutków dla ochrony danych i procedurę uprzednich konsultacji, a wykrywanie nagabywania ograniczyć do obiektywnych wskaźników ryzyka. Dostawcę ma ponadto obciążać szereg obowiązków proceduralnych — zapewnienia nadzoru ludzkiego, mechanizmów odwoławczych, informowania użytkowników oraz corocznej sprawozdawczości — a

²⁵ Motyw 16 dok. Rady ST-11703/26.

²⁶ Zgodnie z art. 2 pkt 7 dyrektywy 2018/1972 „usługa łączności interpersonalnej niewykorzystująca numerów” oznacza usługę łączności interpersonalnej, która nie łączy się z publicznie nadanymi zasobami numeracyjnymi, mianowicie numerem lub numerami z krajowych lub międzynarodowych planów numeracji, ani nie umożliwia połączenia z numerem lub numerami z krajowych lub międzynarodowych planów numeracji.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

przechowywanie danych dopuszczalne jest wyłącznie w ściśle określonych celach i nie dłużej niż 12 miesięcy.

Jak wskazano w rozdziale 2, uzasadnieniem wprowadzenia tego mechanizmu jest chęć przywrócenia stanu sprzed 21 grudnia 2020 roku, a więc sprzed objęcia usług OTT²⁷ ygorami dyrektywy 2002/58/WE. Sam prawodawca, w motywie 8 obecnie procedowanego tekstu, zdaje się częściowo dostrzegać słabość tej argumentacji, stwierdzając wprost, że ograniczenie prawa podstawowego (w tym przypadku prawa do poszanowania życia prywatnego i rodzinnego z art. 7 Karty oraz prawa do ochrony danych osobowych z art. 8 Karty) nie może być uzasadnione wyłącznie tym, że dostawcy stosowali określone technologie w czasie, gdy usługi te nie mieściły się jeszcze w definicji usług łączności elektronicznej²⁸. Rodzi to pytanie, które nie dotyczy legitymowanego celu regulacji, a więc ochrony dzieci przed niegodziwym traktowaniem, będącej, jak wykazano powyżej, celem bezspornie legitymowanym w rozumieniu prawa pierwotnego, lecz elementu legalności ingerencji w rozumieniu art. 8 ust. 2 EKPC, a więc tego, czy ingerencja jest „przewidziana przez ustawę”. Zastrzeżenie to nie dotyczy przy tym formalnej mocy prawnej samego rozporządzenia 2026/1881 jako takiego, jako bezpośrednio stosowany akt prawa unijnego, spełnia ono formalny wymóg „przewidzenia przez ustawę”. Wątpliwość, za Rojszczakiem, dotyczy czegoś innego: czy samo ustanowienie odstępstwa usuwa bezprawność praktyki, która mogła być pozbawiona ważnej podstawy prawnej jeszcze przed 2020 r., skoro przywrócenie bezprawnego stanu rzeczy trudno uznać za działanie zasługujące na aprobatę. Spór toczy się więc nie o legalność samego aktu, lecz o przekonującą argumentację, którym uzasadniono jego przyjęcie. Rzecz w tym, czy sama chęć odtworzenia stanu sprzed 2020 r. stanowi wystarczające uzasadnienie dla przyjęcia, że ingerencja ma ważną podstawę prawną, skoro odtwarzana w ten sposób praktyka mogła być pozbawiona takiej podstawy jeszcze przed tym okresem. Jak wskazuje M. Rojszczak, jeżeli praktyka skanowania korespondencji przez podmioty prywatne była w istocie pozbawiona odpowiedniej podstawy prawnej już przed wejściem w życie Europejskiego kodeksu łączności elektronicznej, co potwierdza orzecznictwo ETPC, zgodnie z którym każda ingerencja w tajemnicę korespondencji, niezależnie od technicznego sposobu jej dokonania, stanowi ingerencję wymagającą podstawy ustawowej, to przywrócenie tej praktyki nie usuwa źródłowej bezprawności, a jedynie przywraca ten bezprawny stan w nowej formie prawnej²⁹.

3. Poprawka o wyłączeniu komunikacji szyfrowanej *end to end*

²⁷ Usługi OTT (*over-the-top*) to nieformalny termin branżowy, oznaczający usługi świadczone przez internet niezależnie od operatora sieci telekomunikacyjnej.

²⁸ Motywy 2 i 9 dokumentu Rady ST-11703/26.

²⁹ M. Rojszczak, *Preventing the dissemination...*, s.6.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

Najistotniejszą zmianą wprowadzoną przez Parlament Europejski w drugim czytaniu jest wyłączenie z zakresu (wtedy projektu) rozporządzenia komunikacji, do której jest, była lub będzie stosowana metoda szyfrowania end-to-end (poprawka 30 do art. 1 oraz poprawki 26cp3, 31cp3, 6 i 21 do art. 3)³⁰. Uzasadnienie tej zmiany zawiera motyw 32, w którym wskazuje się, że szyfrowanie *end-to-end* stanowi istotne narzędzie gwarantujące bezpieczeństwo i poufność komunikacji użytkowników, w tym dzieci, a jego osłabienie mogłoby zostać wykorzystane przez podmioty działające w złej wierze, dlatego też żaden przepis rozporządzenia nie może być interpretowany jako zakazujący lub osłabiający takie szyfrowanie³¹.

Warto również zauważyć, że zmiana ta wpisuje się w linię orzeczniczą ETPC zapoczątkowaną wyrokiem w sprawie *Podchasov v. Rosja*, w którym Trybunał uznał, że nałożenie na dostawców obowiązku osłabienia szyfrowania w celu umożliwienia dostępu organów ścigania do treści komunikacji jest nieproporcjonalne i niekonieczne w społeczeństwie demokratycznym, ponieważ mechanizmy typu „backdoor” (czyli celowo wbudowane luki, umożliwiające dostęp do zaszyfrowanych danych z pominięciem standardowych zabezpieczeń) mogą być wykorzystywane nie tylko przez organy ścigania, lecz również przez przestępców, co narusza istotę prawa do prywatności³². Wyłączenie komunikacji szyfrowanej *end-to-end* z zakresu rozporządzenia można zatem odczytywać jako reakcję prawodawcy unijnego na ten standard oraz jako krok odpowiadający na obawy, które wobec osłabiania szyfrowania wyrażał Europejski Inspektor Ochrony Danych (EIOD) w lutym 2026 roku, rekomendując odpowiednie zabezpieczenia i zwracając uwagę na ryzyko związane ze skanowaniem po stronie klienta jako metodą jego obejścia³³. Warto jednocześnie mieć na względzie, iż przywoływane orzeczenie ETPC odnosiło się jednak wyłącznie do kwestii odszyfrowywania komunikacji E2EE, a więc uzasadnia samą poprawkę wyłączającą taką komunikację z zakresu rozporządzenia, nie przesądzając jednocześnie o proporcjonalności skanowania komunikacji, która nie jest objęta tą metodą szyfrowania (o czym w dalszej części niniejszej analizy).

