

AKT O USŁUGACH CYFROWYCH

Komentarz

redakcja naukowa Dominik Lubasz, Monika Namysłowska

Gabriela Bar, Paweł Biały, Roman Bieda, Edyta Bielak-Jomaa, Piotr Budrewicz
Witold Chomiczewski, Michał Czerniawski, Piotr Drobek, Damian Flisak
Karolina Gałęzowska, Urszula Góral, Agnieszka Jabłonowska, Monika Jagielska
Mariusz Jagielski, Berenika Kaczmarek-Templin, Anna Kobylańska
Marcin Lewoszewski, Dominik Lubasz, Joanna Łuczak-Tarka, Paweł Makowski
Iga Małobęcka-Szwast, Arwid Mednis, Karolina Mojzesowicz, Monika Namysłowska
Zbigniew Okoń, Magdalena Piech, Monika Susańko, Adam Szkurlat, Kamil Szpyt

KOMENTARZE

AKT O USŁUGACH CYFROWYCH

Komentarz

redakcja naukowa Dominik Lubasz, Monika Namysłowska

Gabriela Bar, Paweł Biały, Roman Bieda, Edyta Bielak-Jomaa, Piotr Budrewicz
Witold Chomiczewski, Michał Czerniawski, Piotr Drobek, Damian Flisak
Karolina Gałęzowska, Urszula Góral, Agnieszka Jabłonowska, Monika Jagielska
Mariusz Jagielski, Berenika Kaczmarek-Templin, Anna Kobylańska
Marcin Lewoszewski, Dominik Lubasz, Joanna Łuczak-Tarka, Paweł Makowski
Iga Małobęcka-Szwast, Arwid Mednis, Karolina Mojzesowicz, Monika Namysłowska
Zbigniew Okoń, Magdalena Piech, Monika Susańko, Adam Szkurłat, Kamil Szpyt

KOMENTARZE

Stan prawny na 1 lutego 2024 r.

Recenzent

Dr hab. Grzegorz Sibiga, prof. Instytutu Nauk Prawnych Polskiej Akademii Nauk

Wydawczyni

Monika Pawłowska

Redaktorka prowadząca

Kinga Zajac

Opracowanie redakcyjne

Trzy kropki Joanna Maź

Projekt okładek serii

Wojtek Janikowski, Przemek Dębowski

Poszczególne części komentarza napisali:

Gabriela Bar – art. 22, 23; Paweł Biały – art. 55, 77, 78; Roman Bieda, Piotr Budrewicz – art. 48; Edyta Bielak-Jomaa – art. 49–51, 69, 75, 76, 83; Piotr Budrewicz – art. 44; Witold Chomiczewski – art. 3 pkt II.6, II.7, II.11, II.13; art. 4, 5, 7, 24; Witold Chomiczewski, Magdalena Piech – art. 6; Michał Czerniawski – art. 61–63, 87–91, 93; Piotr Drobek – art. 65, 67, 68, 79, 81, 82; Damian Flisak – art. 3 pkt II.18, II.19; art. 38, 39; Karolina Gałęzowska – art. 36, 37; Karolina Gałęzowska, Arwid Mednis – art. 92; Urszula Góral – art. 3 pkt II.14, II.15; art. 56, 64, 70–72, 80; Agnieszka Jabłonowska, Monika Namysłowska – art. 25; Monika Jagielska, Mariusz Jagielski – art. 29–32; Berenika Kaczmarek-Templin – art. 19–21; Anna Kobyłańska – art. 40, 43; Marcin Lewoszewski – art. 41, 42; Dominik Lubasz – art. 1; art. 3 pkt I, II.1, II.2, II.8, II.12; art. 9, 16; Dominik Lubasz, Witold Chomiczewski – art. 28; Joanna Łuczak-Tarka – art. 3 pkt II.24; art. 52–54; Paweł Makowski – art. 3 pkt II.22; art. 47, 57, 58, 60; Paweł Makowski, Zbigniew Okoń – art. 45; Magdalena Piech, Witold Chomiczewski – art. 8; Iga Małobęcka-Szwast – art. 3 pkt II.21; Iga Małobęcka-Szwast, Magdalena Piech – art. 11–15; Arwid Mednis – art. 3 pkt II.9, II.10, II.16, II.17; art. 34, 35; Arwid Mednis, Karolina Gałęzowska – art. 33; Karolina Mojzesowicz – art. 59, 66, 73, 74; Monika Namysłowska, Agnieszka Jabłonowska – art. 3 pkt II.3; art. 26, 27; Monika Namysłowska, Dominik Lubasz – art. 3 pkt II.23; Zbigniew Okoń, Paweł Makowski – art. 46; Monika Susańko – art. 3 pkt II.4, II.5, II.20; art. 17; Monika Susańko, Zbigniew Okoń, Adam Szkurlat – art. 2; Adam Szkurlat – art. 10, 18; Kamil Szpyt – art. 84–86

© Copyright by Wolters Kluwer Polska Sp. z o.o., 2024

ISBN 978-83-8358-336-5

Wolters Kluwer Polska Sp. z o.o.

Dział Praw Autorskich

01-208 Warszawa, ul. Przyokopowa 33

tel. +48 728 313 462

e-mail: PL-ksiazki@wolterskluger.com

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

Wykaz skrótów	11
Słowo wstępne	23
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)	29
Rozdział I	
Przepisy ogólne	101
Artykuł 1. Przedmiot i zakres stosowania	101
Artykuł 2. Zakres stosowania	127
Artykuł 3. Definicje	157
Rozdział II	
Odpowiedzialność dostawców usług pośrednich	215
Artykuł 4. „Zwykły przekaz”	215
Artykuł 5. „Caching”	228
Artykuł 6. Hosting	241
Artykuł 7. Dobrowolne czynności sprawdzające prowadzone z własnej inicjatywy i zgodność z prawem	270
Artykuł 8. Brak ogólnych obowiązków w zakresie monitorowania lub aktywnego ustalania faktów	280
Artykuł 9. Nakaz podjęcia działań przeciwko nielegalnym treściom	299
Artykuł 10. Nakazy udzielenia informacji	316

Rozdział III

Obowiązki w zakresie należytej staranności na potrzeby przejrzystego i bezpiecznego środowiska internetowego	327
---	------------

Sekcja 1

Obowiązki mające zastosowanie do wszystkich dostawców usług pośrednich	327
---	------------

Artykuł 11. Punkty kontaktowe dla organów państw członkowskich, Komisji i Rady Usług Cyfrowych	327
Artykuł 12. Punkty kontaktowe dla odbiorców usług	339
Artykuł 13. Przedstawiciele prawni	347
Artykuł 14. Warunki korzystania z usług	360
Artykuł 15. Obowiązki sprawozdawcze w zakresie przejrzystości spoczywające na dostawcach usług pośrednich	373

Sekcja 2

Dodatkowe przepisy mające zastosowanie do dostawców usług hostingu, w tym platform internetowych	388
---	------------

Artykuł 16. Mechanizmy zgłaszania i działania	388
Artykuł 17. Uzasadnienie	430
Artykuł 18. Zawiadomienie o podejrzeniu popełnienia przestępstwa	454

Sekcja 3

Dodatkowe przepisy mające zastosowanie do platform internetowych	466
---	------------

Artykuł 19. Wyłączenie dotyczące mikroprzedsiębiorstw i małych przedsiębiorstw	466
Artykuł 20. Wewnętrzny system rozpatrywania skarg	473
Artykuł 21. Pozasądowe rozstrzyganie sporów	488
Artykuł 22. Zaufane podmioty sygnalizujące	513
Artykuł 23. Środki podejmowane przeciwko nadużywaniu i ochrona przed nim ...	528
Artykuł 24. Obowiązki sprawozdawcze w zakresie przejrzystości spoczywające na dostawcach platform internetowych	541
Artykuł 25. Projekt i organizacja interfejsów internetowych	550
Artykuł 26. Reklamy na platformach internetowych	563
Artykuł 27. Przejrzystość systemu rekomendacji	582
Artykuł 28. Ochrona małoletnich w internecie	595

Sekcja 4

Dodatkowe przepisy dotyczące dostawców platform internetowych umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość	606
--	------------

<i>Artykuł 29.</i> Wyłączenie dotyczące mikroprzedsiębiorstw i małych przedsiębiorstw	606
<i>Artykuł 30.</i> Identyfikowalność przedsiębiorców	607
<i>Artykuł 31.</i> Zgodność w fazie projektowania	623
<i>Artykuł 32.</i> Prawo do informacji	637

Sekcja 5

Dodatkowe obowiązki spoczywające na dostawcach bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych w zakresie zarządzania ryzykiem systemowym	647
--	------------

<i>Artykuł 33.</i> Bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe	647
<i>Artykuł 34.</i> Ocena ryzyka	666
<i>Artykuł 35.</i> Zmniejszanie ryzyka	687
<i>Artykuł 36.</i> Mechanizm reagowania kryzysowego	703
<i>Artykuł 37.</i> Niezależny audyt	716
<i>Artykuł 38.</i> System rekomendacji	728
<i>Artykuł 39.</i> Dodatkowa przejrzystość reklam internetowych	737
<i>Artykuł 40.</i> Dostęp do danych i kontrola danych	749
<i>Artykuł 41.</i> Komórka nadzoru przestrzegania niniejszego rozporządzenia	762
<i>Artykuł 42.</i> Obowiązki sprawozdawcze w zakresie przejrzystości	773
<i>Artykuł 43.</i> Opłata nadzorcza	781

Sekcja 6

Inne przepisy dotyczące obowiązków w zakresie należytej staranności	789
--	------------

<i>Artykuł 44.</i> Normy	789
<i>Artykuł 45.</i> Kodeksy postępowania	806
<i>Artykuł 46.</i> Kodeksy postępowania w odniesieniu do reklam internetowych	820
<i>Artykuł 47.</i> Kodeksy postępowania w odniesieniu do dostępności	832
<i>Artykuł 48.</i> Protokoły kryzysowe	839

Rozdział IV

Wdrażanie, współpraca, sankcje i egzekwowanie	855
--	------------

Sekcja 1

Właściwe organy i krajowi koordynatorzy ds. usług cyfrowych	855
--	------------

Artykuł 49. Właściwe organy i koordynatorzy ds. usług cyfrowych	855
Artykuł 50. Wymogi dotyczące koordynatorów ds. usług cyfrowych	870
Artykuł 51. Uprawnienia koordynatorów ds. usług cyfrowych	885
Artykuł 52. Sankcje	906
Artykuł 53. Prawo do wniesienia skargi	917
Artykuł 54. Odszkodowanie	927
Artykuł 55. Sprawozdania z działalności	933

Sekcja 2

Kompetencje, skoordynowane czynności sprawdzające i mechanizmy spójności	940
---	------------

Artykuł 56. Kompetencje	940
Artykuł 57. Wzajemna pomoc	948
Artykuł 58. Współpraca transgraniczna między koordynatorami ds. usług cyfrowych	957
Artykuł 59. Skierowanie sprawy do Komisji	966
Artykuł 60. Wspólne czynności sprawdzające	974

Sekcja 3

Europejska Rada ds. Usług Cyfrowych	983
--	------------

Artykuł 61. Europejska Rada ds. Usług Cyfrowych	983
Artykuł 62. Struktura Rady Usług Cyfrowych	987
Artykuł 63. Zadania Rady Usług Cyfrowych	991

Sekcja 4

Nadzór, czynności sprawdzające, egzekwowanie i monitorowanie w odniesieniu do dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych	994
--	------------

Artykuł 64. Rozwój wiedzy eksperckiej i zdolności	994
Artykuł 65. Egzekwowanie obowiązków dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych	1001

<i>Artykuł 66.</i> Wszczęcie postępowania przez Komisję i współpraca w ramach czynności sprawdzających	1009
<i>Artykuł 67.</i> Wnioski o udzielenie informacji	1016
<i>Artykuł 68.</i> Uprawnienie do odbierania wyjaśnień i przyjmowania oświadczeń	1028
<i>Artykuł 69.</i> Uprawnienia do przeprowadzania kontroli	1035
<i>Artykuł 70.</i> Środki tymczasowe	1051
<i>Artykuł 71.</i> Zobowiązania	1057
<i>Artykuł 72.</i> Działania z zakresu monitorowania	1064
<i>Artykuł 73.</i> Nieprzestrzeganie przepisów	1071
<i>Artykuł 74.</i> Grzywny	1078
<i>Artykuł 75.</i> Wzmoczony nadzór nad środkami zaradczymi w celu wyeliminowania naruszeń obowiązków ustanowionych w rozdziale III sekcja 5	1087
<i>Artykuł 76.</i> Okresowe kary pieniężne	1097
<i>Artykuł 77.</i> Termin przedawnienia dotyczący nakładania sankcji	1106
<i>Artykuł 78.</i> Termin przedawnienia dotyczący wykonania sankcji	1111
<i>Artykuł 79.</i> Prawo do bycia wysłuchanym i prawo dostępu do akt	1115
<i>Artykuł 80.</i> Publikacja decyzji	1126
<i>Artykuł 81.</i> Kontrola przez Trybunał Sprawiedliwości Unii Europejskiej	1130
<i>Artykuł 82.</i> Wnioski dotyczące ograniczeń dostępu i współpraca z sądami krajowymi	1136
<i>Artykuł 83.</i> Akty wykonawcze dotyczące interwencji Komisji	1147
 Sekcja 5	
Wspólne przepisy dotyczące egzekwowania	1154
 <i>Artykuł 84.</i> Tajemnica zawodowa	1154
<i>Artykuł 85.</i> System wymiany informacji	1160
<i>Artykuł 86.</i> Przedstawicielstwo	1166
 Sekcja 6	
Akty delegowane i wykonawcze	1173
 <i>Artykuł 87.</i> Wykonywanie przekazanych uprawnień	1173
<i>Artykuł 88.</i> Procedura komitetowa	1177
 Rozdział V	
Przepisy końcowe	1181
 <i>Artykuł 89.</i> Zmiany dyrektywy 2000/31/WE	1181
<i>Artykuł 90.</i> Zmiany dyrektywy (UE) 2020/1828	1183
<i>Artykuł 91.</i> Przegląd	1184

<i>Artykuł 92. Wcześniejsze stosowanie w stosunku do dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych</i>	1186
<i>Artykuł 93. Wejście w życie i stosowanie</i>	1188
Literatura	1191
Wykaz aktów prawnych	1205
Autorzy	1219

WYKAZ SKRÓTÓW

Akty prawne

- AIA – akt o sztucznej inteligencji, projekt rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji), COM(2021) 206 final, 2021/0106 (COD), Bruksela, 21.04.2021 r., <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021PC0206> (dostęp: 2.01.2024 r.)
- DA – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z 13.12.2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) (Dz.Urz. UE L 2023/2854)
- decyzja nr 768/2008/WE – decyzja Parlamentu Europejskiego i Rady nr 768/2008/WE z 9.07.2008 r. w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu, uchylająca decyzję Rady 93/465/EWG (Dz.Urz. UE L 218, s. 82)
- DGA – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z 30.05.2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz.Urz. UE L 152, s. 1)
- DMA, rozporządzenie 2022/1925 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z 14.09.2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz.Urz. UE L 265, s. 1)
- DSA, rozporządzenie nr 2022/2065 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z 19.10.2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) (Dz.Urz. UE L 277, s. 1)

DSM, dyrektywa 2019/790	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z 17.04.2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz.Urz. UE L 130, s. 92)
dyrektywa 85/374/EWG	– dyrektywa 85/374/EWG Rady z 25.07.1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe (Dz.Urz. WE L 210, s. 29, ze zm.)
dyrektywa 93/13/EWG	– dyrektywa Rady 93/13/EWG z 5.04.1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich (Dz.Urz. UE L 95, s. 29, ze zm.)
dyrektywa 93/83/EWG	– dyrektywa Rady nr 93/83/EWG z 27.09.1993 r. w sprawie koordynacji niektórych zasad dotyczących prawa autorskiego oraz praw pokrewnych stosowanych w odniesieniu do przekazu satelitarnego oraz retransmisji drogą kablową (Dz.Urz. UE L 248, s. 15, ze zm.)
dyrektywa 96/9/WE	– dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z 11.03.1996 r. w sprawie ochrony prawnej baz danych (Dz.Urz. UE L 77, s. 20, ze zm.)
dyrektywa 2000/31/WE	– dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z 8.06.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.Urz. UE L 178, s. 1, ze zm.)
dyrektywa 2001/29/WE	– dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z 22.05.2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.Urz. UE L 167, s. 10, ze zm.)
dyrektywa 2001/84/WE	– dyrektywa 2001/84/WE Parlamentu Europejskiego i Rady z 27.09.2001 r. w sprawie prawa autora do wynagrodzenia z tytułu odsprzedaży oryginalnego egzemplarza dzieła sztuki (Dz.Urz. UE L 272, s. 32)
dyrektywa 2001/95/WE	– dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady z 3.12.2001 r. w sprawie ogólnego bezpieczeństwa produktów (Dz.Urz. UE L 11 z 2002 r., s. 4, ze zm.)
dyrektywa 2002/58/WE	– dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. UE L 201, s. 37, ze zm.)
dyrektywa 2004/48/WE	– dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z 29.04.2004 r. w sprawie egzekwowania praw własności intelektualnej (Dz.Urz. UE L 157, s. 45)

dyrektywa 2005/29/WE	– dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z 11.05.2005 r. dotycząca nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca dyrektywę Rady 84/450/EWG, dyrektywy 97/7/WE, 98/27/WE i 2002/65/WE Parlamentu Europejskiego i Rady oraz rozporządzenie (WE) nr 2006/2004 Parlamentu Europejskiego i Rady („dyrektywa o nieuczciwych praktykach handlowych”) (Dz.Urz. UE L 149, s. 22, ze zm.)
dyrektywa 2006/115/WE	– dyrektywa 2006/115/WE Parlamentu Europejskiego i Rady z 12.12.2006 r. w sprawie prawa najmu i użyczenia oraz niektórych praw pokrewnych prawu autorskiemu w zakresie własności intelektualnej (Dz.Urz. UE L 376, s. 28)
dyrektywa 2006/116/WE	– dyrektywa 2006/116/WE Parlamentu Europejskiego i Rady z 12.12.2006 r. w sprawie czasu ochrony prawa autorskiego i niektórych praw pokrewnych (Dz.Urz. UE L 372, s. 12, ze zm.)
dyrektywa 2006/123/WE	– dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady z 12.12.2006 r. dotycząca usług na rynku wewnętrznym (Dz.Urz. UE L 376, s. 36)
dyrektywa 2009/24/WE	– dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z 23.04.2009 r. w sprawie ochrony prawnej programów komputerowych (Dz.Urz. UE L 111, s. 16)
dyrektywa 2009/48/WE	– dyrektywa Parlamentu Europejskiego i Rady 2009/48/WE z 18.06.2009 r. w sprawie bezpieczeństwa zabawek (Dz.Urz. UE L 170, s. 1)
dyrektywa 2010/13/UE	– dyrektywa Parlamentu Europejskiego i Rady 2010/13/UE z 10.03.2010 r. w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych) (Dz.Urz. UE L 95, s. 1, ze zm.)
dyrektywa 2011/36/UE	– dyrektywa Parlamentu Europejskiego i Rady 2011/36/UE z 5.04.2011 r. w sprawie zapobiegania handlowi ludźmi i zwalczania tego procederu oraz ochrony ofiar, zastępująca decyzję ramową Rady 2002/629/WSiSW (Dz.Urz. UE L 101, s. 1)
dyrektywa 2011/83/UE	– dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z 25.10.2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady (Dz.Urz. UE L 304, s. 64, ze zm.)
dyrektywa 2011/93/UE	– dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z 13.12.2011 r. w sprawie zwalczania niegodziwego traktowania

- w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.Urz. UE L 335, s. 1)
- dyrektywa 2012/28/UE – dyrektywa Parlamentu Europejskiego i Rady 2012/28/UE z 25.10.2012 r. w sprawie niektórych dozwolonych sposobów korzystania z utworów osieroconych (Dz.Urz. UE L 299, s. 5)
- dyrektywa 2013/11/UE – dyrektywa Parlamentu Europejskiego i Rady 2013/11/UE z 21.05.2013 r. w sprawie alternatywnych metod rozstrzygania sporów konsumenckich oraz zmiany rozporządzenia (WE) nr 2006/2004 i dyrektywy 2009/22/WE (dyrektywa w sprawie ADR w sporach konsumenckich) (Dz.Urz. UE L 165, s. 63)
- dyrektywa 2013/33/UE – dyrektywa Parlamentu Europejskiego i Rady 2013/33/UE z 26.06.2013 r. w sprawie ustanowienia norm dotyczących przyjmowania wnioskodawców ubiegających się o ochronę międzynarodową (Dz.Urz. UE L 180, s. 96)
- dyrektywa 2013/36/UE – dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z 26.06.2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE (Dz.Urz. UE L 176, s. 338, ze zm.)
- dyrektywa 2014/26/UE – dyrektywa Parlamentu Europejskiego i Rady 2014/26/UE z 26.02.2014 r. w sprawie zbiorowego zarządzania prawami autorskimi i prawami pokrewnymi oraz udzielania licencji wieloterytorialnych dotyczących praw do utworów muzycznych do korzystania online na rynku wewnętrznym (Dz.Urz. UE L 84, s. 72)
- dyrektywa 2014/56/UE – dyrektywa Parlamentu Europejskiego i Rady 2014/56/UE z 16.06.2014 r. zmieniająca dyrektywę 2006/43/WE w sprawie ustawowych badań rocznych sprawozdań finansowych i skonsolidowanych sprawozdań finansowych (Dz.Urz. UE L 158, s. 196)
- dyrektywa 2015/1535 – dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z 9.09.2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.Urz. UE L 241, s. 1)
- dyrektywa 2016/943 – dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z 8.06.2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Dz.Urz. UE L 157, s. 1)
- dyrektywa 2017/541 – dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z 15.03.2017 r. w sprawie zwalczania terroryzmu i zastępująca

	decyzję ramową Rady 2002/475/WSiSW oraz zmieniającą decyzję Rady 2005/671/WSiSW (Dz.Urz. UE L 88, s. 6)
dyrektywa 2017/1564	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/1564 z 13.09.2017 r. w sprawie niektórych dozwolonych sposobów korzystania z określonych utworów i innych przedmiotów chronionych prawem autorskim i prawami pokrewnymi z korzyścią dla osób niewidomych, osób słabowidzących lub osób z niepełnosprawnościami uniemożliwiającymi zapoznanie się z drukiem oraz w sprawie zmiany dyrektywy 2001/29/WE w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.Urz. UE L 242, s. 6)
dyrektywa 2018/1808	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1808 z 14.11.2018 r. zmieniająca dyrektywę 2010/13/UE w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych) ze względu na zmianę sytuacji na rynku (Dz.Urz. UE L 303, s. 69)
dyrektywa 2019/770	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z 20.05.2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Dz.Urz. UE L 136, s. 1)
dyrektywa 2019/789	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/789 z 17.04.2019 r. ustanawiająca przepisy dotyczące wykonywania praw autorskich i praw pokrewnych mające zastosowanie do niektórych transmisji online prowadzonych przez organizacje radiowe i telewizyjne oraz do reemisji programów telewizyjnych i radiowych oraz zmieniająca dyrektywę Rady 93/83/EWG (Dz.Urz. UE L 130, s. 82)
dyrektywa 2019/790	dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z 17.04.2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz.Urz. UE L 130, s. 92)
dyrektywa 2019/882	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/882 z 17.04.2019 r. w sprawie wymogów dostępności produktów i usług (Dz.Urz. UE L 151, s. 70)
dyrektywa 2019/1024	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z 20.06.2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz.Urz. UE L 172, s. 56)
dyrektywa 2019/2161, dyrektywa Omnibus	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/2161 z 27.11.2019 r. zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę Parlamentu Europejskiego i Rady 98/6/WE, 2005/29/WE

	oraz 2011/83/UE w odniesieniu do lepszego egzekwowania i unowocześnienia unijnych przepisów dotyczących ochrony konsumenta (Dz.Urz. UE L 328, s. 7)
dyrektywa 2020/1828	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2020/1828 z 25.11.2020 r. w sprawie powództw przedstawicielskich wytaczanych w celu ochrony zbiorowych interesów konsumentów i uchylająca dyrektywę 2009/22/WE (Dz.Urz. UE L 409, s. 1, ze zm.)
dyrektywa 2022/2555	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14.12.2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.Urz. UE L 333, s. 80)
dyrektywa 2023/1544	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/1544 z 12.07.2023 r. w sprawie zharmonizowanych przepisów dotyczących wskazywania wyznaczonych zakładów i ustanawiania przedstawicieli prawnych w celu gromadzenia dowodów elektronicznych w postępowaniach karnych (Dz.Urz. UE L 191, s. 181)
dyrektywa audytorska	– dyrektywa 2006/43/WE Parlamentu Europejskiego i Rady z 17.05.2006 r. w sprawie ustawowych badań rocznych sprawozdań finansowych i skonsolidowanych sprawozdań finansowych, zmieniająca dyrektywy Rady 78/660/EWG i 83/349/EWG oraz uchylająca dyrektywę Rady 84/253/EWG (Dz.Urz. UE L 157, s. 87, ze zm.)
EKPCz	– Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie 4.11.1950 r. (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.)
Europejski Kodeks Dobrej Praktyki Administracyjnej	– decyzja w sprawie Kodeksu Dobrej Praktyki Administracyjnej (Dz.Urz. UE C 285 z 2011 r., s. 3)
Europejski kodeks łączności elektronicznej k.c.	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z 11.12.2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (Dz.Urz. UE L 321, s. 36 ze zm.)
k.k.	– ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2023 r. poz. 1610 ze zm.)
	– ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2024 r. poz. 17 ze zm.)
Konstytucja RP	– Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.)
k.p.a.	– ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2023 r. poz. 775 ze zm.)

k.p.c.	– ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2023 r. poz. 1550 ze zm.)
k.p.k.	– ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2024 r. poz. 37)
KPP UE	– Karta praw podstawowych Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 389)
k.s.h.	– ustawa z 15.09.2000 r. – Kodeks spółek handlowych (Dz.U. z 2024 r. poz. 18 ze zm.)
pr. aut.	– ustawa z 4.02.1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2022 r. poz. 2509)
pr. przeds.	– ustawa z 6.03.2018 r. – Prawo przedsiębiorców (Dz.U. z 2023 r. poz. 221 ze zm.)
pr. tel.	– ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2024 r. poz. 34)
RODO	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1)
rozporządzenie 1182/71	– rozporządzenie Rady (EWG, EURATOM) nr 1182/71 z 3.06.1971 r. określające zasady mające zastosowanie do okresów, dat i terminów (Dz.Urz. UE L 124, s. 1, ze zm.)
rozporządzenie 2015/1589	– rozporządzenie Rady (UE) z 13.07.2015 r. ustanawiające szczegółowe zasady stosowania art. 108 Traktatu o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE L 248, s. 9)
rozporządzenie 2016/424	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/424 z 9.03.2016 r. w sprawie urządzeń kolei linowych i uchylenia dyrektywy 2000/9/WE (Dz.Urz. UE L 81, s. 1)
rozporządzenie 2016/794	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z 11.05.2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.Urz. UE L 135, s. 53, ze zm.)
rozporządzenie 2017/1128	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/1128 z 14.06.2017 r. w sprawie transgranicznego przenoszenia na rynku wewnętrznym usług online w zakresie treści (Dz.Urz. UE L 168, s. 1)
rozporządzenie 2017/1563	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/1563 z 13.09.2017 r. w sprawie transgranicznej wymiany między Unią a państwami trzecimi kopii w dostępnych formatach określonych

- utworów i innych przedmiotów chronionych prawem autorskim i prawami pokrewnymi z korzyścią dla osób niewidomych, osób słabowidzących lub osób z niepełnosprawnościami uniemożliwiającymi zapoznanie się z drukiem (Dz.Urz. UE L 242, s. 1)
- rozporządzenie 2017/2394 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2394 z 12.12.2017 r. w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów i uchylające rozporządzenie (WE) nr 2006/2004 (Dz.Urz. UE L 345, s. 1, ze zm.)
- rozporządzenie 2018/1046 – rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 z 18.07.2018 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, zmieniające rozporządzenia (UE) nr 1296/2013, (UE) nr 1301/2013, (UE) nr 1303/2013, (UE) nr 1304/2013, (UE) nr 1309/2013, (UE) nr 1316/2013, (UE) nr 223/2014 i (UE) nr 283/2014 oraz decyzję nr 541/2014/UE, a także uchylające rozporządzenie (UE, Euratom) nr 966/2012 (Dz.Urz. UE L 193, s. 1, ze zm.)
- rozporządzenie 2019/881 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17.04.2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.Urz. UE L 151, s. 15)
- rozporządzenie 2019/1020 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z 20.06.2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.Urz. UE L 169, s. 1, ze zm.)
- rozporządzenie 2019/1148 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1148 z 20.06.2019 r. w sprawie wprowadzania do obrotu i stosowania prekursorów materiałów wybuchowych, zmieniające rozporządzenie (WE) nr 1907/2006 i uchylające rozporządzenie (UE) nr 98/2013 (Dz.Urz. UE L 186, s. 1)
- rozporządzenie 2021/784 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z 29.04.2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz.Urz. UE L 172, s. 79)
- rozporządzenie 2022/1925 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z 14.09.2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/1937 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz.Urz. UE L 265, s. 1)

rozporządzenie 2023/988, ORBP	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/988 z 10.05.2023 r. w sprawie ogólnego bezpieczeństwa produktów, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 i dyrektywę Parlamentu Europejskiego i Rady (UE) 2020/1828 oraz uchylające dyrektywę 2001/95/WE Parlamentu Europejskiego i Rady i dyrektywę Rady 87/357/EWG (Dz.Urz. UE L 135, s. 1)
rozporządzenie 2023/1543	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z 12.07.2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz.Urz. UE L 191, s. 118)
rozporządzenie delegowane 2023/1127	– rozporządzenie delegowane Komisji (UE) 2023/1127 z 2.03.2023 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 o szczegółową metodykę i procedury dotyczące opłat nadzorczych pobieranych przez Komisję od dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych (Dz.Urz. UE L 149, s. 16)
rozporządzenie delegowane 2024/436	– rozporządzenie delegowane Komisji (UE) 2024/436 z 20.10.2023 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 przez ustanowienie przepisów dotyczących przeprowadzania audytów w odniesieniu do bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych (Dz.Urz. UE L 2024/436)
rozporządzenie e-IDAS	– rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23.07.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.Urz. UE L 257, s. 73, ze zm.)
rozporządzenie P2B, rozporządzenie 2019/1150	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1150 z 20.06.2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz.Urz. UE L 186, s. 57)
rozporządzenie nr 1/2003	– rozporządzenie Rady (WE) nr 1/2003 z 16.12.2002 r. w sprawie wprowadzenia w życie reguł konkurencji ustanowionych w art. 81 i 82 Traktatu (Dz.Urz. UE L 1 z 2003 r., s. 1, ze zm.)
rozporządzenie nr 139/2004	– rozporządzenie Rady (WE) nr 139/2004 z 20.01.2004 r. w sprawie kontroli koncentracji przedsiębiorstw (rozporządzenie WE w sprawie kontroli łączenia przedsiębiorstw) (Dz.Urz. UE L 24, s. 1)

rozporządzenie nr 773/2004	– rozporządzenie Komisji (WE) nr 773/2004 z 7.04.2004 r. odnoszące się do prowadzenia przez Komisję postępowań zgodnie z art. 81 i art. 82 Traktatu WE (Dz.Urz. UE L 123, s. 18, ze zm.)
rozporządzenie nr 182/2011	– rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z 16.02.2011 r. ustanawiającym przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.Urz. UE L 55, s. 13)
rozporządzenie nr 1025/2012	– rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z 25.10.2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.Urz. UE L 316, s. 12)
rozporządzenie nr 1215/2012, Bruksela I bis	– rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012 z 12.12.2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (Dz.Urz. UE L 351, s. 1, ze zm.)
rozporządzenie nr 537/2014	– rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 537/2014 z 16.04.2014 r. w sprawie szczegółowych wymogów dotyczących ustawowych badań sprawozdań finansowych jednostek interesu publicznego, uchylające decyzję Komisji 2005/909/WE (Dz.Urz. L 158, s. 77, ze zm.)
rozporządzenie Rzym I	– rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 593/2008 z 17.06.2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Rzym I) (Dz.Urz. UE L 177, s. 6)
rozporządzenie Rzym II	– rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 864/2007 z 11.07.2007 r. dotyczące prawa właściwego dla zobowiązań pozaumownych (Rzym II) (Dz.Urz. UE L 199, s. 40)
rozporządzenie w sprawie IMI	– rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1024/2012 z 25.10.2012 r. w sprawie współpracy administracyjnej za pośrednictwem systemu wymiany informacji na rynku wewnętrznym i uchylające decyzję Komisji 2008/49/WE („rozporządzenie w sprawie IMI”) (Dz.Urz. UE L 316, s. 1, ze zm.)
rozporządzenie wykonawcze 2023/1201	– rozporządzenie wykonawcze Komisji (UE) 2023/1201 z 21.06.2023 r. w sprawie szczegółowych zasad dotyczących prowadzenia przez Komisję niektórych postępowań na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 (akt o usługach cyfrowych) (Dz.Urz. UE L 159, s. 51)
TFUE	– Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 47)

TUE	– Traktat o Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 13)
u.f.p.	– ustawa z 27.08.2009 r. o finansach publicznych (Dz.U. z 2023 r. poz. 1270 ze zm.)
u.i.d.p.	– ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2023 r. poz. 57 ze zm.)
u.o.d.o.	– ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781)
u.o.k.i.k.	– ustawa z 16.02.2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2023 r. poz. 1689 ze zm.)
u.p.k.	– ustawa z 30.05.2014 r. o prawach konsumenta (Dz.U. z 2023 r. poz. 2759 ze zm.)
u.p.n.p.r.	– ustawa z 23.08.2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym (Dz.U. z 2023 r. poz. 845)
u.p.r.s.k.	– ustawa z 23.09.2016 r. o pozasądowym rozwiązywaniu sporów konsumenckich (Dz.U. poz. 1823)
u.s.p.	– ustawa z 29.06.1995 r. o statystyce publicznej (Dz.U. z 2023 r. poz. 773)
u.ś.u.d.e.	– ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344)
u.z.n.k.	– ustawa z 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2022 r. poz. 1233)
zalecenie 2003/361/WE	– zalecenie Komisji 2003/361/WE z 6.05.2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.Urz. WE L 124, s. 36)
zalecenie 2018/334	– zalecenie Komisji (UE) 2018/334 z 1.03.2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie (Dz.Urz. UE L 63, s. 50)

Czasopisma i publikatory

EPS	– Europejski Przegląd Sądowy
GRUR	– Gewerblicher Rechtsschutz und Urheberrecht
HUDOC	– baza orzecznictwa Europejskiego Trybunału Praw Człowieka (European Court of Human Rights)
iKAR	– internetowy Kwartalnik Antymonopolowy i Regulacyjny
JIPITEC	– Journal of Intellectual Property, Information Technology and E-Commerce Law
KPP	– Kwartalnik Prawa Prywatnego
MMR	– Multimedia und Recht
MoP	– Monitor Prawniczy
M. Praw.	– Monitor Prawniczy
NJW	– Neue Juristische Wochenschrift

OSNC	– Orzecznictwo Sądu Najwyższego. Izba Cywilna
PNT	– Prawo Nowych Technologii
PPH	– Przegląd Prawa Handlowego
PS	– Przegląd Sądowy
RPEiS	– Ruch Prawniczy, Ekonomiczny i Socjologiczny
SSRN	– Social Science Research Network
TBSP UJ	– Towarzystwo Biblioteki Słuchaczy Prawa Uniwersytetu Jagiellońskiego

Inne

API	– interfejs oprogramowania aplikacyjnego
BEUC	– The European Consumer Organisation
DUUTO	– dostawca usług udostępniania treści on-line
EIOD	– Europejski Inspektor Ochrony Danych
ETPCz	– Europejski Trybunał Praw Człowieka
EOG	– Europejski Obszar Gospodarczy
EROD	– Europejska Rada Ochrony Danych
MŚP	– małe i średnie przedsiębiorstwa
RBA	– odejście oparte na ryzyku (ang. <i>risk-based approach</i>)
SA	– sąd apelacyjny
SN	– Sąd Najwyższy
SN (7)	– Sąd Najwyższy w składzie siedmiu sędziów
TS	– Trybunał Sprawiedliwości
UE	– Unia Europejska
UKE	– Urząd Komunikacji Elektronicznej
UODO	– Urząd Ochrony Danych Osobowych
UOKiK	– Urząd Ochrony Konkurencji i Konsumentów
VLOP	– bardzo duże platformy internetowe
VLOSE	– bardzo duże wyszukiwarki internetowe
założenia projektu ustawy	– założenia projektu ustawy o zmiennej ustawie o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw wdrażającej 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), https://www.gov.pl/web/cyfryzacja/konsultacje-dotyczace-wdrozenia-aktu-o-uslugach-cyfrowych-digital-services-act (dostęp: 6.01.2024 r.)

SŁOWO WSTĘPNE

1. W pierwotnej wersji zbioru cyfrowych zasad Unii Europejskiej, którą od listopada 2020 r. promuje Komisja Europejska jako sposób regulacji rynków, usług i technologii cyfrowych, akt o usługach cyfrowych (DSA) był formalnie tylko jednym z pięciu głównych rozdziałów większej całości, na którą miały się składać również: akt o zarządzaniu danymi (DGA), akt o rynkach cyfrowych (DMA), akt o sztucznej inteligencji (AIA) i akt o danych (DA). Od początku było jednak jasne, że pozycja DSA w „zbiorze” jest na tyle podstawowa, że uchwalenie tego rozporządzenia jest warunkiem *sine qua non* prowadzenia prac nad resztą aktów.

W momencie zakończenia prac nad niniejszym komentarzem wiemy, że plan Komisji dotyczący całości zbioru ma ogromne szanse na realizację, gdyż cztery z pięciu planowanych aktów zostały uchwalone przed zakończeniem kadencji Komisji Europejskiej i Parlamentu Europejskiego, a ostatni z „rozdziałów” – akt o sztucznej inteligencji – czeka na przekształcenie wstępnej zgody politycznej w ostateczny tekst, który może zostać opublikowany w Dzienniku Urzędowym.

Cokolwiek by się nie stało na finiszu prac nad zbiorem, dwa podstawowe filary – DSA i DMA – stoją stabilnie w centrum wspólnej europejskiej przestrzeni cyfrowej. Cytując słowa komunikatu Komisji Europejskiej, wydane po przyjęciu DSA, jednolity zbiór przepisów dla całej UE stworzy odpowiednie warunki do rozwoju transgranicznych usług cyfrowych, co może doprowadzić do zwiększenia udziału transgranicznego handlu cyfrowego w jednolitym rynku nawet o 2%. Jednocześnie nowe przepisy tworzą gwarancję, że małe platformy internetowe nie będą postawione w nieproporcjonalnie gorszej pozycji, a zarazem nadal będą ponosić pełną odpowiedzialność. Małe firmy – zdaniem Komisji – będą miały pewność prawną, która pozwoli im rozwijać usługi i chronić użytkowników przed nielegalnymi działaniami, gdyż uzyskają wsparcie w postaci norm i wytycznych. Będą też zwolnione z najpoważniejszych obciążeń finansowych, ale zyskają swobodę stosowania sprawdzonych rozwiązań, co pozwoli im uzyskać przewagę konkurencyjną.

2. Akt o usługach cyfrowych nie pojawił się jednak w próżni. Europejski prawodawca musiał odnieść się nie tylko do bezpośrednich poprzedników każdej z części zbioru (o ile takie

poprzedzające akty istniały), lecz także – a może przede wszystkim – oprzeć je na fundamentach wybudowanych w poprzednich latach w Unii. W przypadku DSA oznaczało to inkorporowanie lub zmianę zasad wynikających z aktów takich jak dyrektywa o handlu elektronicznym, przy jednoczesnym oparciu nowych rozwiązań na konstytucyjnych podstawach wypracowanych przez Traktat z Lizbony (prawa podstawowe) dookreślonych w aktach takich jak ogólne rozporządzenie o ochronie danych (RODO).

Niniejszy komentarz został napisany przez autorów, którzy łączą głęboką wiedzę o rynkach cyfrowych i wyzwaniach ich regulacji ze znajomością prawnych i technicznych zagadnień przetwarzania danych osobowych, które jest nieodłączną i podstawową działalnością podmiotów działających na rynkach cyfrowych. Jest to wyjątkowo cenne dla czytelnika, który patrzy na regulację rynków i usług przez pryzmat praw podstawowych do prywatności i ochrony danych osobowych (art. 7 i 8 KPP UE), a taką perspektywę przyjmuję jako europejski inspektor ochrony danych (EIOD). Wiedza całego zespołu komentatorów na temat modeli biznesowych i technologii regulowanych przez każdą z wyżej wymienionych regulacji umożliwia autorom odniesienie ich do zasad ochrony danych osobowych także w przypadku tych przepisów w nowych aktach, które wyraźnie dotyczą definicji, pojęć i obowiązków RODO.

Zachęcam tym samym wszystkich czytelników komentarza do prześledzenia rozważań dotyczących w oczywisty sposób wskazanych powiązań z unijnym prawem dotyczącym ochrony danych (np. art. 26 ust. 3, art. 28 ust. 2 czy art. 38 DSA) lub mogących mieć wpływ na przetwarzanie danych osobowych przez podmioty objęte aktem o usługach cyfrowych. Pozwolę sobie – tytułem zapowiedzi – zwrócić uwagę czytelników na najbardziej znaczące interakcje DSA i RODO. Czytanie całości komentarza będzie bowiem wymagać interpretacji definicji, pojęć lub obowiązków wynikających z RODO. Jednocześnie realizacja niektórych uprawnień i obowiązków wprowadzanych przez DSA będzie wywoływała interakcje z RODO. DSA i RODO realizują różne, ale uzupełniające się cele. Podczas gdy RODO ma na celu ochronę osób fizycznych w odniesieniu do przetwarzania danych osobowych, DSA ma na celu zwalczanie pewnych zjawisk szkodliwych społecznie, takich jak rozpowszechnianie nielegalnych treści, dezinformacja online i inne zagrożenia społeczne. Jednocześnie DSA zawiera kilka przepisów, które będą miały wpływ na przetwarzanie danych osobowych przez platformy internetowe, w tym zasady dotyczące reklamy internetowej, systemów rekomendacji i ochrony małoletnich. Ponadto wiele przepisów DSA odnosi się wprost do ochrony danych osobowych, a także definicji i pojęć w ramach RODO, takich jak „profilowanie” i „szczególne kategorie danych”.

Biorąc pod uwagę silną interakcję z unijnym prawem ochrony danych, konieczne jest zapewnienie spójnego i konsekwentnego podejścia regulacyjnego w odniesieniu do obu instrumentów w praktyce. Żadne z postanowień DSA nie powinno być stosowane ani interpretowane w taki sposób, aby zmniejszać lub ograniczać poziom ochrony oferowany przez unijne prawo o ochronie danych. DSA wyraźnie potwierdza, że pozostaje bez

uszczerbku dla unijnych przepisów o ochronie danych oraz że ochrona osób fizycznych w odniesieniu do przetwarzania danych osobowych podlega wyłącznie unijnym przepisom o ochronie danych.

Niestety DSA, pozostawiając kwestie zarządzania wprowadzaniem w życie zasad wynikających z DSA państwom członkowskim, nie przewiduje zorganizowanej współpracy organów regulacyjnych wykonujących DSA i organów nadzorczych z zakresu danych osobowych. O wskazanie zasad takiej współpracy apelowałem jako EIOD wraz z Europejską Radą Ochrony Danych (EROD).

3. Wśród najważniejszych podobieństw pomiędzy DSA i RODO należy wymienić kwestie związane z oceną i ograniczaniem ryzyka. Przepisy art. 34 i 35 DSA wymagają od tzw. bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych oceny i ograniczania wszelkich ryzyk systemowych wynikających z projektowania, funkcjonowania i korzystania z ich usług. Ta ocena ryzyka musi obejmować m.in. wszelkie rzeczywiste lub przewidywalne negatywne skutki dla wykonywania praw podstawowych, w tym poszanowania życia prywatnego i rodzinnego, ochrony danych osobowych. Ocena ta musi uwzględniać m.in. „praktyki związane z danymi” stosowane przez te podmioty. Obowiązki bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych w zakresie oceny i ograniczania ryzyka pokrywają się w pewnym stopniu z ich obowiązkami opartymi na ryzyku jako administratorów na mocy RODO (w szczególności art. 24, 25, 35 i 36 RODO). Co więcej, niektóre środki mające na celu przeciwdziałanie ryzyku systemowemu będą prawdopodobnie się wiązać z przetwarzaniem danych osobowych, co musi wywołać pytania dotyczące zakresu, w jakim takie przetwarzanie jest zgodne z RODO. Inną kwestią, która może się pojawić, jest to, czy rola komórki ds. przestrzegania DSA (art. 41 DSA) może być połączona z rolą inspektora ochrony danych (art. 37–39 RODO).

Jednym z najważniejszych obszarów regulacyjnych DSA jest zwalczanie nielegalnych treści w internecie. Podczas gdy DSA zakazuje nakładania ogólnego obowiązku monitorowania lub aktywnego ustalania faktów (art. 8), stara się również wyeliminować istniejące czynniki zniechęcające do dobrowolnych dochodzeń z własnej inicjatywy podejmowanych przez dostawców usług pośrednictwa (art. 7). Wysiłki mające na celu identyfikację, wykrywanie, usuwanie lub podejmowanie innych działań w związku z nielegalnymi treściami lub niewłaściwym korzystaniem z usług (np. zawieszenie konta) prawdopodobnie wiązać się z przetwarzaniem danych osobowych, jednak DSA nie określa, w jakim stopniu takie przetwarzanie byłoby zgodne z prawem lub proporcjonalne.

DSA ustanawia szczególne obowiązki dla dostawców platform internetowych w celu zapewnienia przejrzystości reklamy online (art. 26 ust. 1–2). Zakazuje także prezentowania reklam online „opartych na profilowaniu z wykorzystaniem szczególnych kategorii danych” (art. 26 ust. 3). Ważne będzie doprecyzowanie zakresu tego zakazu oraz precyzyjne określenie, w jakich okolicznościach reklama internetowa faktycznie obejmuje

„profilowanie z wykorzystaniem szczególnych kategorii danych” (np. w kontekście targowania użytkowników mediów społecznościowych), z odwołaniem się w tym przypadku bezpośrednio do przepisów RODO.

Zasadę tę rozwinął europejski prawodawca w przepisach art. 28 DSA, zabraniając dostawcom platform internetowych prezentowania reklam opartych na profilowaniu z wykorzystaniem danych osobowych osób małoletnich, gdy są oni świadomi z wystarczającą pewnością, że odbiorca usługi jest osobą małoletnią. Jednocześnie DSA nie zobowiązuje nikogo do przetwarzania dodatkowych danych osobowych jedynie w celu oceny wieku użytkownika. Co więcej, te same przepisy wymagają również od dostawców platform wprowadzenia „odpowiednich i proporcjonalnych środków w celu zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony” małoletnich. Obowiązki te w pewnym stopniu pokrywają się z ochroną dzieci na podstawie przepisów RODO.

Bardzo ciekawym *novum* regulacyjnym są przepisy o dostępie do danych udzielanym – w specjalnym trybie – zweryfikowanym naukowcom, którzy na mocy art. 40 ust. 4 DSA mogą starać się o taki dostęp bezpośredni lub za pośrednictwem interfejsów API. Jakkolwiek szczegółowo nie opisałby europejski prawodawca odpowiednich procedur w dwunastu ustępach art. 40 DSA, to ostatecznie brak sprzeczności tych procedur i ich celów z RODO jest podstawowym wskazaniem dla Komisji Europejskiej (i dla Rady Usług Cyfrowych) przy stanowieniu aktów delegowanych określających warunki techniczne udostępniania danych oraz cele, do których dane te mogą być wykorzystywane.

Wydaje się, że doświadczenia z wdrażania RODO miały również spory wpływ na przepisy DSA dotyczące kodeksów postępowania. Komisja i Rada Usług Cyfrowych są zobowiązane do wspierania ich powstawania i ułatwiania ich opracowywania. Obowiązki te jednak dotyczą jedynie poziomu unijnego i, co więcej, w swoisty sposób obostrzone są sugerowanym terminem na przygotowanie takich dokumentów. Kodeksy mają przyczynić się do właściwego stosowania rozporządzenia, uwzględniając zwłaszcza specyficzne wyzwania związane ze zwalczaniem różnych rodzajów nielegalnych treści i ryzyka systemowego. DSA szczególnie podkreśla wymagania co do ich zgodności z prawem Unii, w szczególności dotyczące konkurencji i ochrony danych osobowych.

4. Przed nami etap wdrożenia DSA w poszczególnych państwach członkowskich. Mam nadzieję, że komentarz będzie stanowić przede wszystkim pomocne narzędzie do praktycznej analizy niełatwych przepisów prawnych budowanych na fundamencie, jaki stanowi prawo unijne.

Akt o usługach cyfrowych jest co prawda rozporządzeniem, a normy wynikające z przepisów rozporządzenia powinny być z zasady obowiązujące bezpośrednio i gotowe do bezpośredniego stosowania. Powinny także wywoływać bezpośredni skutek zarówno w wymiarze horyzontalnym, jak i wertykalnym. A jednak wdrożenie norm z rozporządzeń

w praktyce systemów prawnych państw członkowskich jest zadaniem bardziej złożonym niż binarne rozróżnienie między rozporządzeniem a dyrektywą, gdzie ten drugi rodzaj aktu prawnego określa się jako formułujący jedynie cel i termin jego osiągnięcia. Takie „szkolne rozróżnienie” nie sprawdzało się już przy przepisach dyrektywy o handlu elektronicznym – choćby tych o cashingu, hostingu i mere conduit, które mimo że pochodzące z dyrektywy, dawały się implementować jedynie przez „przepisanie słowo w słowo” do prawa krajowego i przez w miarę zharmonizowane interpretowanie przez organy państw członkowskich, w tym przez sądy. Nie sprawdzało się ono również w wypadku RODO, które choć wydane w formie rozporządzenia, wymagało od początku klasycznej ustawy implementującej, a dziś jest uzupełniane przez rozporządzenie ustanawiające dodatkowe przepisy proceduralne dotyczące egzekwowania RODO.

Stosowanie norm wyprowadzanych z aktu o usługach cyfrowych będzie się łączyło z podobnymi wyzwaniem. Należy jednak ufać, że korzystając z doświadczeń wdrażania aktów takich jak RODO, w pełni świadomi powiązań DSA z aktami: o zarządzaniu danymi, o rynkach cyfrowych, o danych i przyszłym aktem o sztucznej inteligencji, będziemy w stanie sprostać zadaniu budowy konkurencyjnej wspólnej przestrzeni cyfrowej, która przyniesie wszystkim uczestnikom gry rynkowej i użytkownikom poczucie zaufania do panujących w niej reguł.

Bruksela, 23.01.2024 r.

Dr hab. Wojciech R. Wiewiórowski

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)

(Tekst mający znaczenie dla EOG)

(Dz.Urz. UE L 277, s. 1; sprost. Dz.Urz. UE L 163 z 2023 r., s. 107)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,
uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 114,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego¹,

uwzględniając opinię Komitetu Regionów²,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą³,

a także mając na uwadze, co następuje:

- (1) Usługi społeczeństwa informacyjnego, zwłaszcza usługi pośrednie, stały się ważną częścią unijnej gospodarki i życia codziennego obywateli Unii. Dwa-dzieścia lat po przyjęciu obowiązujących ram prawnych regulujących takie usługi, ustanowionych w dyrektywie 2000/31/WE Parlamentu Europejskiego

¹ Dz.Urz. UE C 286 z 2021 r., s. 70.

² Dz.Urz. UE C 440 z 2021 r., s. 67.

³ Stanowisko Parlamentu Europejskiego z 5.07.2022 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z 4.10.2022 r.

i Rady⁴, nowe i innowacyjne modele biznesowe i usługi, takie jak internetowe serwisy społecznościowe i internetowe platformy umożliwiające konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość, pozwoliły użytkownikom biznesowym i konsumentom na przekazywanie i uzyskiwanie dostępu do informacji oraz zawieranie transakcji na nowe sposoby. Większość obywateli Unii korzysta obecnie z tych usług na co dzień. Jednakże transformacja cyfrowa i wzmożone korzystanie z tych usług przyniosły również nowe zagrożenia i wyzwania dla indywidualnych odbiorców danej usługi, przedsiębiorstw i całego społeczeństwa.

- (2) Państwa członkowskie coraz częściej wprowadzają przepisy krajowe dotyczące spraw objętych zakresem stosowania niniejszego rozporządzeniem lub rozważają wprowadzenie takich przepisów, nakładając w szczególności wymogi w zakresie należytej staranności obowiązujące dostawców usług pośrednich dotyczące tego, w jaki sposób podmioty te powinny podchodzić do problemu nielegalnych treści, dezinformacji online i innych zagrożeń społecznych. Takie rozbieżne przepisy krajowe mają negatywny wpływ na rynek wewnętrzny, który zgodnie z art. 26 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) obejmuje obszar bez granic wewnętrznych, w którym jest zapewniony swobodny przepływ towarów i usług oraz swoboda przedsiębiorczości, biorąc pod uwagę z natury transgraniczny charakter internetu, który jest powszechnie wykorzystywany w celu świadczenia tych usług. Konieczna jest harmonizacja warunków świadczenia usług pośrednich na całym rynku wewnętrznym, aby zapewnić przedsiębiorstwom dostęp do nowych rynków i możliwości czerpania korzyści z rynku wewnętrznego przy jednoczesnym zapewnieniu większego wyboru konsumentom i innym odbiorcom usług. Do celów niniejszego rozporządzenia za „odbiorców usługi” uważa się użytkowników biznesowych, konsumentów i innych użytkowników.
- (3) Odpowiedzialne zachowanie i działanie z należytą starannością dostawców usług pośrednich ma zasadnicze znaczenie dla bezpiecznego, przewidywalnego i godnego zaufania środowiska internetowego oraz dla umożliwienia obywatelom Unii i innym osobom korzystania z przysługujących im praw podstawowych zagwarantowanych w Karcie praw podstawowych Unii Europejskiej (zwanej dalej „Kartą”), w szczególności z wolności wypowiedzi i informacji, wolności prowadzenia działalności gospodarczej, prawa do niedyskryminacji, a także z wysokiego poziomu ochrony konsumentów.
- (4) Dlatego też, w celu ochrony rynku wewnętrznego i poprawienia jego funkcjonowania należy ustanowić zestaw jednolitych, skutecznych i proporcjonalnych obowiązkowych zasad na poziomie Unii. Niniejsze rozporządzenie zapewnia

⁴ Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z 8.06.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.Urz. UE L 178, s. 1).

warunki umożliwiające wprowadzanie innowacyjnych usług cyfrowych na rynku wewnętrznym i zwiększanie ich skali. Zbliżenie krajowych środków regulacyjnych na poziomie Unii dotyczących wymogów obowiązujących dostawców usług pośrednich jest konieczne w celu uniknięcia fragmentacji rynku wewnętrznego i położenia jej kresu oraz zapewnienia pewności prawa, a tym samym ograniczenia niepewności po stronie deweloperów i wspierania interoperacyjności. Stosowanie wymogów neutralnych pod względem technologicznym nie powinno utrudniać innowacji, lecz je stymulować.

- (5) Niniejsze rozporządzenie powinno mieć zastosowanie do dostawców niektórych usług społeczeństwa informacyjnego zgodnie z definicją w dyrektywie (UE) 2015/1535 Parlamentu Europejskiego i Rady⁵, tj. każdej usługi normalnie świadczonej za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy. W szczególności niniejsze rozporządzenie powinno mieć zastosowanie do dostawców usług pośrednich, w szczególności usług pośrednich polegających na świadczeniu usług znanych jako usługi „zwykłego przekazu”, „cachingu” i „hostingu”, biorąc pod uwagę, że wykładniczy wzrost korzystania z tych usług, głównie we wszelkiego rodzaju zgodnych z prawem i użytecznych społecznie celach, zwiększył również ich rolę w pośrednictwie w zakresie niezgodnych z prawem lub w inny sposób szkodliwych informacji i działań oraz ich rozpowszechnianiu.
- (6) W praktyce niektórzy dostawcy usług pośrednich pośredniczą w zakresie usług, które mogą, ale nie muszą być świadczone drogą elektroniczną, takich jak zdalne usługi technologii informacyjnej, transport, zakwaterowanie lub usługi doręczeń. Niniejsze rozporządzenie powinno mieć zastosowanie wyłącznie do usług pośrednich i nie powinno mieć wpływu na wymogi określone w prawie Unii lub prawie krajowym dotyczące produktów lub usług, których świadczenie odbywa się poprzez usługi pośrednie, w tym w sytuacjach, w których usługa pośrednia stanowi integralną część innej usługi, która nie jest usługą pośrednią zgodnie z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej.
- (7) Aby zapewnić skuteczność przepisów ustanowionych w niniejszym rozporządzeniu oraz równe warunki działania na rynku wewnętrznym, przepisy te powinny mieć zastosowanie do dostawców usług pośrednich, niezależnie od ich miejsca siedziby lub miejsca, w którym się znajdują, o ile oferują oni usługi w Unii, czego dowodem jest istotne powiązanie z Unią.
- (8) Należy uznać, że takie istotne powiązanie z Unią zachodzi, jeżeli dostawca usług ma siedzibę w Unii lub, w przypadku braku takiej siedziby, jeżeli liczba odbiorców usługi w co najmniej jednym państwie członkowskim jest znaczna

⁵ Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z 9.09.2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz.Urz. UE L 241, s. 1).

w stosunku do liczby ludności danego państwa członkowskiego lub państw członkowskich lub na podstawie ukierunkowania działalności na co najmniej jedno państwo członkowskie. To, czy działalność jest ukierunkowana na co najmniej jedno państwo członkowskie można ustalić na podstawie wszelkich istotnych okoliczności, w tym takich czynników, jak posługiwanie się językiem lub walutą, których powszechnie używa się w tym państwie członkowskim, lub możliwość składania zamówień na produkty lub usługi, lub korzystanie z odpowiedniej domeny najwyższego poziomu. Ukierunkowanie działalności na państwo członkowskie może również wynikać z dostępności aplikacji w danym krajowym sklepie z aplikacjami, z obecności reklam na rynku lokalnym lub z posługiwania się w reklamach językiem używanym w tym państwie członkowskim, lub z zarządzania relacjami z klientem polegającego na przykład na obsłudze klientów w języku powszechnie używanym w tym państwie członkowskim. W przypadku gdy dostawca usług kieruje swoją działalność do co najmniej jednego państwa członkowskiego w rozumieniu art. 17 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1215/2012⁶, należy również domniemywać, że zachodzi istotne powiązanie. Natomiast sama tylko techniczna dostępność strony internetowej z Unii nie może, wyłącznie na tej podstawie, być uznana za ustanawiającą istotne powiązanie z Unią.

- (9) Niniejsze rozporządzenie w pełni harmonizuje przepisy mające zastosowanie do usług pośrednich na rynku wewnętrznym w celu zapewnienia bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego, przeciwdziałania rozpowszechnianiu nielegalnych treści w internecie oraz zagrożeniom społecznym, jakie może stwarzać rozpowszechnianie dezinformacji lub innych treści, w którym to środowisku prawa podstawowe zapisane w Karcie są skutecznie chronione, a innowacje są wspierane. W rezultacie – o ile nie jest to wyraźnie przewidziane w niniejszym rozporządzeniu – państwa członkowskie nie powinny przyjmować lub utrzymywać w mocy dodatkowych wymogów krajowych w odniesieniu do spraw objętych zakresem niniejszego rozporządzenia, ponieważ miałyby to wpływ na bezpośrednie i jednolite stosowanie w pełni zharmonizowanych przepisów mających zastosowanie do dostawców usług pośrednich zgodnie z celami niniejszego rozporządzenia. Nie powinno to wykluczać możliwości stosowania innych przepisów krajowych mających zastosowanie do dostawców usług pośrednich, zgodnie z prawem Unii, w tym dyrektywą 2000/31/WE, w szczególności z jej art. 3, w przypadku gdy przepisy prawa krajowego służą realizacji uzasadnionych celów leżących w interesie publicznym, innych niż cele niniejszego rozporządzenia.

⁶ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012 z 12.12.2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (Dz.Urz. UE L 351, s. 1).

(10) Niniejsze rozporządzenie powinno pozostawać bez uszczerbku dla innych aktów prawa Unii regulujących świadczenie usług społeczeństwa informacyjnego w ujęciu ogólnym, regulujących inne aspekty świadczenia usług pośrednich na rynku wewnętrznym lub określających i uzupełniających przepisy zharmonizowane określone w niniejszym rozporządzeniu, takich jak dyrektywa Parlamentu Europejskiego i Rady 2010/13/UE⁷, łącznie z jej przepisami dotyczącymi platform udostępniania plików wideo, rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1148⁸, (UE) 2019/1150⁹, (UE) 2021/784¹⁰ i (UE) 2021/1232¹¹ oraz dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady¹², jak również przepisy prawa Unii ustanowione w rozporządzeniu w sprawie europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych oraz w dyrektywie ustanawiającej zharmonizowane przepisy dotyczące mianowania przedstawicieli prawnych w celu gromadzenia dowodów na potrzeby postępowań karnych.

Podobnie w celu zapewnienia jasności niniejsze rozporządzenie powinno pozostawać bez uszczerbku dla prawa Unii dotyczącego ochrony konsumentów, w szczególności, rozporządzeń Parlamentu Europejskiego i Rady (UE) 2017/2394¹³ i (UE) 2019/1020¹⁴ oraz dyrektyw Parlamentu Europejskiego i Rady

⁷ Dyrektywa Parlamentu Europejskiego i Rady 2010/13/UE z 10.03.2010 r. w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych) (Dz.Urz. UE L 95, s. 1).

⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1148 z 20.06.2019 r. w sprawie wprowadzania do obrotu i stosowania prekursorów materiałów wybuchowych, zmieniające rozporządzenie (WE) nr 1907/2006 i uchylające rozporządzenie (UE) nr 98/2013 (Dz.Urz. UE L 186, s. 1).

⁹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1150 z 20.06.2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz.Urz. UE L 186, s. 57).

¹⁰ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z 29.04.2021 r. w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym (Dz.Urz. UE L 172, s. 79).

¹¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1232 z 14.07.2021 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 (Dz.Urz. UE L 274, s. 41).

¹² Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. UE L 201, s. 37).

¹³ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2394 z 12.12.2017 r. w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów i uchylające rozporządzenie (WE) nr 2006/2004 (Dz.Urz. UE L 345, s. 1).

¹⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z 20.06.2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE oraz rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011 (Dz.Urz. UE L 169, s. 1).

2001/95/WE¹⁵, 2005/29/WE¹⁶, 2011/83/UE¹⁷ i 2013/11/UE¹⁸, a także dyrektywy Rady 93/13/EWG¹⁹ jak również dla prawa Unii dotyczącego ochrony danych osobowych, w szczególności rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679²⁰.

Niniejsze rozporządzenie powinno również pozostawać bez uszczerbku dla przepisów Unii w dziedzinie prawa prywatnego międzynarodowego, w szczególności w zakresie własności oraz uznawania i wykonywania orzeczeń sądowych w sprawach cywilnych i handlowych, takich jak rozporządzenie (UE) nr 1215/2012, oraz prawa właściwego dla zobowiązań umownych i pozaumownych. Ochrona osób fizycznych w zakresie przetwarzania danych osobowych podlega wyłącznie przepisom prawa Unii w tej dziedzinie, w szczególności rozporządzeniu (UE) 2016/679 i dyrektywie 2002/58/WE. Niniejsze rozporządzenie powinno również pozostawać bez uszczerbku dla prawa Unii w zakresie warunków pracy oraz prawa Unii w zakresie współpracy sądowej w sprawach cywilnych i współpracy wymiarów sprawiedliwości w sprawach karnych. Jednakże w zakresie, w jakim te akty prawa Unii realizują te same cele, które zostały określone w niniejszym rozporządzeniu, przepisy niniejszego rozporządzenia powinny mieć zastosowanie w odniesieniu do spraw, których nie uwzględniono lub które nie w pełni uwzględniono w tych innych aktach prawnych, jak również w odniesieniu do spraw, w przypadku których te inne akty prawne pozostawiają państwom członkowskim możliwość przyjęcia pewnych środków na poziomie krajowym.

(11) Należy wyjaśnić, że niniejsze rozporządzenie pozostaje bez uszczerbku dla prawa Unii w zakresie prawa autorskiego i praw pokrewnych, w tym

¹⁵ Dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady z 3.12.2001 r. w sprawie ogólnego bezpieczeństwa produktów (Dz.Urz. UE L 11 z 2002 r., s. 4).

¹⁶ Dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z 11.05.2005 r. dotycząca nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca dyrektywę Rady 84/450/EWG, dyrektywy Parlamentu Europejskiego i Rady 97/7/WE, 98/27/WE i 2002/65/WE oraz rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 2006/2004 (dyrektywa o nieuczciwych praktykach handlowych) (Dz.Urz. UE L 149, s. 22).

¹⁷ Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z 25.10.2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę Parlamentu Europejskiego i Rady 1999/44/WE oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę Parlamentu Europejskiego i Rady 97/7/WE (Dz.Urz. UE L 304, s. 64).

¹⁸ Dyrektywa Parlamentu Europejskiego i Rady 2013/11/UE z 21.05.2013 r. w sprawie alternatywnych metod rozstrzygania sporów konsumenckich oraz zmiany rozporządzenia (WE) nr 2006/2004 i dyrektywy 2009/22/WE (Dz.Urz. UE L 165, s. 63).

¹⁹ Dyrektywa Rady 93/13/EWG z 5.04.1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich (Dz.Urz. UE L 95, s. 29).

²⁰ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1).

dyrektyw Parlamentu Europejskiego i Rady 2001/29/WE²¹, 2004/48/WE²² i (UE) 2019/790²³, które ustanawiają szczególne zasady i procedury, które powinny pozostać nienaruszone.

- (12) Aby osiągnąć cel zakładający zapewnienie bezpiecznego, przewidywalnego i godnego zaufania środowiska internetowego, do celów niniejszego rozporządzenia pojęcie „nielegalnych treści” powinno w szerokim zakresie odzwierciedlać istniejące przepisy w środowisku pozainternetowym. W szczególności pojęcie „nielegalnych treści” należy zdefiniować szeroko, tak by obejmowało informacje dotyczące nielegalnych treści, produktów, usług i działań. Pojęcie to należy rozumieć w szczególności jako odnoszące się do informacji, niezależnie od ich formy, które zgodnie z obowiązującym prawem są albo same w sobie nielegalne, takich jak nielegalne nawoływanie do nienawiści lub treści o charakterze terrorystycznym i niezgodne z prawem treści dyskryminujące, albo które stają się nielegalne na mocy obowiązujących przepisów ze względu na fakt, iż odnoszą się one do nielegalnych działań. Przykładowo może to być udostępnianie obrazów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych, bezprawne udostępnianie prywatnych obrazów bez zgody, cyberstalking, sprzedaż produktów niespełniających wymogów lub podrabionych, sprzedaż towarów lub świadczenie usług z naruszeniem prawa ochrony konsumentów, nieuprawnione wykorzystanie materiałów chronionych prawem autorskim, nielegalne oferowanie usług zakwaterowania lub nielegalna sprzedaż żywych zwierząt. Z kolei film wideo naocznego świadka potencjalnego przestępstwa nie powinien być uważany za nielegalną treść tylko dlatego, że przedstawia on czyn zabroniony, w przypadku gdy nagrywanie lub rozpowszechnianie takiego filmu wśród ogółu społeczeństwa nie jest nielegalne na mocy prawa krajowego lub prawa Unii. W tym zakresie nie ma znaczenia, czy nielegalny charakter informacji lub działania wynika z prawa Unii czy z prawa krajowego, które jest zgodne z prawem Unii, oraz jaki jest dokładny charakter lub przedmiot danego prawa.
- (13) Biorąc pod uwagę szczególne cechy przedmiotowych usług i związaną z nimi potrzebę nałożenia na dostawców tych usług określonych szczególnych obowiązków, należy wyodrębnić w ramach określonej w niniejszym rozporządzeniu szerszej kategorii dostawców usług hostingu podkategorię platform internetowych. Platformy internetowe, takie jak serwisy społecznościowe lub internetowe platformy umożliwiające konsumentom zawieranie z przedsiębiorcami umów

²¹ Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z 22.05.2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.Urz. UE L 167, s. 10).

²² Dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z 29.04.2004 r. w sprawie egzekwowania praw własności intelektualnej (Dz.Urz. UE L 157, s. 45).

²³ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z 17.04.2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz.Urz. UE L 130, s. 92).

zawieranych na odległość, należy zdefiniować jako dostawców usług hostingu, którzy nie tylko przechowują informacje przekazane przez odbiorców usługi na ich żądanie, ale także rozpowszechniają publicznie te informacje na żądanie odbiorców usługi. Aby jednak uniknąć nakładania zbyt szerokiego zakresu obowiązków, dostawców usług hostingu nie należy uznawać za platformy internetowe, w przypadku gdy publiczne rozpowszechnianie jest zaledwie nieznaczną i wyłącznie poboczną cechą, która jest nierozdzielnie powiązana z inną usługą, lub nieznaczną funkcją głównej usługi, której to cechy lub funkcji z obiektywnych względów technicznych nie można wykorzystywać bez tej innej lub głównej usługi, a włączenie takiej cechy lub funkcji nie jest sposobem na obejście stosowania przepisów niniejszego rozporządzenia mających zastosowanie do platform internetowych. Na przykład taką cechą może stanowić sekcja gazety internetowej przeznaczona na komentarze, w przypadku której jest oczywiste, że ma ona charakter poboczny w stosunku do głównej usługi, jaką jest publikowanie wiadomości, za które odpowiedzialność redakcyjną ponosi wydawca. Natomiast przechowywanie komentarzy w sieci społecznościowej należy uznać za usługę platformy internetowej, gdy oczywiste jest, że nie jest to nieznaczna cecha oferowanej usługi, nawet jeżeli ma ona charakter poboczny w stosunku do publikowania wpisów odbiorców usługi. Do celów niniejszego rozporządzenia usługi przetwarzania w chmurze lub usługi hostingu internetowego nie powinny być uznawane za platformę internetową, jeżeli publiczne rozpowszechnianie określonych informacji stanowi nieznaczną i poboczną cechę lub nieznaczną funkcję takich usług.

Ponadto usługi przetwarzania w chmurze i usługi hostingu internetowego pełniące funkcję infrastruktury, na przykład jako podstawa infrastruktury do świadczenia usług przechowywania i przetwarzania danych w aplikacji internetowej, na stronie lub na platformie internetowej, same w sobie nie powinny być postrzegane jako publiczne rozpowszechnianie informacji przechowywanych lub przetwarzanych na żądanie odbiorcy aplikacji, strony lub platformy internetowej, dla której jest ona hostem.

- (14) Stosowane w niniejszym rozporządzeniu pojęcie „publicznego rozpowszechniania” powinno obejmować udostępnianie informacji potencjalnie nieograniczonej liczbie osób, czyli zapewnienie łatwego dostępu do informacji ogółowi odbiorców usługi bez konieczności podejmowania dalszych działań przez odbiorcę usługi zapewniającej te informacje, niezależnie od tego, czy osoby te faktycznie korzystają z dostępu do tych informacji. W związku z tym w przypadku gdy dostęp do informacji wymaga rejestracji lub dopuszczenia do udziału w grupie odbiorców usługi, informacje te należy uznawać za publicznie rozpowszechniane jedynie wtedy, gdy odbiorcy usługi poszukujący dostępu do informacji są automatycznie rejestrowani lub dopuszczani do udziału w grupie odbiorców usługi bez konieczności podejmowania decyzji lub dokonywania wyboru przez człowieka co do tego, komu przyznać taki dostęp. Usługi łączności

- interpersonalnej zgodnie z definicją w dyrektywie Parlamentu Europejskiego i Rady (UE) 2018/1972²⁴, takie jak poczta elektroniczna lub usługi przesyłania wiadomości prywatnych, nie są objęte definicją platform internetowych, ponieważ są one wykorzystywane w celu łączności interpersonalnej między ograniczoną liczbą osób określoną przez nadawcę komunikatu. Określone w niniejszym rozporządzeniu obowiązki dostawców platform internetowych mogą jednak mieć zastosowanie do usług, które umożliwiają udostępnianie informacji potencjalnie nieograniczonej liczbie odbiorców, nieokreślonej przez nadawcę komunikatu, na przykład poprzez publiczne grupy lub otwarte kanały. Informacje należy uznawać za publicznie rozpowszechniane w rozumieniu niniejszego rozporządzenia wyłącznie wówczas, gdy rozpowszechnianie ma miejsce na bezpośrednie żądanie odbiorcy usługi, który przekazał te informacje.
- (15) W przypadku gdy tylko niektóre z usług świadczonych przez dostawcę są objęte zakresem niniejszego rozporządzenia lub gdy usługi świadczone przez dostawcę są objęte różnymi sekcjami niniejszego rozporządzenia, odpowiednie przepisy niniejszego rozporządzenia powinny mieć zastosowanie wyłącznie w odniesieniu do tych usług, które są objęte ich zakresem.
- (16) Pewność prawa wynikająca z horyzontalnych ram warunkowych wyłączeń odpowiedzialności dostawców usług pośrednich, ustanowionych w dyrektywie 2000/31/WE, pozwoliła na wprowadzenie wielu nowych usług na całym rynku wewnętrznym i zwiększenie ich skali. Ramy te należy zatem zachować. Z uwagi na rozbieżności w transpozycji i stosowaniu odpowiednich przepisów na poziomie krajowym oraz w celu zapewnienia jasności i spójności ramy te należy jednak włączyć do niniejszego rozporządzenia. Należy również wyjaśnić niektóre elementy tych ram, uwzględniając orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej.
- (17) Odpowiednie przepisy niniejszego rozporządzenia dotyczące odpowiedzialności dostawców usług pośrednich powinny określać jedynie sytuacje, w których dostawca danych usług pośrednich nie może zostać pociągnięty do odpowiedzialności za nielegalne treści przekazane przez odbiorców usługi. Przepisów tych nie należy rozumieć jako stanowiących pozytywną podstawę do ustalenia odpowiedzialności dostawcy, którą należy określić w mających zastosowanie przepisach prawa Unii lub prawa krajowego. Ponadto wyłączenia odpowiedzialności ustanowione w niniejszym rozporządzeniu powinny mieć zastosowanie w odniesieniu do każdego rodzaju odpowiedzialności w zakresie dowolnego rodzaju nielegalnych treści, niezależnie od dokładnego przedmiotu lub charakteru tych przepisów.
- (18) Wyłączenia odpowiedzialności ustanowione w niniejszym rozporządzeniu nie powinny mieć zastosowania, w przypadku gdy dostawca usług pośrednich

²⁴ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z 11.12.2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (Dz.Urz. UE L 321, s. 36).

zamiast ograniczać się do świadczenia usług w sposób neutralny poprzez czysto techniczne i automatyczne przetwarzanie informacji przekazanych przez odbiorcę usług, odgrywa aktywną rolę, która może pozwolić mu na powzięcie wiedzy o tych informacjach lub sprawowanie nad nimi kontroli. Wyłączenia te nie powinny zatem być dostępne w przypadku odpowiedzialności za informacje przekazane nie przez odbiorcę usługi, lecz przez samego dostawcę usługi pośredniej, w tym w przypadku gdy odpowiedzialność redakcyjną za opracowanie tych informacji ponosi dany dostawca.