Poprawka nie rozwiązuje jednak, a jedynie przesuw, centralny problem regulacji. Skanowaniu w dalszym ciągu podlegać będą wszystkie usługi nieszyfrowane metodą *end-to-end* (m.in. znaczna część poczty elektronicznej oraz część komunikatorów, np. Gmail czy standardowe tryby komunikacji w aplikacjach takich jak Telegram, który oferuje szyfrowanie typu *end-to-end*

³¹ Motyw 32 dokumentu Rady ST-11703/26

³² ETPC, wyrok z 13.02.2024 r., *Podchasov przeciwko Rosji*, skarga nr 33696/19, §§ 76–81.

³³ European Data Protection Supervisor, Opinion 7/2026 on the Proposal for a Regulation extending the application of Regulation (EU) 2021/1232, 16.02.2026, pkt 29; https://www.edps.europa.eu/system/files/2026-02/26-02-16_opinion-extending-application-regulation-2021-1232_en.pdf, dostęp: 28 lipca 2026.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

jako tryb opcjonalny), a więc korespondencja milionów użytkowników, którzy nie mają wpływu na wybór technologii szyfrowania stosowanej przez danego dostawcę. Co więcej, sam podział usług na szyfrowane i nieszyfrowane *end-to-end* bywa w praktyce płynny: jak pokazuje przykład Telegramu, ta sama aplikacja domyślnie stosuje szyfrowanie transportowe zarówno w czatach grupowych, jak i w komunikacji indywidualnej, oferując pełne szyfrowanie end-to-end jedynie jako opcjonalny tryb (tzw. Secret Chats), świadomie wybierany przez użytkownika³⁴. Wyłączenie szyfrowania E2EE osłabia więc najdalej idący zarzut o ryzyku „końca szyfrowania”, nie eliminując jednak zasadniczych wątpliwości dotyczących proporcjonalności blankietowego skanowania treści nieszyfrowanych, które pozostają przedmiotem rozważań następnego rozdziału.

4. Kwestia zgodności założeń projektu rozporządzenia z postanowieniami Karty Praw Podstawowych

Ocena zgodności mechanizmu skanowania z Kartą Praw Podstawowych UE wymaga w pierwszej kolejności rozstrzygnięcia kwestii, czy gwarancje art. 7 i 8 Karty, zawierające odpowiednio prawo do poszanowania życia prywatnego i komunikowania się oraz prawo do ochrony danych osobowych w ogóle znajdują zastosowanie do relacji między prywatnym dostawcą usług a użytkownikiem, jako że jej postanowienia wiążą wprost instytucje Unii oraz państwa członkowskie działające w zakresie stosowania prawa unijnego, a nie podmioty prywatne.

Po pierwsze, art. 51 ust. 1 Karty przesądza wprost, że jej postanowienia wiążą prawodawcę Unii przy stanowieniu prawa, a więc ocenie pod kątem zgodności z Kartą podlega w pierwszej kolejności sam akt unijny ustanawiający odstępstwo, a nie bezpośrednio działania konkretnego dostawcy usług³⁵.

Po drugie, niezależnie od tego, odpowiedzi na pytanie o standard oceny samego mechanizmu skanowania dostarcza koncepcja dostawcy jako „agenta państwa” (*agent of the state*)³⁶: skoro ostatecznym celem skanowania nie jest poprawa jakości usługi, lecz wykrycie przestępstwa i przekazanie informacji organom ścigania na podstawie ram prawnych ustanowionych przez prawodawcę unijnego, działanie dostawcy należy oceniać według standardów właściwych dla

³⁴ M. Rojszczak, 'End-to-end encryption, chat control, and the future of the right to encryption in digital services' (2026) 12(1) *Journal of Cybersecurity*, s. 3.

³⁵ Art. 51 ust. 1 Karty Praw Podstawowych UE, zgodnie z którym postanowienia Karty mają zastosowanie do instytucji Unii oraz do państw członkowskich wyłącznie w zakresie stosowania przez nie prawa Unii.

³⁶ Do takiego poglądu odwołuje się m.in. M. Rojszczak w *Preventing the dissemination...*, s. 8.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

nadzoru sprawowanego przez władzę publiczną, a nie według standardów pozytywnych obowiązków państwa w relacjach horyzontalnych.

Koncepcja ta, choć u Rojszczaka zasygnalizowana jedynie pomocniczo, zasługuje na rozwinięcie, ponieważ jej przyjęcie może przesądzić o tym, jaki standard ochrony praw podstawowych można by zastosować do oceny mechanizmu ustanowionego rozporządzeniem.

Za uznaniem dostawcy usług za agenta władzy publicznej (*agent of the state*) można by przywołać dwa niezależne argumenty. Po pierwsze, choć rozporządzenie nie nakłada na dostawcę obowiązku wdrożenia mechanizmu skanowania, to od chwili wykrycia podejrzenia materiału CSAM dostawca traci swobodę decyzyjną, a więc jest zobowiązany do niezwłocznego zgłoszenia takiego przypadku właściwym organom³⁷. Po drugie, skoro celem przetwarzania danych nie jest poprawa jakości czy bezpieczeństwa świadczonej usługi (a więc interes własny, gospodarczy dostawcy), lecz identyfikacja przestępstw i przekazanie informacji organom ścigania, to działanie takie realizuje funkcję typowo publiczną, nie prywatną³⁸.

Podstawy tak rozumianej koncepcji dostarcza przede wszystkim orzecznictwo Europejskiego Trybunału Praw Człowieka. M. Rojszczak, w tym samym miejscu, w którym sygnalizuje możliwość zakwalifikowania dostawcy jako agenta państwa, wskazuje na wypracowaną przez Trybunał koncepcję „decydującego udziału” władzy publicznej (*crucial contribution*), powołując się na sprawy A. przeciwko Francji oraz M.M. przeciwko Holandii, w których osoby prywatne nagrywające rozmowy z inicjatywy lub na żądanie policji uznano za działające w imieniu państwa, mimo braku formalnego umocowania ustawowego do takiego działania³⁹.

Dla ilustracji porównawczej warto też odnotować, że zbliżoną koncepcję zna prawo amerykańskie, w postaci testu „agenta rządu” (*government agent*) wypracowanego na gruncie IV Poprawki do Konstytucji USA (ochrona przed nieuzasadnionymi przeszukaniem) – pobieżnie wspomina o niej zresztą sam M. Rojszczak w przywoływanej publikacji⁴⁰. Punktem wyjścia amerykańskiej doktryny jest wyrok Sądu Najwyższego USA w sprawie *Skinner przeciwko Railway Labor Executives' Association*, w którym uznano, że podmiot prywatny może działać jako agent państwa nawet wtedy, gdy przepis, na podstawie którego działa, ma charakter

³⁷ Art. 3 ust. 1 lit. j rozporządzenia; zob. też M. Rojszczak, 'Preventing the dissemination of child sexual abuse material (CSAM) with surveillance technologies: The case of EU Regulation 2021/1232' (2025) 56 Computer Law & Security Review 106097, s. 8.