- (19) Ze względu na odmienny charakter działań z zakresu „zwykłego przekazu”, „cachingu” i „hostingu” oraz różne położenie i możliwości dostawców przedmiotowych usług należy rozróżnić przepisy mające zastosowanie do tych rodzajów działań w zakresie, w jakim na podstawie niniejszego rozporządzenia podlegają one różnym wymogom i warunkom, a ich zakres różni się, zgodnie z wykładnią Trybunału Sprawiedliwości Unii Europejskiej.
- (20) W przypadku gdy dostawca usług pośrednich umyślnie współpracuje z odbiorcą usługi w celu podjęcia nielegalnych działań, nie należy uznawać, że usługę wyświadczono w sposób neutralny i w związku z tym dostawca usług nie powinien mieć możliwości korzystania z wyłączeń odpowiedzialności określonych w niniejszym rozporządzeniu. Powinno mieć to miejsce na przykład wówczas, gdy dostawca oferuje usługę, której głównym celem jest ułatwienie nielegalnych działań, przykładowo poprzez wyraźne stwierdzenie, że ma on na celu ułatwienie nielegalnych działań lub że jego usługi nadają się do tego celu. Sam fakt, że w ramach danej usługi oferowana jest szyfrowana transmisja danych lub inne systemy uniemożliwiające identyfikację użytkownika, nie powinien jako taki być uznawany za ułatwianie nielegalnych działań.
- (21) Dostawca powinien mieć możliwość korzystania z wyłączeń odpowiedzialności w odniesieniu do usług „zwykłego przekazu” i „cachingu”, jeżeli nie ma on żadnego związku z przekazywanymi lub udostępnianymi informacjami. Wymaga to między innymi, aby dostawca nie modyfikował informacji, które przekazuje lub które udostępnia. Nie należy jednak rozumieć, że wymóg ten obejmuje czynności o charakterze technicznym, które mają miejsce podczas transmisji lub udostępniania, jeżeli takie czynności nie wpływają na integralność przekazywanych lub udostępnianych informacji.
- (22) Aby móc korzystać z wyłączenia odpowiedzialności dotyczącego usług hostingu dostawca powinien, od chwili uzyskania faktycznej wiedzy lub wiadomości o nielegalnych działaniach lub nielegalnych treściach, niezwłocznie podjąć działania w celu usunięcia tych treści lub uniemożliwienia dostępu do nich. Usuwanie lub uniemożliwianie dostępu powinno być przeprowadzane z poszanowaniem praw podstawowych odbiorców usługi, w tym prawa do wolności wypowiedzi i informacji. Dostawca może uzyskać taką faktyczną wiedzę lub wiadomość o nielegalnym charakterze treści między innymi w drodze czynności sprawdzających prowadzonych z własnej inicjatywy lub zgłoszeń przekazanych

mu przez osoby lub podmioty zgodnie z niniejszym rozporządzeniem, o ile takie zgłoszenia są wystarczająco precyzyjne i odpowiednio uzasadnione, aby umożliwić działającemu z należytą starannością podmiotowi gospodarczemu rozsądną identyfikację i ocenę potencjalnie nielegalnych treści oraz, w stosownych przypadkach, podjęcie przeciwko nim działań. Takiej faktycznej wiedzy lub wiadomości nie można jednak uznać za uzyskane wyłącznie na podstawie tego, że dostawca jest ogólnie świadomy faktu, że jego usługa jest również wykorzystywana do przechowywania nielegalnych treści. Co więcej, fakt, że dostawca dokonuje automatycznej indeksacji informacji zamieszczonych w ramach jego usługi, że usługa ta zawiera funkcję wyszukiwania lub że rekomenduje informacje na podstawie profilu lub ustawień odbiorców usługi, nie jest wystarczający, aby uznać, że dostawca ten posiada „konkretną” wiedzę o nielegalnych działaniach podejmowanych za pośrednictwem tej platformy lub o przechowywaniu na niej nielegalnych treści.

- (23) Wyłączenie odpowiedzialności nie powinno mieć zastosowania, jeżeli odbiorca usługi działa z upoważnienia lub pod kontrolą dostawcy usługi hostingu. Jeżeli na przykład dostawca platformy internetowej, która umożliwia konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość, ustala ceny towarów lub usług oferowanych przez przedsiębiorcę, można uznać, że przedsiębiorca działa z upoważnienia tej platformy internetowej lub pod jej kontrolą.
- (24) Aby zapewnić skuteczną ochronę konsumentów dokonujących transakcji handlowych w internecie z udziałem pośredników, niektórzy dostawcy usług hostingu, mianowicie platformy internetowe, które umożliwiają konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość, nie powinni mieć możliwości korzystania z wyłączeń odpowiedzialności dotyczących dostawców usług hostingu ustanowionych w niniejszym rozporządzeniu w zakresie, w jakim te platformy internetowe prezentują istotne informacje dotyczące przedmiotowych transakcji w sposób wzbudzający u konsumentów przekonanie, że informacje te przekazały same platformy internetowe lub przedsiębiorcy działający z ich upoważnienia lub pod ich kontrolą, a zatem że te platformy internetowe posiadają wiedzę na temat tych informacji lub sprawują nad nimi kontrolę, nawet jeżeli w rzeczywistości może być inaczej. Przykładem takiego zachowania mogłaby być sytuacja, gdy platforma internetowa nie pokazuje wyraźnie tożsamości przedsiębiorcy, jak wymaga tego niniejsze rozporządzenie, gdy platforma internetowa nie ujawnia danych dotyczących tożsamości lub danych kontaktowych przedsiębiorcy aż do momentu zawarcia umowy między przedsiębiorcą a konsumentem lub jeżeli platforma internetowa wprowadza produkt bądź usługę do obrotu we własnym imieniu, a nie w imieniu przedsiębiorcy, który dostarczy produkt lub będzie świadczył usługę. W tym kontekście należy obiektywnie ustalić, na podstawie wszystkich istotnych okoliczności, czy prezentacja istotnych informacji może wzbudzać u przeciętnego konsumenta przekonanie, że przedmiotowe informacje zostały

przekazane przez samą platformę internetową lub przez przedsiębiorców działających z jej upoważnienia lub pod jej kontrolą.

- (25) Wyłączenia odpowiedzialności ustanowione w niniejszym rozporządzeniu nie powinny mieć wpływu na możliwość wydawania różnego rodzaju nakazów wobec dostawców usług pośrednich, nawet jeżeli spełniają oni warunki określone jako element tych wyłączeń. Nakazy takie mogą w szczególności przybierać formę nakazów sądów lub organów administracyjnych, wydanych zgodnie z prawem Unii, nakazujących zaprzestanie naruszania lub zapobieżenia mu, w tym również usunięcie nielegalnych treści określonych w takich nakazach lub uniemożliwienia dostępu do nich.
- (26) Aby stworzyć pewność prawa i nie zniechęcać do działań mających na celu wykrywanie, identyfikację i zwalczanie nielegalnych treści, podejmowanych dobrowolnie przez dostawców wszelkiego rodzaju usług pośrednich, należy wyjaśnić, że sam fakt, iż dostawcy podejmują takie działania, nie uniemożliwia wyłączeń odpowiedzialności określonych w niniejszym rozporządzeniu, pod warunkiem że działania te są prowadzone w dobrej wierze i z zachowaniem należytej staranności. Warunkiem działania w dobrej wierze i z zachowaniem należytej staranności powinno być działanie w sposób obiektywny, niedyskryminacyjny i proporcjonalny, z należyтым uwzględnieniem praw i prawnie uzasadnionych interesów wszystkich zaangażowanych stron, oraz zapewnienie niezbędnych zabezpieczeń przed nieuzasadnionym usuwaniem legalnych treści, zgodnie z celem i wymogami niniejszego rozporządzenia. W tym celu zainteresowani dostawcy powinni na przykład podjąć rozsądne środki w celu zapewnienia, aby w przypadku wykorzystywania zautomatyzowanych narzędzi do prowadzenia takich działań dana technologia była wystarczająco wiarygodna, tak aby w jak największym stopniu ograniczyć liczbę błędów. Ponadto należy wyjaśnić, że sam fakt, iż dostawcy podejmują w dobrej wierze środki w celu spełnienia wymogów prawa Unii, w tym wymogów określonych w niniejszym rozporządzeniu w odniesieniu do wdrożenia warunków korzystania z ich usług, nie powinien uniemożliwiać wyłączeń odpowiedzialności ustanowionych w niniejszym rozporządzeniu. W związku z tym przy ustalaniu, czy dostawca może powoływać się na wyłączenie odpowiedzialności, w szczególności w odniesieniu do tego, czy świadczy on swoje usługi w sposób neutralny i w związku z tym może być objęty zakresem stosowania odpowiedniego przepisu, nie należy brać pod uwagę takich działań i środków, które dostawca mógł podjąć, co nie oznacza jednak, że dostawca musi się koniecznie na takie wyłączenie powołać. Dobrowolne działania nie powinny być wykorzystywane do obchodzenia obowiązków, jakie spoczywają na dostawcach usług pośrednich na mocy niniejszego rozporządzenia.
- (27) Chociaż w przepisach niniejszego rozporządzenia dotyczących odpowiedzialności dostawców usług pośrednich skoncentrowano się na wyłączeniu odpowiedzialności dostawców usług pośrednich, należy przypomnieć, że pomimo ogólnie istotnej roli, jaką odgrywają tacy dostawcy, problemu nielegalnych

treści i działań w internecie nie należy rozwiązywać skupiając się wyłącznie na odpowiedzialności i obowiązkach takich dostawców. W miarę możliwości osoby trzecie, poszkodowane przez nielegalne treści przekazywane lub przechowywane w internecie, powinny starać się rozwiązywać konflikty związane z takimi treściami bez angażowania odpowiednich dostawców usług pośrednich. Odbiorców usługi należy pociągać do odpowiedzialności, jeżeli stanowią tak mające zastosowanie przepisy prawa Unii i prawa krajowego określające taką odpowiedzialność, za nielegalne treści, które przekazują i mogą rozpowszechniać publicznie za pomocą usług pośrednich. W stosownych przypadkach w zapobieganiu rozpowszechnianiu nielegalnych treści w internecie, zgodnie z mającymi zastosowanie przepisami prawa, powinny również pomagać inne podmioty, takie jak moderatorzy grup w zamkniętych środowiskach internetowych, w szczególności w przypadku dużych grup. Ponadto w przypadku gdy konieczny jest udział dostawców usług społeczeństwa informacyjnego, w tym dostawców usług pośrednich, wszelkie żądania lub nakazy dotyczące takiego udziału należy co do zasady kierować do konkretnego dostawcy posiadającego techniczną i operacyjną możliwość podjęcia działań przeciwko określonym nielegalnym treściom, aby zapobiec ewentualnym negatywnym skutkom dla dostępności i osiągalności informacji, które nie stanowią nielegalnych treści, oraz zminimalizować takie skutki.

- (28) Od 2000 r. wprowadzono nowe technologie, które poprawiają dostępność, efektywność, szybkość, niezawodność, zdolność i bezpieczeństwo systemów służących do transmisji i przechowywania danych w internecie oraz ich „znajdawalność”, co prowadzi do coraz bardziej złożonego ekosystemu cyfrowego. W tym zakresie należy przypomnieć, że dostawcy usług tworzący i ułatwiający podstawową architekturę logiczną i właściwe funkcjonowanie internetu, w tym pomocnicze funkcje techniczne, mogą również korzystać z wyłączeń odpowiedzialności określonych w niniejszym rozporządzeniu w zakresie, w jakim ich usługi kwalifikują się jako usługi „zwykłego przekazu”, „cachingu” lub „hostingu”. Usługi takie obejmują, w zależności od przypadku, lokalne sieci radiowe, usługi systemu nazw domen (DNS), rejestry nazw domen najwyższego poziomu, rejestratory, organy certyfikacji wydające certyfikaty cyfrowe, wirtualne sieci prywatne, wyszukiwarki internetowe, usługi infrastruktury chmury obliczeniowej lub sieci dostarczania treści, które umożliwiają, lokalizują lub ulepszają funkcje innych dostawców usług pośrednich. Podobnie znacząco rozwinęły się również usługi wykorzystywane na potrzeby łączności oraz techniczne środki ich świadczenia, co doprowadziło do powstania usług online, takich jak telefonia internetowa, usługi przesyłania wiadomości i usługi aplikacji webmail, w których łączność odbywa się za pośrednictwem usługi dostępu do internetu. Również te usługi mogą korzystać z wyłączeń odpowiedzialności w zakresie, w jakim kwalifikują się jako usługa „zwykłego przekazu”, „cachingu” lub „hostingu”.

- (29) Usługi pośrednie obejmują szeroki zakres działalności gospodarczej, która jest prowadzona online i stale się rozwija w celu zapewnienia szybkiej i bezpiecznej transmisji informacji oraz wygody wszystkim uczestnikom ekosystemu cyfrowego. Przykładowo, usługi pośrednie polegające na „zwykłym przekazie” obejmują generyczne kategorie usług, takie jak punkty wymiany ruchu internetowego, punkty dostępu bezprzewodowego, wirtualne sieci prywatne, usługi i resolwery DNS, rejestry nazw domen najwyższego poziomu, rejestratorzy, organy certyfikacji wydające certyfikaty cyfrowe, telefonia internetowa i inne usługi łączności interpersonalnej, natomiast generyczne przykłady usług pośrednich polegających na „cachingu” obejmują wyłącznie zapewnianie sieci dostarczania treści, odwrotnych serwerów proxy lub serwerów proxy adaptacji treści. Takie usługi mają kluczowe znaczenie dla zapewnienia sprawnej i efektywnej transmisji informacji dostarczanych w internecie. Przykładowe „usługi hostingu” obejmują kategorie usług takie, jak przetwarzanie w chmurze, web hosting, odpłatne usługi odsyłania czy usługi umożliwiające wymianę informacji i treści online, w tym przechowywanie i udostępnianie plików. Usługi pośrednie mogą być świadczone oddzielnie, jako część innego rodzaju usługi pośredniej, lub równocześnie z innymi usługami pośrednimi. To, czy dana usługa jest usługą „zwykłego przekazu”, „cachingu” czy „hostingu”, zależy wyłącznie od jej funkcji technicznych, które mogą ewoluować w czasie, i powinno być oceniane indywidualnie.
- (30) Na dostawcach usług pośrednich nie powinien spoczywać obowiązek monitorowania – ani na mocy prawa, ani w praktyce – w odniesieniu do obowiązków o charakterze ogólnym. Nie dotyczy to obowiązków monitorowania w konkretnym przypadku oraz, w szczególności, nie wpływa to na nakazy organów krajowych wydane zgodnie z ustawodawstwem krajowym zgodnym z prawem Unii, stosownie do wykładni Trybunału Sprawiedliwości Unii Europejskiej, oraz zgodnie z warunkami ustanowionymi w niniejszym rozporządzeniu. Żadnego z przepisów niniejszego rozporządzenia nie należy interpretować jako nałożenia ogólnego obowiązku monitorowania ani ogólnego obowiązku aktywnego ustalania faktów, ani też jako nałożenia na dostawców ogólnego obowiązku podejmowania aktywnych działań w odniesieniu do nielegalnych treści.
- (31) W zależności od systemu prawnego każdego państwa członkowskiego i danej dziedziny prawa, krajowe organy sądowe lub administracyjne, w tym organy ścigania, mogą nakazać dostawcom usług pośrednich podjęcie działań przeciwko określonej nielegalnej treści lub określonym nielegalnym treściom lub udzielenie pewnych określonych informacji. Przepisy krajowe, na podstawie których wydaje się takie nakazy, znacznie się od siebie różnią, a nakazy te coraz częściej dotyczą sytuacji transgranicznych. W celu zapewnienia skutecznego i efektywnego stosowania się do tych nakazów, w szczególności w kontekście transgranicznym, tak aby zainteresowane organy publiczne mogły wykonywać

swoje zadania, a dostawcy nie podlegali żadnym nieproporcjonalnym obciążeniom, bez nadmiernego naruszania praw i prawnie uzasadnionych interesów osób trzecich, należy określić pewne warunki, które nakazy te powinny spełniać, oraz pewne dodatkowe wymogi dotyczące wykonywania tych nakazów. W związku z tym niniejsze rozporządzenie powinno harmonizować tylko niektóre szczególne warunki minimalne, jakie takie nakazy powinny spełniać, aby nałożyć na dostawców usług pośrednich obowiązek informowania odpowiednich organów o działaniach podjętych w odpowiedzi na te nakazy. W związku z tym niniejsze rozporządzenie nie stanowi podstawy prawnej do wydawania takich nakazów ani nie określa ich zakresu terytorialnego czy transgranicznego egzekwowania.

- (32) Mające zastosowanie prawo Unii lub prawo krajowe, na podstawie których nakazy te są wydawane, może wprowadzać dodatkowe warunki i powinno stanowić podstawę egzekwowania odpowiednich nakazów. W przypadku niezastosowania się do takich nakazów wydające nakaz państwo członkowskie powinno mieć możliwość egzekwowania tych nakazów zgodnie ze swoim prawem krajowym. Mające zastosowanie prawo krajowe powinno być zgodne z prawem Unii, w tym Kartą i postanowieniami TFUE dotyczącymi swobody przedsiębiorczości i swobody świadczenia usług wewnątrz Unii, w szczególności w odniesieniu do usług gier hazardowych i zakładów. Stosowanie takich przepisów krajowych w celu egzekwowania odpowiednich nakazów pozostaje również bez uszczerbku dla mających zastosowanie unijnych aktów prawnych ani zawartych przez Unię lub przez państwa członkowskie międzynarodowych umów dotyczących transgranicznego uznawania, wykonywania i egzekwowania tych nakazów, w szczególności w sprawach cywilnych i karnych. Z drugiej strony egzekwowanie obowiązku informowania odpowiednich organów o działaniach podjętych w odpowiedzi na te nakazy, w przeciwieństwie do wykonania samych nakazów, powinno podlegać przepisom określonym w niniejszym rozporządzeniu.
- (33) Dostawca usług pośrednich powinien bez zbędnej zwłoki informować organ wydający o wszelkich działaniach następczych podjętych w związku z takimi nakazami w terminach określonych w odpowiednich przepisach prawa Unii lub prawa krajowego.
- (34) Odpowiednie organy krajowe powinny mieć możliwość wydawania takich nakazów w odniesieniu do treści uznanych za nielegalne lub nakazów udzielenia informacji na podstawie prawa Unii lub prawa krajowego zgodnego z prawem Unii, w szczególności z Kartą, i kierowania tych nakazów do dostawców usług pośrednich, w tym dostawców mających siedzibę w innym państwie członkowskim. Niniejsze rozporządzenie powinno jednak pozostawać bez uszczerbku dla prawa Unii w dziedzinie współpracy sądowej w sprawach cywilnych lub karnych, w tym rozporządzenia (UE) nr 1215/2012 i rozporządzenia w sprawie europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia

dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych, ani krajowego prawa karnego procesowego lub prawa cywilnego procesowego. Dlatego też w przypadku, gdy w kontekście postępowania karnego lub cywilnego prawo to przewiduje warunki dodatkowe w stosunku do warunków przewidzianych w niniejszym rozporządzeniu w odniesieniu do nakazów podjęcia działań przeciwko nielegalnym treściom lub nakazów udzielenia informacji lub z nimi niezgodne, warunki przewidziane w niniejszym rozporządzeniu mogą nie mieć zastosowania lub mogą zostać dostosowane. W szczególności nałożony na koordynatora ds. usług cyfrowych z państwa członkowskiego organu wydającego nakaz obowiązek przekazania kopii nakazów wszystkim pozostałym koordynatorom ds. usług cyfrowych może nie mieć zastosowania w kontekście postępowania karnego lub może zostać dostosowany, w przypadku gdy tak stanowi mające zastosowanie krajowe prawo karne procesowe.

Ponadto obowiązek zamieszczania w nakazach uzasadnienia wyjaśniającego, dlaczego dana informacja stanowi nielegalne treści, powinien w razie potrzeby zostać dostosowany na mocy mającego zastosowanie krajowego prawa karnego procesowego w odniesieniu do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych oraz wykrywania i ścigania przestępstw. Wreszcie, termin wykonania nałożonego na dostawców usług pośrednich obowiązku udzielenia informacji odbiorcy usługi może zostać odroczony zgodnie z mającym zastosowanie prawem Unii lub prawem krajowymi, w szczególności w kontekście postępowania karnego, cywilnego lub administracyjnego. Dodatkowo nakazy powinny być wydawane zgodnie z rozporządzeniem (UE) 2016/679 oraz ustanowionym w niniejszym rozporządzeniu zakazem nakładania ogólnych obowiązków monitorowania informacji lub aktywnego ustalania faktów lub okoliczności wskazujących na nielegalną działalność. Warunki i wymogi określone w niniejszym rozporządzeniu, które mają zastosowanie do nakazów podjęcia działań przeciwko nielegalnym treściom, pozostają bez uszczerbku dla innych aktów Unii, w których przewidziano podobne systemy podejmowania działań przeciwko konkretnym rodzajom nielegalnych treści, takich jak rozporządzenie (UE) 2021/784, rozporządzenie (UE) 2019/1020 lub rozporządzenie (UE) 2017/2394, w którym przyznano szczególne uprawnienia do wydawania nakazu udzielenia informacji organom ścigania w zakresie ochrony konsumentów państw członkowskich, zaś warunki i wymogi mające zastosowanie do nakazów udzielenia informacji pozostają bez uszczerbku dla innych aktów Unii zawierających podobne odpowiednie przepisy dla poszczególnych sektorów. Wspomniane warunki i wymogi powinny pozostawać bez uszczerbku dla przepisów dotyczących zatrzymywania i zabezpieczenia na podstawie mającego zastosowanie prawa krajowego zgodnego z prawem Unii oraz wnioskami organów ścigania o zachowanie poufności związanych z nieujawnianiem informacji. Te warunki i wymogi nie powinny wpływać na możliwość wymagania przez

państwa członkowskie od dostawcy usług pośrednich zapobiegania naruszeniu, zgodnie z prawem Unii, w tym z niniejszym rozporządzeniem, a w szczególności z zakazem ogólnych obowiązków w zakresie monitorowania.

- (35) Warunki i wymogi określone w niniejszym rozporządzeniu powinny być spełnione najpóźniej w momencie przekazania nakazu zainteresowanemu dostawcy. Dlatego też nakaz może zostać wydany w jednym z języków urzędowych organu danego państwa członkowskiego wydającego nakaz. Jeżeli jednak jest to inny język, niż język zadeklarowany przez dostawcę usług pośrednich lub inny język urzędowy państw członkowskich, uzgodniony przez organ wydający nakaz i dostawcę usług pośrednich, do przekazywanego nakazu należy dołączyć tłumaczenie co najmniej tych elementów nakazu, które są określone w niniejszym rozporządzeniu. W przypadku gdy dostawca usług pośrednich uzgodnił z organami państwa członkowskiego używanie określonego języka, należy go zachęcać do akceptowania nakazów wydanych w tym języku przez organy innych państw członkowskich. Nakazy powinny zawierać elementy umożliwiające adresatowi zidentyfikowanie organu wydającego, w tym w stosownych przypadkach dane kontaktowe punktu kontaktowego w ramach tego organu, oraz weryfikację autentyczności nakazu.
- (36) Zakres terytorialny takich nakazów podjęcia działań przeciwko nielegalnym treściom powinien być jasno określony na podstawie mających zastosowanie przepisów prawa Unii lub prawa krajowego umożliwiających wydanie nakazu i nie powinien wykraczać poza zakres absolutnie niezbędny do osiągnięcia celów nakazu. W tym zakresie krajowy organ sądowy lub administracyjny wydający nakaz, którym może być również organ ścigania, powinien zrównoważyć cel, jaki nakaz ma osiągnąć, zgodnie z podstawą prawną umożliwiającą jego wydanie, z prawami i prawnie uzasadnionymi interesami wszystkich osób trzecich, na które nakaz może mieć wpływ, w szczególności z ich prawami podstawowymi wynikającymi z Karty. W szczególności w kontekście transgranicznym, nakaz powinien być w zasadzie skuteczny tylko na terytorium wydającego nakaz państwa członkowskiego, chyba że nielegalny charakter treści wynika bezpośrednio z prawa Unii lub organ wydający nakaz uważa, że odpowiednie prawa wymagają szerszego zakresu terytorialnego, zgodnie z prawem Unii i prawem międzynarodowym oraz przy uwzględnieniu interesów kurtuazji międzynarodowej.
- (37) Nakazy udzielenia informacji regulowane niniejszym rozporządzeniem dotyczą przedstawienia konkretnych informacji na temat indywidualnych odbiorców danej usługi pośredniej wskazanych w tych nakazach w celu ustalenia, czy odbiorcy usług przestrzegają mających zastosowanie przepisów Unii lub przepisów krajowych. Takie nakazy powinny nakazywać udzielenie informacji mających na celu umożliwienie identyfikacji odbiorców danej usługi. W związku z tym wymogi niniejszego rozporządzenia dotyczące udzielenia informacji nie obejmują nakazów odnoszących się do informacji na temat grupy odbiorców usługi, którzy nie są wyraźnie wskazani, w tym nakazów udzielenia

zbiorczych informacji wymaganych do celów statystycznych lub kształtowania polityki opartej na dowodach.

- (38) Nakazy podjęcia działań przeciwko nielegalnym treściom i udzielenia informacji podlegają przepisom zabezpieczającym kompetencje państwa członkowskiego, w którym dostawca, do którego skierowany jest nakaz, ma siedzibę, oraz przepisom ustanawiającym w niektórych przypadkach możliwe odstępstwa od tych kompetencji, określone w art. 3 dyrektywy 2000/31/WE, o ile spełniono warunki wymienione w tym artykule. Biorąc pod uwagę, że przedmiotowe nakazy odnoszą się odpowiednio do określonych nielegalnych treści i informacji, w przypadku gdy są skierowane do dostawców usług pośrednich z siedzibą w innym państwie członkowskim, co do zasady nie ograniczają one swobody tych dostawców w zakresie transgranicznego świadczenia usług. W związku z tym zasady określone w art. 3 dyrektywy 2000/31/WE, w tym zasady dotyczące konieczności uzasadnienia środków stanowiących odstępstwo od kompetencji państwa członkowskiego, w którym dostawca usług ma siedzibę, z pewnych określonych powodów oraz w zakresie zgłaszania takich środków, nie mają zastosowania do tych nakazów.
- (39) Wymogi dotyczące udzielania informacji o mechanizmach odwoławczych, dostępnych dla dostawcy usługi pośredniej i odbiorcy usługi, który przekazał treści, obejmują wymóg udzielenia informacji na temat administracyjnych mechanizmów rozpatrywania skarg oraz sądowych środków odwoławczych, w tym odwołań od nakazów wydanych przez organy sądowe. Ponadto koordynatorzy ds. usług cyfrowych mogą opracować krajowe narzędzia i wytyczne dotyczące mechanizmów wnoszenia skarg i mechanizmów odwoławczych mających zastosowanie na ich terytorium, aby ułatwić odbiorcom usługi dostęp do takich mechanizmów. Ponadto stosując niniejsze rozporządzenie, państwa członkowskie powinny przestrzegać podstawowego prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu ustanowionego w art. 47 Karty. Niniejsze rozporządzenie nie powinno zatem uniemożliwiać odpowiednim krajowym organom sądowym lub administracyjnym wydawania, na podstawie mającego zastosowanie prawa Unii lub prawa krajowego, nakazu przywrócenia treści, w przypadku gdy treści te były zgodne z warunkami korzystania z usług dostawcy usług pośrednich, ale zostały błędnie uznane przez tego dostawcę za nielegalne i usunięte.
- (40) Aby osiągnąć cele określone w niniejszym rozporządzeniu, w szczególności poprawić funkcjonowanie rynku wewnętrznego oraz zapewnić bezpieczne i przejrzyste środowisko internetowe, należy ustanowić jasny, skuteczny, przewidywalny i wyważony zestaw zharmonizowanych obowiązków w zakresie należytej staranności dla dostawców usług pośrednich. Celem tych obowiązków powinno być w szczególności zagwarantowanie osiągnięcia różnych celów polityki publicznej, takich jak bezpieczeństwo i zaufanie odbiorców usługi, w tym konsumentów, małoletnich i użytkowników szczególnie narażonych na ryzyko

stania się ofiarą nawoływania do nienawiści, molestowania seksualnego lub innych dyskryminujących działań, ochrona odpowiednich praw podstawowych zapisanych w Karcie, zapewnienie rzeczywistej rozliczalności tych dostawców oraz wzmocnienie pozycji odbiorców i innych zainteresowanych stron przy jednoczesnym ułatwieniu niezbędnego nadzoru przez właściwe organy.

- (41) W związku z tym istotne jest, aby obowiązki w zakresie należytej staranności były dostosowane do rodzaju, wielkości i charakteru danej usługi pośredniej. Niniejsze rozporządzenie określa zatem podstawowe obowiązki mające zastosowanie do wszystkich dostawców usług pośrednich, a także dodatkowe obowiązki dostawców usług hostingu, w szczególności dostawców platform internetowych oraz bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych. W zakresie, w jakim dostawcy usług pośrednich należą do kilku różnych kategorii z uwagi na charakter świadczonych usług i wielkość, powinni oni wypełniać wszystkie odpowiednie obowiązki wynikające z niniejszego rozporządzenia w odniesieniu do tych usług. Te zharmonizowane obowiązki w zakresie należytej staranności, które powinny być rozsądne i niearbitralne, są potrzebne, aby zaradzić zidentyfikowanym obawom dotyczącym porządku publicznego, takim jak ochrona prawnie uzasadnionych interesów odbiorców usług, zwalczanie nielegalnych praktyk i ochrona praw podstawowych zapisanych w Karcie. Obowiązki w zakresie należytej staranności są niezależne od kwestii odpowiedzialności dostawców usług pośrednich, należy je zatem oceniać oddzielnie.
- (42) Aby ułatwić sprawną i skuteczną komunikację dwustronną, w tym – w stosownych przypadkach – poprzez potwierdzenie otrzymania stosownych komunikatów, w sprawach objętych zakresem niniejszego rozporządzenia, dostawcy usług pośrednich powinni być zobowiązani do wyznaczenia pojedynczego elektronicznego punktu kontaktowego oraz do publikowania i aktualizowania odpowiednich informacji dotyczących tego punktu kontaktowego, w tym również języków, których należy używać w takiej komunikacji. Z elektronicznego punktu kontaktowego mogą również korzystać zaufane podmioty sygnalizujące oraz podmioty profesjonalne pozostające w szczególnym stosunku z dostawcą usług pośrednich. W odróżnieniu od przedstawiciela prawnego elektroniczny punkt kontaktowy powinien służyć celom operacyjnym i nie powinno się wymagać, by miał fizyczną lokalizację. Dostawcy usług pośrednich mogą wyznaczyć ten sam pojedynczy punkt kontaktowy na potrzeby niniejszego rozporządzenia oraz na potrzeby innych aktów prawa Unii. Przy określaniu języków komunikacji zachęca się dostawców usług pośrednich do zapewnienia, by wybrane języki same w sobie nie stanowiły przeszkody w komunikacji. W razie potrzeby dostawcy usług pośrednich i organy państw członkowskich powinny mieć możliwość wypracowania odrębnego porozumienia w sprawie języka komunikacji lub poszukać alternatywnych rozwiązań służących pokonaniu bariery językowej, także poprzez wykorzystanie wszelkich

dostępnych środków technologicznych lub wewnętrznych i zewnętrznych zasobów kadrowych.

- (43) Dostawcy usług pośrednich powinni być również zobowiązani do wyznaczenia jednego punktu kontaktowego dla odbiorców usług, który umożliwia szybką, bezpośrednią i skuteczną komunikację w szczególności za pomocą łatwo dostępnych środków, takich jak numery telefonu, adresy poczty elektronicznej, elektroniczne formularze kontaktowe, chatboty lub komunikatory internetowe. Należy wyraźnie wskazać, kiedy odbiorca usługi komunikuje się z chatbotem. Dostawcy usług pośrednich powinni umożliwiać odbiorcom usług wybór środków bezpośredniej i skutecznej komunikacji, które nie opierają się wyłącznie na zautomatyzowanych narzędziach. Dostawcy usług pośrednich powinni dołożyć wszelkich rozsądnych starań, aby zagwarantować wystarczające zasoby ludzkie i finansowe potrzebne do zapewnienia terminowej i skutecznej komunikacji.
- (44) Dostawcy usług pośrednich, którzy mają siedzibę w państwie trzecim i oferują usługi w Unii, powinni wyznaczyć dysponującego wystarczającymi uprawnieniami przedstawiciela prawnego w Unii oraz udzielić odpowiednim organom informacji dotyczących ich przedstawicieli prawnych i podać takie informacje do wiadomości publicznej. Aby wypełnić ten obowiązek, tacy dostawcy usług pośrednich powinni zapewnić, by wyznaczony przedstawiciel prawny dysponował uprawnieniami i zasobami niezbędnymi do współpracy z odpowiednimi organami. Warunek ten byłby spełniony na przykład w przypadku, gdy dostawca usług pośrednich wyznacza do tego celu spółkę zależną w ramach tej samej grupy, do której należy dostawca, lub spółkę dominującą, jeżeli ta spółka zależna lub spółka dominująca ma siedzibę w Unii. Nie byłby jednak spełniony wówczas, gdy przykładowo przedstawiciel prawny jest objęty postępowaniem dotyczącym restrukturyzacji, upadłości lub niewypłacalności osób fizycznych lub przedsiębiorstw. Obowiązek ten powinien umożliwić skuteczny nadzór i, w razie potrzeby, egzekwowanie niniejszego rozporządzenia w odniesieniu do tych dostawców. Przedstawiciel prawny powinien mieć możliwość otrzymania upoważnienia, zgodnie z prawem krajowym, od więcej niż jednego dostawcy usług pośrednich. Przedstawiciel prawny powinien mieć możliwość pełnienia również funkcji punktu kontaktowego, pod warunkiem że spełniono odpowiednie wymogi niniejszego rozporządzenia.
- (45) Chociaż zasadniczo należy przestrzegać swobody umów przysługującej dostawcom usług pośrednich, należy ustanowić pewne zasady dotyczące treści, stosowania i egzekwowania warunków korzystania z usług tych dostawców w celu zapewnienia przejrzystości, ochrony odbiorców usługi oraz unikania nieuczciwych lub arbitralnych wyników. Dostawcy usług pośrednich w warunkach korzystania z ich usług powinni wyraźnie podawać i aktualizować informacje o powodach, dla których mogą ograniczyć świadczenie swoich usług. Warunki te powinny w szczególności zawierać informacje na temat wszelkich polityk, procedur, środków i narzędzi wykorzystywanych do celów moderowania treści,

w tym algorytmicznego podejmowaniu decyzji i weryfikacji przez człowieka, a także na temat regulaminu wewnętrznego systemu rozpatrywania skarg. Powinny one również zawierać łatwo dostępne informacje na temat prawa do zakończenia korzystania z usługi. Dostawcy usług pośrednich mogą wykorzystywać elementy graficzne w warunkach świadczenia usług, takie jak ikony lub obrazki, do zilustrowania głównych elementów wymogów informacyjnych określonych w niniejszym rozporządzeniu. Dostawcy powinni informować odbiorców swojej usługi za pomocą odpowiednich środków o istotnych zmianach wprowadzonych w warunkach korzystania z usług, na przykład w przypadku zmiany zasad dotyczących informacji dozwolonych na temat ich usługi, lub o innych tego rodzaju zmianach, które mogą mieć bezpośredni wpływ na zdolność odbiorców do korzystania z usługi.

- (46) Dostawcy usług pośrednich, które są skierowane przede wszystkim do małoletnich, na przykład z uwagi na projekt usługi lub rodzaj związanych z nią działań marketingowych, lub z których korzystają w przeważającej mierze małoletni, powinni dołożyć szczególnych starań, aby w sposób łatwo zrozumiały dla małoletnich wyjaśnić warunki korzystania z usług.
- (47) Opracowując, stosując i egzekwując te ograniczenia, dostawcy usług pośrednich powinni działać w sposób niearbitralny i niedyskryminacyjny oraz uwzględniać prawa i prawnie uzasadnione interesy odbiorców usługi, w tym prawa podstawowe zapisane w Karcie. Na przykład dostawcy bardzo dużych platform internetowych powinni w szczególności należycie uwzględniać wolność wypowiedzi i informacji, w tym wolność mediów i ich pluralizm. Wszyscy dostawcy usług pośrednich powinni również należycie uwzględniać odpowiednie międzynarodowe standardy ochrony praw człowieka, takie jak wytyczne Organizacji Narodów Zjednoczonych dotyczące biznesu i praw człowieka.
- (48) Ze względu na swą szczególną rolę i zasięg, na bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe należy nałożyć dodatkowe wymogi dotyczące informacji i przejrzystości ich warunków korzystania z usług. W związku z tym dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni udostępniać swoje warunki korzystania z usług w językach urzędowych wszystkich państw członkowskich, w których oferują swoje usługi, a także powinni przekazywać odbiorcom usług zwięzłe i łatwe do odczytania streszczenie głównych elementów warunków korzystania z usług. W streszczeniach takich należy wskazać główne elementy wymogów informacyjnych, w tym możliwość łatwego niezaakceptowania klauzul opcjonalnych.
- (49) Aby zapewnić odpowiedni poziom przejrzystości i rozliczalności, dostawcy usług pośrednich powinni co roku podawać do wiadomości publicznej sprawozdanie w formacie nadającym się do odczytu maszynowego, zgodnie ze zharmonizowanymi wymogami zawartymi w niniejszym rozporządzeniu, dotyczące moderowania treści, w którym brali udział, w tym środków

wprowadzonych w rezultacie stosowania i egzekwowania warunków korzystania z ich usług. Aby uniknąć nieproporcjonalnych obciążeń, obowiązki sprawozdawcze w zakresie przejrzystości nie powinny mieć jednak zastosowania do dostawców będących mikroprzedsiębiorstwami lub małymi przedsiębiorstwami zgodnie z definicją w zaleceniu Komisji 2003/361/WE²⁵, którzy nie są bardzo dużymi platformami internetowymi w rozumieniu niniejszego rozporządzenia.

- (50) Dostawcy usług hostingu odgrywają szczególnie ważną rolę w zwalczaniu nielegalnych treści w internecie, ponieważ przechowują informacje przekazane przez odbiorców usługi i na ich żądanie oraz zazwyczaj umożliwiają innym odbiorcom dostęp do tych informacji, niekiedy na dużą skalę. Ważne jest, aby wszyscy dostawcy usług hostingu, niezależnie od wielkości, wprowadzili łatwo dostępne i przyjazne dla użytkownika mechanizmy zgłaszania i działania, które ułatwiają zgłaszanie dostawcy usług hostingu określonych informacji uznanych przez zgłaszającego za treści nielegalne („zgłoszenie”), zgodnie z którymi dostawca ten może podjąć decyzję, czy zgadza się z taką oceną oraz czy chce usunąć nielegalne treści lub uniemożliwić dostęp do nich („działanie”). Mechanizmy takie powinny być łatwe do zidentyfikowania, zlokalizowane w pobliżu przedmiotowych informacji oraz co najmniej tak łatwe do znalezienia i wykorzystania, jak mechanizmy zgłaszania treści naruszających warunki korzystania z usług dostawcy usług hostingu. Z zastrzeżeniem spełnienia wymogów dotyczących zgłoszeń, osoby lub podmioty powinny mieć możliwość zgłaszania wielu potencjalnie nielegalnych treści w jednym zgłoszeniu w celu zapewnienia skutecznego działania mechanizmów zgłaszania i działania. Mechanizm zgłaszania powinien umożliwiać identyfikację osoby lub podmiotu dokonujących zgłoszenia, ale nie powinien jej wymagać. W przypadku niektórych rodzajów zgłaszanych informacji tożsamość osoby lub podmiotu dokonujących zgłoszenia może być konieczna do ustalenia, czy dane informacje stanowią potencjalne treści nielegalne. Obowiązek wprowadzenia mechanizmów zgłaszania i działania powinien mieć zastosowanie na przykład do usług przechowywania i udostępniania plików, usług hostingu stron internetowych, serwerów reklamowych i usług typu pastebin, o ile kwalifikują się one jako usługi hostingu objęte niniejszym rozporządzeniem.
- (51) Uwzględniając potrzebę należytego uwzględnienia zagwarantowanych w Kartie praw podstawowych wszystkich zainteresowanych stron, wszelkie działania podejmowane przez dostawcę usług hostingu w związku z otrzymaniem zgłoszenia powinny być ściśle ukierunkowane, to znaczy powinny służyć usunięciu określonych informacji uznanych za nielegalne treści lub uniemożliwieniu dostępu do nich, jednak bez nadmiernego naruszania wolności wypowiedzi i informacji odbiorców usługi. Zgłoszenia powinny zatem co do zasady być

²⁵ Zalecenie Komisji 2003/361/WE z 6.05.2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.Urz. UE L 124, s. 36).

kierowane do dostawców usług hostingu, w przypadku których można zasadnie oczekiwać, że posiadają oni techniczną i operacyjną zdolność do podjęcia działań przeciwko takim określonym informacjom. Dostawcy usług hostingu, którzy otrzymują zgłoszenie, w związku z którym z przyczyn technicznych lub operacyjnych nie mogą usunąć określonej informacji, powinni poinformować o tym osobę lub podmiot, które dokonały zgłoszenia.

- (52) Przepisy dotyczące takich mechanizmów zgłaszania i działania powinny być zharmonizowane na poziomie Unii, aby zapewnić terminowe i niearbitralne przetwarzanie zgłoszeń z zachowaniem należytej staranności na podstawie jednolitych, przejrzystych i jasnych zasad, które zapewniają solidne gwarancje ochrony praw i prawnie uzasadnionych interesów wszystkich zainteresowanych stron, w szczególności ich praw podstawowych zagwarantowanych w Karcie, niezależnie od państwa członkowskiego, w którym strony te mają siedzibę lub miejsce pobytu, oraz niezależnie od odnośnej dziedziny prawa. Te prawa podstawowe obejmują między innymi w przypadku odbiorców usług: prawo do wolności wypowiedzi i informacji, prawo do poszanowania życia prywatnego i rodzinnego, prawo do ochrony danych osobowych, prawo do niedyskryminacji oraz prawo do skutecznego środka prawnego; w przypadku dostawców usług: wolność prowadzenia działalności gospodarczej, w tym swobodę zawierania umów; w przypadku stron poszkodowanych przez nielegalne treści: prawo do godności ludzkiej, prawa dziecka, prawo do ochrony własności, w tym własności intelektualnej, oraz prawo do niedyskryminacji. Dostawcy usług hostingu powinni podejmować działania w odpowiedzi na zgłoszenia w sposób terminowy, w szczególności z uwzględnieniem rodzaju nielegalnych treści, które są zgłaszane, i pilności działań, które mają zostać podjęte. Na przykład można oczekiwać, że tacy dostawcy podejmą niezwłoczne działania, gdy zgłaszane są potencjalnie nielegalne treści wiążące się z zagrożeniem życia lub bezpieczeństwa osób. Po podjęciu decyzji o tym, czy podjąć działania w odpowiedzi na dane zgłoszenie czy takich działań nie podejmować, dostawca usług hostingu powinien bez zbędnej zwłoki poinformować osobę lub podmiot zgłaszające określone treści.
- (53) Mechanizmy zgłaszania i działania powinny umożliwiać dokonywanie zgłoszeń, które są wystarczająco precyzyjne i odpowiednio uzasadnione, aby umożliwić danemu dostawcy usług hostingu podjęcie z należytą starannością świadomej decyzji, zgodnej z wolnością wypowiedzi i informacji, w odniesieniu do treści, których dotyczy zgłoszenie, w szczególności w odniesieniu do tego, czy treści te należy uznać za nielegalne oraz czy należy je usunąć lub uniemożliwić dostęp do nich. Mechanizmy te powinny ułatwiać dokonywanie zawiadomień, które zawierają wyjaśnienie powodów, dla których osoba lub podmiot dokonujący zgłoszenia uznają treść za nielegalną, a także wyraźne określenie lokalizacji takiej treści. Jeżeli zgłoszenie zawiera wystarczające informacje, aby umożliwić dostawcy usług hostingu działającemu z należytą starannością stwierdzenie,

bez szczegółowej analizy prawnej, iż treści są w sposób oczywisty nielegalne, zgłoszenie należy uznać za stanowiące podstawę do uzyskania faktycznej wiedzy lub wiadomości o nielegalnej treści. Z wyjątkiem dokonywania zgłoszeń dotyczących przestępstw, o których mowa w art. 3–7 dyrektywy Parlamentu Europejskiego i Rady 2011/93/UE²⁶, mechanizmy te powinny wymagać od osoby lub podmiotu dokonujących zgłoszenia ujawnienia tożsamości, aby uniknąć nadużyć.

- (54) W przypadku gdy dostawca usług hostingu decyduje się, ze względu na to, że przekazane przez odbiorców usług informacje stanowią nielegalne treści lub są niezgodne z jego warunkami korzystania z usług, usunąć informacje przekazane przez odbiorcę usługi lub uniemożliwić dostęp do nich, lub w inny sposób ograniczyć ich widoczność lub monetyzację, na przykład po otrzymaniu zgłoszenia lub działając z własnej inicjatywy, w tym przy wykorzystaniu wyłącznie zautomatyzowanych środków, dostawca ten powinien w sposób jasny i łatwo zrozumiały poinformować odbiorcę o swojej decyzji, powodach jej podjęcia oraz dostępnych możliwościach odwołania się od tej decyzji, mając na uwadze negatywne konsekwencje, jakie takie decyzje mogą mieć dla odbiorcy, w tym dla możliwości wykonywania przez niego prawa podstawowego do wolności wypowiedzi. Obowiązek ten powinien mieć zastosowanie niezależnie od powodów podjęcia decyzji, w szczególności niezależnie od tego, czy działanie podjęto ze względu na uznanie zgłoszonych informacji za nielegalne treści lub za informacje niezgodne z mającymi zastosowanie warunkami korzystania z usług. Jeżeli decyzję podjęto po otrzymaniu zgłoszenia, dostawca usług hostingu powinien ujawnić tożsamość osoby lub podmiotu, które dokonały zgłoszenia odbiorcy usług, wyłącznie wówczas, gdy informacje te są niezbędne do stwierdzenia nielegalności treści, na przykład w przypadku naruszenia praw własności intelektualnej.
- (55) Ograniczenie widoczności może polegać na depozycjonowaniu w ramach plasowania lub w systemach rekomendacji, a także na ograniczeniu dostępności usługi dla co najmniej jednego odbiorcy usługi lub zablokowanie widoczności wpisów danego użytkownika dla całej społeczności internetowej poza autorem bez jego wiadomości (tzw. „shadow banning”). Monetyzację informacji przekazywanych przez odbiorcę usługi za pośrednictwem wpływów z reklam można ograniczyć poprzez zawieszenie lub zakończenie płatności pieniężnych lub wypłaty dochodów związanych z danymi informacjami. Obowiązek przedstawienia uzasadnienia nie powinien jednak mieć zastosowania w odniesieniu do wprowadzających w błąd treści handlowych o dużej objętości, rozpowszechnianych w drodze zamierzonej manipulacji usługi, w szczególności nieautentycznego

²⁶ Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z 13.12.2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.Urz. UE L 335, s. 1).

korzystania z usługi, takiego jak korzystanie z botów lub fałszywych kont, lub innych nieuczciwych sposobów korzystania z usługi. Niezależnie od innych możliwości odwołania się od decyzji dostawcy usług hostingu, odbiorca usługi powinien zawsze mieć prawo do skutecznego środka prawnego przed sądem zgodnie z przepisami prawa krajowego.

- (56) Dostawca usług hostingu może w niektórych przypadkach uzyskać, na przykład w drodze zgłoszenia przez stronę zgłaszającą lub za pomocą własnych podejmowanych dobrowolnie środków, informacje dotyczące określonej działalności odbiorcy usługi, takiej jak przekazywanie niektórych rodzajów nielegalnych treści, które racjonalnie uzasadniają – uwzględniając wszystkie istotne okoliczności, których dostawca usług hostingu ma świadomość – podejrzenie, że ten odbiorca mógł popełnić, może właśnie popełniać lub może popełnić przestępstwo zagrażające życiu lub bezpieczeństwu osoby lub osób, takie jak przestępstwa określone w dyrektywie Parlamentu Europejskiego i Rady 2011/36/UE²⁷, dyrektywie 2011/93/UE lub dyrektywie Parlamentu Europejskiego i Rady (UE) 2017/541²⁸. Przykładowo określone treści mogą rodzić podejrzenie, że stanowią zagrożenie publiczne, takie jak podżeganie do terroryzmu w rozumieniu art. 21 dyrektywy (UE) 2017/541. W takich przypadkach dostawca usług hostingu powinien niezwłocznie poinformować właściwe organy ścigania o takim podejrzeniu. Dostawca usług hostingu powinien przekazać wszystkie dostępne mu informacje na ten temat, w tym, w stosownych przypadkach, daną treść i, jeżeli jest dostępny, czas publikacji tej treści, wraz ze wskazaną strefą czasową, wyjaśnienie swoich podejrzeń oraz informacje niezbędne do zlokalizowania i zidentyfikowania odpowiedniego odbiorcy usługi. Niniejsze rozporządzenie nie stanowi podstawy prawnej do profilowania odbiorców usług w celu ewentualnego identyfikowania przestępstw przez dostawców usług hostingu. Informując organy ścigania, dostawcy usług hostingu powinni również przestrzegać innych mających zastosowanie przepisów prawa Unii lub prawa krajowego dotyczących ochrony praw i wolności osób.
- (57) Aby uniknąć nieproporcjonalnych obciążeń, dodatkowe obowiązki nałożone na mocy niniejszego rozporządzenia na dostawców platform internetowych, w tym platform umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość, nie powinny mieć zastosowania do dostawców, którzy kwalifikują się jako mikroprzedsiębiorstwa lub małe przedsiębiorstwa zgodnie z definicją w zaleceniu 2003/361/WE. Z tego samego powodu dodatkowe obowiązki nie powinny mieć również zastosowania do dostawców platform

²⁷ Dyrektywa Parlamentu Europejskiego i Rady 2011/36/UE z 5.04.2011 r. w sprawie zapobiegania handlowi ludźmi i zwalczania tego procederu oraz ochrony ofiar, zastępująca dyrektywę ramową Rady 2002/629/WSiSW (Dz.Urz. UE L 101, s. 1).

²⁸ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/541 z 15.03.2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW (Dz.Urz. UE L 88, s. 6).

internetowych, którzy wcześniej kwalifikowali się jako mikroprzedsiębiorstwa lub małe przedsiębiorstwa, w terminie 12 miesięcy od utraty przez nich tego statusu. Tacy dostawcy nie powinni być wyłączeni z obowiązku przekazywania informacji na temat średniej liczby aktywnych miesięcznie odbiorców usługi na wniosek koordynatora ds. usług cyfrowych właściwy dla miejsca siedziby lub na wniosek Komisji. Biorąc jednak pod uwagę, że bardzo duże platformy internetowe lub bardzo duże wyszukiwarki internetowe mają większy zasięg i większy wpływ na sposób, w jaki odbiorcy usługi uzyskują informacje i komunikują się w internecie, tacy dostawcy nie powinni korzystać z tego wyłączenia, bez względu na to, czy kwalifikują się lub niedawno kwalifikowali się jako mikroprzedsiębiorstwa lub małe przedsiębiorstwa. Przepisy konsolidacyjne ustanowione w zaleceniu 2003/361/WE pomagają w zapewnieniu zapobiegania przypadkom obchodzenia tych dodatkowych obowiązków. Żaden z przepisów niniejszego rozporządzenia nie uniemożliwia dostawcom platform internetowych objętym tym wyłączeniem ustanowienia, na zasadzie dobrowolności, systemu wypełniającego co najmniej jeden z tych obowiązków.

- (58) Odbiorcy usługi powinni mieć możliwość łatwego i skutecznego zaskarżania niektórych decyzji dostawców platform internetowych dotyczących nielegalnych treści lub ich niezgodności z warunkami korzystania z usług, jeżeli decyzje takie mają dla nich negatywne skutki. W związku z tym dostawcy platform internetowych powinni być zobowiązani do zapewnienia wewnętrznych systemów rozpatrywania skarg, które spełniają określone warunki mające na celu zapewnienie łatwego dostępu do tych systemów i doprowadzenie do szybkiego, niedyskryminującego, niearbitralnego i sprawiedliwego rozstrzygnięcia i które podlegają weryfikacji człowieka w przypadku wykorzystania zautomatyzowanych środków. Takie systemy powinny umożliwiać wszystkim odbiorcom usługi wniesienie skargi i nie powinny określać wymogów formalnych, takich jak odesłanie do konkretnych, odpowiednich przepisów prawnych lub szczegółowych wyjaśnień prawnych. Odbiorcy usługi, którzy dokonali zgłoszenia za pośrednictwem mechanizmu zgłaszania i działania przewidzianego w niniejszym rozporządzeniu lub za pośrednictwem mechanizmu zgłaszania treści naruszających warunki korzystania z usług dostawcy platform internetowych powinni być uprawnieni do korzystania z mechanizmu rozpatrywania skarg w celu zaskarżenia decyzji dostawcy platform internetowych dotyczącej ich zgłoszeń, w tym również w przypadku gdy uznają, że działania podjęte przez tego dostawcę nie były odpowiednie. Możliwość wniesienia skargi w celu uchylenia zaskarżonych decyzji powinna być dostępna przez co najmniej sześć miesięcy, począwszy od momentu poinformowania odbiorcy usługi o decyzji przez dostawcę platform internetowych.
- (59) Ponadto należy przewidzieć możliwość zaangażowania się, w dobrej wierze, w pozasądowe rozstrzyganie takich sporów, w tym sporów, których zadowalające rozstrzygnięcie z wykorzystaniem wewnętrznych systemów rozpatrywania

skarg nie było możliwe, przez certyfikowane organy, które dysponują niezbędną niezależnością, środkami i wiedzą ekspercką, aby wykonywać swoje działania w sposób sprawiedliwy, szybki i oszczędny. Niezależność pozasądowych organów rozstrzygania sporów należy zapewnić również na poziomie osób fizycznych odpowiedzialnych za rozstrzyganie sporów, w tym za pomocą zasad dotyczących konfliktu interesów. Opłaty pobierane przez pozasądowe organy rozstrzygania sporów powinny być rozsądne, przystępne, atrakcyjne, niewygórowane dla konsumentów i proporcjonalne, oraz ustalane indywidualnie dla każdego przypadku. W przypadku gdy organ pozasądowego rozstrzygania sporów jest certyfikowany przez właściwego koordynatora ds. usług cyfrowych, certyfikacja ta powinna być ważna we wszystkich państwach członkowskich. Dostawcy platform internetowych powinni mieć możliwość odmowy uczestniczenia w pozasądowym postępowaniu w sprawie rozstrzygania sporów na podstawie niniejszego rozporządzenia, jeżeli ten sam spór, w szczególności w odniesieniu do danych informacji i podstaw wydania zaskarżonej decyzji, skutków decyzji oraz podstaw zaskarżenia decyzji, jest już przedmiotem toczącego się postępowania przed właściwym sądem lub innym właściwym organem pozasądowego rozstrzygania sporów lub został już rozstrzygnięty w takim postępowaniu. Odbiorcy usługi powinni mieć możliwość wyboru między wewnętrznym mechanizmem rozpatrywania skarg, pozasądowym rozstrzygnięciem sporów oraz możliwością wszczęcia, na każdym etapie, postępowania sądowego. Ponieważ wynik pozasądowego postępowania w sprawie rozstrzygania sporów nie jest wiążący, nie należy uniemożliwiać stronom wszczynania postępowania sądowego w odniesieniu do tego samego sporu. Stworzone w ten sposób możliwości zaskarżania decyzji dostawców platform internetowych nie powinny jednak pod żadnym względem naruszać możliwości skorzystania z sądowych środków odwoławczych zgodnie z prawem danego państwa członkowskiego, a tym samym nie powinny wpływać na wykonywanie prawa do skutecznego środka prawnego na mocy art. 47 Karty. Przepisy niniejszego rozporządzenia dotyczące pozasądowego rozstrzygania sporów nie powinny zobowiązywać państw członkowskich do ustanowienia organów pozasądowego rozstrzygania sporów.

- (60) W przypadku sporów o charakterze umownym między konsumentami a przedsiębiorstwami dotyczących nabycia towarów lub usług, dyrektywa 2013/11/UE zapewnia unijnym konsumentom i przedsiębiorstwom w Unii dostęp do posiadających certyfikaty jakości podmiotów zajmujących się alternatywnym rozstrzygnięciem sporów. W tym zakresie należy wyjaśnić, że przepisy niniejszego rozporządzenia dotyczące pozasądowego rozstrzygania sporów pozostają bez uszczerbku dla tej dyrektywy, w tym dla wynikającego z niej prawa konsumentów do wycofania się z postępowania na dowolnym etapie, jeżeli będą niezadowoleni ze skuteczności lub z przebiegu postępowania.
- (61) Działanie przeciwko nielegalnym treściom można podejmować szybciej i jest ono rzetelniejsze, jeżeli dostawcy platform internetowych wprowadzają

niezbędne środki w celu zapewnienia priorytetowego traktowania zgłoszeń dokonywanych przez zaufane podmioty sygnalizujące, działające w wyznaczonych dziedzinach, w których dysponują wiedzą specjalistyczną, za pośrednictwem mechanizmów zgłaszania i działania wymaganych na podstawie niniejszego rozporządzenia, bez uszczerbku dla wymogu przetwarzania wszystkich zgłoszeń dokonywanych w ramach tych mechanizmów i podejmowania decyzji w ich sprawie w sposób terminowy i niearbitralny oraz z zachowaniem należytej staranności. Status zaufanego podmiotu sygnalizującego powinien być przyznawany przez koordynatora ds. usług cyfrowych państwa członkowskiego, w którym osoba ubiegająca się o ten status ma siedzibę; status ten powinien być uznawany przez wszystkich dostawców platform internetowych objętych zakresem stosowania niniejszego rozporządzenia. Status zaufanego podmiotu sygnalizującego należy przyznawać wyłącznie podmiotom, a nie osobom, które to podmioty wykazały między innymi, że posiadają szczególną wiedzę ekspercką i kompetencje w zakresie zwalczania nielegalnych treści oraz że działają w sposób dokładny, obiektywny i z zachowaniem należytej staranności. Podmioty takie mogą mieć charakter publiczny, na przykład w przypadku treści o charakterze terrorystycznym mogą to być jednostki ds. zgłaszania podejrzanych treści w internecie krajowych organów ścigania lub Agencji Unii Europejskiej ds. Współpracy Organów Ścigania („Europol”); mogą być to także organizacje pozarządowe i podmioty prywatne lub mieszane, takie jak organizacje należące do sieci gorących linii stowarzyszenia INHOPE służących do zgłaszania materiałów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych oraz organizacje zajmujące się zgłaszaniem nielegalnych treści rasistowskich i ksenofobicznych w internecie. Aby uniknąć obniżenia wartości dodanej takiego mechanizmu, ogólna liczba osób, którym przyznano status zaufanych podmiotów sygnalizujących na mocy niniejszego rozporządzenia, powinna być ograniczona. W szczególności do ubiegania się o status zaufanych podmiotów sygnalizujących zachęca się stowarzyszenia branżowe reprezentujące interesy swoich członków, bez uszczerbku dla prawa podmiotów prywatnych lub osób do zawierania dwustronnych umów z dostawcami platform internetowych.

- (62) Zaufane podmioty sygnalizujące powinny publikować łatwo zrozumiałe i szczegółowe sprawozdania dotyczące zgłoszeń dokonanych zgodnie z niniejszym rozporządzeniem. Sprawozdania te powinny zawierać informacje, takie jak liczba zgłoszeń pogrupowanych według tożsamości dostawcy usług hostingu, rodzaju treści oraz działań podjętych przez dostawcę. Ze względu na to, że zaufane podmioty sygnalizujące wykazują się wiedzą ekspercką i kompetencjami, można oczekiwać, że rozpatrywanie zgłoszeń dokonanych przez te podmioty będzie mniej uciążliwe, a tym samym będzie trwało krócej w porównaniu ze zgłoszeniami dokonywanymi przez innych odbiorców usługi. Niemniej jednak średni czas potrzebny na rozpatrzenie zgłoszenia może być nadal różny w zależności od czynników, w tym rodzaju nielegalnej treści, jakości zgłoszeń

oraz faktycznych procedur technicznych wprowadzonych w celu dokonywania takich zgłoszeń.

Dla przykładu, mimo, iż kodeks postępowania w zakresie zwalczania nielegalnego nawoływania do nienawiści w internecie z 2016 r. stanowi punkt odniesienia dla uczestniczących przedsiębiorstw, jeżeli chodzi o czas potrzebny na rozpatrzenie ważnych zgłoszeń w celu usunięcia nielegalnego nawoływania do nienawiści, inne rodzaje nielegalnych treści mogą wymagać znacznie odmiennego czasu do rozpatrzenia w zależności od konkretnych faktów i okoliczności oraz rodzajów odpowiednich nielegalnych treści. Aby uniknąć nadużywania statusu zaufanego podmiotu sygnalizującego, powinna istnieć możliwość zawieszenia takiego statusu, jeżeli koordynator ds. usług cyfrowych właściwy dla miejsca siedziby podjął czynności sprawdzające z uzasadnionych powodów. Przepisów niniejszego rozporządzenia dotyczących zaufanych podmiotów sygnalizujących nie należy rozumieć jako uniemożliwiające dostawcom platform internetowych podobnego traktowania zgłoszeń dokonywanych przez podmioty lub osoby, którym nie przyznano statusu zaufanego podmiotu sygnalizującego na podstawie niniejszego rozporządzenia, lub podejmowania innego rodzaju współpracy z innymi podmiotami zgodnie z mającymi zastosowanie przepisami, w tym z niniejszym rozporządzeniem oraz z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/794²⁹. Przepisy niniejszego rozporządzenia nie powinny uniemożliwiać dostawcom platform internetowych korzystania z takich zaufanych podmiotów sygnalizujących lub podobnych mechanizmów w celu podejmowania szybkich i rzetelnych działań przeciwko treściom, które są niezgodne z warunkami korzystania z usług tych dostawców, w szczególności przeciwko treściom, które są szkodliwe dla odbiorców usługi podatnych na zagrożenia, takich jak małoletni.

- (63) Nadużywanie platform internetowych polegające na częstym przekazywaniu oczywiście nielegalnych treści lub częstym dokonywaniu oczywiście bezzasadnych zgłoszeń lub częstym wnoszeniu oczywiście bezzasadnych skarg w ramach – odpowiednio – mechanizmów i systemów ustanowionych na podstawie niniejszego rozporządzenia osłabia zaufanie oraz szkodzi prawom i prawnie uzasadnionym interesom zainteresowanych stron. Dlatego też konieczne jest wprowadzenie odpowiednich, proporcjonalnych i skutecznych zabezpieczeń przed takim nadużywaniem, które muszą respektować prawa i prawnie uzasadnione interesy wszystkich zaangażowanych stron, w tym mające zastosowanie podstawowe prawa i wolności zapisane w Karcie, w szczególności wolność wypowiedzi. Informacje należy uważać za stanowiące oczywiście nielegalne treści, a zgłoszenia lub skargi należy uważać za oczywiście bezzasadne,

²⁹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z 11.05.2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.Urz. UE L 135, s. 53).

jeżeli dla osoby nieposiadającej wiedzy fachowej jest oczywiste, bez przeprowadzenia jakiegokolwiek merytorycznej analizy, że treści są nielegalne, a zgłoszenia lub skargi – bezzasadne.

- (64) Pod pewnymi warunkami dostawcy platform internetowych powinni tymczasowo zawiesić działania podejmowane w odniesieniu do osoby dopuszczającej się nadużyć. Pozostaje to bez uszczerbku dla swobody określania przez dostawców platform internetowych warunków korzystania z ich usług i przyjmowania bardziej rygorystycznych środków w przypadku oczywiście nielegalnych treści związanych z poważnymi przestępstwami, takich jak materiały dotyczące niegodziwego traktowania dzieci w celach seksualnych. W celu zapewnienia przejrzystości możliwość tę należy jasno i wystarczająco szczegółowo określić w warunkach korzystania z usług platform internetowych. Od decyzji podejmowanych w tym zakresie przez dostawców platform internetowych powinna zawsze przysługiwać możliwość odwołania się i decyzje takie powinny podlegać nadzorowi właściwego koordynatora ds. usług cyfrowych. Przed podjęciem decyzji o zawieszeniu, dostawcy platform internetowych powinni wysłać uprzednie ostrzeżenie, które powinno zawierać uzasadnienie ewentualnego zawieszenia i przedstawiać środki odwoławcze od takiej decyzji. Podejmując decyzję o zawieszeniu, dostawcy platform internetowych powinni przesłać uzasadnienie zgodnie z przepisami ustanowionymi w niniejszym rozporządzeniu. Przepisy niniejszego rozporządzenia dotyczące nadużywania nie powinny uniemożliwiać dostawcom platform internetowych wprowadzania innych środków w celu rozwiązania problemu przekazywania nielegalnych treści przez odbiorców ich usług lub innego rodzaju nadużywania ich usług, w tym poprzez naruszenie warunków korzystania z ich usług, zgodnie z mającym zastosowanie prawem Unii i prawem krajowym. Przepisy te pozostają bez uszczerbku dla możliwości pociągnięcia do odpowiedzialności osób dopuszczających się nadużyć, w tym za szkody, którą przewidziano w prawie Unii lub prawie krajowym.
- (65) Ze względu na szczególne obowiązki i zobowiązania dostawców platform internetowych powinni oni podlegać obowiązkowi sprawozdawczym w zakresie przejrzystości, które mają zastosowanie dodatkowo do obowiązków sprawozdawczych w zakresie przejrzystości mających zastosowanie do wszystkich dostawców usług pośrednich na mocy niniejszego rozporządzenia. Do celów ustalenia, czy platformy internetowe i wyszukiwarki internetowe mogą być, odpowiednio, bardzo dużymi platformami internetowymi lub bardzo dużymi wyszukiwarkami internetowymi, które podlegają określonym dodatkowym obowiązkom na mocy niniejszego rozporządzenia, obowiązki sprawozdawcze w zakresie przejrzystości dotyczące platform internetowych i wyszukiwarek internetowych powinny obejmować określone obowiązki związane z publikowaniem i przekazywaniem informacji na temat średniej liczby aktywnych miesięcznie odbiorców usług w Unii.

- (66) Aby zapewnić przejrzystość i umożliwić kontrolę decyzji dostawców platform internetowych dotyczących moderowania treści oraz monitorowanie rozpowszechniania nielegalnych treści w internecie, Komisja powinna prowadzić i publikować bazę danych zawierającą decyzje dostawców platform internetowych wraz z uzasadnieniami, w przypadku gdy usuwają oni informacje lub w inny sposób ograniczają ich dostępność lub dostęp do nich. Aby baza danych była stale aktualizowana, dostawcy platform internetowych powinni bez zbędnej zwłoki przedkładać w standardowym formacie decyzje i uzasadnienia po podjęciu decyzji, aby umożliwić aktualizację w czasie rzeczywistym, jeżeli jest to technicznie możliwe i proporcjonalne w stosunku do środków danej platformy internetowej. Ustrukturyzowana baza danych powinna umożliwiać dostęp do istotnych informacji i składanie odpowiednich zapytań, w szczególności w przypadku potencjalnie nielegalnych treści.
- (67) Zwodnicze interfejsy na interfejsach internetowych platform internetowych to praktyki, które w istotny sposób zniekształcają lub ograniczają, celowo lub w praktyce, zdolność odbiorców usługi do dokonywania niezależnych i świadomych wyborów lub podejmowania takich decyzji. Praktyki te mogą być wykorzystywane w celu nakłonięcia odbiorców usługi do niepożądanego zachowania lub do podejmowania niepożądanych decyzji, które mają dla nich negatywne skutki. Dostawcom platform internetowych należy zatem zakazać wprowadzania w błąd lub nakłaniania odbiorców usługi do określonego działania oraz osłabiania lub ograniczania autonomii, wpływania na podejmowanie decyzji lub wybory dokonywane przez odbiorców usługi poprzez strukturę, sposób zaprojektowania lub funkcje interfejsu internetowego lub jego części. Powinno to obejmować między innymi projektowanie w sposób podstępny możliwości dokonywania wyborów w celu nakłonięcia odbiorców usługi do działań, które przynoszą korzyści dostawcy platform internetowych, lecz które mogą nie leżeć w interesie odbiorców usługi, prezentowanie wyborów w sposób nieneutralny, na przykład poprzez wyraźniejsze eksponowanie pewnych opcji przy pomocy elementów wizualnych, dźwiękowych lub innych, kiedy odbiorca usługi jest proszony o podjęcie decyzji. Powinno to również obejmować wielokrotne zwracanie się do odbiorcy usługi o dokonanie wyboru, jeżeli takiego wyboru już dokonano, znacznie bardziej uciążliwą procedurę anulowania usługi niż jej wybór lub też utrudnianie dokonywania pewnych wyborów bądź też sprawianie, że ich dokonanie jest bardziej czasochłonne niż w przypadku innych wyborów, bezzasadne utrudnianie zaprzestania zakupów lub wypisania się z danej platformy internetowej umożliwiającej konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość oraz dezorientowanie odbiorców usługi poprzez zachęcanie ich do podejmowania decyzji dotyczących transakcji lub poprzez domyślne ustawienia, które są bardzo trudne do zmiany, a zatem powodowanie nieracjonalnej stroniczości procesu podejmowania decyzji przez usługobiorcę w sposób,

który zniekształca i ogranicza jego autonomię, podejmowanie decyzji i wybór. Przepisów zapobiegających stosowaniu zwodniczych interfejsów nie należy jednak rozumieć jako uniemożliwiających dostawcom bezpośrednią interakcję z odbiorcami usługi i oferowanie im nowych lub dodatkowych usług. Legalne praktyki, na przykład reklamowe, które są zgodne z prawem Unii, nie powinny same w sobie być uznawane za zwodnicze interfejsy. Przepisy dotyczące zwodniczych interfejsów należy interpretować w taki sposób, aby obejmowały zakazane praktyki wchodzące w zakres stosowania niniejszego rozporządzenia w zakresie, w jakim praktyki te nie są już objęte zakresem stosowania dyrektywy 2005/29/WE lub rozporządzenia (UE) 2016/679.

- (68) Reklama internetowa odgrywa ważną rolę w środowisku internetowym, w tym w odniesieniu do udostępniania platform internetowych, na których świadczenie usługi jest niekiedy w całości lub po części finansowane bezpośrednio lub pośrednio z przychodów reklamowych. Reklama internetowa może jednak przyczyniać się do powstania znaczących zagrożeń, począwszy od reklam, które same w sobie stanowią nielegalne treści, poprzez zapewnianie zachęt finansowych do publikowania lub akcentowania nielegalnych lub w inny sposób szkodliwych treści i działań w internecie, aż po dyskryminujące prezentowanie reklam, które ma wpływ na równe traktowanie i równość szans obywateli. Oprócz wymogów wynikających z art. 6 dyrektywy 2000/31/WE dostawców platform internetowych należy zobowiązać zatem do zapewnienia odbiorcom usługi określonych zindywidualizowanych informacji niezbędnych do zrozumienia, kiedy i w jakim imieniu prezentowana jest reklama. Powinni oni zapewnić, by informacje te były wyraźne, między innymi za pomocą standardowych znaków wizualnych lub dźwiękowych, łatwo rozpoznawalne i jednoznaczne dla przeciętnego odbiorcy usługi; informacje powinny też być dostosowane do charakteru interfejsu internetowego konkretnej usługi. Ponadto odbiorcy usługi powinni dysponować informacjami, dostępnymi bezpośrednio z interfejsu internetowego, gdzie reklama jest prezentowana, na temat głównych parametrów wykorzystywanych do ustalenia, jakie konkretne reklamy są im prezentowane, stanowiącymi rzeczywiste wyjaśnienie stojącej za tym logiki, w tym na temat tego, czy reklamy są wyświetlane na podstawie profilowania.

Takie wyjaśnienia powinny obejmować informacje na temat metody wykorzystanej do prezentacji reklamy, na przykład, czy jest to reklama kontekstowa czy też innego rodzaju, oraz, w stosownych przypadkach, na temat zastosowanych głównych kryteriów profilowania; odbiorcę usługi należy również informować o wszelkich dostępnych mu środkach służących zmianie takich kryteriów. Określone w niniejszym rozporządzeniu wymogi dotyczące udzielania informacji związanych z reklamą pozostają bez uszczerbku dla stosowania odpowiednich przepisów rozporządzenia (UE) 2016/679, w szczególności przepisów dotyczących prawa do sprzeciwu, zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania, a w szczególności

potrzeby uzyskania zgody osoby, której dane dotyczą, przed przetwarzaniem danych osobowych do celów ukierunkowania reklam. Podobnie pozostają one bez uszczerbku dla przepisów ustanowionych w dyrektywie 2002/58/WE, w szczególności przepisów dotyczących przechowywania informacji w urządzeniach końcowych i dostępu do informacji w nich przechowywanych. Wreszcie niniejsze rozporządzenie uzupełnia stosowanie dyrektywy 2010/13/UE, która nakłada środki umożliwiające użytkownikom deklarowanie handlowych przekazów audiowizualnych w filmach wideo stworzonych przez użytkownika. Uzupełnia ona też obowiązki przedsiębiorców dotyczące ujawniania komunikatów handlowych wynikające z dyrektywy 2005/29/WE.