³⁸ M. Rojszczak, Preventing the dissemination..., s. 8.

³⁹ M. Rojszczak, Preventing the dissemination..., s. 8.

⁴⁰ M. Rojszczak, Preventing the dissemination..., s. 8.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

fakultatywny; sąd uznał, że władza publiczna „zrobiła więcej niż zajęła bierne stanowisko wobec badanego działania prywatnego”⁴¹.

Federalne sądy apelacyjne doprecyzowały ten standard, wyodrębniając trzy kryteria: zachętę lub udział władzy publicznej (*government encouragement or participation*), korzyść państwa z takiego działania (*government benefits*) oraz niezależną motywację podmiotu prywatnego (*the private actor's independent motivations*), przy czym ta ostatnia nie wyklucza automatycznie statusu agenta⁴².

Krishna, stosując te kryteria do projektowanej ustawy Earn it Act, łączącej fakultatywność z obowiązkiem zgłoszenia, konkluduje, że objęte nią platformy najprawdopodobniej spełniałyby test agenta rządu⁴³. Najbliższą analogię stanowi też sprawa United States przeciwko Ackerman, w której organizację NCMEC uznano za agenta państwa mimo braku ustawowego obowiązku analizowania zgłoszeń, wyłącznie na podstawie zachęty i korzyści po stronie władzy publicznej⁴⁴.

Przenoszenie tej doktryny na grunt europejski wymaga jednak istotnej ostrożności metodologicznej i ma w niniejszej analizie charakter wyłącznie pomocniczy. Została ona wypracowana w zupełnie innym kontekście normatywnym, a więc jako odpowiedź na pytanie, czy ochrona konstytucyjna, przysługująca w tym systemie prawnym wyłącznie wobec działania państwa, w ogóle znajduje zastosowanie do działania podmiotu prywatnego.

W tym kontekście warto podkreślić, że problematyka poruszana na łamach niniejszej analizy ma charakter precedensowy, jako że TSUE i ETPC wypowiadały się dotychczas w przedmiocie obowiązkowej retencji danych i inwigilacji przez służby specjalne, nie odnosząc się do kwestii dobrowolnego skanowania treści przez firmy prywatne w kontekście wykrywania materiałów CSAM⁴⁵.

Oba mechanizmy łączy natomiast kilka cech: 1) obejmują one przetwarzanie danych związanych z komunikacją elektroniczną, wszystkich użytkowników danej usługi, niezależnie od jakiegokolwiek związku z podejrzeniem popełnienia przestępstwa, 2) celem przetwarzania jest

⁴¹ A. Krishna, Internet.Gov: Tech Companies as Government Agents and the Future of the Fight Against Child Sexual Abuse (2021) 109 California Law Review 1581, s. 1611.

⁴² A. Krishna, Internet.Gov: Tech..., s. 1611-1612.

⁴³ A. Krishna, Internet.Gov: Tech..., s. 1624.

⁴⁴ A. Krishna, Internet.Gov: Tech..., s. 1613-1614.

⁴⁵ w szczególności TSUE, Digital Rights Ireland (C-293/12 i C-594/12), Tele2 Sverige (C-203/15 i C-698/15), La Quadrature du Net (C-511/18, C-512/18 i C-520/18) oraz Prokuratuur (C-746/18); a także ETPC, Roman Zakharov przeciwko Rosji (47143/06) oraz Podchasov przeciwko Rosji (33696/19).



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

wsparcie organów ścigania, 3) oba stanowią ingerencję w prawa gwarantowane dyrektywą 2002/58/WE oraz art. 7 i 8 Karty, podlegając z testowi proporcjonalności z art. 52 ust. 1 Karty.

Różnią się one jednak w kilku istotnych aspektach. Należy bowiem zauważyć, że 1) retencja danych ma charakter obligatoryjny, nałożony na mocy przepisów prawa na wszystkich operatorów, podczas gdy skanowanie CSAM jest fakultatywne, będąc zależnym od woli dostawców, 2) retencja dotyczy wyłącznie danych o ruchu i lokalizacji, a nie treści komunikacji, co miało kluczowe znaczenie w orzeczeniu zapadłym w sprawie *Digital Rights Ireland*⁴⁶, podczas gdy skanowanie materiałów CSAM obejmuje bezpośrednio treść korespondencji, 3) retencja polega na gromadzeniu danych „na wszelki wypadek”, bez z góry określonego celu, tymczasem skanowanie materiałów CSAM jest ukierunkowane na wykrycie określonego rodzaju treści, z natychmiastowym zgłoszeniem, bez elementu bezterminowego przechowywania, 4) w przypadku retencji danych dostęp organów ścigania do zgromadzonych danych stanowi kolejny, odrębny i następczy etap, poddany kontroli niezależnego organu (wyrok w sprawie *Prokuratuur*)⁴⁷, natomiast przy skanowaniu CSAM to dostawca sam dokonuje analizy i podejmuje decyzję o zgłoszeniu, bez analogicznego etapu kontroli ze strony niezależnego organu.

Warto w tym miejscu odnotować sprawy *Scarlet Extended* oraz *SABAM v. Netlog*⁴⁸, które dotyczyły nakazanego sądownie, a nie dobrowolnego, monitorowania treści przechowywanych odpowiednio przez dostawcę internetu i portal społecznościowy, nie zaś wyłącznie treści udostępnianych publicznie. Trybunał uznał tam, że nałożenie na dostawcę usług obowiązku ogólnego i prewencyjnego monitorowania wszystkich przesyłanych przez użytkowników treści narusza między innymi prawa użytkowników z art. 8 i 11 Karty.

Trybunał, oceniając zgodność środków nadzoru z zasadą proporcjonalności, koncentruje się na obiektywnym zakresie i charakterze ingerencji w prawa podstawowe, nie zaś na tym, czy środek ten został nakazany, czy podjęty z własnej inicjatywy podmiotu go stosującego. Ta ostatnia okoliczność ma znaczenie dopiero na etapie ustalania, czy podmiot prywatny działa jako agent władzy publicznej.

Mechanizm skanowania CSAM różni się od tego stanu faktycznego brakiem elementu przymusu (dostawca działa dobrowolnie, nie na mocy nakazu sądowego), co jednak nie osłabia, lecz raczej wzmacnia wątpliwości: skoro Trybunał uznał obowiązek monitorowania za niedopuszczalny nawet wtedy, gdy wynikał z nakazu sądowego (a więc z zachowaniem pewnej formy kontroli),

⁴⁶ Pkt 39 tego orzeczenia.

⁴⁷ Pkt 51 tego orzeczenia.