- (69) Jeżeli odbiorcom usługi prezentuje się reklamy oparte na technikach targetowania, zoptymalizowane tak, aby odpowiadały ich zainteresowaniom i potencjalnie odwoływały się do ich słabości, może to mieć szczególnie poważne skutki negatywne. W niektórych przypadkach techniki manipulacyjne mogą negatywnie wpływać na całe grupy i zwiększać szkody społeczne, na przykład przyczyniając się do kampanii dezinformacyjnych lub dyskryminując niektóre grupy. Platformy internetowe są szczególnie wrażliwym środowiskiem, jeżeli chodzi o takie praktyki, i stwarzają większe zagrożenie społeczne. W związku z tym dostawcy platform internetowych nie powinni prezentować reklam opartych na profilowaniu zgodnie z definicją w art. 4 pkt 4 rozporządzenia (UE) 2016/679 z wykorzystaniem szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 tego, w tym poprzez stosowanie kategorii profilowania opartych na tych szczególnych kategoriach. Zakaz ten pozostaje bez uszczerbku dla obowiązków mających zastosowanie do dostawców platform internetowych lub innych dostawców usług bądź reklamodawców uczestniczących w rozpowszechnianiu reklam na mocy prawa Unii dotyczącego ochrony danych osobowych.
- (70) Podstawową częścią działalności platformy internetowej jest sposób szeregowania i prezentowania informacji na jej interfejsie internetowym, aby ułatwić i zoptymalizować dostęp do informacji odbiorcom usługi. Odbywa się to na przykład poprzez algorytmiczne sugerowanie, plasowanie i szeregowanie informacji, wyróżnianie za pomocą tekstu lub innych przedstawień graficznych lub w inny sposób selekcjonowanie informacji przekazywanych przez odbiorców. Takie systemy rekomendacji mogą mieć znaczący wpływ na zdolność odbiorców do wyszukiwania informacji i interakcji z nimi w internecie, także w celu ułatwienia odbiorcom usługi wyszukiwania odpowiednich informacji i przyczynienia się do poprawy doświadczeń użytkowników. Odgrywają one również ważną rolę w akcentowaniu pewnych wiadomości, wirusowym rozpowszechnianiu informacji i stymulowaniu zachowań w internecie. W związku z tym platformy internetowe powinny stale zapewniać, aby odbiorcy ich usługi byli należycie poinformowani o tym, jak systemy rekomendacji oddziałują na sposób prezentowania im informacji oraz aby mieli wpływ na to, jak prezentowane

są im informacje. Powinny one jasno przedstawiać parametry takich systemów rekomendacji w łatwo zrozumiały sposób, aby zapewnić, by odbiorcy usługi rozumieli, w jaki sposób szeregowane są przedstawiane im informacje. Parametry te powinny obejmować co najmniej najważniejsze kryteria służące określaniu informacji sugerowanych odbiorcy usługi oraz powody ich odpowiedniego znaczenia, w tym przypadki, w których informacje są szeregowane na podstawie profilowania i zachowania w internecie.

- (71) Ochrona małoletnich jest ważnym celem polityki Unii. Platformę internetową można uznać za dostępną dla małoletnich, jeżeli warunki korzystania z jej usług umożliwiają małoletnim korzystanie z usługi, gdy jej usługa jest skierowana do małoletnich lub korzystają z niej w przeważającej mierze małoletni, lub gdy dostawca w inny sposób ma świadomość, że niektórzy odbiorcy jego usługi są małoletni, na przykład dlatego, że w innych celach przetwarza już dane osobowe odbiorców usługi ujawniające ich wiek. Dostawcy platform internetowych, z których korzystają małoletni, powinni wprowadzić odpowiednie i proporcjonalne środki w celu ochrony małoletnich, na przykład poprzez domyślne, w stosownych przypadkach, projektowanie swoich interfejsów internetowych lub ich części z zachowaniem najwyższego poziomu prywatności, bezpieczeństwa i ochrony małoletnich, a także poprzez przyjmowanie norm ochrony małoletnich lub stosowanie kodeksów postępowania służących ochronie małoletnich. Powinni oni uwzględniać najlepsze praktyki i dostępne wytyczne, takie jak te zawarte w komunikacie Komisji pt. „Cyfrowa dekada dla dzieci i młodzieży: nowa europejska strategia na rzecz lepszego internetu dla dzieci (BIK+)”. Dostawcy platform internetowych nie powinni prezentować reklam opartych na profilowaniu z wykorzystaniem danych osobowych odbiorcy usługi, jeżeli wiedzą z wystarczającą pewnością, że odbiorca usługi jest małoletni. Zgodnie z rozporządzeniem (UE) 2016/679, w szczególności z zasadą minimalizacji danych przewidzianą w art. 5 ust. 1 lit. c) tego rozporządzenia, zakaz ten nie powinien powodować, iż dostawca platformy internetowej będzie utrzymywał, pozyskiwał lub przetwarzał większą ilość danych osobowych niż już posiada w celu oceny, czy odbiorca usługi jest małoletni. W związku z tym obowiązek ten nie powinien zachęcać dostawców platform internetowych do gromadzenia danych dotyczących wieku odbiorcy usługi przed skorzystaniem przez niego z usługi. Obowiązek ten powinien pozostawać bez uszczerbku dla prawa Unii w zakresie ochrony danych osobowych.
- (72) Aby przyczynić się do tworzenia bezpiecznego, godnego zaufania i przejrzystego środowiska internetowego dla konsumentów, a także dla innych zainteresowanych stron, takich jak konkurujący przedsiębiorcy i posiadacze praw własności intelektualnej, oraz aby zniechęcić przedsiębiorców do sprzedawania produktów lub usług z naruszeniem mających zastosowanie przepisów, platformy internetowe umożliwiające konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość powinny zapewniać możliwość zidentyfikowania

takich przedsiębiorców. W związku z tym przedsiębiorca powinien być zobowiązany do przekazywania dostawcom platform internetowych umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość niektórych istotnych informacji, między innymi do celów propagowania wiadomości na temat produktów lub ich oferowania. Wymóg ten powinien mieć również zastosowanie do przedsiębiorców, którzy na podstawie umów bazowych propagują wiadomości o produktach lub usługach w imieniu marek. Tacy dostawcy platform internetowych powinni przechowywać wszystkie informacje w bezpieczny sposób przez okres obowiązywania stosunku umownego z danym przedsiębiorcą i przez kolejne sześć miesięcy, aby umożliwić dochodzenie roszczeń od danego przedsiębiorcy lub wykonanie nakazów związanych z tym przedsiębiorcą.

Ten obowiązek jest niezbędny i proporcjonalny, by umożliwić organom publicznym i podmiotom prywatnym mającym prawnie uzasadniony interes uzyskanie dostępu do tych informacji, między innymi w drodze nakazów udzielenia informacji, o których mowa w niniejszym rozporządzeniu, zgodnie z mającym zastosowanie prawem, w tym z przepisami dotyczącymi ochrony danych osobowych. Obowiązek ten nie wpływa na potencjalny obowiązek zachowania pewnych treści przez dłuższe okresy, w oparciu o inne przepisy prawa Unii lub przepisy prawa krajowego zgodne z prawem Unii. Bez uszczerbku dla definicji przewidzianej w niniejszym rozporządzeniu, każdy przedsiębiorca, niezależnie od tego, czy jest osobą fizyczną czy prawną, określony na podstawie art. 6a ust. 1 lit. b) dyrektywy 2011/83/UE i art. 7 ust. 4 lit. f) dyrektywy 2005/29/WE, powinien być możliwy do zidentyfikowania, w przypadku gdy oferuje produkt lub usługę za pośrednictwem platformy internetowej. Dyrektywa 2000/31/WE zobowiązuje wszystkich dostawców usług społeczeństwa informacyjnego do zapewnienia odbiorcom usługi i właściwym organom łatwego, bezpośredniego i stałego dostępu do pewnych informacji umożliwiających identyfikację wszystkich dostawców. Wymogi w zakresie identyfikowalności dotyczące dostawców platform internetowych umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość, określone w niniejszym rozporządzeniu, nie mają wpływu na stosowanie dyrektywy Rady (UE) 2021/514³⁰, która służy realizacji innych uzasadnionych celów leżących w interesie publicznym.

- (73) Aby zapewnić skuteczne i odpowiednie stosowanie tego obowiązku bez nakładania nieproporcjonalnych obciążeń, dostawcy platform internetowych umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość powinni dołożyć wszelkich starań w celu oceny wiarygodności informacji przekazywanych przez zainteresowanych przedsiębiorców,

³⁰ Dyrektywa Rady (UE) 2021/514 z 22.03.2021 r. zmieniająca dyrektywę 2011/16/UE w sprawie współpracy administracyjnej w dziedzinie opodatkowania (Dz.Urz. UE L 104, s. 1).

w szczególności wykorzystując ogólnodostępne oficjalne internetowe bazy danych i interfejsy internetowe, takie jak krajowe rejestry handlowe i system wymiany informacji o VAT, lub zwrócić się do zainteresowanych przedsiębiorców o dostarczenie wiarygodnych dokumentów potwierdzających, takich jak kopie dokumentów tożsamości, uwierzytelnione wyciągi z rachunków płatniczych, zaświadczenia o prowadzeniu działalności gospodarczej i zaświadczenia z rejestrów handlowych. Aby wypełnić ten obowiązek, mogą oni również korzystać z innych źródeł, dostępnych do użytku na odległość, które oferują podobny stopień wiarygodności. Nie należy jednak wymagać od zainteresowanych dostawców platform internetowych, aby podejmowali nadmierne lub kosztowne działania zmierzające do ustaleniu faktów w internecie ani przeprowadzali nieproporcjonalną weryfikację na miejscu. Nie należy również rozumieć, że tacy dostawcy, którzy dołożyli wszelkich starań wymaganych w niniejszym rozporządzeniu, gwarantują wiarygodność informacji skierowanych do konsumentów lub innych zainteresowanych stron.

- (74) Dostawcy platform internetowych umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość powinni projektować i organizować swój interfejs internetowy w sposób umożliwiający przedsiębiorcom wypełnianie obowiązków wynikających z odpowiednich przepisów prawa Unii, w szczególności wymogów określonych w art. 6 i 8 dyrektywy 2011/83/UE, art. 7 dyrektywy 2005/29/WE, art. 5 i 6 dyrektywy 2000/31/WE oraz art. 3 dyrektywy 98/6/WE Parlamentu Europejskiego i Rady³¹. W tym celu zainteresowani dostawcy platform internetowych powinni dołożyć wszelkich starań, by ocenić, czy przedsiębiorcy korzystający z ich usług zamieścili kompletne informacje na ich interfejsach internetowych, zgodnie z odpowiednimi mającymi zastosowanie przepisami prawa Unii. Dostawcy platform internetowych powinni zapewnić, aby produkty lub usługi nie były oferowane, dopóki takie informacje nie są kompletne. Nie powinno to oznaczać nałożenia na zainteresowanych dostawców platform internetowych obowiązku ogólnego monitorowania produktów lub usług oferowanych przez przedsiębiorców za pośrednictwem ich usług ani ogólnego obowiązku ustalania faktów, w szczególności dokonywania oceny prawdziwości informacji przekazywanych przez przedsiębiorców. Interfejsy internetowe powinny być przyjazne dla użytkowników i łatwo dostępne dla przedsiębiorców i konsumentów. Dodatkowo, po umożliwieniu przedsiębiorcy oferowania produktu lub usługi, zainteresowani dostawcy platform internetowych powinni dołożyć rozsądnych starań, aby losowo sprawdzić, czy oferowane produkty lub usługi zostały zidentyfikowane jako nielegalne w jakichkolwiek oficjalnych, ogólnodostępnych internetowych bazach danych lub interfejsach internetowych nadających się do odczytu maszynowego, dostępnych w państwie

³¹ Dyrektywa 98/6/WE Parlamentu Europejskiego i Rady z 16.02.1998 r. w sprawie ochrony konsumenta przez podawanie cen produktów oferowanych konsumentom (Dz.Urz. UE L 80, s. 27).

członkowskim lub w Unii. Komisja powinna również zachęcać do identyfikowalności produktów za pomocą rozwiązań technologicznych, takich jak podpisane cyfrowo fotokody (kody QR) lub niewymienialne tokeny. Komisja powinna wspierać opracowywanie norm, a w przypadku ich braku – rozwiązań rynkowych, które mogą być do zaakceptowania przez zainteresowane strony.

- (75) Biorąc pod uwagę znaczenie bardzo dużych platform internetowych ze względu na ich zasięg, w szczególności wyrażony liczbą odbiorców usługi, dla ułatwienia debaty publicznej, transakcji gospodarczych i publicznego rozpowszechniania informacji, opinii i pomysłów oraz dla wywierania wpływu na sposób, w jaki odbiorcy uzyskują i przekazują informacje w internecie, konieczne jest nałożenie na dostawców tych platform szczególnych obowiązków, dodatkowych w stosunku do obowiązków mających zastosowanie do wszystkich platform internetowych. Ze względu na ich kluczową rolę w znajdowaniu i udostępnianiu informacji w internecie konieczne jest również nałożenie tych obowiązków, w zakresie, w jakim mają one zastosowanie, na dostawców bardzo dużych wyszukiwarek internetowych. Te dodatkowe obowiązki spoczywające na dostawcach bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych są konieczne, aby zaradzić takim obawom dotyczącym porządku publicznego, ponieważ brakuje alternatywnych i mniej restrykcyjnych środków, które pozwoliłyby skutecznie osiągnąć ten sam rezultat.
- (76) Bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe mogą powodować zagrożenia społeczne, których zakres i skutki są inne niż w przypadku mniejszych platform. Dostawcy takich bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni zatem spełniać najwyższą normę dotyczącą obowiązków w zakresie należytej staranności, proporcjonalnie do wywoływanych przez nich skutków społecznych. Gdy liczba aktywnych odbiorców platformy internetowej lub aktywnych odbiorców wyszukiwarki internetowej, obliczona jako średnia za okres sześciu miesięcy, osiągnie znaczący udział w ludności Unii, ryzyko systemowe, jakie stwarza platforma internetowa lub wyszukiwarka internetowa, może mieć nieproporcjonalny wpływ w Unii. Należy uznać, że taki znaczny zasięg występuje, w przypadku gdy taka liczba przekracza próg operacyjny ustalony na poziomie 45 mln osób, co odpowiada 10 % ludności Unii. Ten próg operacyjny powinien być aktualizowany i w związku z tym należy przekazać Komisji uprawnienia do uzupełniania, w razie potrzeby, przepisów niniejszego rozporządzenia w drodze aktów delegowanych.
- (77) Aby określić zasięg danej platformy internetowej lub wyszukiwarki internetowej, konieczne jest ustalenie średniej liczby aktywnych odbiorców każdej usługi indywidualnie. W związku z tym średnia liczba aktywnych miesięcznie odbiorców platformy internetowej powinna odzwierciedlać wszystkich odbiorców faktycznie korzystających z usługi co najmniej raz w danym okresie poprzez zetknięcie się z informacjami rozpowszechnianymi na interfejsie internetowym

platformy internetowej, jak na przykład oglądanie ich, słuchanie ich lub dostarczanie informacji, tak jak przedsiębiorcy na internetowej platformie handlowej umożliwiającej konsumentom zawieranie z przedsiębiorstwami umów zawieranych na odległość.

Do celów niniejszego rozporządzenia korzystanie nie ogranicza się do interakcji z informacjami poprzez kliknięcie, komentowanie, tworzenie hiperłączy, udostępnianie, nabywanie lub przeprowadzanie transakcji na platformie internetowej. W konsekwencji pojęcie aktywnego odbiorcy usługi niekoniecznie pokrywa się z pojęciem zarejestrowanego użytkownika usługi. Jeżeli chodzi o wyszukiwarki internetowe, pojęcie aktywnego odbiorcy usługi powinna obejmować osoby, które oglądają informacje na swoim interfejsie internetowym, ale nie powinna obejmować na przykład właścicieli stron internetowych indeksowanych przez wyszukiwarkę internetową, ponieważ nie korzystają oni aktywnie z tej usługi. Liczba aktywnych odbiorców usługi powinna obejmować wszystkich indywidualnych odbiorców usługi, którzy korzystają z danej usługi. W tym celu odbiorca usługi, który korzysta z różnych interfejsów internetowych, takich jak strony internetowe lub aplikacje, w tym również w przypadku, gdy dostęp do usług odbywa się za pośrednictwem różnych ujednoliconych formatów adresowania zasobów (adresy URL) lub nazw domen, powinien, w miarę możliwości, być liczony tylko jeden raz. Pojęcie aktywnego odbiorcy usługi nie powinno jednak obejmować przypadkowego korzystania z usługi przez odbiorców innych dostawców usług pośrednich, którzy pośrednio udostępniają informacje przechowywane przez dostawcę platform internetowych poprzez tworzenie hiperłączy lub indeksowanie przez dostawcę wyszukiwarki internetowej. Ponadto niniejsze rozporządzenie nie nakłada na dostawców platform internetowych lub wyszukiwarek internetowych obowiązku szczególnego śledzenia osób fizycznych w internecie. Jeżeli tacy dostawcy są w stanie pomijać zautomatyzowanych użytkowników, takich jak boty lub programy do wydobywania danych, bez dalszego przetwarzania danych osobowych i śledzenia, mogą to czynić. Na określenie liczby aktywnych odbiorców usług mogą mieć wpływ zmiany rynkowe i techniczne, w związku z czym należy przekazać Komisji uprawnienia do uzupełniania przepisów niniejszego rozporządzenia w drodze aktów delegowanych ustanawiających metodykę określania aktywnych odbiorców platformy internetowej lub wyszukiwarki internetowej, odzwierciedlającą w razie potrzeby charakter usługi i sposób, w jaki zachodzi interakcja między usługą a jej odbiorcą.

- (78) Ze względu na efekty sieciowe charakteryzujące gospodarkę platform baza użytkowników platformy internetowej lub wyszukiwarki internetowej może szybko się powiększyć i osiągnąć rozmiary bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej, co wiąże się z oddziaływaniem na rynek wewnętrzny. Może się tak stać w przypadku wzrostu wykładniczego następującego w krótkich okresach lub dużej globalnej obecności i obrotów

pozwalających platformie internetowej lub wyszukiwarce internetowej na pełne wykorzystanie efektów sieciowych oraz korzyści skali i zakresu. Wysoki roczny obrót lub kapitalizacja rynkowa mogą w szczególności wskazywać na szybką skalowalność pod względem dotarcia do użytkowników. W takich przypadkach koordynator ds. usług cyfrowych właściwy dla miejsca siedziby lub Komisja powinni mieć możliwość wnioskowania o częstsze składanie przez dostawcę platformy internetowej lub wyszukiwarki internetowej sprawozdań dotyczących liczby aktywnych odbiorców usługi, aby móc w odpowiednim czasie określić moment, w którym tę platformę lub tę wyszukiwarkę należy wskazać jako – odpowiednio – bardzo dużą platformę internetową lub bardzo dużą wyszukiwarkę internetową do celów niniejszego rozporządzenia.

- (79) Sposób korzystania z bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych może mieć istotny wpływ na bezpieczeństwo w internecie, kształtowanie opinii publicznej i dyskursu publicznego, a także handel w internecie. Sposób, w jaki projektują one swoje usługi, jest zasadniczo zoptymalizowany pod kątem przynoszenia korzyści ich modelom biznesowym, które często opierają się na reklamie, i może wywoływać problemy społeczne. Do skutecznego rozpoznania i ograniczenia ryzyka oraz szkód społecznych i gospodarczych, które mogą powstać, niezbędna jest skuteczna regulacja i egzekwowanie. Zgodnie z niniejszym rozporządzeniem dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni zatem oceniać ryzyko systemowe wynikające z projektu, funkcjonowania i korzystania z ich usług, a także z potencjalnego nadużywania usług przez odbiorców usługi, oraz powinni wprowadzać odpowiednie środki zmniejszające to ryzyko, przy jednoczesnym poszanowaniu praw podstawowych. Określając znaczenie potencjalnych negatywnych skutków i wpływu, dostawcy powinni rozważyć dotkliwość potencjalnego wpływu i prawdopodobieństwo wystąpienia całości takiego ryzyka systemowego. Na przykład mogliby ocenić, czy potencjalny negatywny wpływ może dotyczyć dużej liczby osób, czy jest on nieodwracalny, lub czy trudno jest naprawić i przywrócić sytuację istniejącą przed wystąpieniem potencjalnego wpływu.
- (80) Cztery kategorie ryzyka systemowego wymagają dogłębnej oceny ze strony dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych. Pierwsza kategoria dotyczy ryzyka związanego z rozpowszechnianiem nielegalnych treści, między innymi rozpowszechnianiem materiałów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych lub nielegalne nawoływanie do nienawiści lub inne rodzaje nadużywania ich usług do celów przestępczych, a także dopuszczaniem się nielegalnych działań, takich jak sprzedaż produktów lub usług zakazanych prawem Unii lub prawem krajowym, w tym produktów niebezpiecznych lub podrobionych, oraz nielegalny handel zwierzętami. Na przykład takie rozpowszechnianie lub działania mogą stanowić znaczące ryzyko systemowe w przypadku, gdy dostęp do nielegalnych

treści może szybko i szeroko rozprzestrzeniać się za pośrednictwem kont o szczególnie dużym zasięgu lub innych środków akcentujących. Dostawcy bardzo dużych platform internetowych oraz bardzo dużych wyszukiwarek internetowych powinni oceniać ryzyko rozpowszechniania nielegalnych treści niezależnie od tego, czy dane informacje są również niezgodne z warunkami korzystania z ich usług. Ocena ta pozostaje bez uszczerbku dla osobistej odpowiedzialności odbiorcy usługi bardzo dużych platform internetowych lub właścicieli stron internetowych indeksowanych przez bardzo duże wyszukiwarki internetowe za ewentualny nielegalny charakter ich działalności na podstawie obowiązującego prawa.

- (81) Druga kategoria dotyczy faktycznego lub przewidywalnego wpływu usługi na wykonywanie chronionych Kartą praw podstawowych, w tym godności ludzkiej, wolności wypowiedzi i informacji, w tym wolności i pluralizmu mediów, prawa do życia prywatnego, ochrony danych, prawa do niedyskryminacji, praw dziecka i ochrony konsumentów. Takie ryzyko może wystąpić na przykład w związku z projektem systemów algorytmicznych wykorzystywanych przez bardzo dużą platformę internetową lub bardzo dużą wyszukiwarkę internetową lub z nadużywaniem ich usług polegającym na dokonywaniu zgłoszeń stanowiących nadużycie lub stosowaniu innych metod tłumienia wypowiedzi lub ograniczania konkurencji. Przy ocenie rodzajów ryzyka w odniesieniu do praw dziecka dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni przeanalizować na przykład, w jakim stopniu projekt i funkcjonowanie danej usługi są łatwo zrozumiałe dla małoletnich, a także w jaki sposób – poprzez świadczoną przez nich usługę – małoletni mogą zetknąć się z treściami, które mogą mieć szkodliwy wpływ na ich zdrowie oraz rozwój fizyczny, psychiczny i moralny. Takie ryzyko może powstać na przykład w związku z projektem interfejsów internetowych, które umyślnie lub nieumyślnie wykorzystują słabe strony i niedoświadczenie małoletnich lub które mogą powodować zachowania nałogowe.
- (82) Trzecia kategoria ryzyka dotyczy faktycznego lub przewidywalnego negatywnego wpływu na procesy demokratyczne, dyskurs obywatelski i procesy wyborcze, a także na bezpieczeństwo publiczne.
- (83) Czwarta kategoria ryzyka wynika z podobnych obaw związanych z projektowaniem i funkcjonowaniem bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych lub korzystaniem z nich, w tym poprzez manipulację, co ma faktyczny lub przewidywalny negatywny wpływ na ochronę zdrowia publicznego, małoletnich oraz poważne negatywne konsekwencje dla fizycznego i psychicznego dobrostanu osoby, lub na przemoc ze względu na płeć. Takie ryzyko może również wynikać ze skoordynowanych kampanii dezinformacyjnych dotyczących zdrowia publicznego lub z projektowania interfejsów internetowych, które mogą stymulować uzależnienia behawioralne u odbiorców usług.

- (84) Oceniając takie ryzyko systemowe, dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni skupić się na systemach lub innych elementach, które mogą przyczynić się do powstania ryzyka, w tym na wszystkich systemach algorytmicznych, które mogą być istotne, w szczególności na swoich systemach rekomendacji i systemach reklamowych, zwracając uwagę na powiązane praktyki w zakresie gromadzenia i wykorzystywania danych. Powinni oni również ocenić, czy warunki korzystania z ich usług oraz ich egzekwowanie są odpowiednie, a także dokonać oceny swoich procesów moderacji treści, narzędzi technicznych i przydzielonych zasobów. Oceniając ryzyko systemowe określone w niniejszym rozporządzeniu, dostawcy ci powinni również skupić się na informacjach, które nie są nielegalne, ale przyczyniają się do powstania ryzyka systemowego określonego w niniejszym rozporządzeniu. Tacy dostawcy powinni zatem zwracać szczególną uwagę na to, w jaki sposób ich usługi są wykorzystywane do rozpowszechniania lub akcentowania wprowadzających w błąd lub zwodniczych treści, w tym dezinformacji. W przypadku gdy algorytmiczne akcentowanie informacji przyczynia się do ryzyka systemowego, dostawcy ci powinni należycie uwzględnić to w swoich ocenach ryzyka. Jeżeli ryzyko ma charakter lokalny lub występują różnice językowe, dostawcy ci powinni również uwzględnić to w swoich ocenach ryzyka. Dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni w szczególności ocenić, w jaki sposób projekt i funkcjonowanie ich usług, a także celowa i często skoordynowana manipulacja oraz korzystanie z ich usług, lub systemowe naruszenie warunków korzystania z usług, przyczyniają się do takiego ryzyka. Ryzyko takie może powstać na przykład w wyniku nieautentycznego korzystania z usługi, takiego jak zakładanie fałszywych kont, korzystanie z botów lub oszukańcze korzystanie z usługi oraz innych zautomatyzowanych lub częściowo zautomatyzowanych zachowań, które mogą prowadzić do szybkiego i szerokiego publicznego rozpowszechniania informacji stanowiących nielegalne treści lub treści niezgodne z warunkami korzystania z usług platformy internetowej lub wyszukiwarki internetowej oraz przyczyniać się do prowadzenia kampanii dezinformacyjnych.
- (85) Aby kolejne oceny ryzyka mogły opierać się na poprzednich ocenach i uwzględniać zmiany w zakresie zidentyfikowanego ryzyka, a także aby ułatwić działania w zakresie czynności sprawdzających i egzekwowanie, dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni przechowywać wszystkie dokumenty potwierdzające dotyczące przeprowadzonych przez nich ocen ryzyka, takie jak informacje na temat ich przygotowania, dane bazowe oraz dane dotyczące testowania ich systemów algorytmicznych.
- (86) Dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni wdrożyć, z poszanowaniem praw podstawowych, niezbędne środki w celu ograniczania z należytą starannością ryzyka systemowego określonego w ocenach ryzyka. Wszelkie przyjęte środki powinny być

zgodne z wymogami w zakresie należytej staranności określonymi w niniejszym rozporządzeniu oraz racjonalne i skuteczne w ograniczaniu określonych rodzajów ryzyka systemowego. Powinny one być proporcjonalne w świetle możliwości ekonomicznych dostawcy bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej oraz potrzeby unikania niepotrzebnych ograniczeń w korzystaniu z ich usług, z należyтым uwzględnieniem potencjalnych negatywnych skutków dla tych praw podstawowych. Dostawcy ci powinni zwrócić szczególną uwagę na wpływ na wolność wypowiedzi.

- (87) Dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni rozważyć, w ramach takich środków zmniejszających ryzyko, na przykład dostosowanie wszelkich niezbędnych projektów, cech lub funkcjonowania ich usług, takich jak projekt interfejsu internetowego. Powinni oni w razie potrzeby dostosować i stosować warunki korzystania z ich usług, zgodnie z przepisami niniejszego rozporządzenia dotyczącymi warunków korzystania z usług. Inne odpowiednie środki mogą obejmować dostosowanie systemów moderowania treści i procesów wewnętrznych lub dostosowanie procesów decyzyjnych i zasobów, w tym personelu moderującego treści, szkoleń dla takiego personelu oraz jego lokalnej wiedzy eksperckiej. Dotyczy to w szczególności szybkości i jakości przetwarzania zgłoszeń. W tym względzie na przykład przyjęty w 2016 r. Kodeks postępowania w zakresie zwalczania nielegalnego nawoływania do nienawiści w internecie stanowi punkt odniesienia, zgodnie z którym ważne zgłoszenia dotyczące usunięcia nielegalnej mowy nienawiści powinny być rozpatrywane w czasie krótszym niż 24 godziny. Dostawcy bardzo dużych platform internetowych, w szczególności tych wykorzystywanych głównie do publicznego rozpowszechniania treści pornograficznych, powinni z należyłą starannością wypełniać wszystkie swoje obowiązki wynikające z niniejszego rozporządzenia w odniesieniu do nielegalnych treści stanowiących cyberprzemoc, w tym nielegalnych treści pornograficznych, w szczególności w celu zapewnienia ofiarom możliwości skutecznego wykonywania przysługujących im praw w odniesieniu do treści stanowiących udostępnianie bez zgody treści intymnych lub zmanipulowanych, poprzez szybkie rozpatrywanie zgłoszeń i usuwanie takich treści bez zbędnej zwłoki. Rozpatrywanie zgłoszeń dotyczących innych rodzajów nielegalnych treści może wymagać dłuższego lub krótszego czasu, w zależności od konkretnych faktów i okoliczności oraz rodzajów poszczególnych nielegalnych treści. Dostawcy ci mogą również nawiązać lub zacieśnić współpracę z zaufanymi podmiotami sygnalizującymi oraz organizować sesje szkoleniowe i wymianę z organizacjami będącymi zaufanymi podmiotami sygnalizującymi.
- (88) Dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni również podchodzić z należyłą starannością do środków, jakie podejmują w celu testowania i w razie potrzeby dostosowywania swoich systemów algorytmicznych, a zwłaszcza systemów rekomendacji. Może

zaistnieć potrzeba złagodzenia negatywnych skutków spersonalizowanych rekomendacji i skorygowania kryteriów stosowanych w ich rekomendacjach. Katalizatorem ryzyka systemowego mogą być również systemy reklamowe stosowane przez dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych. Dostawcy ci powinni rozważyć podjęcie środków naprawczych, takich jak pozbawienie wpływów z reklam w przypadku określonych informacji, lub innych działań, takich jak poprawa widoczności autorytatywnych źródeł informacji, lub bardziej strukturalne dostosowanie swoich systemów reklamowych. Dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych mogą być zmuszeni do wzmocnienia swoich wewnętrznych procesów lub nadzoru nad wszelkimi swoimi działaniami, w szczególności w zakresie wykrywania ryzyka systemowego, oraz do przeprowadzania częstszych lub bardziej ukierunkowanych ocen ryzyka związanych z nowymi funkcjami. W szczególności, jeżeli ryzyko dotyczy różnych platform internetowych lub wyszukiwarek internetowych, powinni oni współpracować z innymi dostawcami usług, między innymi inicjując opracowanie kodeksów postępowania lub innych środków samoregulacyjnych lub przyłączając się do już istniejących kodeksów lub środków. Powinni oni także rozważyć działania mające na celu podnoszenie świadomości, w szczególności gdy ryzyko związane jest z kampaniami dezinformacyjnymi.

- (89) Dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni, przy podejmowaniu środków takich jak dostosowanie projektu usług i interfejsu internetowego, brać pod uwagę najlepszy interes małoletnich, w szczególności gdy ich usługi są skierowane do małoletnich lub gdy korzystają z nich w przeważającej mierze małoletni. Powinni oni zapewniać, by ich usługi były zorganizowane w taki sposób, by małoletni mieli łatwy dostęp do mechanizmów przewidzianych w niniejszym rozporządzeniu, w tym mechanizmów zgłoszeń i działań oraz mechanizmów rozpatrywania skarg. Powinni oni również podejmować środki w celu ochrony małoletnich przed treściami mogącymi zaszkodzić ich rozwojowi fizycznemu, psychicznemu lub moralnemu oraz zapewniać narzędzia umożliwiające warunkowy dostęp do takich informacji. Wybierając odpowiednie środki zmniejszające ryzyko, dostawcy mogą uwzględnić, w stosownych przypadkach, najlepsze praktyki branżowe, w tym praktyki ustanowione w drodze samoregulacyjnej współpracy, takie jak kodeksy postępowania, a także powinni uwzględnić wytyczne Komisji.
- (90) Dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni zapewnić, aby ich podejście do oceny i zmniejszania ryzyka opierało się na najlepszych dostępnych informacjach i spostrzeżeniach naukowych oraz aby sprawdzali oni swoje założenia z grupami, na które ryzyko i podejmowane środki mają największy wpływ. W tym celu powinni w stosownych przypadkach przeprowadzać oceny ryzyka i opracowywać środki zmniejszające ryzyko z udziałem przedstawicieli odbiorców usług,

przedstawicieli grup, na które ich usługi mogą wywierać wpływ, niezależnych ekspertów i organizacji społeczeństwa obywatelskiego. Powinny oni dążyć do włączenia takich konsultacji do swoich metodyk oceny ryzyka i projektowania środków zmniejszających ryzyko, w tym, w stosownych przypadkach, badań ankietowych, grup dyskusyjnych, okrągłych stołów oraz innych metod konsultacji i projektowania. Przy ocenie, czy dany środek jest racjonalny, proporcjonalny i skuteczny, należy zwrócić szczególną uwagę na prawo do wolności wypowiedzi.

- (91) W czasach kryzysu może zaistnieć potrzeba pilnego podjęcia pewnych szczególnych środków przez dostawców bardzo dużych platform internetowych, oprócz środków, które podjęliby w związku z ich innymi obowiązkami wynikającymi z niniejszego rozporządzenia. W tym względzie należy uznać, że kryzys ma miejsce w przypadku wystąpienia nadzwyczajnych okoliczności, które mogą prowadzić do poważnego zagrożenia bezpieczeństwa publicznego lub zdrowia publicznego w Unii lub jej znacznych częściach. Takie kryzysy mogą wynikać z konfliktów zbrojnych lub aktów terrorystycznych, w tym pojawiających się konfliktów lub aktów terrorystycznych, klęsk żywiołowych, takich jak trzęsienia ziemi i huragany, a także pandemii i innych poważnych transgranicznych zagrożeń dla zdrowia publicznego. Komisja powinna mieć możliwość żądania od dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, na podstawie zalecenia Europejskiej Rady ds. Usług Cyfrowych (zwanej dalej „Radą Usług Cyfrowych”), aby w trybie pilnym podjęli działania w sytuacjach kryzysowych. Środki, które ci dostawcy mogą określić i których zastosowanie mogą rozważyć, mogą obejmować na przykład dostosowanie procesów moderacji treści i zwiększenie zasobów przeznaczonych do moderowania treści, dostosowanie warunków korzystania z usług, odpowiednich systemów algorytmicznych i systemów reklamowych, dalszą intensyfikację współpracy z zaufanymi podmiotami sygnalizującymi, podejmowanie działań uświadamiających i promowanie wiarygodnych informacji oraz dostosowanie projektu swoich interfejsów internetowych. Należy ustanowić niezbędne wymogi w celu zapewnienia, aby takie środki były podejmowane w bardzo krótkim czasie oraz aby mechanizm reagowania kryzysowego był stosowany tylko wtedy, gdy jest to absolutnie niezbędne, a wszelkie środki podejmowane w ramach tego mechanizmu były skuteczne i proporcjonalne, z należyтым uwzględnieniem praw i prawnie uzasadnionych interesów wszystkich zainteresowanych stron. Stosowanie tego mechanizmu powinno pozostawać bez uszczerbku dla innych przepisów niniejszego rozporządzenia, takich jak przepisy dotyczące oceny ryzyka i środków zmniejszających ryzyko oraz ich egzekwowania, a także przepisów dotyczących protokołów kryzysowych.

- (92) Biorąc pod uwagę potrzebę zapewnienia weryfikacji przez niezależnych ekspertów, dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni być rozliczani, w drodze niezależnych audytów, z wypełniania obowiązków ustanowionych w niniejszym rozporządzeniu

oraz, w stosownych przypadkach, wszelkich zobowiązań uzupełniających podjętych zgodnie z kodeksami postępowania i protokołami kryzysowymi. Aby zapewnić przeprowadzanie audytów w sposób skuteczny, efektywny i terminowy, dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni zapewnić niezbędną współpracę i pomoc organizacjom przeprowadzającym audyty, w tym poprzez umożliwienie audytorowi dostępu do wszystkich istotnych danych i pomieszczeń niezbędnych do prawidłowego przeprowadzenia audytu, w tym, w stosownych przypadkach, do danych związanych z systemami algorytmicznymi, oraz poprzez udzielanie odpowiedzi na pytania ustne lub pisemne. Audytorzy powinni posiadać również możliwość korzystania z innych źródeł obiektywnych informacji, w tym z badań prowadzonych przez zweryfikowanych badaczy. Dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych nie powinni zakłócać przeprowadzania audytu. Audyty powinny być przeprowadzane zgodnie z najlepszymi praktykami branżowymi oraz wysoką etyką zawodową i obiektywizmem, z należyтым uwzględnieniem, w stosownych przypadkach, norm dotyczących audytów i kodeksów postępowania. Audytorzy powinni zagwarantować poufność, bezpieczeństwo i integralność informacji, takich jak tajemnice przedsiębiorstwa, które uzyskują podczas wykonywania swoich zadań. Ta gwarancja nie powinna być środkiem służącym do obejścia obowiązków w zakresie audytu ustanowionych w niniejszym rozporządzeniu. Audytorzy powinni dysponować niezbędną wiedzą ekspercką w dziedzinie zarządzania ryzykiem oraz kompetencje techniczne w zakresie przeprowadzania audytu algorytmów. Audytorzy powinni być niezależni, aby mogli wykonywać swoje zadania w odpowiedni i godny zaufania sposób. Powinni oni spełniać podstawowe wymogi w zakresie niezależności w odniesieniu do zakazanych usług niezwiązanych z audytem, rotacji firm audytorskich oraz honorariów bezwarunkowych. Jeżeli ich niezależność i kompetencje techniczne budzą wątpliwości, powinni zrezygnować z wykonania zlecenia audytu lub powstrzymać się od jego wykonania.