⁴⁸ TSUE, wyrok z 24.11.2011, C-70/10, *Scarlet Extended*, pkt 39 i 54 oraz TSUE, wyrok z 16.02.2012, C-360/10, *SABAM v. Netlog*, pkt 48–51.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

to tym bardziej wątpliwości budzi mechanizm pozbawiony jakiegokolwiek analogicznej kontroli, oparty wyłącznie na autonomicznej decyzji dostawcy.

Należy przy tym zastrzec, że sytuacja użytkownika usługi objętej mechanizmem skanowania różni się od sytuacji osoby poddanej tajnej kontroli operacyjnej zarządzanej przez sąd na wniosek organu ścigania. Dostawca ma obowiązek poinformować użytkowników o fakcie skanowania, o zastosowanej technologii oraz o jego wpływie na poufność komunikacji, a użytkownik, godząc się na regulamin usługi, formalnie wyraża na to zgodę i zachowuje możliwość rezygnacji z usługi, jeśli mu to nie odpowiada⁴⁹.

Zastrzeżenie to nie usuwa jednak w pełni wskazanej wątpliwości.

Po pierwsze, tak rozumiana zgoda ma niewiele wspólnego ze standardem zgody wymagany do przetwarzania danych osobowych na gruncie RODO, który wymaga zgody dobrowolnej, konkretnej i jednoznacznej, a nie jedynie biernej akceptacji regulaminu jako warunku korzystania z usługi⁵⁰. Zastrzeżenie to zachowuje aktualność również wobec faktu, że sama regulacja pochodzi od prawodawcy unijnego. Rozporządzenie wprost zastrzega bowiem, że nie stanowi samodzielnej podstawy prawnej przetwarzania danych osobowych, a jedynie usuwa przeszkodę wynikającą z dyrektywy 2002/58/WE, pozostawiając dostawcom obowiązek wykazania własnej podstawy przetwarzania na gruncie art. 6 RODO⁵¹.

Po drugie, w przypadku pewnych usług, takich jak powszechnie używana poczta elektroniczna czy komunikatory, „rezygnacja z usługi” bywa w praktyce fikcją, skoro brak realnej, równoważnej alternatywy funkcjonalnej zmusza użytkownika do wyboru między akceptacją skanowania a wykluczeniem z podstawowych narzędzi komunikacji cyfrowej. Zastrzeżenie to nie neguje istnienia technicznych alternatyw korzystających z szyfrowania end-to-end, takich jak Signal, których rozporządzenie istotnie nie obejmuje. Problem leży jednak nie w dostępności takich narzędzi, lecz w efekcie sieciowym charakterystycznym dla usług komunikacyjnych: ich użyteczność zależy od tego, kto z kręgu kontaktów użytkownika korzysta z tej samej usługi, a nie wyłącznie od jej właściwości technicznych. Nie zmienia to jednak zasadniczej różnicy w naturze obu środków: mechanizm ustanowiony rozporządzeniem pozostaje jawny i poddany obowiązkom informacyjnym, podczas gdy kontrola operacyjna z istoty rzeczy jest niejawna wobec osoby nią objętej.

Przedstawione powyżej rozróżnienie pozwala wskazać, które elementy orzecznictwa dotyczące retencji danych można przenieść w drodze analogii, a które nie. W tym kontekście można

⁴⁹ Art. 3 ust. 1 lit. g pkt (v) rozporządzenia.

⁵⁰ Art. 4 pkt 11 oraz art. 7 ust. 4 rozporządzenia (UE) 2016/679.

⁵¹ Motyw 14 i 19 rozporządzenia.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

przywołać rozróżnienie pomiędzy środkami ukierunkowanymi a środkami ogólnymi i niezróżnicowanymi, na co Trybunał zwrócił uwagę w orzeczeniu *La Quadrature du Net*⁵². TSUE wskazał tam, że dopuszczalne są jedynie środki, których zakres wyznaczają obiektywne i niedyskryminacyjne przesłanki, takie jak np. krąg osób podejrzanych o związek z przestępstwem, co pozwala odróżnić te środki od środków obejmujących z góry wszystkich użytkowników korzystających z usługi. Mechanizm zawarty w rozporządzeniu pozostaje w tym rozumieniu środkiem o charakterze niezróżnicowanym, jako że obejmuje korespondencję wszystkich użytkowników usługi, bez zastosowania jakiegokolwiek obiektywnego kryterium ryzyka czy podejrzenia.

Z kolei w wyroku *Tele2 Sverige* Trybunał doprecyzował, że sama użyteczność środka nadzoru dla realizacji interesu ogólnego nie przesądza jeszcze o jego konieczności, a środek ingerujący w prawa podstawowe musi pozostać wyjątkiem, nie zaś normą ogólną. Powyższe uwagi można również odnieść do mechanizmu skanowania określonego w rozporządzeniu.

Można także zastosować mechanizm a fortiori standard wskazany w orzeczeniu *Digital Rights Ireland*, dotyczący istoty prawa do prywatności. Skoro retencja danych nie narusza istoty tego prawa właśnie dlatego, że nie obejmuje treści komunikacji, to to mechanizm analizujący treść komunikacji tym bardziej wymaga wnikliwej oceny pod tym kątem. Mówiąc innymi słowy, skoro środek mniej inwazyjny budził wątpliwości co do proporcjonalności, to środek o bardziej inwazyjnym charakterze wymaga równie surowej, jak nie surowszej analizy.

Nie można natomiast bezpośrednio przenieść wymogu uprzedniej kontroli niezależnego organu z wyroku *Prokuratuur*. Wyrok ten dotyczył kontroli dostępu organów ścigania do danych już zgromadzonych i przechowywanych przez dostawcę na mocy odrębnego obowiązku retencji, a więc kontroli nad kolejnym, następczym etapem wykorzystania danych, oddzielonym od samego ich gromadzenia. Tymczasem przy skanowaniu CSAM nie występuje analogiczny, wyodrębniony etap „dostępu” po stronie władzy publicznej: to sam dostawca, działając na własną rękę, dokonuje analizy treści i podejmuje decyzję o ewentualnym zgłoszeniu, bez pośrednictwa jakiegokolwiek organu kontrolującego ten proces. Wymóg z wyroku *Prokuratuur* nie przekłada się więc wprost na ten odmienny model, choć jak wskazano powyżej sam brak takiej kontroli pozostaje istotnym elementem krytycznej oceny mechanizmu.

Zastosowanie tego standardu do mechanizmu przewidzianego w projekcie rozporządzenia prowadzi do poważnych wątpliwości. Przepis art. 3 ust. 1 rozporządzenia nie zawiera bowiem żadnych ograniczeń co do kategorii użytkowników czy okoliczności uzasadniających objęcie ich

⁵² TSUE, wyrok z 6.10.2020, sprawy połączone C-511/18, C-512/18 i C-520/18, *La Quadrature du Net*, ECLI:EU:C:2020:791, pkt 149.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

korrespondencji analizą, ponieważ to sam dostawca decyduje, czy i w jakim zakresie skanować komunikację wszystkich swoich klientów. Tymczasem to nie liczba osób objętych środkiem, lecz brak zróżnicowania, a więc przetwarzanie danych osób niepowiązanych z żadnym podejrzeniem na równi z pozostałymi, decyduje o niezróżnicowanym (a nie ukierunkowanym) charakterze środka w rozumieniu przywołanego orzecznictwa. Dodatkowym elementem wzmacniającym wątpliwości jest brak wymogu uprzedniej kontroli sądowej lub niezależnego organu przed uruchomieniem skanowania, co sygnalizowano w orzeczeniu zapadłym w sprawie Prokuratuur⁵³. Warto przy tym zauważyć, że w sprawie Meta v. Bundeskartellamt Trybunał wprost stwierdził, że cel polegający na udzielaniu informacji organom ścigania, zmierzający do zapobiegania przestępstwom, nie może co do zasady stanowić samodzielnej podstawy prawnej przetwarzania danych przez podmiot prywatny, chyba że wynika to z ciężącego na nim obowiązku prawnego, oraz że taki podmiot nie może powoływać się na ochronę żywotnych interesów użytkowników w sposób abstrakcyjny i prewencyjny⁵⁴. Powyższe uwagi mają bezpośrednie znaczenie dla oceny podstaw prawnych dostawców korzystających z fakultatywnego (a więc pozbawionego obowiązku prawnego) mechanizmu przewidzianego w rozporządzeniu.

Wątpliwości te potęguje problem przewidywalności prawa: w sprawie Roman Zakharov ETPC sformułował katalog minimalnych zabezpieczeń, jakie prawo musi przewidywać, aby zapobiec nadużyciom władzy przy stosowaniu tajnego nadzoru, obejmujący rodzaj przestępstw uzasadniających zarządzenie przechwytywania komunikacji, definicję kategorii osób nim objętych, ograniczenie czasu trwania kontroli, procedurę badania, wykorzystywania i przechowywania danych, środki ostrożności przy ich przekazywaniu innym podmiotom oraz okoliczności ich usunięcia lub zniszczenia⁵⁵. Tymczasem rozporządzenie pozostawia dostawcom pełną swobodę co do wyboru konkretnej technologii, zakresu przetwarzanych danych oraz — co szczególnie istotne — podstawy prawnej przetwarzania na gruncie RODO. EIOD w opinii z lutego 2026 r. rekomenduje wprost, aby projekt uzupełniono o wyraźną podstawę przetwarzania w rozumieniu art. 6 ust. 1 lit. e w zw. z art. 6 ust. 3 RODO, tak by dobrowolne przetwarzanie danych przez dostawców w celu wykrywania CSAM online mogło zostać zakwalifikowane jako wykonywanie zadania realizowanego w interesie publicznym⁵⁶. Tymczasem motyw 14 rozporządzenia wciąż zastrzega, że rozporządzenie nie stanowi podstawy prawnej przetwarzania danych — rekomendacja EIOD pozostaje więc nieuwzględniona, co

⁵³ TSUE, wyrok z 2.03.2021, C-746/18, Prokuratuur, pkt 39 i 54.

⁵⁴ TSUE, wyrok z 4.07.2023, C-252/21, Meta v. Bundeskartellamt, pkt 124 i 137.

⁵⁵ ETPC, wyrok z 4.12.2015 r., Roman Zakharov przeciwko Rosji, skarga nr 47143/06, § 231.

⁵⁶ EDPS, Opinion 7/2026 (przyp. 30), pkt 21–22 i 31(1).



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

budzi poważne wątpliwości co do spełnienia wymogu z art. 52 ust. 1 Karty, zgodnie z którym ograniczenie prawa podstawowego musi być „przewidziane przez ustawę”⁵⁷.

5. Argumenty za rozporządzeniem

Analiza krytyczna rozporządzenia, prowadzona w dalszej części niniejszego opracowania, wymaga również uwzględnienia racji przemawiających za jego przyjęciem. Należy przy tym zauważyć, że racje te nie sprowadzają się wyłącznie do ogólnikowego odwołania się do słuszności celu regulacji, lecz znajdują oparcie zarówno w treści rozporządzenia, jak i w orzecznictwie europejskim dotyczącym pozytywnych obowiązków państwa wobec ofiar przestępstw (o czym dalej).

Punktem wyjścia jest legitymowany, a wręcz nakazany przez prawo pierwotne cel regulacji. Motyw 4 rozporządzenia wprost odwołuje się do art. 3 ust. 1 Konwencji o prawach dziecka, zgodnie z którym we wszystkich działaniach dotyczących dzieci, podejmowanych przez publiczne lub prywatne instytucje opieki społecznej, sądy, władze administracyjne lub ciała ustawodawcze, sprawą nadrzędną będzie najlepsze zabezpieczenie interesów dziecka⁵⁸. W tym samym motywie omawianej regulacji przywołany zostaje art. 24 ust. 2 Karty, na mocy którego we wszystkich działaniach dotyczących dzieci, zarówno podejmowanych przez władze publiczne jak i instytucje prywatne, należy przede wszystkim uwzględnić najlepszy interes dziecka. Wskazano tam także, że ochrona dzieci przed niegodziwym traktowaniem w celach seksualnych stanowi jeden z priorytetów Unii, a cyfryzacja, przynosząc społeczeństwu liczne korzyści, przyczyniła się zarazem do wzrostu tego zjawiska w internecie. Sam Europejski Inspektor Ochrony Danych, mimo krytycznego podejścia wobec poszczególnych rozwiązań rozporządzenia, nie kwestionuje, że zwalczanie niegodziwego traktowania dzieci w celach seksualnych stanowi cel interesu ogólnego uznany przez Unię⁵⁹, co oznacza, że spór dotyczy nie tyle legitymacji celu, ile proporcjonalności zastosowanych środków. Za przyjęciem regulacji przemawia dodatkowo perspektywa praw ofiar. Na poparcie tej tezy można przywołać orzeczenie wydane przez Europejski Trybunał Praw Człowieka w sprawie K.U. przeciwko Finlandii⁶⁰. Sprawa dotyczyła sytuacji, w której nieznana osoba zamieściła w internecie, bez wiedzy i zgody małoletniego, ogłoszenie o charakterze seksualnym, a organy krajowe odmówiły ustalenia tożsamości sprawcy, powołując się na tajemnicę telekomunikacji. Trybunał uznał, że na państwie ciąży pozytywny obowiązek wynikający z art. 8 Europejskiej Konwencji Praw

⁵⁷ Motyw 14 dokumentu Rady ST-11703/26

⁵⁸ Konwencja o prawach dziecka, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 20 listopada 1989 roku, Dz.U. 1991 nr 120 poz. 526; <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19911200526>, dostęp: 18 sierpnia 2026.

⁵⁹ European Data Protection Supervisor, Opinion 7/2026, pkt. 6.