- (93) Sprawozdanie z audytu powinno być uzasadnione, aby przedstawiało ono rzeczywisty obraz podjętych działań i wyciągniętych wniosków. Powinno stanowić dodatkową podstawę środków przyjmowanych przez dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych w celu wypełnienia obowiązków wynikających z niniejszego rozporządzenia, a w stosownych przypadkach zawierać propozycje ulepszenia takich środków. Po otrzymaniu sprawozdania z audytu należy je przekazać koordynatorowi ds. usług cyfrowych właściwemu dla miejsca siedziby, Komisji oraz Radzie Usług Cyfrowych. Dostawcy powinni również bez zbędnej zwłoki przekazać po zakończeniu wszystkie sprawozdania z oceny ryzyka i środków zmniejszających ryzyko, a także sprawozdanie z realizacji audytu dostawcy bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej, pokazujące,

w jaki sposób odnieśli się oni do zaleceń audytu. Sprawozdanie z audytu powinno zawierać opinię audytową opartą na wnioskach wyciągniętych z uzyskanych dowodów audytowych. „Pozytywna opinia” powinna zostać wydana wówczas, gdy wszystkie dowody wskazują na to, że dostawca bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej wypełnia obowiązki ustanowione w niniejszym rozporządzeniu lub, w stosownych przypadkach, wypełnia wszelkie zobowiązania podjęte zgodnie z kodeksem postępowania lub protokołem kryzysowym, w szczególności przez określenie, ocenę i zmniejszenie ryzyka systemowego stwarzanego przez jego system i usługi. W przypadku gdy audytor chce przekazać uwagi, które nie mają istotnego wpływu na wynik audytu, „pozytywną opinię” należy opatrzyć uwagami. „Negatywna opinia” powinna zostać wydana, jeżeli audytor uzna, że dostawca bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej nie przestrzega niniejszego rozporządzenia lub nie wypełnia podjętych zobowiązań. W przypadku gdy w opinii audytowej nie zawarto wniosków dotyczących określonych elementów objętych zakresem audytu, do opinii audytowej należy dołączyć wyjaśnienie przyczyn braku takich wniosków. W stosownych przypadkach sprawozdanie powinno zawierać opis określonych elementów, które nie mogły zostać poddane audytowi, oraz wyjaśnienie, dlaczego nie mogły one zostać poddane audytowi.

- (94) Obowiązki w zakresie oceny i zmniejszania ryzyka powinny, w poszczególnych przypadkach, wiązać się z koniecznością przeprowadzenia przez dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych oceny projektu swoich systemów rekomendacji i w razie potrzeby ich dostosowania, na przykład przez podjęcie środków mających na celu zapobieganie uprzedzeniom prowadzącym do dyskryminacji osób podatnych na zagrożenia lub minimalizowanie tych uprzedzeń, w szczególności w przypadku, gdy takie dostosowanie jest zgodne z przepisami dotyczącymi ochrony danych i gdy informacje są spersonalizowane na podstawie szczególnych kategorii danych osobowych, o których mowa w art. 9 rozporządzenia (UE) 2016/679. Ponadto, uzupełniając obowiązki w zakresie przejrzystości mające zastosowanie do platform internetowych w odniesieniu do ich systemów rekomendacji, dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni konsekwentnie zapewniać odbiorcom ich usług alternatywne opcje, które nie opierają się na profilowaniu w rozumieniu rozporządzenia (UE) 2016/679, w odniesieniu do głównych parametrów ich systemów rekomendacji. Takie opcje powinny być bezpośrednio dostępne za pośrednictwem interfejsu internetowego, na którym przedstawiane są zalecenia.
- (95) Systemy reklamowe wykorzystywane przez bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe stwarzają szczególne ryzyko i wymagają dalszego nadzoru publicznego i regulacyjnego ze względu na ich skalę i zdolność ukierunkowania usługi na odbiorców i docierania do nich na

podstawie ich zachowania w ramach interfejsu internetowego tej platformy lub wyszukiwarki i poza nim. Bardzo duże platformy internetowe lub bardzo duże wyszukiwarki internetowe powinny zapewniać publiczny dostęp do repozytoriów reklam prezentowanych na ich interfejsach internetowych w celu ułatwienia nadzoru i badań nad pojawiającymi się zagrożeniami wynikającymi z dystrybucji reklam w internecie, na przykład w odniesieniu do nielegalnych reklam lub technik manipulacyjnych i dezinformacji, która w sposób realny i przewidywalny wpływa negatywnie na zdrowie publiczne, bezpieczeństwo publiczne, dyskurs obywatelski, udział w życiu politycznym i równość. Repozytoria powinny zawierać treść reklam, w tym nazwę produktu, usługi lub marki oraz przedmiot reklamy, i powiązane z nimi dane dotyczące reklamodawcy, oraz, jeżeli jest to inna osoba, osoby fizycznej lub prawnej, która zapłaciła za reklamę, i dostarczania reklam, w szczególności w przypadku ukierunkowania reklam. Informacje te powinny obejmować zarówno informacje na temat kryteriów ukierunkowania oraz dostarczania reklam, w szczególności gdy reklamy są dostarczane osobom podatnym na zagrożenia, takim jak małoletni.

- (96) Aby odpowiednio monitorować i oceniać wypełnianie przez bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe obowiązków ustanowionych w niniejszym rozporządzeniu, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby lub Komisja mogą zażądać dostępu do określonych danych, w tym danych związanych z algorytmami, lub ich zgłaszania. Wymóg taki może obejmować na przykład dane niezbędne do oceny ryzyka i możliwych szkód powodowanych przez systemy bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej, dane dotyczące dokładności, funkcjonowania i testowania systemów algorytmicznych służących do moderowania treści, systemów rekomendacji lub systemów reklamowych, w tym w stosownych przypadkach dane i algorytmy szkoleniowe, lub dane dotyczące procesów i wyników moderowania treści lub wewnętrznych systemów rozpatrywania skarg w rozumieniu niniejszego rozporządzenia. Taki dostęp do danych nie powinien obejmować wniosków o przedstawienie konkretnych informacji o indywidualnych odbiorcach usługi do celów ustalenia, czy przestrzegają oni innych mających zastosowanie przepisów prawa Unii lub prawa krajowego. Prowadzone przez badaczy analizy ewolucji i powagi ryzyka systemowego w internecie mają szczególne znaczenie dla niwelowania asymetrii informacji i tworzenia odpornego systemu zmniejszania ryzyka, ponieważ dostarczają informacji dostawcom platform internetowych, dostawcom wyszukiwarek internetowych, koordynatorom ds. usług cyfrowych, innym właściwym organom, Komisji i społeczeństwu.
- (97) Niniejsze rozporządzenie stanowi zatem ramy zapewniające dostęp do danych z bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych zweryfikowanym badaczom powiązanym z organizacją badawczą w rozumieniu art. 2 dyrektywy (UE) 2019/790, co może obejmować, do

celów niniejszego rozporządzenia, organizacje społeczeństwa obywatelskiego prowadzące badania naukowe, których głównym celem jest wspieranie ich zadań leżących w interesie publicznym. Wszystkie wnioski o dostęp do danych na podstawie tych ram powinny być proporcjonalne i odpowiednio chronić prawa i prawnie uzasadnione interesy, w tym ochronę danych osobowych, tajemnice przedsiębiorstwa i inne informacje poufne bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych i wszelkich innych zainteresowanych stron, w tym odbiorców usług. Aby jednak zapewnić osiągnięcie celu niniejszego rozporządzenia, uwzględnienie interesów handlowych dostawców nie powinno prowadzić do odmowy udzielenia dostępu do danych niezbędnych do realizacji konkretnego celu badawczego zgodnie z wnioskiem złożonym na podstawie niniejszego rozporządzenia. W związku z tym, bez uszczerbku dla dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/943³², dostawcy powinni zapewnić badaczom odpowiedni dostęp, w tym, w razie potrzeby, poprzez zastosowanie zabezpieczeń technicznych, takich jak przestrzenie danych. Wnioski o dostęp do danych mogą dotyczyć na przykład liczby wyświetleń lub, w stosownych przypadkach, innych rodzajów dostępu odbiorców usług do treści przed ich usunięciem przez dostawców bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych.

- (98) Dodatkowo, w przypadku gdy dane są publicznie dostępne, tacy dostawcy nie powinni uniemożliwiać badaczom spełniającym odpowiedni zestaw kryteriów wykorzystywania tych danych do celów badawczych, które przyczyniają się do wykrywania, identyfikacji i zrozumienia ryzyka systemowego. Powinni oni udzielić takim badaczom dostępu, w tym, o ile jest to technicznie możliwe, w czasie rzeczywistym, do publicznie dostępnych danych, na przykład dotyczących zagregowanych interakcji z treściami pochodzącymi ze stron publicznych, od grup publicznych lub osób publicznych, w tym danych dotyczących wrażenia i zaangażowania, takich jak liczba reakcji, udostępnień i komentarzy odbiorców usług. Należy zachęcać dostawców bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych do współpracy z badaczami i zapewniania szerszego dostępu do danych na potrzeby monitorowania problemów społecznych poprzez dobrowolne działania, w tym poprzez zobowiązania i procedury uzgodnione w ramach kodeksów postępowania lub protokołów kryzysowych. Tacy dostawcy i badacze powinni zwracać szczególną uwagę na ochronę danych osobowych i zapewniać zgodność przetwarzania danych osobowych z rozporządzeniem (UE) 2016/679. Dostawcy powinni anonimizować lub pseudonimizować dane osobowe, z wyjątkiem przypadków, w których uniemożliwiłoby to osiągnięcie zamierzonego celu badawczego.

³² Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z 8.06.2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskaniem, wykorzystywaniem i ujawnianiem (Dz.Urz. UE L 157, s. 1).

- (99) Ze względu na złożoność funkcjonowania wdrożonych systemów oraz ryzyko systemowe stwarzane dla społeczeństwa dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni ustanowić komórkę nadzoru przestrzegania niniejszego rozporządzenia, która powinna być niezależna od komórek operacyjnych tych dostawców. Kierownik komórki nadzoru przestrzegania niniejszego rozporządzenia powinien podlegać bezpośrednio kierownictwu dostawcy, w tym w odniesieniu do obaw związanych z nieprzestrzeganiem przepisów niniejszego rozporządzenia. Pracownicy ds. nadzoru przestrzegania niniejszego rozporządzenia pracujący w ramach komórki nadzoru przestrzegania niniejszego rozporządzenia powinni posiadać kwalifikacje, wiedzę, doświadczenie i umiejętności niezbędne do stosowania środków w praktyce i monitorowania przestrzegania niniejszego rozporządzenia w ramach organizacji dostawców bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej. Dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinni zapewnić, by komórka nadzoru przestrzegania niniejszego rozporządzenia była właściwie i terminowo włączana we wszystkie sprawy związane z niniejszym rozporządzeniem, w tym w ocenę ryzyka i strategię zmniejszania ryzyka oraz konkretne środki, a także w proces oceny wypełniania, w stosownych przypadkach, zobowiązań podjętych przez tych dostawców na podstawie kodeksów postępowania i protokołów kryzysowych, które stosują.
- (100) Ze względu na dodatkowe ryzyko związane z ich działalnością i dodatkowe obowiązki wynikające z niniejszego rozporządzenia dodatkowe wymogi dotyczące przejrzystości powinny mieć zastosowanie w szczególności do bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, zwłaszcza w celu składania kompleksowych sprawozdań z przeprowadzonych ocen ryzyka i późniejszych środków przyjętych zgodnie z niniejszym rozporządzeniem.
- (101) Komisja powinna dysponować wszelkimi zasobami, takimi jak zasoby ludzkie, wiedza specjalistyczna czy środki finansowe, niezbędnymi do realizacji swoich zadań wynikających z niniejszego rozporządzenia. Aby zapewnić dostępność zasobów niezbędnych do odpowiedniego nadzoru na poziomie unijnym na mocy niniejszego rozporządzenia oraz biorąc pod uwagę, że państwa członkowskie powinny być uprawnione do pobierania opłat nadzorczych od dostawców mających siedzibę na ich terytorium w związku z zadaniami związanymi z nadzorem i egzekwowaniem wykonywanymi przez ich organy, Komisja powinna pobierać opłaty nadzorcze, których wysokość powinna być określana co roku, od bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych. Całkowita kwota pobieranych rocznych opłat nadzorczych powinna być ustalana na podstawie całkowitej kwoty kosztów ponoszonych przez Komisję w związku z wykonywaniem zadań nadzorczych wynikających z niniejszego rozporządzenia, oszacowanych rozsądnie z odpowiednim wyprzedzeniem.

Kwota ta powinna obejmować koszty związane z wykonywaniem konkretnych uprawnień i zadań dotyczących nadzoru, czynności sprawdzających, egzekwowania i monitorowania w odniesieniu do dostawców bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych, w tym koszty związane ze wskazaniem jako bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe lub z utworzeniem, utrzymywaniem i funkcjonowaniem baz danych przewidzianych w niniejszym rozporządzeniu.

Kwota ta powinna również obejmować koszty związane z utworzeniem, utrzymaniem i funkcjonowaniem podstawowej infrastruktury informacyjnej i instytucjonalnej na potrzeby współpracy między koordynatorami ds. usług cyfrowych, Radą Usług Cyfrowych i Komisją, z uwzględnieniem faktu, że ze względu na swój rozmiar i zasięg bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe mają znaczący wpływ na zasoby potrzebne do wsparcia takiej infrastruktury. Oszacowanie kosztów całkowitych powinno uwzględniać koszty nadzoru poniesione w poprzednim roku, w tym, w stosownych przypadkach, koszty przekraczające wysokość indywidualnej rocznej opłaty nadzorczej pobranej w poprzednim roku. Zewnętrzne dochody przeznaczone na określony cel, wynikające z rocznej opłaty nadzorczej, można wykorzystać na finansowanie dodatkowych zasobów ludzkich, takich jak pracownicy kontraktowi i oddelegowani eksperci krajowi, oraz na inne wydatki związane z realizacją zadań powierzonych Komisji na mocy niniejszego rozporządzenia. Roczna opłata nadzorcza pobierana od dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych powinna być proporcjonalna do wielkości usługi, odzwierciedlonej w liczbie aktywnych odbiorców usługi w Unii. Ponadto indywidualna roczna opłata nadzorcza nie powinna przekraczać ogólnego pułapu dla każdego dostawcy bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej, przy uwzględnieniu możliwości finansowych dostawcy wskazanej usługi lub usług.

- (102) Aby ułatwić skuteczne i spójne stosowanie obowiązków określonych w niniejszym rozporządzeniu, które mogą wymagać wdrożenia za pomocą środków technologicznych, ważne jest promowanie dobrowolnych norm obejmujących niektóre procedury techniczne, w przypadku gdy branża może pomóc w opracowaniu znormalizowanych środków służących wspieraniu dostawców usług pośrednich w zakresie przestrzegania niniejszego rozporządzenia, takich jak umożliwienie dokonywania zgłoszeń, w tym za pomocą interfejsów programowania aplikacyjnego, norm związanych z warunkami korzystania z usług lub norm związanych z audytami lub norm dotyczących interoperacyjności repozytoriów reklam. Ponadto normy takie mogłyby obejmować normy związane z reklamą internetową, systemami rekomendacji, dostępnością i ochroną małoletnich w internecie. Dostawcy usług pośrednich mogą przyjmować takie normy, ale samo ich przyjęcie nie oznacza, że niniejsze rozporządzenie jest przestrzegane. Jednocześnie, zapewniając najlepsze praktyki, takie normy

mogą być szczególnie przydatne w przypadku stosunkowo małych dostawców usług pośrednich. W normach tych można by odpowiednio rozróżnić poszczególne rodzaje nielegalnych treści lub poszczególne rodzaje usług pośrednich.

- (103) Komisja i Rada Usług Cyfrowych powinny zachęcać do opracowywania dobrowolnych kodeksów postępowania, a także do wdrażania postanowień tych kodeksów, aby przyczynić się do stosowania niniejszego rozporządzenia. Komisja i Rada Usług Cyfrowych powinny dążyć do tego, aby w kodeksach postępowania wyraźnie określono charakter realizowanych celów leżących w interesie publicznym, zawarto mechanizmy niezależnej oceny realizacji tych celów oraz aby wyraźnie określono rolę odpowiednich organów. Szczególną uwagę należy zwrócić na unikanie negatywnych skutków dla bezpieczeństwa, ochrony prywatności i danych osobowych, a także na zakaz nakładania ogólnych obowiązków w zakresie monitorowania. Wdrażanie kodeksów postępowania powinno być wymierne i podlegać nadzorowi publicznemu, nie powinno jednak naruszać dobrowolnego charakteru takich kodeksów i swobody zainteresowanych stron w podejmowaniu decyzji o przystąpieniu do kodeksu. W pewnych okolicznościach ważne jest, aby bardzo duże platformy internetowe współpracowały przy opracowywaniu i przestrzeganiu konkretnych kodeksów postępowania. Żaden z przepisów niniejszego rozporządzenia nie uniemożliwia innym dostawcom usług przestrzegania tych samych norm w zakresie należytej staranności, przyjmowania najlepszych praktyk i korzystania z wytycznych udzielanych przez Komisję i Radę Usług Cyfrowych przez przystąpienie do tych samych kodeksów postępowania.
- (104) Należy określić w niniejszym rozporządzeniu pewne obszary wymagające uwzględnienia przy opracowywaniu takich kodeksów postępowania. W szczególności środki zmniejszające ryzyko związane z określonymi rodzajami nielegalnych treści powinny być przedmiotem porozumień samoregulacyjnych i współregulacyjnych. Innym obszarem, który należy uwzględnić, jest możliwy negatywny wpływ ryzyka systemowego na społeczeństwo i demokrację, czego przykładem są dezinformacja lub działania manipulacyjne i nadużycia lub wszelkie negatywne skutki dla małoletnich. Obszar ten obejmuje skoordynowane działania ukierunkowane na akcentowanie informacji, w tym dezinformacji, na przykład wykorzystywanie botów lub fałszywych kont do tworzenia celowo nieprawdziwych lub wprowadzających w błąd informacji, niekiedy w celu uzyskania korzyści ekonomicznych, które są szczególnie szkodliwe dla odbiorców usługi podatnych na zagrożenia, takich jak małoletni. W przypadku takich obszarów przestrzeganie i stosowanie danego kodeksu postępowania przez bardzo dużą platformę internetową lub bardzo dużą wyszukiwarkę internetową można uznać za odpowiedni środek zmniejszający ryzyko. Przy ustalaniu, czy dana platforma internetowa lub wyszukiwarka internetowa naruszyła obowiązki ustanowione w niniejszym rozporządzeniu, można wziąć pod uwagę w stosownych przypadkach odrzucenie przez dostawcę danej platformy internetowej lub

wyszukiwarki internetowej, bez odpowiednich wyjaśnień, zaproszenia Komisji do uczestnictwa w stosowaniu takiego kodeksu postępowania. Fakt uczestnictwa w danym kodeksie postępowania i jego wdrażania nie powinien sam w sobie oznaczać, że niniejsze rozporządzenie jest przestrzegane.

- (105) Kodeksy postępowania powinny ułatwiać dostępność bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, zgodnie z prawem Unii i prawem krajowym, aby ułatwić przewidywalne korzystanie z nich przez osoby z niepełnosprawnościami. W szczególności kodeksy postępowania mogłyby zapewniać, aby informacje były przedstawiane w sposób dostrzegalny, funkcjonalny, zrozumiały i solidny, oraz aby formularze i środki, opracowane na podstawie niniejszego rozporządzenia, były udostępniane w sposób łatwy do znalezienia i dostępny dla osób z niepełnosprawnościami.
- (106) Przepisy dotyczące kodeksów postępowania zamieszczone w niniejszym rozporządzeniu mogłyby służyć jako podstawa podjętych już działań samoregulacyjnych na poziomie Unii, w tym systemu zobowiązań do zapewnienia bezpieczeństwa produktów (Product Safety Pledge), Protokołu ustaleń w sprawie sprzedaży podrobionych towarów w internecie, kodeksu postępowania w sprawie przeciwdziałania nielegalnemu nawoływaniu do nienawiści w internecie oraz kodeksu postępowania w zakresie zwalczania dezinformacji. W szczególności w odniesieniu do tego ostatniego dokumentu, po wydaniu przez Komisję wytycznych, wzmocniono kodeks praktyk w zakresie zwalczania dezinformacji zgodnie z zapowiedzią zawartą w europejskim planie działania na rzecz demokracji.
- (107) Udostępnianie reklam internetowych odbywa się na ogół z udziałem kilku podmiotów, w tym z wykorzystaniem usług pośrednich, które łączą wydawców reklam z reklamodawcami. Kodeksy postępowania powinny wspierać i uzupełniać określone w niniejszym rozporządzeniu obowiązki w zakresie przejrzystości dotyczące reklamy spoczywające na dostawcach platform internetowych, bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, aby zapewnić elastyczne i skuteczne mechanizmy ułatwiające i zwiększające wypełnianie tych obowiązków, w szczególności w zakresie sposobów transmisji odpowiednich informacji. Powinno to obejmować ułatwienie transmisji informacji o reklamodawcy, który płaci za reklamę, gdy jest nim inny podmiot niż osoba fizyczna lub prawna, w imieniu której reklama jest prezentowana na interfejsie internetowym platformy internetowej. Kodeksy postępowania powinny również obejmować środki zapewniające odpowiednie udostępnianie istotnych informacji na temat monetyzacji danych w całym łańcuchu wartości. Udział wielu zainteresowanych stron powinien zapewnić szerokie poparcie dla tych kodeksów postępowania, ich wykonalność pod względem technicznym, skuteczność i najwyższy poziom przyjazności dla użytkownika, aby zapewnić osiągnięcie celów, którym służą obowiązki w zakresie przejrzystości. Aby zapewnić skuteczność kodeksów postępowania, Komisja powinna przewidzieć

mechanizmy oceny przy opracowywaniu kodeksów postępowania. W stosownych przypadkach Komisja może zwrócić się do Agencji Praw Podstawowych lub Europejskiego Inspektora Ochrony Danych o wyrażenie opinii na temat danego kodeksu postępowania.

- (108) Oprócz mechanizmu reagowania kryzysowego w przypadku bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, Komisja może wystąpić z inicjatywą opracowania dobrowolnych protokołów kryzysowych w celu skoordynowania szybkiej, zbiorowej i transgranicznej reakcji w środowisku internetowym. Może mieć to miejsce na przykład wtedy, gdy platformy internetowe są nadużywane do szybkiego rozpowszechniania nielegalnych treści lub dezinformacji lub gdy zachodzi potrzeba szybkiego rozpowszechnienia wiarygodnych informacji. W świetle ważnej roli bardzo dużych platform internetowych w rozpowszechnianiu informacji w naszych społeczeństwach i w kontekście transgranicznym dostawców takich platform należy zachęcać do opracowywania i stosowania konkretnych protokołów kryzysowych. Takie protokoły kryzysowe powinny być uruchamiane tylko na ograniczony okres, a przyjęte środki powinny być również ograniczone do tego, co jest absolutnie niezbędne do zaradzenia nadzwyczajnym okolicznościom. Środki te powinny być zgodne z niniejszym rozporządzeniem i nie powinny prowadzić do nałożenia na uczestniczących w nich dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych ogólnego obowiązku monitorowania informacji, które dostawcy ci przekazują lub przechowują, ani do aktywnego ustalania faktów lub okoliczności wskazujących na nielegalne treści.
- (109) Aby zapewnić odpowiedni nadzór i egzekwowanie obowiązków ustanowionych w niniejszym rozporządzeniu, państwa członkowskie powinny wyznaczyć co najmniej jeden organ i powierzyć mu zadanie nadzorowania stosowania i egzekwowania niniejszego rozporządzenia, bez uszczerbku dla możliwości wyznaczenia istniejącego organu i jego formy prawnej zgodnie z prawem krajowym. Państwa członkowskie powinny jednak mieć możliwość powierzenia szczególnych zadań i kompetencji w zakresie nadzorowania lub egzekwowania stosowania niniejszego rozporządzenia, na przykład w odniesieniu do określonych sektorów, w których uprawnione mogą być również istniejące organy, więcej niż jednemu właściwemu organowi, w tym organom regulacyjnym ds. łączności elektronicznej, organom regulacyjnym ds. mediów lub organom ochrony konsumentów, stosownie do krajowej struktury konstytucyjnej, organizacyjnej i administracyjnej. Wykonując swoje zadania, wszystkie właściwe organy powinny przyczyniać się do realizacji celów niniejszego rozporządzenia, a mianowicie do prawidłowego funkcjonowania rynku wewnętrznego usług pośrednich, na którym zharmonizowane przepisy dotyczące bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego, które ułatwia innowacje, a w szczególności obowiązki w zakresie należytej staranności

mające zastosowanie do różnych kategorii dostawców usług pośrednich, są skutecznie nadzorowane i egzekwowane, z myślą o zapewnieniu skutecznej ochrony praw podstawowych zapisanych w Karcie, w tym zasady ochrony konsumentów. Niniejsze rozporządzenie nie nakłada na państwa członkowskie obowiązku powierzenia właściwym organom zadania rozstrzygania o zgodności z prawem określonych treści.

- (110) Ze względu na transgraniczny charakter przedmiotowych usług oraz horyzontalny zakres obowiązków wprowadzonych niniejszym rozporządzeniem jeden z organów, któremu powierzono zadanie nadzorowania stosowania i, w razie potrzeby, egzekwowania niniejszego rozporządzenia w każdym państwie członkowskim powinien nosić miano koordynatora ds. usług cyfrowych. Jeżeli do nadzorowania stosowania i egzekwowania niniejszego rozporządzenia wyznaczono więcej niż jeden właściwy organ, na koordynatora ds. usług cyfrowych w tym państwie członkowskim należy wyznaczyć tylko jeden taki organ. Koordynator ds. usług cyfrowych powinien działać jako pojedynczy punkt kontaktowy w odniesieniu do wszystkich spraw związanych ze stosowaniem niniejszego rozporządzenia dla Komisji, Rady Usług Cyfrowych, koordynatorów ds. usług cyfrowych z innych państw członkowskich, jak również dla innych właściwych organów danego państwa członkowskiego. W szczególności, w przypadku gdy w danym państwie członkowskim zadania wynikające z niniejszego rozporządzenia powierzono kilku właściwym organom, koordynator ds. usług cyfrowych powinien pełnić funkcje koordynacyjne i współpracować z tymi organami zgodnie z prawem krajowym określającym ich odpowiednie zadania, bez uszczerbku dla niezależnej oceny przeprowadzonej przez pozostałe właściwe organy. Choć koordynator ds. usług cyfrowych nie stoi wyżej w hierarchii niż inne właściwe organy w ramach wykonywania ich zadań, powinien on zapewnić skuteczne zaangażowanie wszystkich odpowiednich właściwych organów oraz powinien terminowo przedstawiać ich ocenę w kontekście współpracy w zakresie nadzorowania i egzekwowania na poziomie unijnym. Co więcej, oprócz przewidzianych w niniejszym rozporządzeniu szczególnych mechanizmów dotyczących współpracy na poziomie unijnym, państwa członkowskie powinny również zapewnić współpracę pomiędzy koordynatorem ds. usług cyfrowych a innymi właściwymi organami wyznaczonymi na poziomie krajowym, w stosownych przypadkach przy wykorzystaniu odpowiednich narzędzi, takich jak łączenie zasobów, wspólne grupy zadaniowe, wspólne czynności sprawdzające i mechanizmy wzajemnej współpracy.
- (111) Koordynator ds. usług cyfrowych, jak również inne właściwe organy wyznaczone na podstawie niniejszego rozporządzenia, odgrywają kluczową rolę w zapewnianiu skuteczności praw i obowiązków ustanowionych w niniejszym rozporządzeniu oraz realizacji jego celów. W związku z tym konieczne jest zapewnienie, aby organy te dysponowały niezbędnymi środkami, w tym zasobami finansowymi i kadrowymi, w celu nadzorowania wszystkich dostawców usług

pośrednich podlegających ich kompetencji, w interesie wszystkich obywateli Unii. Ze względu na różnorodność dostawców usług pośrednich i wykorzystywanie przez nich zaawansowanej technologii przy świadczeniu ich usług, bardzo istotne jest też, by koordynator ds. usług cyfrowych i odpowiednie właściwe organy dysponowali odpowiednią liczbą pracowników i ekspertów posiadających specjalistyczne umiejętności oraz zaawansowanymi środkami technicznymi, a także by niezależnie zarządzali zasobami finansowymi niezbędnymi do wykonywania ich zadań. Ponadto poziom zasobów powinien uwzględniać wielkość, złożoność i potencjalny wpływ społeczny dostawców usług pośrednich podlegających ich kompetencji, a także zasięg ich usług w całej Unii. Niniejsze rozporządzenie pozostaje bez uszczerbku dla możliwości ustanowienia przez państwa członkowskie mechanizmów finansowania opartych na opłatach nadzorczych pobieranych od dostawców usług pośrednich na mocy prawa krajowego zgodnego z prawem Unii, w zakresie, w jakim opłaty te są pobierane od dostawców usług pośrednich mających główne miejsce prowadzenia działalności w danym państwie członkowskim, w jakim są one absolutnie ograniczone do tego, co jest konieczne i proporcjonalne do pokrycia kosztów realizacji zadań powierzonych właściwym organom na mocy niniejszego rozporządzenia, z wyłączeniem zadań powierzonych Komisji, oraz w jakim zapewniona jest odpowiednia przejrzystość w zakresie nakładania i wykorzystywania takich opłat nadzorczych.

- (112) Właściwe organy wyznaczone na podstawie niniejszego rozporządzenia powinny również działać w pełni niezależnie od podmiotów prywatnych i publicznych, bez obowiązku lub możliwości zwracania się, między innymi do rządu, o instrukcje lub ich otrzymywanie oraz bez uszczerbku dla szczególnych obowiązków w zakresie współpracy z innymi właściwymi organami, koordynatorami ds. usług cyfrowych, Radą Usług Cyfrowych i Komisją. Z drugiej strony niezależność tych organów nie powinna oznaczać, że nie mogą one podlegać, zgodnie z konstytucjami krajowymi i bez zagrażania realizacji celów określonych w niniejszym rozporządzeniu, proporcjonalnym mechanizmom w zakresie rozliczalności w odniesieniu do ogólnych działań koordynatorów ds. usług cyfrowych, takich jak ich wydatki finansowe lub składanie sprawozdań parlamentom narodowym. Wymóg niezależności nie powinien też uniemożliwiać wykonywania kontroli sądowej ani konsultowania się lub regularnej wymiany poglądów z innymi organami krajowymi, w tym w stosownych przypadkach organami ścigania, organami zarządzania kryzysowego lub organami ochrony konsumentów, w celu wzajemnego informowania się o trwających czynnościach sprawdzających, bez wywierania wpływu na wykonywanie ich odpowiednich uprawnień.
- (113) Państwa członkowskie mogą wyznaczyć istniejący organ krajowy do pełnienia funkcji koordynatora ds. usług cyfrowych lub wykonywania określonych zadań w celu nadzorowania stosowania i egzekwowania niniejszego rozporządzenia,

pod warunkiem że taki wyznaczony organ spełnia wymogi ustanowione w niniejszym rozporządzeniu, w tym w zakresie jego niezależności. Ponadto państwa członkowskie co do zasady mogą łączyć funkcje w ramach istniejącego organu, zgodnie z prawem Unii. Środki w tym zakresie mogą obejmować między innymi zakaz odwołania prezesa lub członka zarządu organu kolegialnego istniejącego organu przed upływem kadencji wyłącznie z powodu przeprowadzenia reformy instytucjonalnej polegającej na połączeniu różnych funkcji w ramach jednego organu, w przypadku braku przepisów gwarantujących, że takie odwołanie nie zagraża niezależności i bezstronności tych członków.

- (114) Państwa członkowskie powinny zapewnić koordynatorowi ds. usług cyfrowych oraz każdemu innemu właściwemu organowi wyznaczonemu na podstawie niniejszego rozporządzenia uprawnienia i środki wystarczające do zapewnienia skutecznych czynności sprawdzających i skutecznego egzekwowania, stosownie do zadań powierzonych tym organom. Obejmuje to uprawnienie właściwych organów do przyjmowania środków tymczasowych zgodnie z prawem krajowym w przypadku ryzyka wystąpienia poważnej szkody. Takie środki tymczasowe, które mogą obejmować nakaz zaprzestania danego zarzucanego naruszenia lub jego usunięcia, nie powinny wykraczać poza to, co jest niezbędne do zapewnienia, by zapobiec wystąpieniu poważnej szkody do czasu podjęcia ostatecznej decyzji. Koordynatorzy ds. usług cyfrowych powinni w szczególności mieć możliwość wyszukiwania i uzyskiwania informacji, które znajdują się na ich terytorium, w tym w kontekście wspólnych czynności sprawdzających, z należytym uwzględnieniem faktu, że środki nadzoru i egzekwowania dotyczące dostawcy podlegającego jurysdykcji innego państwa członkowskiego lub Komisji powinny zostać przyjęte przez koordynatora ds. usług cyfrowych tego innego państwa członkowskiego, w stosownych przypadkach zgodnie z procedurami dotyczącymi współpracy transgranicznej lub, w stosownych przypadkach, przez Komisję.
- (115) Państwa członkowskie powinny określić w prawie krajowym, zgodnie z prawem Unii, a w szczególności z niniejszym rozporządzeniem i Kartą, szczegółowe warunki i ograniczenia wykonywania przez swoich koordynatorów ds. usług cyfrowych oraz, w stosownych przypadkach, inne właściwe organy, na podstawie niniejszego rozporządzenia, uprawnień w zakresie czynności sprawdzających i uprawnień w zakresie egzekwowania.
- (116) Przy wykonywaniu tych uprawnień właściwe organy powinny przestrzegać mających zastosowanie przepisów krajowych dotyczących procedur i spraw, takich jak konieczność uzyskania uprzedniej zgody organu sądowego na wejście do niektórych pomieszczeń oraz prawnicza tajemnica zawodowa. Przepisy te powinny w szczególności zapewniać poszanowanie praw podstawowych do skutecznego środka prawnego i dostępu do bezstronnego sądu, w tym prawa do obrony, a także prawa do poszanowania życia prywatnego. W związku z tym gwarancje przewidziane w odniesieniu do postępowań Komisji na podstawie

niniejszego rozporządzenia mogłyby służyć jako właściwy punkt odniesienia. Przed wydaniem jakiegokolwiek ostatecznej decyzji należy zagwarantować przeprowadzenie uprzedniego, sprawiedliwego i bezstronnego postępowania, w tym prawo do bycia wysłuchanym przysługujące zainteresowanym osobom oraz prawo dostępu do akt, przy jednoczesnym poszanowaniu poufności oraz tajemnicy zawodowej i handlowej, jak również obowiązku podania rzeczywistych powodów podjęcia decyzji. Przeprowadzenie takiego postępowania nie powinno jednak wykluczać przyjęcia środków w należycie uzasadnionych, pilnych przypadkach oraz z zastrzeżeniem odpowiednich warunków i ustaleń proceduralnych. Wykonywanie uprawnień powinno być również proporcjonalne między innymi do charakteru i ogólnej faktycznej lub potencjalnej szkody spowodowanej naruszeniem lub podejrzeniem naruszenia. Właściwe organy powinny uwzględniać wszystkie istotne fakty i okoliczności sprawy, w tym informacje zebrane przez właściwe organy w innych państwach członkowskich.

- (117) Państwa członkowskie powinny zapewnić możliwość karania za naruszenia obowiązków ustanowionych w niniejszym rozporządzeniu w sposób skuteczny, proporcjonalny i odstrasżający, uwzględniając charakter, ciężar, powtarzalność i czas trwania naruszenia oraz mając na uwadze interes publiczny, zakres i rodzaj prowadzonej działalności, jak również możliwości ekonomiczne podmiotu dopuszczającego się naruszenia. W szczególności w przypadku nakładania sankcji należy uwzględnić, czy dany dostawca usług pośrednich systematycznie lub w sposób powtarzający się nie wypełnia swoich obowiązków wynikających z niniejszego rozporządzenia, a także, w stosownych przypadkach, liczbę poszkodowanych odbiorców usług, umyślny lub nieumyślny charakter naruszenia oraz prowadzenie przez dostawcę działalności w kilku państwach członkowskich. W przypadku gdy niniejsze rozporządzenie przewiduje maksymalną wysokość grzywnien lub okresowej kary pieniężnej, ta maksymalna wysokość powinna mieć zastosowanie w odniesieniu do poszczególnych naruszeń niniejszego rozporządzenia i pozostawać bez uszczerbku dla dostosowań grzywnien lub okresowych kar pieniężnych w odniesieniu do poszczególnych naruszeń. Państwa członkowskie powinny zapewnić, by grzywny lub okresowe kary pieniężne nakładane za naruszenia były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstrasżające, poprzez ustanowienie krajowych przepisów i procedur zgodnie z niniejszym rozporządzeniem, z uwzględnieniem wszystkich kryteriów dotyczących ogólnych warunków nakładania grzywnien lub okresowych kar pieniężnych.
- (118) Aby zapewnić skuteczne egzekwowanie obowiązków ustanowionych w niniejszym rozporządzeniu, osoby lub organizacje przedstawicielskie powinny mieć możliwość wnoszenia dowolnych skarg dotyczących wypełniania tych obowiązków do koordynatora ds. usług cyfrowych na terytorium, na którym otrzymały usługę, bez uszczerbku dla przepisów niniejszego rozporządzenia dotyczących podziału kompetencji, ani mających zastosowanie przepisów dotyczących

rozpatrywania skarg zgodnie z krajowymi zasadami dobrej administracji. Skargi mogą zawierać rzetelny przegląd obaw związanych z wypełnianiem obowiązków przez danego dostawcę usług pośrednich; mogą także dostarczyć koordynatorowi ds. usług cyfrowych informacji o bardziej przekrojowych kwestiach. Jeżeli dana sprawa wymaga współpracy transgranicznej, koordynator ds. usług cyfrowych powinien zaangażować inne właściwe organy krajowe, jak również koordynatora ds. usług cyfrowych innego państwa członkowskiego, w szczególności państwa członkowskiego, w którym dany dostawca usług pośrednich ma siedzibę.