⁶⁰ ETPC, wyrok z 2.12.2008r., K.U. przeciwko Finlandii, skarga nr 2872/02.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

Człowieka⁶¹ (przepis ten gwarantuje prawo do poszanowania życia prywatnego i rodzinnego, miejsca zamieszkania oraz korespondencji), polegający na kryminalizacji przestępstw przeciwko integralności fizycznej i psychicznej jednostki oraz na wzmacnianiu odstraszającego skutku takiej kryminalizacji poprzez zapewnienie skutecznego dochodzenia i ścigania sprawców, przy czym obowiązek ten nabiera szczególnej wagi, gdy zagrożone jest dobro dziecka⁶². ETPC wskazał wprost, że poufność komunikacji, choć stanowi wartość pierwszorzędą, nie ma charakteru absolutnego i musi niekiedy ustąpić innym uzasadnionym celom, takim jak zapobieganie przestępczości czy ochrona praw i wolności innych osób⁶³. Trybunał w konsekwencji uznał, że bierność fińskiego ustawodawcy, który nie zapewnił mechanizmu umożliwiającego identyfikację sprawcy umieszczającego w internecie treści o charakterze seksualnym dotyczące małoletniego, sama stanowiła naruszenie Konwencji⁶⁴.

Analizując wskazane powyżej orzeczenie warto mieć jednocześnie na względzie, iż dotyczyło ono obowiązku ujawnienia danych sprawcy (autora ogłoszenia), nie zaś skanowania treści prywatnej komunikacji, tak jak ma to miejsce w przypadku mechanizmu zawartego w rozporządzeniu. Niemniej, w kontekście przedmiotu niniejszej analizy znaczenie ma coś innego: zasada, że brak działania ze strony państwa może stanowić naruszenie praw ofiar. Sam mechanizm ma przy tym znaczenie nie tylko dla identyfikacji sprawców, lecz także dla ograniczania dalszego rozpowszechniania już wykrytych materiałów, co samo w sobie stanowi formę ochrony ofiar przed powtarzającą się wiktyimizacją, na co zwrócono uwagę w rozporządzeniu⁶⁵.

Za przyjęciem rozporządzenia przemawia również konstrukcja samego mechanizmu, który nie jest pozbawiony elementów różnicujących intensywność ingerencji w zależności od rodzaju zagrożenia. Omawiana regulacja wyróżnia bowiem dwie kategorie technologii: 1) haszowanie, stosowane wyłącznie do porównywania zdjęć i filmów ze zweryfikowaną bazą już znanych materiałów CSAM oraz 2) klasyfikatory i systemy sztucznej inteligencji, wykorzystywane do analizy tekstu lub danych o ruchu (w tym obrazów i filmów) w celu wykrywania nowych materiałów lub wzorców wskazujących na nagabywanie dzieci⁶⁶. Rozporządzenie przewiduje ponadto dodatkowe zabezpieczenie proceduralne, obejmujące dwie sytuacje: stosowanie technologii nieużywanej wcześniej przez żadnego dostawcę (niezależnie od jej rodzaju) oraz,

⁶¹ Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, Dz.U. 1993 nr 61 poz. 284; <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19930610284>, dostęp: 18 sierpnia 2026.

⁶² ETPC, wyrok K.U. przeciwko Finlandii, §§ 43 i 46.

⁶³ Tamże, § 49.

⁶⁴ Tamże, §§ 49-50.

⁶⁵ Motyw 7 rozporządzenia.

⁶⁶ Motyw 7 rozporządzenia.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

niezależnie od momentu jej wdrożenia, stosowanie technologii służącej wykrywaniu nagabywania dzieci, a więc w praktyce zawsze technologii z kategorii klasyfikatorów. W obu przypadkach dostawca musi wykazać zgodność z pisemnymi zaleceniami organu nadzorczego wydanymi w toku procedury uprzednich konsultacji⁶⁷ oraz ograniczenia wykrywania nagabywania do zobiektywizowanych wskaźników ryzyka, takich jak różnica wieku między uczestnikami komunikacji, czy prawdopodobny udział dziecka w skanowanej komunikacji⁶⁸. Rozporządzenie eliminuje przy tym ryzyko objęcia jego zakresem zachowań niestanowiących przestępstwa, zastrzegając wprost, że nie reguluje ono polityk państw członkowskich wobec dobrowolnych aktywności seksualnych między rówieśnikami, stanowiących naturalny element rozwoju człowieka⁶⁹. Do tego dochodzą wyłączenia o charakterze bardziej kategorycznym: komunikacja szyfrowana metodą *end-to-end* oraz komunikacja głosowa pozostają poza zakresem rozporządzenia w całości, niezależnie od zastosowanej technologii⁷⁰.

Z drugiej strony należy zaznaczyć, że wskazane powyżej zróżnicowanie dotyczy wyłącznie zastosowanej technologii, a nie kręgu objętych nią użytkowników. Kwestia ta, jak wykazano we wcześniejszej części niniejszej analizy, ma zasadnicze znaczenie z punktu widzenia standardu wypracowanego w orzecznictwie TSUE, zgodnie z którym o niezróżnicowanym charakterze środka decyduje nie rodzaj czy stopień zaawansowania zastosowanej technologii, lecz brak selekcji osób objętych jego zakresem według obiektywnego kryterium ryzyka lub podejrzenia. Dlatego też opisane zróżnicowanie technologiczne nie usuwa wątpliwości dotyczących zakresu podmiotowego mechanizmu.

Z perspektywy najlepszego interesu dziecka wynikającego z art. 24 ust. 2 Karty należy jednak zauważyć, że przywołane wyżej argumenty koncentrują się wyłącznie na sytuacji dziecka jako ofiary lub potencjalnej ofiary niegodziwego traktowania. Tymczasem zasada ta nakazuje uwzględnienie najlepszego interesu dziecka we wszystkich działaniach go dotyczących, a więc również w odniesieniu do dzieci będących zwykłymi użytkownikami usług objętych mechanizmem skanowania, których prywatna korespondencja, w tym z rodzicami, rówieśnikami czy zaufanymi osobami dorosłymi, podlega tej samej, niezróżnicowanej analizie. Najlepszy interes dziecka nie przemawia zatem jednoznacznie za mechanizmem ani przeciw niemu, lecz wymaga wyważenia interesu dzieci-ofiar w skutecznej ochronie z interesem wszystkich pozostałych małoletnich użytkowników w poszanowaniu poufności ich komunikacji, co stanowi przedmiot dalszej, szczegółowej analizy proporcjonalności.

⁶⁷ Art. 3 ust. 1 lit. d) rozporządzenia.

⁶⁸ Art. 3 ust. 1 lit. f) rozporządzenia.

⁶⁹ Motyw 6 rozporządzenia.