- (119) Państwa członkowskie powinny zadbać, aby koordynatorzy ds. usług cyfrowych mogli wprowadzać środki, które są skuteczne w zwalczaniu niektórych szczególnie poważnych i uporczywych naruszeń niniejszego rozporządzenia oraz proporcjonalne do takich naruszeń. W szczególności w przypadku gdy środki te mogą mieć wpływ na prawa i interesy osób trzecich, co może mieć miejsce w szczególności w przypadku ograniczenia dostępu do interfejsów internetowych, należy nałożyć wymóg, aby środki te podlegały dodatkowym zabezpieczeniom. Potencjalnie poszkodowanym osobom trzecim należy zapewnić w szczególności możliwość wysłuchania, a takie nakazy należy wydawać jedynie wówczas, gdy można zasadnie uznać, że w innych aktach prawa Unii lub prawa krajowego nie przewidziano uprawnień do wprowadzania takich środków, na przykład w celu ochrony zbiorowych interesów konsumentów, zapewnienia szybkiego usunięcia stron internetowych zawierających lub rozpowszechniających pornografię dziecięcą lub uniemożliwienia dostępu do usług, które osoba trzecia wykorzystuje, aby naruszać prawo własności intelektualnej.
- (120) Taki nakaz ograniczenia dostępu nie powinien wykraczać poza to, co jest konieczne do osiągnięcia jego celu. Z tego względu powinien on mieć charakter tymczasowy i co do zasady dotyczyć dostawcy usług pośrednich, takiego jak odpowiedni dostawca usług hostingu, dostawca usług internetowych lub rejestr lub rejestrator domen, który jest w stanie w uzasadniony sposób osiągnąć ten cel bez nadmiernego ograniczania dostępu do zgodnych z prawem informacji.
- (121) Bez uszczerbku dla ustanowionych w niniejszym rozporządzeniu przepisów dotyczących wyłączenia z odpowiedzialności w odniesieniu do informacji przekazywanych lub przechowywanych na żądanie odbiorcy usługi, dostawca usług pośrednich powinien ponosić odpowiedzialność za szkody poniesione przez odbiorców usługi spowodowane naruszeniem obowiązków określonych w niniejszym rozporządzeniu przez tego dostawcę. Takie odszkodowanie powinno być zgodne z przepisami i procedurami określonymi w obowiązującym prawie krajowym i powinno pozostawać bez uszczerbku dla innych możliwości odwołania się dostępnych na mocy przepisów o ochronie konsumentów.
- (122) Koordynator ds. usług cyfrowych powinien regularnie publikować, na przykład na swojej stronie internetowej, sprawozdanie z działań przeprowadzonych na podstawie niniejszego rozporządzenia. W szczególności sprawozdanie to

powinno być publikowane w formacie nadającym się do odczytu maszynowego i obejmować przegląd otrzymanych skarg i podjętych działań następczych, czyli między innymi ogólną liczbę otrzymanych skarg i liczbę skarg, które doprowadziły do podjęcia formalnych czynności sprawdzających lub do przekazania sprawy do innych koordynatorów ds. usług cyfrowych, bez zamieszczania jakichkolwiek danych osobowych. Biorąc pod uwagę, że koordynator ds. usług cyfrowych również otrzymuje, za pośrednictwem systemu wymiany informacji, informacje o nakazach podjęcia działań przeciwko nielegalnym treściom lub udzielenia informacji regulowanych niniejszym rozporządzeniem, powinien umieszczać w swoim sprawozdaniu rocznym liczbę i kategorie takich nakazów skierowanych do dostawców usług pośrednich, wydanych przez organy sądowe i administracyjne w jego państwie członkowskim.

- (123) W celu zapewnienia jasności, prostoty i skuteczności, uprawnienia w zakresie nadzorowania i egzekwowania obowiązków wynikających z niniejszego rozporządzenia powinny zostać powierzone właściwym organom w państwie członkowskim, w którym znajduje się główne miejsce prowadzenia działalności dostawcy usług pośrednich, to znaczy, w którym ma on swoją siedzibę główną lub statutową, w ramach której wykonywane są główne funkcje finansowe i sprawowany jest nadzór operacyjny. W przypadku dostawców, którzy nie mają siedziby w Unii, ale oferują usługi w Unii i w związku z tym są objęci zakresem stosowania niniejszego rozporządzenia, kompetencję powinno posiadać państwo członkowskie, w którym dostawcy ci wyznaczili swojego przedstawiciela prawnego, biorąc pod uwagę funkcję przedstawicieli prawnych w rozumieniu niniejszego rozporządzenia. W interesie skutecznego stosowania niniejszego rozporządzenia wszystkie państwa członkowskie lub Komisja, w stosownych przypadkach, powinny jednak posiadać kompetencję w odniesieniu do dostawców, którzy nie wyznaczili przedstawiciela prawnego. Kompetencja ta może być wykonywana przez dowolny właściwy organ lub Komisję, pod warunkiem że dostawca nie jest objęty postępowaniem dotyczącym egzekwowania w odniesieniu do tych samych faktów prowadzonym przez inny właściwy organ lub Komisję. Aby zapewnić przestrzeganie zasady *ne bis in idem*, a w szczególności uniknąć sytuacji, w której to samo naruszenie obowiązków ustanowionych w niniejszym rozporządzeniu jest karane więcej niż jeden raz, każde państwo członkowskie, które zamierza wykonywać swoje kompetencje w odniesieniu do takich dostawców, powinno bez zbędnej zwłoki poinformować o tym wszystkie inne organy, w tym Komisję, za pośrednictwem systemu wymiany informacji ustanowionego do celów niniejszego rozporządzenia.
- (124) Ze względu na ich potencjalny wpływ i wyzwania związane ze skutecznym nadzorem nad nimi, potrzebne są szczególne przepisy dotyczące nadzoru i egzekwowania w odniesieniu do dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych. Komisja powinna być odpowiedzialna, w stosownych przypadkach przy wsparciu właściwych organów

krajowych, za nadzór nad kwestiami systemowymi, takimi jak kwestie mające duży wpływ na zbiorowe interesy odbiorców usługi, oraz za ich publiczne egzekwowanie. W związku z tym Komisja powinna posiadać wyłączne uprawnienia w zakresie nadzoru i egzekwowania dodatkowych obowiązków w zakresie zarządzania ryzykiem systemowym nałożonych na dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych w niniejszym rozporządzeniu. Wyłączne uprawnienia Komisji powinny pozostawać bez uszczerbku dla niektórych zadań administracyjnych powierzonych w niniejszym rozporządzeniu właściwym organom państwa członkowskiego siedziby, takich jak weryfikacja badaczy.

(125) Komisja i właściwe organy krajowe powinny wspólnie wykonywać uprawnienia w zakresie nadzoru i egzekwowania obowiązków w zakresie należytej staranności, innych niż dodatkowe obowiązki w zakresie zarządzania ryzykiem systemowym nałożone w niniejszym rozporządzeniu na dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych. Z jednej strony, Komisja mogłaby być w wielu przypadkach lepiej przygotowana do zajmowania się systemowymi naruszeniami popełnianymi przez tych dostawców, takimi jak naruszenia mające wpływ na wiele państw członkowskich, poważne powtarzające się naruszenia lub dotyczące nieustanowienia skutecznych mechanizmów wymaganych na mocy niniejszego rozporządzenia. Z drugiej strony, właściwe organy w państwie członkowskim, w którym znajduje się główne miejsce prowadzenia działalności dostawcy bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej, mogłyby być lepiej przygotowane do zajęcia się indywidualnymi naruszeniami popełnianymi przez tych dostawców, które nie powodują żadnych problemów systemowych lub transgranicznych. W celu zapewnienia skuteczności, uniknięcia powielania działań i zagwarantowania przestrzegania zasady *ne bis in idem*, to Komisja powinna oceniać, czy w danym przypadku uważa za stosowne wykonywanie tych kompetencji dzielonych, a po wszczęciu postępowania państwa członkowskie nie powinny mieć już takiej możliwości. Państwa członkowskie powinny ściśle współpracować zarówno ze sobą, jak i z Komisją, a Komisja powinna ściśle współpracować z państwami członkowskimi, aby zapewnić sprawne i skuteczne funkcjonowanie systemu nadzoru i egzekwowania ustanowionego niniejszym rozporządzeniem.

(126) Przepisy niniejszego rozporządzenia dotyczące podziału kompetencji powinny pozostawać bez uszczerbku dla przepisów prawa Unii i krajowych przepisów prawa prywatnego międzynarodowego dotyczących jurysdykcji i prawa właściwego w sprawach cywilnych i handlowych, takich jak postępowania wszczynane przez konsumentów przed sądami państwa członkowskiego swego miejsca zamieszkania, zgodnie z odpowiednimi przepisami prawa Unii. W odniesieniu do obowiązków nałożonych niniejszym rozporządzeniem na dostawców usług pośrednich w zakresie informowania organu wydającego o działaniach podjętych

w odpowiedzi na nakazy podjęcia działań przeciwko nielegalnym treściom i nakazy udzielenia informacji, przepisy dotyczące podziału kompetencji powinny mieć zastosowanie wyłącznie do nadzoru nad egzekwowaniem tych obowiązków, a nie do innych spraw związanych z nakazem, takich jak kompetencje do wydania nakazu.

- (127) Ze względu na transgraniczne i międzysektorowe znaczenie usług pośrednich, konieczny jest wysoki poziom współpracy, by zapewnić spójne stosowanie niniejszego rozporządzenia oraz dostępność odpowiednich informacji poprzez system wymiany informacji w celu wykonywania zadań w zakresie egzekwowania. Współpraca może przybierać różne formy w zależności od poruszanych kwestii, bez uszczerbku dla konkretnych wspólnych czynności sprawdzających. W każdym razie konieczne jest, by koordynator ds. usług cyfrowych właściwy dla miejsca siedziby dostawcy usług pośrednich poinformował innych koordynatorów ds. usług cyfrowych o kwestiach oraz czynnościach sprawdzających dotyczących danego dostawcy oraz o działaniach, jakie mają zostać wobec niego podjęte. Co więcej, gdy właściwy organ w jednym z państw członkowskich posiada informacje istotne do celów czynności sprawdzających prowadzonych przez właściwe organy państwa członkowskiego miejsca siedziby, lub gdy jest on w stanie zgromadzić takie informacje znajdujące się na jego terytorium, do których właściwe organy w państwie członkowskim miejsca siedziby nie mają dostępu, koordynator ds. usług cyfrowych właściwy dla miejsca przeznaczenia powinien terminowo udzielić wsparcia koordynatorowi ds. usług cyfrowych właściwemu dla miejsca siedziby, między innymi poprzez wykonywanie swoich uprawnień w zakresie czynności sprawdzających zgodnie z mającymi zastosowanie procedurami krajowymi i Kartą. Osoba, do której skierowane są takie środki podejmowane w ramach czynności sprawdzających, powinna się do nich zastosować i ponieść odpowiedzialność w przypadku niezastosowania się do nich, a właściwe organy w państwie członkowskim miejsca siedziby powinny móc korzystać z informacji zgromadzonych w drodze wzajemnej pomocy, aby zapewnić zgodność z niniejszym rozporządzeniem.
- (128) Koordynator ds. usług cyfrowych właściwy dla miejsca przeznaczenia, w szczególności, w stosownych przypadkach, na podstawie otrzymanych skarg lub informacji przekazanych przez inne właściwe organy krajowe lub Radę Usług Cyfrowych w przypadku kwestii obejmujących co najmniej trzy państwa członkowskie, powinien mieć możliwość zwrócenia się do koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby o podjęcie działań w zakresie czynności sprawdzających lub egzekwowania w odniesieniu do dostawcy podlegającego jego kompetencji. Takie wnioski o podjęcie działania powinny opierać się na dobrze uzasadnionych dowodach wskazujących na istnienie zarzucanego naruszenia mającego negatywny wpływ na zbiorowe interesy odbiorców usługi w jego państwie członkowskim lub mające negatywne skutki społeczne. Koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien

mieć możliwość skorzystania z wzajemnej pomocy lub zaproszenia koordynatora ds. usług cyfrowych występującego z wnioskiem do wspólnych czynności sprawdzających, jeżeli do podjęcia decyzji potrzebne są dalsze informacje, bez uszczerbku dla możliwości zwrócenia się do Komisji o ocenę sprawy, jeżeli ma ona powody, aby podejrzewać, że w grę może wchodzić naruszenie systemowe przez bardzo dużą platformę internetową lub bardzo dużą wyszukiwarkę internetową.

- (129) Rada Usług Cyfrowych powinna mieć możliwość skierowania sprawy do Komisji w razie braku zgody co do ocen lub zastosowanych lub proponowanych środków lub w razie nieprzyjęcia żadnych środków zgodnie z niniejszym rozporządzeniem w następstwie wniosku o współpracę transgraniczną lub wspólne czynności sprawdzające. W przypadku gdy na podstawie informacji udostępnionych przez zainteresowane organy Komisja uzna, że proponowane środki, w tym proponowana wysokość grzywien, nie mogą zapewnić skutecznego wyegzekwowania obowiązków ustanowionych w niniejszym rozporządzeniu, powinna odpowiednio mieć możliwość wyrażenia swoich poważnych wątpliwości i zwrócenia się do właściwego koordynatora ds. usług cyfrowych z wnioskiem o ponowną ocenę sprawy i wprowadzenie niezbędnych środków w celu zapewnienia przestrzegania niniejszego rozporządzenia w terminie określonym. Możliwość ta pozostaje bez uszczerbku dla ogólnego obowiązku Komisji dotyczącego nadzoru stosowania – i w stosownych przypadkach egzekwowania – prawa Unii pod kontrolą Trybunału Sprawiedliwości Unii Europejskiej zgodnie z Traktatami.
- (130) Aby ułatwić transgraniczny nadzór i czynności sprawdzające dotyczące obowiązków ustanowionych w niniejszym rozporządzeniu obejmujące kilka państw członkowskich, koordynator ds. usług cyfrowych właściwy dla miejsca siedziby powinien móc – poprzez system wymiany informacji – zaprosić innych koordynatorów ds. usług cyfrowych do uczestnictwa we wspólnych czynności sprawdzających dotyczących zarzucanego naruszenia niniejszego rozporządzenia. Inni koordynatorzy ds. usług cyfrowych oraz, w stosownych przypadkach, inne właściwe organy powinni mieć możliwość przyłączenia się do czynności sprawdzających zaproponowanych przez koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby, chyba że koordynator ten uzna, że zbyt duża liczba uczestniczących organów może mieć wpływ na skuteczność czynności sprawdzających, biorąc pod uwagę cechy zarzucanego naruszenia oraz brak bezpośredniego wpływu na odbiorców usługi w tych państwach członkowskich. Wspólne czynności sprawdzające mogą obejmować różne działania, które powinny być koordynowane przez koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby, zgodnie z możliwościami uczestniczących organów, takie jak skoordynowane gromadzenie danych, łączenie zasobów, grupy zadaniowe, skoordynowane wnioski o udzielenie informacji lub wspólne kontrole pomieszczeń. Wszystkie właściwe organy uczestniczące we wspólnych czynności

sprawdzających powinny współpracować z koordynatorem ds. usług cyfrowych właściwym dla miejsca siedziby, w tym poprzez wykonywanie swoich uprawnień w zakresie czynności sprawdzających w obrębie swoich terytoriów, zgodnie z mającymi zastosowanie procedurami krajowymi. Wspólne czynności sprawdzające powinny zostać zakończone w określonych ramach czasowych i doprowadzić do opracowania sprawozdania końcowego uwzględniającego wkłady wszystkich uczestniczących właściwych organów. Również Rada Usług Cyfrowych, na wniosek co najmniej trzech koordynatorów ds. usług cyfrowych właściwych dla miejsca przeznaczenia, może zalecić koordynatorowi ds. usług cyfrowych właściwemu dla miejsca siedziby podjęcie takich wspólnych czynności sprawdzających i udzielenie wskazówek co do ich organizacji. Aby uniknąć impasu, Rada Usług Cyfrowych powinna mieć możliwość w określonych przypadkach skierowania sprawy do Komisji, w tym w sytuacji, gdy koordynator ds. usług cyfrowych właściwy dla miejsca siedziby odmawia podjęcia czynności sprawdzających, a Rada Usług Cyfrowych nie zgadza się z podanym uzasadnieniem.

- (131) Aby zapewnić spójne stosowanie niniejszego rozporządzenia, należy ustanowić niezależną grupę doradcą na poziomie unijnym, Europejską Radę ds. Usług Cyfrowych, która powinna wspierać Komisję i pomagać w koordynowaniu działań koordynatorów ds. usług cyfrowych. Rada Usług Cyfrowych powinna składać się z koordynatorów ds. usług cyfrowych, jeżeli zostali oni wyznaczeni, bez uszczerbku dla możliwości zapraszania przez koordynatorów ds. usług cyfrowych na jej posiedzenia lub wyznaczania przez nich delegatów ad hoc z innych właściwych organów, którym powierzono określone zadania na podstawie niniejszego rozporządzenia, jeżeli jest to wymagane zgodnie z ich krajowym podziałem zadań i kompetencji. W przypadku kilku uczestników z jednego państwa członkowskiego prawo do głosowania powinno ograniczać się do jednego przedstawiciela na państwo członkowskie.
- (132) Rada Usług Cyfrowych powinna współuczestniczyć w osiągnięciu wspólnej unijnej perspektywy w zakresie spójnego stosowania niniejszego rozporządzenia oraz we współpracy między właściwymi organami, między innymi udzielając Komisji i koordynatorom ds. usług cyfrowych porad dotyczących odpowiednich środków w ramach czynności sprawdzających i środków w ramach egzekwowania, w szczególności w odniesieniu do dostawców bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych, oraz uwzględniając w szczególności swobodę świadczenia usług w całej Unii przez dostawców usług pośrednich. Rada Usług Cyfrowych powinna także współuczestniczyć w opracowywaniu odpowiednich wzorów i kodeksów postępowania oraz w analizie pojawiających się ogólnych tendencji w rozwoju usług cyfrowych w Unii, między innymi wydając opinie lub zalecenia w sprawach związanych z normami.
- (133) W tym celu Rada Usług Cyfrowych powinna mieć możliwość przyjmowania opinii, wniosków i zaleceń kierowanych do koordynatorów ds. usług cyfrowych lub innych właściwych organów krajowych. Choć te opinie, wnioski i zalecenia

nie są prawnie wiążące, to decyzja o niezastosowaniu się do nich powinna być odpowiednio uzasadniona i może zostać uwzględniona przez Komisję przy ocenie przestrzegania przez dane państwo członkowskie niniejszego rozporządzenia.

- (134) W Radzie Usług Cyfrowych powinni zasiadać przedstawiciele koordynatorów ds. usług cyfrowych oraz ewentualnych innych właściwych organów pod przewodnictwem Komisji w celu zapewnienia w pełni europejskiego wymiaru oceny spraw przedłożonych Radzie Usług Cyfrowych. Biorąc pod uwagę możliwe elementy przekrojowe, które mogą być istotne dla innych ram regulacyjnych na poziomie unijnym, Rada Usług Cyfrowych – w zakresie niezbędnym do wykonywania swoich zadań – powinna mieć możliwość współpracy z innymi organami, jednostkami organizacyjnymi i grupami doradczymi Unii, których obowiązki dotyczą takich dziedzin, jak równość, w tym równouprawnienie płci, oraz niedyskryminacja, ochrona danych, łączność elektroniczna, usługi audiowizualne, wykrywanie nadużyć finansowych na szkodę budżetowi Unii w odniesieniu do należności celnych oraz prowadzenie dochodzeń w ich sprawie, ochrona konsumentów lub prawo konkurencji.
- (135) Komisja, poprzez funkcję przewodniczącego, powinna być członkiem Rady Usług Cyfrowych bez praw do głosowania. Poprzez funkcję przewodniczącego Komisja powinna zapewniać, aby porządek obrad ustalano zgodnie z wnioskami członków Rady Usług Cyfrowych, jak określono w regulaminie wewnętrznym oraz zgodnie z obowiązkami Rady Usług Cyfrowych określonymi w niniejszym rozporządzeniu.
- (136) Biorąc pod uwagę potrzebę zapewnienia wsparcia dla działań Rady Usług Cyfrowych, Rada Usług Cyfrowych powinna mieć możliwość korzystania z wiedzy eksperckiej i zasobów ludzkich Komisji oraz właściwych organów krajowych. Szczególne ustalenia operacyjne dotyczące wewnętrznego funkcjonowania Rady Usług Cyfrowych należy uszczegółowić w jej regulaminie wewnętrznym.
- (137) Z uwagi na znaczenie bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych oraz ich zasięg i wpływ, niewypełnianie przez nie spoczywających na nich obowiązków może wpływać na dużą liczbę odbiorców usług w różnych państwach członkowskich oraz może powodować ogromne szkody społeczne, przy czym zidentyfikowanie niewypełniania takich obowiązków oraz zaradzenie temu problemowi może także być wyjątkowo trudne. Z tego względu Komisja, we współpracy z koordynatorami ds. usług cyfrowych i Radą Usług Cyfrowych, powinna rozwijać wiedzę ekspercką i zdolności Unii w odniesieniu do nadzoru nad bardzo dużymi platformami internetowymi i bardzo dużymi wyszukiwarkami internetowymi. Z tego też względu Komisja powinna mieć możliwość koordynowania działań i korzystania z wiedzy eksperckiej i zasobów takich organów, na przykład poprzez stałe lub tymczasowe analizowanie konkretnych tendencji lub problemów pojawiających się w odniesieniu do co najmniej jednej bardzo dużej platformy internetowej

lub bardzo dużej wyszukiwarki internetowej. Państwa członkowskie powinny współpracować z Komisją przy rozwijaniu takich zdolności, w tym, w stosownych przypadkach, poprzez oddelegowanie personelu oraz przyczynianie się do tworzenia wspólnych unijnych zdolności nadzorczych. Aby rozwijać wiedzę fachową i zdolności Unii, Komisja może też wykorzystywać wiedzę ekspercką i zdolności Obserwatorium Gospodarki Platform Internetowych utworzonego na mocy decyzji Komisji z dnia 26 kwietnia 2018 r. ustanawiającej grupę ekspertów w ramach Obserwatorium Gospodarki Platform Internetowych, odpowiednich organów eksperckich, a także centrów doskonałości. Komisja może zaprosić ekspertów posiadających konkretną wiedzę ekspercką, w tym w szczególności zweryfikowanych badaczy, przedstawicieli agencji i organów Unii, przedstawicieli branży, stowarzyszenia reprezentujące użytkowników lub społeczeństwo obywatelskie, organizacje międzynarodowe, ekspertów z sektora prywatnego oraz inne zainteresowane podmioty.

- (138) Komisja powinna móc z własnej inicjatywy badać naruszenia, zgodnie z uprawnieniami przewidzianymi w niniejszym rozporządzeniu, między innymi poprzez zwracanie się o dostęp do danych, zwracanie się o informacje lub przeprowadzanie kontroli, a także poprzez korzystanie ze wsparcia koordynatorów ds. usług cyfrowych. W przypadku gdy nadzór sprawowany przez właściwe organy krajowe nad poszczególnymi zarzucanymi naruszeniami ze strony dostawców bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych wskazuje na kwestie systemowe, takie jak kwestie mające duży wpływ na zbiorowe interesy odbiorców usługi, koordynatorzy ds. usług cyfrowych powinni mieć możliwość – na podstawie należycie uzasadnionego wniosku – przekazania takich kwestii Komisji. Taki wniosek powinien zawierać co najmniej wszystkie niezbędne fakty i okoliczności uzasadniające zarzucane naruszenie i jego systemowy charakter. W zależności od wyniku własnej oceny Komisja powinna mieć możliwość podjęcia niezbędnych środków w ramach czynności sprawdzających i środków w ramach egzekwowania na podstawie niniejszego rozporządzenia, w tym w stosownych przypadkach podjęcia czynności sprawdzających lub przyjęcia środków tymczasowych.
- (139) Aby skutecznie wykonywać swoje zadania, Komisja powinna zachować pewien margines uznaniowości, jeżeli chodzi o decyzje o wszczęciu postępowania przeciwko dostawcom bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych. Po wszczęciu przez Komisję postępowania należy pozbawić zainteresowanych koordynatorów ds. usług cyfrowych właściwych dla miejsca siedziby możliwości wykonywania ich uprawnień w zakresie czynności sprawdzających i uprawnień w zakresie egzekwowania w odniesieniu do danych praktyk dostawcy bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej, aby uniknąć nakładania się działań, niespójności oraz ryzyka naruszenia zasady *ne bis in idem*. Komisja powinna jednak mieć możliwość zwrócenia się do koordynatorów ds. usług cyfrowych

o indywidualny lub wspólny wkład w dane czynności sprawdzające. Zgodnie z obowiązkiem lojalnej współpracy koordynator ds. usług cyfrowych powinien dołożyć wszelkich starań, by spełnić uzasadnione i proporcjonalne wnioski, z którymi zwróciła się Komisja w kontekście czynności sprawdzających. Ponadto koordynator ds. usług cyfrowych właściwy dla miejsca siedziby, a także Rada Usług Cyfrowych oraz, w stosownych przypadkach, inni koordynatorzy ds. usług cyfrowych, powinni przekazać Komisji wszelkie niezbędne informacje oraz udzielić jej wsparcia, aby umożliwić jej skuteczne wykonywanie zadań, w tym informacje zgromadzone w kontekście działań związanych z gromadzeniem danych lub dostępem do danych, w zakresie, w jakim nie uniemożliwia tego podstawa prawna, na podstawie której dane informacje zostały zgromadzone. Z kolei Komisja powinna na bieżąco informować koordynatora ds. usług cyfrowych właściwego dla miejsca siedziby i Radę Usług Cyfrowych o wykonywaniu swoich uprawnień, w szczególności w przypadku, gdy zamierza wszcząć postępowanie i skorzystać ze swoich uprawnień w zakresie czynności sprawdzających. Ponadto, jeżeli Komisja przedstawia danym dostawcom bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych swoje wstępne ustalenia, w tym wszelkie kwestie, odnośnie do których zgłasza zastrzeżenia, powinna je przedstawić również Radzie Usług Cyfrowych. Rada Usług Cyfrowych powinna przekazać swoje stanowisko odnośnie do przedstawionych przez Komisję zastrzeżeń i oceny; Komisja powinna uwzględnić to stanowisko w uzasadnieniu swojej ostatecznej decyzji.

- (140) Biorąc pod uwagę zarówno szczególne wyzwania, które mogą wynikać z dążenia do zapewnienia przestrzegania przepisów przez dostawców bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych, jak i znaczenie skuteczności takich działań, uwzględniając rozmiar oraz wpływ takich dostawców, a także szkody, jakie mogą oni spowodować, Komisja powinna dysponować szerokimi uprawnieniami w zakresie czynności sprawdzających i uprawnieniami w zakresie egzekwowania, aby móc prowadzić czynności sprawdzające oraz egzekwować i monitorować przestrzeganie przepisów ustanowionych w niniejszym rozporządzeniu z pełnym poszanowaniem dla podstawowego prawa do bycia wysłuchanym i prawa dostępu do akt sprawy w toku postępowania dotyczącego egzekwowania, zasady proporcjonalności oraz praw i interesów zainteresowanych stron.
- (141) Komisja powinna mieć możliwość zwrócenia się o informacje niezbędne do zapewnienia skutecznego wdrożenia i wypełniania w całej Unii obowiązków ustanowionych w niniejszym rozporządzeniu. Komisja powinna mieć w szczególności dostęp do istotnych dokumentów, danych i informacji niezbędnych do podjęcia i prowadzenia czynności sprawdzających oraz monitorowania wypełniania odpowiednich obowiązków ustanowionych w niniejszym rozporządzeniu, niezależnie od tego, w czym posiadaniu znajdują się przedmiotowe dokumenty, dane lub informacje, oraz niezależnie od tego, w jakiej są formie lub

w jakim formacie, na jakim nośniku są przechowywane lub w jakim dokładnie miejscu. Komisja powinna mieć możliwość zażądania bezpośrednio – w drodze należycie uzasadnionego wniosku o udzielenie informacji – od odpowiedniego dostawcy bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej, a także od wszelkich innych osób fizycznych lub prawnych działających w celach związanych z ich działalnością handlową, gospodarczą, rzemieślniczą lub zawodową, w przypadku których można zasadnie oczekiwać, że dysponują informacjami związanymi z podejrzeniem naruszenia lub naruszeniem, stosownie do przypadku, przekazania wszelkich istotnych dowodów, danych i informacji. Ponadto na potrzeby niniejszego rozporządzenia Komisja powinna mieć możliwość zwrócenia się o wszelkie istotne informacje do dowolnego organu publicznego, podmiotu lub agencji w państwie członkowskim. Komisja powinna mieć możliwość zażądania dostępu – w ramach wykonywania uprawnień w zakresie czynności sprawdzających, takich jak wnioski o udzielenie informacji lub odbieranie wyjaśnień – do dokumentów, danych, informacji, baz danych i algorytmów odpowiednich osób oraz wyjaśnień z nimi związanych, a także do odbierania – za ich zgodą – wyjaśnień od osób fizycznych lub prawnych, które mogą być w posiadaniu użytecznych informacji, oraz do rejestrowania ich oświadczeń za pomocą wszelkich środków technicznych. Komisji powinna być także uprawniona do przeprowadzania kontroli niezbędnych do egzekwowania odpowiednich przepisów niniejszego rozporządzenia. Celem tych uprawnień w zakresie czynności sprawdzających jest uzupełnienie możliwości zwrócenia się przez Komisję o wsparcie do koordynatorów ds. usług cyfrowych i organów innych państw członkowskich, na przykład poprzez przekazanie informacji lub wsparcie w wykonywaniu tych uprawnień.

- (142) Środki tymczasowe mogą być ważnym narzędziem zapewniającym, aby w czasie trwania czynności sprawdzających, naruszenie będące jego przedmiotem nie prowadziło do ryzyka wyrządzenia poważnej szkody odbiorcom usługi. Narzędzie to jest ważne dla uniknięcia zmian, które byłoby bardzo trudno odwrócić za pomocą decyzji Komisji przyjmowanej na zakończenie postępowania. Komisja powinna zatem mieć uprawnienia do nakładania – w drodze decyzji – środków tymczasowych w kontekście postępowania wszczętego z myślą o ewentualnym przyjęciu decyzji stwierdzającej nieprzestrzeganie przepisów. Uprawnienia te powinny mieć zastosowanie w przypadkach, w których Komisja stwierdziła *prima facie* naruszenie obowiązków wynikających z niniejszego rozporządzenia przez dostawcę bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej. Decyzja nakładająca środki tymczasowe powinna mieć zastosowanie jedynie przez czas oznaczony, który upływa wraz z zakończeniem postępowania przez Komisję, albo w ustalonym okresie, który może zostać przedłużony, jeżeli to konieczne i stosowne.
- (143) Komisja powinna być uprawniona do podejmowania działań koniecznych do monitorowania skutecznego wdrażania i wypełniania obowiązków

ustanowionych w niniejszym rozporządzeniu. Takie działania powinny obejmować możliwość powoływania niezależnych ekspertów zewnętrznych oraz audytorów udzielających wsparcia Komisji w tym procesie – w stosownych przypadkach wspomniani eksperci i audytorzy mogą pochodzić z właściwych organów państw członkowskich, takich jak organy ochrony danych lub konsumentów. Powołując audytorów, Komisja powinna zapewnić wystarczającą rotację.

- (144) Wypełnianie odpowiednich obowiązków nałożonych niniejszym rozporządzeniem powinno być egzekwowane za pomocą grzywien i okresowych kar pieniężnych. W tym celu należy określić także odpowiednie poziomy grzywny i okresowych kar pieniężnych za niewypełnianie obowiązków i naruszanie przepisów proceduralnych, z zastrzeżeniem odpowiednich terminów przedawnienia, zgodnie z zasadami proporcjonalności oraz zasadą *ne bis in idem*. Aby zapewnić poszanowanie tych zasad, Komisja i odpowiednie organy krajowe powinny koordynować swoje wysiłki w zakresie egzekwowania. W szczególności Komisja powinna uwzględniać wszelkie grzywny i sankcje nałożone na tę samą osobę prawną w odniesieniu do tych samych faktów w drodze ostatecznej decyzji w postępowaniu dotyczącym naruszenia innych przepisów unijnych lub krajowych, tak by zapewnić, aby łącznie nałożone grzywny i sankcje były proporcjonalne i odpowiadały wadze popełnionych naruszeń. Wszystkie decyzje podejmowane przez Komisję na mocy niniejszego rozporządzenia podlegają kontroli Trybunału Sprawiedliwości Unii Europejskiej zgodnie z TFUE. Trybunał Sprawiedliwości Unii Europejskiej powinien mieć nieograniczone prawo orzekania w odniesieniu do grzywien i kar pieniężnych zgodnie z art. 261 TFUE.
- (145) Ze względu na potencjalne znaczące skutki społeczne naruszenia dodatkowych obowiązków zarządzania ryzykiem systemowym mających zastosowanie wyłącznie do bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych oraz aby zaradzić takim obawom dotyczącym porządku publicznego, należy przewidzieć system wzmocnionego nadzoru nad wszelkimi działaniami podejmowanymi w celu skutecznego zaprzestania naruszeń niniejszego rozporządzenia i usuwania ich. Dlatego też po stwierdzeniu naruszenia jednego z przepisów niniejszego rozporządzenia, które mają zastosowanie wyłącznie do bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych, i w razie potrzeby ukaraniu za nie, Komisja powinna zwrócić się do dostawcy takiej platformy lub takiej wyszukiwarki o opracowanie szczegółowego planu działania mającego na celu usunięcie w przyszłości wszelkich skutków naruszenia oraz o przekazanie takiego planu działania koordynatorom ds. usług cyfrowych, Komisji i Radzie Usług Cyfrowych w terminie określonym przez Komisję. Komisja, z uwzględnieniem opinii Rady Usług Cyfrowych, powinna ustalić, czy środki zawarte w tym planie działania są wystarczające do zaradzenia naruszeniu, zwracając przy tym również uwagę na

to, czy proponowane środki obejmują przestrzeganie odpowiedniego kodeksu postępowania. Komisja powinna również monitorować wszelkie dalsze środki podejmowane przez danego dostawcę bardzo dużej platformy internetowej lub bardzo dużej wyszukiwarki internetowej zgodnie z jego planem działania i uwzględniać przy tym także wyniki niezależnego audytu tego dostawcy. Jeżeli po wdrożeniu planu działania Komisja nadal będzie uważać, że dane naruszenie nie zostało w pełni usunięte w pełni lub gdy plan ten nie został przekazany lub został uznany za nieodpowiedni, powinna ona móc skorzystać z uprawnień w zakresie czynności sprawdzających lub uprawnień w zakresie egzekwowania na mocy niniejszego rozporządzenia, w tym z uprawnień do nakładania okresowych kar pieniężnych i wszczęcia procedury w celu uniemożliwienia dostępu do usługi, której dotyczy naruszenie.

- (146) Zainteresowani dostawcy bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych oraz inne osoby, w stosunku do których Komisja wykonuje swoje uprawnienia i których interesów może dotyczyć decyzja, powinni mieć możliwość uprzedniego przedstawienia uwag, zaś podjęte decyzje powinny zostać podane do szerokiej wiadomości publicznej. W celu zapewnienia zainteresowanym stronom prawa do obrony, w szczególności prawa dostępu do akt, istotne jest, aby informacje poufne podlegały ochronie. Ponadto, zachowując poufność informacji, Komisja powinna zapewnić, aby wszelkie informacje, na których opiera się jej decyzja, zostały ujawnione w zakresie, który umożliwia adresatowi decyzji zrozumienie stanu faktycznego i wnioskowania, które doprowadziły do jej podjęcia.
- (147) W celu zagwarantowania zharmonizowanego stosowania i egzekwowania niniejszego rozporządzenia ważne jest zapewnienie, aby organy krajowe, w tym sądy krajowe, posiadały wszystkie informacje niezbędne do zapewnienia, by ich decyzje nie były sprzeczne z decyzją przyjętą przez Komisję na podstawie niniejszego rozporządzenia. Pozostaje to bez uszczerbku dla art. 267 TFUE.
- (148) Skuteczne egzekwowanie i monitorowanie niniejszego rozporządzenia wymaga sprawnej wymiany informacji w czasie rzeczywistym pomiędzy koordynatorami ds. usług cyfrowych, Radą Usług Cyfrowych i Komisją, w ramach przepływów informacji i procedur określonych w niniejszym rozporządzeniu. W stosownych przypadkach może to również uzasadniać dostęp innych właściwych organów do tego systemu. Jednocześnie, ze względu na to, że wymieniane informacje mogą mieć charakter poufny lub zawierać dane osobowe, powinny być one w dalszym ciągu chronione przed nieuprawnionym dostępem, zgodnie z celami, do których zostały zgromadzone. Z tego powodu wszelka komunikacja między tymi organami powinna się odbywać w ramach wiarygodnego i bezpiecznego systemu wymiany informacji, którego szczegóły powinny zostać określone w akcie wykonawczym. Taki system wymiany informacji może się opierać na istniejących narzędziach rynku wewnętrznego w zakresie, w jakim mogą one realizować cele niniejszego rozporządzenia w sposób oszczędny.