⁷⁰ Art. 1 ust. 2 i 3 rozporządzenia.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

6. Ocena skuteczności

Ocena proporcjonalności mechanizmu przewidzianego w rozporządzeniu, w tym w szczególności spełnienia kryterium konieczności, wymaga uwzględnienia danych dotyczących jego rzeczywistej skuteczności. Sprawozdanie Komisji Europejskiej z listopada 2025 r. z wdrażania rozporządzenia (UE) 2021/1232 wskazuje na istotne zróżnicowanie współczynników błędu między poszczególnymi dostawcami: od 0% (LinkedIn) i 0,12–0,32% (Meta) przez 0,54–1,14% (Google, wyłącznie w zakresie technologii dopasowywania skrótów) po 13–20% (Yubo, wyłącznie w zakresie wykrywania nowych materiałów i nagabywania dzieci)⁷¹. Komisja zastrzega przy tym, że dostawcy stosowali różne, niejednolite metody obliczania tego wskaźnika, co ogranicza porównywalność przedstawionych danych, a Microsoft nie dysponował danymi wystarczającymi do jego wyliczenia w ogóle⁷². Skalę stosowania mechanizmu ilustrują dane dotyczące jednego z największych dostawców: w 2023 r. Microsoft zeskanował ponad 11 miliardów jednostek danych, identyfikując na ich podstawie ok. 32 tysiące przypadków CSAM na całym świecie, co oznacza, że jedynie ok. 0,0002% wszystkich przeskanowanych jednostek danych zawierało materiały CSAM⁷³. Wskaźnik ten nie stanowi miary zawodności czy błędu technologii, lecz odzwierciedla naturalnie niską częstość występowania nielegalnych treści na tle całego wolumenu komunikacji elektronicznej. Komisja przyznaje przy tym, że dane przekazywane przez państwa członkowskie pozostają niekompletne i fragmentaryczne, co uniemożliwia przedstawienie kompleksowego i wiarygodnego obrazu liczby zgłoszeń, zidentyfikowanych dzieci oraz skazanych sprawców, zastrzegając jednocześnie, że brak jest przesłanek świadczących o tym, iż zastosowanie odstępstwa nie jest proporcjonalne⁷⁴.

Rzetelność wymaga przywołania również argumentu przemawiającego za mechanizmem: nawet przy tych ograniczeniach doprowadził on w ciągu kilku lat funkcjonowania rozporządzenia do wykrycia dziesiątek tysięcy przypadków materiałów przedstawiających niegodziwe traktowanie dzieci, co stanowi konkretny, choć trudny do precyzyjnego zmierzenia, rezultat.

Zestawienie powyższych danych z testem proporcjonalności wypracowanym w orzecznictwie TSUE prowadzi do niejednoznacznego wniosku. Co do przydatności środka do realizacji celu, dane nie budzą wątpliwości: mechanizm doprowadził do wykrycia dziesiątek tysięcy

⁷¹ Komunikat Komisji, sprawozdanie z wdrażania rozporządzenia (UE) 2021/1232, COM(2025) 740 final z 27.11.2025, pkt 2.1.6, tabela 5

⁷² Tamże.

⁷³ M. Rojszczak, 'Preventing the dissemination of child sexual abuse material (CSAM) with surveillance technologies: The case of EU Regulation 2021/1232' (2025) 56 Computer Law & Security Review 106097, s. 10.

⁷⁴ COM(2025) 740 final, s. 40-41.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

przypadków CSAM, a więc w oczywisty sposób przyczynia się do realizacji celu regulacji. Ocena konieczności jest już znacznie trudniejsza: sama Komisja przyznaje, że dane przekazywane przez państwa członkowskie są niekompletne i fragmentaryczne, co uniemożliwia rzetelne porównanie skuteczności mechanizmu z alternatywnymi, mniej ingerującymi środkami. Zgodnie z utrwalonym orzecznictwem TSUE, sama użyteczność środka dla realizacji celu interesu ogólnego nie przesądza jeszcze o jego konieczności⁷⁵. Wobec braku pełnych danych pozwalających ocenić, czy analogiczny rezultat dałoby się osiągnąć środkiem mniej dotkliwym dla prywatności wszystkich użytkowników, ciężar wykazania konieczności tak daleko idącej ingerencji, spoczywający co do zasady na prawodawcy wprowadzającym środek ingerujący w prawa podstawowe, nie został w pełni udźwignięty. Wreszcie, na poziomie proporcjonalności sensu stricto, dane o wskaźniku 0,0002% wykrytych przypadków w stosunku do całego przeskanowanego wolumenu komunikacji dobitnie ilustrują skalę ingerencji ponoszonej przez ogromną większość użytkowników niemających żadnego związku z omawianym przestępstwem, w zamian za korzyść skoncentrowaną na relatywnie niewielkiej liczbie wykrytych przypadków. Rozstrzygnięcie, czy tak rozłożony bilans kosztów i korzyści spełnia standard proporcjonalności, wymaga więc wyważenia, którego przeprowadzenie w pełni utrudnia właśnie niekompletność danych sprawozdawczych, na którą zwraca uwagę sama Komisja.

Głosowanie w Parlamencie Europejskim

Przywrócenie rozporządzenia nastąpiło w ramach zwykłej procedury ustawodawczej z art. 294 TFUE, w drugim czytaniu, w którym Parlament Europejski mógł odrzucić stanowisko Rady wyłącznie bezwzględną większością głosów wszystkich swoich członków (361 głosów). W głosowaniu 9 lipca 2026 r., przeprowadzonym w trybie pilnym z art. 68 i 170 Regulaminu PE⁷⁶, o który wystąpiła Europejska Partia Ludowa jako największa frakcja Parlamentu, 314 posłów opowiedziało się za odrzuceniem przywrócenia rozporządzenia, a 276 przeciwko odrzuceniu⁷⁷; wniosek nie osiągnął jednak wymaganego progu 361 głosów, wskutek czego stanowisko Rady, uzupełnione o przyjęte poprawki (w tym wyłączenie E2EE), stało się stanowiskiem Parlamentu w drugim czytaniu, a nie ostatecznie przyjętym aktem — tekst musi teraz wrócić do Rady, która w terminie trzech miesięcy może go zaakceptować albo skierować sprawę do komitetu pojednawczego. Tryb pilny, choć sam w sobie przewidziany w Regulaminie i zgodny z prawem,

⁷⁵ M. Rojszczak, Preventing the dissemination..., s. 6, powołujący się na wyrok TSUE z 7.11.2013, C-473/12, IPI, ECLI:EU:C:2013:715, pkt 39.

⁷⁶ Regulamin Parlamentu Europejskiego, art. 68 i 170.

⁷⁷ European Parliament, 'Combating child sexual abuse online: support for more limited ePrivacy derogation', 09.07.2026; <https://www.europarl.europa.eu/news/en/press-room/20260706IPR46318/combating-child-sexual-abuse-support-for-a-more-limited-eprivacy-derogation>, dostęp: 29 lipca 2026.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

wyeliminował etap prac komisji LIBE i sprawił, że akt był procedowany dalej z powodu nieosiągnięcia formalnego progu proceduralnego, co rodzi poważne wątpliwości co do jakości procesu legislacyjnego, choć formalnie pozostaje zgodne z Traktatem.

Na marginesie należy odnotować, że Rada Unii Europejskiej 23 lipca 2026 r., a więc już po zamknięciu niniejszej analizy, udzieliła ostatecznej zgody na tekst przyjęty przez Parlament Europejski w drugim czytaniu, kończąc tym samym procedurę ustawodawczą; rozporządzenie oczekuje obecnie na publikację w Dzienniku Urzędowym UE⁷⁸.

7. Wnioski

Przeprowadzona analiza prowadzi do konkluzji, że rozporządzenie, mimo niewątpliwie legitymowanego i głęboko zakorzenionego w prawie pierwotnym celu, jakim jest ochrona dzieci przed niegodziwym traktowaniem w celach seksualnych w internecie, budzi poważne wątpliwości co do zgodności z prawem Unii Europejskiej. Wątpliwości te dotyczą w szczególności mechanizmu ustanowionego w art. 3 ust. 1 rozporządzenia, oparte na dobrowolnym, pozbawionym uprzedniej kontroli sądowej skanowaniu treści komunikacji wszystkich użytkowników usługi, ocenianego na tle art. 7 i 8 Karty (poszanowanie życia prywatnego i ochrona danych osobowych) w związku z art. 52 ust. 1 Karty (wymóg proporcjonalności ograniczeń praw podstawowych). Nie wynikają z zakwestionowania samego celu regulacji, ponieważ, jak wykazano, cel ten znajduje oparcie zarówno w art. 24 Karty i Konwencji o prawach dziecka, jak i w orzecznictwie ETPC dotyczącym pozytywnych obowiązków państwa wobec ofiar przestępstw (K.U. przeciwko Finlandii), lecz z oceny proporcjonalności zastosowanych środków.

Rozporządzenie wprowadza pewne elementy różnicujące intensywność ingerencji: rozróżnienie haszowania od klasyfikatorów sztucznej inteligencji, dodatkowe zabezpieczenia proceduralne dla nowych technologii i wykrywania nagabywania, wyłączenie komunikacji szyfrowanej end-to-end oraz komunikacji głosowej. Zróżnicowanie to dotyczy jednak wyłącznie rodzaju zastosowanej technologii, nie zaś kręgu objętych nią użytkowników, a to właśnie brak selekcji podmiotowej, a nie rodzaj technologii, decyduje w świetle orzecznictwa TSUE o niezróżnicowanym charakterze środka.

Na tym tle krytyczna ocena mechanizmu opiera się na dwóch głównych filarach. Po pierwsze, rozporządzenie w dalszym ciągu nie zapewnia jasnej podstawy prawnej przetwarzania danych osobowych w rozumieniu RODO, mimo że problem ten sygnalizowany jest przez Europejskiego

⁷⁸ Rada Unii Europejskiej, komunikat prasowy „Fighting child sexual abuse online: interim measure protecting children now reinstated”; <https://www.consilium.europa.eu/en/press/press-releases/2026/07/23/fighting-child-sexual-abuse-online-interim-measure-protecting-children-now-reinstated/>, dostęp: 29 lipca 2027.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

Inspektora Ochrony Danych od lat, a rekomendowane rozwiązanie, czyli oparcie przetwarzania na art. 6 ust. 1 lit. e RODO, nie zostało dotąd uwzględnione w tekście aktu. Po drugie, mechanizm dobrowolnego, niezróżnicowanego skanowania korespondencji wszystkich użytkowników usług nieszyfrowanych end-to-end budzi wątpliwości w świetle utrwalonego orzecznictwa Trybunału Sprawiedliwości dotyczącego proporcjonalności i istoty prawa do prywatności, w szczególności wobec braku wymogu uprzedniej, niezależnej kontroli takich działań, a więc elementu, który TSUE uznaje za konieczny w analogicznym kontekście dostępu do danych objętych tajemnicą komunikowania.

Żaden z przedstawionych zarzutów, rozpatrywany osobno, nie prowadzi do wniosku o oczywistej niezgodności rozporządzenia z prawem Unii. Kumulatywne współwystępowanie braku jasnej podstawy prawnej przetwarzania oraz niezróżnicowanego charakteru mechanizmu skanowania, przy jednoczesnym braku uprzedniej niezależnej kontroli, stanowi jednak, w świetle przywołanego orzecznictwa, wystarczającą podstawę dla sformułowania poważnych wątpliwości co do zgodności rozporządzenia ze standardem wynikającym z art. 7, 8 i 52 ust. 1 Karty Praw Podstawowych Unii Europejskiej.

Ostrożności wymaga przy tym ocena skuteczności mechanizmu. Dostępne dane wskazują raczej na jej empiryczną nierozstrzygniętość niż na dowiedzioną nieskuteczność, ponieważ zróżnicowane, częściowo niejednolite metodologicznie współczynniki błędów poszczególnych dostawców oraz brak wykazanego związku między liczbą zgłoszeń a liczbą wyroków skazujących nie pozwalają jednoznacznie potwierdzić konieczności mechanizmu w jego obecnym kształcie, choć jednocześnie Komisja Europejska nie stwierdziła, by mechanizm był nieproporcjonalny.

Powyższa krytyka nie oznacza jednak, że jedyną alternatywą pozostaje bierne oczekiwanie na popełnienie przestępstwa i działanie organów ścigania wyłącznie post factum. Wskazane wątpliwości dotyczą bowiem nie samego celu regulacji, lecz przyjętego modelu jego realizacji, opartego na dobrowolnym i pozbawionym zewnętrznej kontroli mechanizmie skanowania prowadzonym przez podmioty prywatne według własnego uznania. Alternatywę stanowić może model oparty na nakazie wydawanym przez niezależny organ i poddanym kontroli sądowej, taki jak przewidziany w projekcie docelowego rozporządzenia CSAM, gdzie zakres i czas trwania ingerencji są z góry określone decyzją administracyjną, a nie pozostawione swobodnej decyzji dostawcy usługi⁷⁹. Model ten nie wymaga przy tym odrębnej autoryzacji sądowej każdej analizowanej wiadomości z osobna, lecz nakazu wydawanego wobec danej usługi lub technologii jako całości, przy czym prawo do zaskarżenia takiego nakazu przysługuje

⁷⁹ Zob. M. Rojszczak, 'Preventing the dissemination...', s. 11.



*Razem w obronie
życia, wolności, rodziny
i suwerenności!*

przed jego ostatecznym wydaniem⁸⁰. Rozwiązanie to, choć wciąż niedoskonałe, bo nie obejmuje kontroli sądowej samego sposobu wykonania nakazu przez dostawcę⁸¹, pozwala przynajmniej częściowo pogodzić potrzebę niezależnego nadzoru z koniecznością przetwarzania danych na dużą skalę.

Patryk Ignaszczak – analityk Centrum Prawa Międzynarodowego Ordo Iuris

⁸⁰ Zob. M. Rojszczak, 'Preventing the dissemination...', s. 11.

⁸¹ Zob. M. Rojszczak, 'Preventing the dissemination...', s. 12.