- (149) Bez uszczerbku dla prawa odbiorców usług do zwrócenia się od przedstawiciela zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2020/1828³³ lub do wszelkich innych rodzajów przedstawicielstwa na mocy prawa krajowego, odbiorcy usług powinni również mieć prawo do upoważnienia osoby prawnej lub organu publicznego do wykonywania ich praw przewidzianych w niniejszym rozporządzeniu. Takie prawa mogą obejmować prawa związane z dokonywaniem zgłoszeń, zaskarżaniem decyzji podjętych przez dostawców usług pośrednich oraz wnoszeniem skarg przeciwko dostawcom w związku z naruszeniami niniejszego rozporządzenia. Niektóre organy, organizacje i stowarzyszenia posiadają szczególną wiedzę ekspercką i kompetencje w zakresie wykrywania i sygnalizowania błędnych lub nieuzasadnionych decyzji dotyczących moderowania treści, a ich skargi wnoszone w imieniu odbiorców usługi mogą mieć pozytywny wpływ ogólnie na wolność słowa i informacji, dlatego dostawcy platform internetowych powinni rozpatrywać te skargi bez zbędnej zwłoki.
- (150) Mając na względzie skuteczność i efektywność, Komisja powinna przeprowadzić ogólną oceną niniejszego rozporządzenia. W szczególności ta ogólna ocena powinna dotyczyć między innymi zakresu usług objętych niniejszym rozporządzeniem, relacji zachodzących z innymi aktami prawnymi, wpływu niniejszego rozporządzenia na funkcjonowanie rynku wewnętrznego, w szczególności w odniesieniu do usług cyfrowych, wdrażania kodeksów postępowania, obowiązku wyznaczenia przedstawiciela prawnego mającego siedzibę lub miejsce zamieszkania w Unii, wpływu obowiązków na małe przedsiębiorstwa i mikroprzedsiębiorstwa, skuteczności mechanizmu nadzoru i egzekwowania oraz wpływu na prawo do wolności wypowiedzi i informacji. Ponadto, aby uniknąć nieproporcjonalnych obciążeń i zapewnić stałą skuteczność niniejszego rozporządzenia, w ciągu trzech lat od rozpoczęcia stosowania niniejszego rozporządzenia Komisja powinna przeprowadzić ocenę wpływu obowiązków określonych w niniejszym rozporządzeniu na małe i średnie przedsiębiorstwa, a w ciągu trzech lat od jego wejścia w życie – ocenę zakresu usług objętych niniejszym rozporządzeniem, w szczególności w odniesieniu do bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, oraz relacji zachodzących z innymi aktami prawnymi.
- (151) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze w odniesieniu do ustanowienia wzorów określających formę, treść i inne szczegóły sprawozdań dotyczących moderowania treści, do określenia kwoty rocznej opłaty nadzorczej pobieranej od dostawców bardzo dużych platform internetowych oraz bardzo

³³ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2020/1828 z 25.11.2020 r. w sprawie powództw przedstawicielskich wytaczanych w celu ochrony zbiorowych interesów konsumentów i uchylająca dyrektywę 2009/22/WE (Dz.Urz. UE L 409, s. 1).

dużych wyszukiwarek internetowych, do ustanawiania praktycznych ustaleń dotyczących postępowania, wysłuchania i wynegocjowanego ujawnienia informacji w kontekście nadzoru, dochodzenia, egzekwowania i monitorowania w odniesieniu do dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, a także do określenia praktycznych i operacyjnych ustaleń na potrzeby funkcjonowania systemu wymiany informacji i jego interoperacyjności z pozostałymi odpowiednimi systemami. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011³⁴.

- (152) Aby osiągnąć cele określone w niniejszym rozporządzeniu, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE w celu uzupełnienia niniejszego rozporządzenia, w odniesieniu do kryteriów identyfikacji bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, etapów procedury, metodyk audytowych i wzorów sprawozdań w odniesieniu do audytów, specyfikacji technicznych dotyczących wniosków o dostęp, a także szczegółowych metodyk i procedur określania opłaty nadzorczej. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa³⁵. W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.
- (153) Niniejsze rozporządzenie nie narusza praw podstawowych uznanych w Karcie praw podstawowych ani praw podstawowych stanowiących ogólne zasady prawa Unii. W związku z tym niniejsze rozporządzenie powinno być interpretowane i stosowane zgodnie z tymi prawami podstawowymi, w tym dotyczącymi wolności wypowiedzi i informacji oraz wolności i pluralizmu mediów. Wykonując uprawnienia określone w niniejszym rozporządzeniu, wszystkie zaangażowane organy publiczne powinny dążyć – w sytuacjach, w których występuje konflikt odpowiednich praw podstawowych – do osiągnięcia właściwej równowagi między danymi prawami zgodnie z zasadą proporcjonalności.
- (154) Zważywszy na zakres i skutki zagrożenia społecznego, jakie mogą powodować bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe, konieczność pilnego przeciwdziałania takiemu zagrożeniu oraz zdolność do

³⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z 16.02.2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.Urz. UE L 55, s. 13).

³⁵ Dz.Urz. UE L 123 z 2016 r., s. 1.

podjęcia niezbędnych środków, zasadnym jest ograniczenie czasu, po upływie którego rozpocznie się stosowanie niniejszego rozporządzenia do dostawców takich usług.

(155) Ponieważ cele niniejszego rozporządzenia, mianowicie przyczynianie się do prawidłowego funkcjonowania rynku wewnętrznego oraz zapewnienie bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego, w którym prawa podstawowe zapisane w Karcie praw podstawowych są odpowiednio chronione, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, gdyż działając samodzielnie, nie mogą one osiągnąć niezbędnej harmonizacji i współpracy, natomiast ze względu na zakres terytorialny i podmiotowy możliwe jest ich lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów.

(156) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725³⁶ skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał swoją opinię w dniu 10 lutego 2021 r.³⁷,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

³⁶ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z 23.10.2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.Urz. UE L 295, s. 39).

³⁷ Dz.Urz. UE C 149 z 2021 r., s. 3.

ROZDZIAŁ I

Przepisy ogólne

Artykuł 1

Przedmiot i zakres stosowania

1. Celem niniejszego rozporządzenia jest przyczynienie się do właściwego funkcjonowania rynku wewnętrznego usług pośrednich poprzez ustanowienie zharmonizowanych przepisów dotyczących bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego, które ułatwia innowacje i w którym skutecznie chronione są prawa podstawowe zapisane w Karcie, w tym zasada ochrony konsumentów.

2. W niniejszym rozporządzeniu ustanawia się zharmonizowane przepisy dotyczące świadczenia usług pośrednich na rynku wewnętrznym. Ustanawia się w szczególności:

- a) ramy warunkowego wyłączenia odpowiedzialności dostawców usług pośrednich;
- b) przepisy dotyczące szczególnych obowiązków w zakresie należytej staranności dostosowane do określonych szczególnych kategorii dostawców usług pośrednich;
- c) przepisy dotyczące wdrażania i egzekwowania niniejszego rozporządzenia, w tym w odniesieniu do współpracy i koordynacji między właściwymi organami.

Spis treści

I.	Uwagi wprowadzające	102
1.	Znaczenie	102
2.	Struktura	105
3.	Odniesienie do definicji pojęć	106
II.	Cel i zakres zastosowania	107
III.	Komentarz	108
1.	Wybór instrumentu	108
2.	Cele rozporządzenia	110
3.	Podmioty chronione	112

4. Zakres zastosowania	115
5. Wyłączenia odpowiedzialności dostawców usług pośrednich	116
6. Szczególne obowiązki w zakresie należytej staranności dostosowane do określonych szczególnych kategorii dostawców usług pośrednich	117
7. Przepisy dotyczące wdrażania i egzekwowania niniejszego rozporządzenia, w tym w odniesieniu do współpracy i koordynacji między właściwymi organami	120
IV. Korelacje z innymi przepisami	120
V. Perspektywy	121
1. Akty delegowane	121
2. Akty wykonawcze	122
3. Akty krajowe	123
4. Wytyczne	125
5. Kodeksy	126

Motywy: 1–5, 9, 10, 12, 13, 16, 17, 40, 41

I. Uwagi wprowadzające

1. Znaczenie

1. Tempo i skala zmian zachodzących w handlu internetowym skłoniły prawodawcę unijnego, co akcentuje w motywie 1 DSA, do przyjęcia nowych regulacji prawnych, które mają być odpowiedzią na nowe zagrożenia i wyzwania pojawiające się w tej sferze obrotu, zwłaszcza w kontekście rozpowszechniania nielegalnych treści. Jak podkreśla Komisja w uzasadnieniu wniosku legislacyjnego, od czasu przyjęcia dyrektywy 2000/31/WE pojawiły się nowe i innowacyjne (cyfrowe) usługi społeczeństwa informacyjnego, które zmieniają codzienne życie obywateli Unii oraz kształtują i modyfikują sposoby komunikacji, łączności, konsumpcji i prowadzenia działalności gospodarczej przez obywateli. Usługi te w dużym stopniu przyczyniły się do transformacji społecznej i ekonomicznej w Unii i na świecie³⁸. Jednocześnie ich wykorzystanie wiąże się z nowymi zagrożeniami i wyzwaniami zarówno dla całego społeczeństwa, jak i poszczególnych osób korzystających z takich usług. Usługi cyfrowe mogą wspierać proces osiągnięcia celów zrównoważonego rozwoju, przyczyniając się do zrównoważonego wzrostu gospodarczego i rozwoju społecznego oraz zrównoważenia środowiskowego. Kryzys związany z koronawirusem dodatkowo uwidocznił znaczenie technologii cyfrowych we wszystkich sferach współczesnego życia.

³⁸ COM(2020) 825 final.

Wyraźnie ukazał uzależnienie gospodarki i społeczeństwa od usług cyfrowych oraz uwypuklił zarówno korzyści, jak i zagrożenia wynikające z obowiązujących ram dotyczących funkcjonowania usług cyfrowych.

2. W komunikacie pt. „Kształtowanie cyfrowej przyszłości Europy” Komisja zobowiązała się do aktualizacji przepisów horyzontalnych, w których określono zadania i obowiązki dostawców usług cyfrowych, w szczególności platform internetowych³⁹. Ponadto w kolejnych dokumentach unijnych, poczynawszy od pierwszego raportu Komisji z oceny stosowania dyrektywy 2000/31/WE⁴⁰, przez rezolucję Parlamentu Europejskiego z 5.02.2009 r. w sprawie handlu międzynarodowego i Internetu (2008/2204(INI)) – „Handel międzynarodowy i Internet” i komunikat „Europejska agenda cyfrowa” z 26.08.2010 r.⁴¹, a skończywszy na rezolucjach Parlamentu Europejskiego: w sprawie poprawy funkcjonowania jednolitego rynku⁴², w sprawie dostosowania przepisów prawa handlowego i cywilnego do podmiotów gospodarczych prowadzących działalność internetową⁴³ i w sprawie praw podstawowych⁴⁴, podnoszono, że rozważenia i podjęcia ewentualnych działań prawodawczych wymaga rewizja dyrektywy 2000/31/WE i m.in. wprowadzenia procedury *notice and takedown*. Zwłaszcza w wspomnianej rezolucji pt. „Akt prawny o usługach cyfrowych: dostosowanie przepisów prawa handlowego i cywilnego do podmiotów gospodarczych prowadzących działalność internetową” Parlament Europejski wyraźnie wezwał do zwiększenia poziomu sprawiedliwości, przejrzystości i odpowiedzialności w zakresie procedur moderowania treści usług cyfrowych, zapewnienia poszanowania praw podstawowych oraz zagwarantowania niezależnych środków zaskarżenia.

Wspólnym elementem wspomnianych rezolucji Parlamentu Europejskiego jest wezwanie Komisji do zachowania podstawowych zasad określonych w dyrektywie o handlu elektronicznym oraz do ochrony praw podstawowych w środowisku internetowym, a także ochrony anonimowości w internecie w każdym przypadku, gdy jest to technicznie możliwe⁴⁵. W rezolucjach tych Parlament Europejski wzywa do zapewnienia przejrzystości, obowiązków informacyjnych i rozliczalności w odniesieniu do dostawców usług cyfrowych oraz opowiada się za skutecznymi zobowiązaniami do zwalczania nielegalnych treści w internecie.

3. W ramach tych założeń został opracowany i przedłożony przez Komisję projekt aktu o usługach cyfrowych stanowiący jeden z elementów legislacyjnego pakietu cyfrowego, w skład którego wchodzi również akt o rynkach cyfrowych (DMA), akt o zarządzaniu

³⁹ Zob. https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf (dostęp: 2.01.2024 r.).

⁴⁰ COM(2003) 702 final.

⁴¹ COM(2010) 245 final.

⁴² Akt prawny o usługach cyfrowych: poprawa funkcjonowania jednolitego rynku, 2020/2018(INL).

⁴³ Akt prawny o usługach cyfrowych: dostosowanie przepisów prawa handlowego i cywilnego do podmiotów gospodarczych prowadzących działalność internetową, 2020/2019(INL).

⁴⁴ Akt prawny o usługach cyfrowych i związane z nim kwestie z zakresu praw podstawowych, 2020/2022(INI).

⁴⁵ Uzasadnienie wniosku legislacyjnego, COM(2020) 825 final.

danymi (DGA), akt o danych (DA) i akt o sztucznej inteligencji (AIA)⁴⁶. Uzupełniają one i częściowo modyfikują dotychczasową regulację dyrektywy 2000/31/WE, a także rozporządzenie 2019/1150 (rozporządzenie *platform-to-business*).

4. Komisja przedłożyła **wniosek legislacyjny w dniu 15.12.2020 r.**⁴⁷ Akt o usługach cyfrowych ostatecznie został uchwalony po przeprowadzeniu zwykłej procedury legislacyjnej 19.10.2022 r., a opublikowany w Dzienniku Urzędowym Unii Europejskiej 27.10.2022 r. i wszedł w życie 16.11.2022 r.

Rozporządzenie **zaczęło być stosowane od 17.02.2024 r.**

5. Niektóre przepisy dotyczące **dostawców bardzo dużych platform internetowych (VLOP) i bardzo dużych wyszukiwarek internetowych (VLOSE)** stosuje się jednak już od 16.11.2022 r., w tym obowiązki sprawozdawcze, niezależne audyty, udostępnianie danych i nadzór, czynności sprawdzające, egzekwowanie i monitorowanie⁴⁸. Do 17.02.2023 r., a następnie co najmniej raz na sześć miesięcy, platformy internetowe i wyszukiwarki internetowe zobowiązane zostały do publikacji informacji na temat średniej liczby aktywnych miesięcznie odbiorców usługi w Unii, obliczonej jako średnia liczba w okresie poprzednich sześciu miesięcy, w publicznie dostępnej sekcji swojego interfejsu internetowego. Związane jest to z kwalifikacją danych platform lub wyszukiwarek jako VLOP lub VLOSE, w związku z nałożeniem na nich dodatkowych obowiązków⁴⁹. W akcie o usługach cyfrowych ustanowiono bowiem wynoszący 45 mln próg średniej liczby aktywnych miesięcznie odbiorców usługi w Unii jako kryterium pozwalające wskazać usługi takich dostawców jako bardzo duże platformy internetowe oraz jako bardzo duże wyszukiwarki⁵⁰.

W dniu 25.04.2023 r. Komisja wyznaczyła 17 platform i 2 wyszukiwarki jako, odpowiednio, VLOP i VLOSE⁵¹. Kolejne wskazania nastąpiły 20.12.2023 r.⁵² Zgodnie z art. 92 DSA

⁴⁶ Szerzej na temat relacji aktu o usługach cyfrowych do innych aktów prawnych zob. komentarz do art. 2 DSA.

⁴⁷ COM(2020) 825 final.

⁴⁸ Zob. szerzej komentarz do art. 93 DSA.

⁴⁹ Zob. art. 34–43 DSA i komentarze do tych przepisów.

⁵⁰ Zob. art. 33 DSA. Wytyczne dotyczące wymogu publikowania numerów użytkowników, <https://digital-strategy.ec.europa.eu/pl/library/dsa-guidance-requirement-publish-user-numbers> (dostęp: 2.01.2024 r.).

⁵¹ Dokument Komisji wydany na podstawie art. 33 ust. 4 DSA, PUB/2023/821: Bardzo duże platformy internetowe i bardzo duże wyszukiwarki wskazane na podstawie art. 33 ust. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) – 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.U. L 277 z 27.10.2022, s. 1), 2023/C 249/02. Zob. także https://ec.europa.eu/commission/presscorner/detail/pl/ip_23_2413 (dostęp: 2.01.2024 r.): Bardzo duże platformy internetowe: Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zaland. Bardzo duże wyszukiwarki internetowe: Bing i Google Search.

⁵² Bardzo duże platformy internetowe: Pornhub, Stripchat, XVideos, <https://digital-strategy.ec.europa.eu/pl/news/commission-designates-second-set-very-large-online-platforms-under-digital-services-act> (dostęp: 2.01.2024 r.).

z upływem czterech miesięcy od powiadomienia danego dostawcy o jego statusie rozporządzenie ma do niego zastosowanie jeszcze przed dniem 17.02.2024 r.

6. Rozporządzenie wprowadza obowiązki oraz system przejrzystości i rozliczalności dla dostawców **usług pośrednich**, takich jak usługi dostępu do internetu, usługi hostingowe, np. usługi przetwarzania w chmurze i usługi hostingu internetowego, rejestry nazw domen, internetowe platformy handlowe, sklepy z aplikacjami, platformy wspierające gospodarkę współpracy, sieci społecznościowe, platformy wymiany treści, internetowe platformy dotyczące podróży i zakwaterowania. Rozporządzenie zawiera szczegółowe przepisy, którym podlegają **dostawcy bardzo dużych platform internetowych (VLOP)** wykorzystywane przez ponad 10% z 450 mln konsumentów w UE oraz **bardzo duże wyszukiwarki internetowe (VLOSE)** wykorzystywane przez ponad 10% z 450 mln konsumentów w UE⁵³.

2. Struktura

7. W art. 1 DSA określone zostają przedmiot, cel i ogólny zakres zastosowania regulacji aktu o usługach cyfrowych. Zakres przedmiotowy uzupełniany jest regulacją art. 2 DSA, który wskazuje na zakres terytorialny zastosowania regulacji, wyłączenia i relacje aktu o usługach cyfrowych do innych aktów prawa unijnego.
8. W ust. 1 określony zostaje cel regulacji skorelowany z podstawą prawną wydania komentowanego aktu prawnego, tj. art. 114 w zw. z art. 26 TFUE, stanowiącym podstawę działań harmonizacyjnych w celu ustanowienia lub zapewnienia funkcjonowania rynku wewnętrznego w UE. Głównym celem rozporządzenia jest w konsekwencji, jak podkreśla Komisja w uzasadnieniu wniosku legislacyjnego, zapewnienie prawidłowego funkcjonowania rynku wewnętrznego, w szczególności w związku ze świadczeniem transgranicznych usług cyfrowych, w tym usług pośrednich, z uwzględnieniem wyważenia zasad i praw określonych w KPP UE, także ochrony konsumentów. Aby to osiągnąć, w myśl art. 1 ust. 1 DSA i uzasadnienia wniosku legislacyjnego rozporządzenie harmonizuje warunki rozwoju innowacyjnych usług transgranicznych w Unii dzięki usunięciu przeszkód i zapobieganiu pojawianiu się przeszkód w prowadzeniu takiej działalności gospodarczej, wynikających z różnic w sposobie, w jaki opracowywane są przepisy krajowe, oraz wyznaczenie ram prawnych dla bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego⁵⁴.
9. Zakresem przedmiotowym regulacja obejmuje, w szczególności następujące obszary:
 - a) warunkowego wyłączenia odpowiedzialności dostawców usług pośrednich;
 - b) szczególnych obowiązków w zakresie należytej staranności dostosowane do określonych szczególnych kategorii dostawców usług pośrednich;

⁵³ Zob. <https://eur-lex.europa.eu/EN/legal-content/summary/digital-services-act.html> (dostęp: 2.01.2024 r.).

⁵⁴ Uzasadnienie wniosku legislacyjnego, COM(2020) 825 final.

- c) wdrażania i egzekwowania rozporządzenia, w tym w odniesieniu do współpracy i koordynacji między właściwymi organami.

3. Odniesienie do definicji pojęć

10. Z perspektywy regulacji art. 1 DSA kluczowe, a zdefiniowane w art. 3 DSA, pojęcia to:
- **usługa społeczeństwa informacyjnego** – oznacza każdą usługę, zgodnie z definicją w art. 1 ust. 1 lit. b dyrektywy 2015/1535, do którego odsyła art. 3 lit. a DSA, normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług;
 - **konsument** – na postawie art. 3 lit. c DSA oznacza osobę fizyczną, która działa w celach innych niż jej działalność handlowa, gospodarcza, rzemieślnicza lub zawodowa;
 - **oferować usługi w Unii** – zgodnie z art. 3 lit. d DSA oznacza umożliwiać osobom fizycznym lub prawnym w co najmniej jednym państwie członkowskim korzystanie z usług dostawcy usług pośrednich, który posiada istotne powiązanie z Unią;
 - **usługa pośrednia** – zdefiniowana w art. 3 lit. g DSA oznacza jedną z następujących usług społeczeństwa informacyjnego:
 - (i) usługa „zwykłego przekazu” polegająca na transmisji w sieci telekomunikacyjnej informacji przekazanych przez odbiorcę usługi lub na zapewnianiu dostępu do sieci telekomunikacyjnej;
 - (ii) usługa „cachingu” polegająca na transmisji w sieci telekomunikacyjnej informacji przekazanych przez odbiorcę usługi, obejmującą automatyczne, pośrednie i krótkotrwałe przechowywanie tej informacji, dokonywane wyłącznie w celu usprawnienia późniejszej transmisji informacji na żądanie innych odbiorców;
 - (iii) usługa „hostingu” polegająca na przechowywaniu informacji przekazanych przez odbiorcę usługi oraz na jego żądanie⁵⁵;
 - **platforma internetowa** – zgodnie z art. 3 lit. i DSA oznacza usługę hostingu, która na żądanie odbiorcy usługi przechowuje i rozpowszechnia publicznie informacje, chyba że takie działanie jest nieznaczną lub wyłącznie poboczną cechą innej usługi lub nieznaczną funkcją głównej usługi, i ze względów obiektywnych i technicznych nie można z niej skorzystać bez takiej innej usługi, a włączenie takiej cechy lub funkcji w taką inną usługę nie jest sposobem na obejście stosowania niniejszego rozporządzenia;
 - **wyszukiwarka internetowa** – na podstawie art. 3 lit. j DSA oznacza usługę pośrednią, która umożliwia użytkownikom dokonywanie zapytań w celu wyszukiwania – co do zasady – wszystkich stron internetowych lub wszystkich stron internetowych w danym języku za pomocą zapytania na jakikolwiek temat przez podanie słowa kluczowego, zapytania głosowego, wyrażenia lub innej wartości wejściowej i która podaje wyniki wyszukiwania w dowolnym formacie, w którym można znaleźć informacje związane z zadaniem zapytaniem;

⁵⁵ Na temat wyszukiwarek internetowych jako usług pośrednich zob. komentarze do art. 3 i 6 DSA.

- **koordynator ds. usług cyfrowych właściwy dla miejsca siedziby** – w myśl art. 3 lit. n DSA oznacza koordynatora ds. usług cyfrowych państwa członkowskiego, w którym znajduje się główne miejsce prowadzenia działalności dostawcy usługi pośredniej lub w którym jego przedstawiciel prawny ma miejsce zamieszkania lub siedzibę;
- **koordynator ds. usług cyfrowych właściwy dla miejsca przeznaczenia** – zgodnie z art. 3 lit. o DSA oznacza koordynatora ds. usług cyfrowych państwa członkowskiego, w którym świadczona jest usługa pośrednia.

II. Cel i zakres zastosowania

11. Głównymi celami regulacji jest **zapewnienie prawidłowego funkcjonowania rynku wewnętrznego, zwłaszcza w zakresie świadczenia transgranicznych usług cyfrowych**, w tym przede wszystkim usług pośrednich oraz stworzenie bezpieczniejszej przestrzeni cyfrowej, w której **chronione są podstawowe prawa wszystkich użytkowników usług cyfrowych**. Równocześnie celem prawodawcy unijnego jest ustanowienie **równych warunków działania w celu wspierania innowacji, wzrostu i konkurencyjności**, zarówno na jednolitym rynku europejskim, jak i na całym świecie⁵⁶. Cele te mają charakter równorzędny, ale i autonomiczny. Ich osiągnięciu podporządkowany został zakres regulacji. W akcie u usługach cyfrowych wprowadzono zharmonizowane przepisy dotyczące świadczenia **usług pośrednich na rynku wewnętrznym**, ustanawiając w szczególności:
 - a) ramy warunkowego wyłączenia odpowiedzialności dostawców usług pośrednich;
 - b) przepisy dotyczące szczególnych obowiązków w zakresie należytej staranności dostosowane do określonych szczególnych kategorii dostawców usług pośrednich;
 - c) przepisy dotyczące wdrażania i egzekwowania rozporządzenia, w tym w odniesieniu do współpracy i koordynacji między właściwymi organami.
12. Komentowany przepis stanowi **punkt odniesienia dla wykładni** szczegółowych przepisów rozporządzenia, wyznaczając w połączeniu z art. 2 DSA ramy regulacyjne⁵⁷. Ma to istotne znaczenie w kontekście jednoznacznego celu ochronnego i szerokiego kręgu podmiotów chronionych, co do zasady odnoszącego się do uczestników nieprofesjonalnych, co jest głównym kryterium odróżniającym DSA od DMA czy regulacji rozporządzenia P2B (ang. *platform-to-business*). Nie jest to jednak kryterium w pełni jednoznaczne, bowiem zakres podmiotowy aktu o usługach cyfrowych, zarówno jeśli chodzi o **adresatów obowiązków, jak i podmioty chronione, został ujęty szeroko**, w tym pierwszym przypadku chodzi o podmioty świadczące usługi cyfrowe, przede wszystkim usługi pośrednie. W tym drugim natomiast przypadku o wszystkich użytkownikach tychże usług cyfrowych, ale także innych uczestników obrotu, których prawa mogą być naruszone. Szczególnie

⁵⁶ Uzasadnienie wniosku legislacyjnego, COM(2020) 825 final.

⁵⁷ M. Grochowski [w:] *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, red. M. Grochowski, Warszawa 2024, s. 77.

widoczne jest to w zakresie regulacji wyłączeń odpowiedzialności⁵⁸, procedury zawiadomienia i działania (art. 16 DSA) oraz obowiązków nakładanych na dostawców VLOP i VLOSE⁵⁹. Jest to konsekwencją przyjętego **horyzontalnego charakteru regulacji**.

III. Komentarz

1. Wybór instrumentu

13. Podstawą dla wydania aktu o usługach cyfrowych jest art. 114 ust. 1 w zw. z art. 26 TFUE zawierający regulację kompetencji ogólnej związanej z urzeczywistnianiem rynku wewnętrznego. W tym trybie w zwykłej procedurze ustawodawczej i po konsultacji z Komitetem Ekonomiczno-Społecznym mogą być przyjmowane środki dotyczące zbliżenia przepisów ustawowych zarówno w formie dyrektyw, jak i rozporządzeń.
14. Komisja podjęła decyzję o przedstawieniu wniosku, wybierając formę rozporządzenia, w celu zapewnienia spójnego poziomu ochrony w całej Unii i uniknięcia rozbieżności utrudniających swobodne świadczenie odnośnych usług na rynku wewnętrznym, a także w celu zagwarantowania jednakowej ochrony praw oraz jednakowych obowiązków przedsiębiorstw i konsumentów na całym rynku wewnętrznym. Jest to konieczne do zapewnienia pewności prawa i przejrzystości zarówno podmiotom gospodarczym, jak i konsumentom. Rozporządzenie, według Komisji, zapewnia ponadto spójne monitorowanie praw i obowiązków oraz równoważne sankcje we wszystkich państwach członkowskich, a także skuteczną współpracę między organami nadzorczymi poszczególnych państw członkowskich i na szczeblu unijnym⁶⁰.

Wybór rozporządzenia, jako aktu prawnego na szczeblu unijnym, wynika właśnie z konstatacji, że celów regulacji w jednolity sposób nie są w stanie osiągnąć w wystarczającym stopniu państwa członkowskie. Komisja w uzasadnieniu wniosku legislacyjnego podkreśla, że z uwagi na fakt, iż internet z natury ma charakter transgraniczny, działania legislacyjne na szczeblu krajowym, o których mowa powyżej, utrudniają świadczenie i odbiór usług na terytorium całej Unii i są nieskuteczne, jeżeli chodzi o zapewnienie bezpieczeństwa i jednakowego poziomu ochrony praw obywateli Unii i unijnych przedsiębiorstw w internecie⁶¹. Harmonizacja warunków rozwoju innowacyjnych transgranicznych usług cyfrowych w Unii z zachowaniem bezpiecznego środowiska internetowego jest możliwa wyłącznie na szczeblu unijnym. Prawodawca unijny uzasadnia zatem przyjęcie opisanego środka legislacyjnego i zakresu regulacji realizacją zasady pomocniczości oraz zasady proporcjonalności, o których mowa w art. 5 TUE.

⁵⁸ Zob. art. 4–6 DSA.

⁵⁹ Zob. art. 33 i n. DSA.

⁶⁰ Uzasadnienie wniosku legislacyjnego, COM(2020) 825 final.

⁶¹ Uzasadnienie wniosku legislacyjnego, COM(2020) 825 final.

15. **Zgodnie z art. 288 TFUE rozporządzenie ma zasięg ogólny oraz wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich** (ang. *direct effect*)⁶². W konsekwencji więc, odmiennie niż dyrektywa, której podmiotowy zakres związania obejmuje co do zasady państwa członkowskie, do których jest kierowana, i to w odniesieniu do rezultatu, który ma być osiągnięty, przy pozostawieniu swobody wyboru formy i środków transpozycyjnych, nie wymaga podejmowania przez ustawodawców krajowych aktywności legislacyjnej o zróżnicowanym ponad minimalny wyznaczony dyrektywą poziomie⁶³.
16. W celu zapewnienia stosowania rozporządzenia w krajowych porządkach prawnych, mimo bezpośredniego stosowania, konieczna jest jednak ingerencja ustawodawcza w poszczególnych państwach członkowskich. Wynika to przede wszystkim z przyjętej w prawie europejskim zasady **autonomii proceduralnej** państw członkowskich. Konieczne jest zatem stworzenie na szczeblu krajowym odpowiednich przepisów obejmujących zagadnienia instytucjonalne i proceduralne⁶⁴.

Istotą zasady autonomii proceduralnej jest przyjęcie, że w razie braku regulacji w prawie unijnym państwa członkowskie korzystają ze **swobody stanowienia reguł proceduralnych**. Swoboda ta jednakże podlega dwóm zasadom ograniczającym, tj. zasadzie równoważności (ang. *principle of equivalence*) i zasadzie skuteczności (ang. *principle of effectiveness*).

Zgodnie z **zasadą równoważności** prawo krajowe nie może regulować uprawnień wynikających z prawa unijnego w sposób mniej korzystny niż wynikających z prawa krajowego. **Zasada skuteczności** przesądza zaś, że procedura ustanowiona w prawie krajowym nie może prowadzić do uniemożliwienia lub znacznego utrudnienia (ang. *excessively difficult*) realizowania praw przyznanych w prawie unijnym. W tym kontekście autonomia proceduralna podlega ograniczeniom i przepisy procedury mogą być objęte kognicją Trybunału Sprawiedliwości, zwłaszcza w sytuacji naruszania przez nie drugiej ze wskazanych zasad. Zwrócił na to uwagę TS w wyroku z 6.10.1981 r., C-246/80, C. Broekmeulen przeciwko Huisarts Registratie Commissie⁶⁵.

⁶² Rozporządzenie wywołuje pełny skutek bezpośredni, a zatem zarówno wertykalny, jak i horyzontalny, co zostało potwierdzone w wyroku TS z 14.12.1971 r., C-43/71, *Politi s.a.s. przeciwko Ministrowi Finansów Republiki Włoskiej*, EU:C:1971:122.

⁶³ W pewnych przypadkach, zgodnie z orzecznictwem Trybunału Sprawiedliwości, możliwe jest również bezpośrednie stosowanie dyrektyw. Celem ma być ochrona praw jednostek. Ponadto – aby normy dyrektywy były możliwe do bezpośredniego zastosowania w sytuacji uchybienia przez państwo członkowskie obowiązkom transpozycyjnym w oznaczonym terminie – muszą mieć one charakter bezwarunkowy oraz dostatecznie jasny i precyzyjny (wyrok TS z 4.12.1974 r., C-41/74, *Yvonne van Duyn przeciwko Home Office*, EU:C:1974:133). Co do ograniczonego bezpośredniego zastosowania dyrektywy (wertykalnego skutku bezpośredniego – *vertical direct effect*) zob. wyrok TS z 5.04.1979 r., C-148/78, *Postępowanie karne przeciwko Tullio Ratti*, EU:C:1979:110.

⁶⁴ Prawodawca unijny w art. 9 ust. 6 DSA wskazał także wprost, że warunki i wymogi ustanowione w art. 9 DSA odnoszące się do nakazów sądowych lub administracyjnych pozostają bez uszczerbku dla krajowego prawa cywilnego procesowego i krajowego prawa karnego procesowego.

⁶⁵ EU:C:1981:218. Na temat przepisów podlegających ocenie przez pryzmat zasady autonomii proceduralnej i jej ograniczeń, zwłaszcza zasady efektywności, zob. dodatkowo wyrok TS z 5.03.1996 r. w sprawach połączonych

17. Wybór środka legistacyjnego ma swoje konsekwencje związane z wykładnią jego przepisów. Zgodnie bowiem z utrwalonym orzecnictwem Trybunału Sprawiedliwości treści przepisu prawa Unii, który nie zawiera żadnego wyraźnego odesłania do prawa państw członkowskich w celu określenia jego znaczenia i zakresu, należy zazwyczaj nadawać w całej Unii autonomiczną i jednolitą wykładnię, której należy dokonywać z uwzględnieniem w szczególności treści tego przepisu, realizowanych przez niego celów oraz kontekstu, w jaki się on wpisuje⁶⁶.

2. Cele rozporządzenia

18. Celami aktu o usługach cyfrowych są:
- a) zapewnienie prawidłowego funkcjonowania rynku wewnętrznego w zakresie świadczenia transgranicznych usług cyfrowych;
 - b) ochrona podstawowych praw wszystkich użytkowników usług cyfrowych;
 - c) wspieranie innowacji, wzrostu i konkurencyjności na jednolitym rynku europejskim.
19. Mają one charakter **równorzędny, ale i autonomiczny**. Dla ich osiągnięcia konieczne jest jednak ich zbalansowanie, co widać przede wszystkim w obszarach regulacji wyłączeń odpowiedzialności dostawców usług pośrednich oraz szczególnych obowiązków nałożonych na dostawców platform internetowych, a zwłaszcza dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych, które zostają obciążone szeregiem obowiązków mitygacji ryzyk systemowych, takich jak:
- a) ryzyko rozpowszechniania nielegalnych treści za pośrednictwem ich usług;
 - b) ryzyko wystąpienia faktycznych lub przewidywalnych negatywnych skutków dla wykonywania praw podstawowych, w szczególności prawa podstawowego do: godności ludzkiej – zapisanego w art. 1 KPP UE, poszanowania życia prywatnego

C-46/93 i C-48/93, Brasserie du Pêcheur SA przeciwko Bundesrepublik Deutschland i The Queen przeciwko Secretary of State for Transport, EU:C:1996:79. Zob. także wyroki TS: z 13.12.2017 r., C-403/16, Soufiane El Hassani przeciwko Ministrowi Spraw Zagranicznych, EU:C:2017:960, pkt 26; z 15.09.2022 r., C-18/21, Uniqä Versicherungen AG przeciwko VU, EU:C:2022:682, pkt 36; z 21.06.2022 r., C-817/19, Ligue des droits humains ASBL przeciwko Conseil des ministres, EU:C:2022:491, pkt 297 oraz z 4.05.2023 r., C-300/21, UI przeciwko Österreichische Post AG, EU:C:2023:370, pkt 53 i 54. Na temat autonomii proceduralnej zob. A. Wróbel, *Autonomia proceduralna państw członkowskich. Zasada efektywności i zasada efektywnej ochrony sądowej w prawie Unii Europejskiej*, RPEiS 2005/1, s. 35 i n.; D. Miąsik, *Zasada efektywności prawa wspólnotowego [w:] Stosowanie prawa Unii Europejskiej przez sądy*, red. A. Wróbel, Kraków 2005, s. 315–316; K. Kowalik-Bańczyk, *Procedural Autonomy of Member States and the EU Rights of Defence in Antitrust Proceedings*, „Yearbook of Antitrust and Regulatory Studies” 2012/5(6), 218 i n.; A. Kołyszko, P. Dyrberg, *Zasada autonomii proceduralnej w prawie Unii Europejskiej i jej ograniczenia w praktyce*, „Temidium” 2014/4. Zob. również D. Lubasz [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, art. 31, uwaga 7.

⁶⁶ Wyrok TS z 14.12.2023 r., C-340/21, VB przeciwko Natsionalna agentsia za prihodite, EU:C:2023:986, pkt 23, zob. podobnie wyroki TS: z 18.01.1984 r., C-327/82, Ekro BV Vee- en Vleeshandel przeciwko Produktschap voor Vee en Vlees, EU:C:1984:11, pkt 11; z 1.10.2019 r., C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. przeciwko Planet49 GmbH, EU:C:2019:801, pkt 47, 48; a także z 4.05.2023 r., C-300/21, UI przeciwko Österreichische Post AG (Szkoda niemajątkowa związana z przetwarzaniem danych osobowych), EU:C:2023:370, pkt 29.

i rodzinnego – zapisanego w art. 7 KPP UE, ochrony danych osobowych – zapisanego w art. 8 KPP UE, wolności wypowiedzi i informacji, w tym wolności i pluralizmu mediów – zapisanego w art. 11 KPP UE, niedyskryminacji – zapisanego w art. 21 KPP UE, przestrzegania praw dziecka – zapisanego w art. 24 KPP UE, i wysokiej jakości ochrony konsumentów – zapisanego w art. 38 KPP UE;

- c) ryzyko wystąpienia faktycznych lub przewidywalnych negatywnych skutków dla dyskursu obywatelskiego i procesów wyborczych oraz dla bezpieczeństwa publicznego;
- d) ryzyko wystąpienia faktycznych lub przewidywalnych negatywnych skutków w odniesieniu do przemocy ze względu na płeć, ochrony zdrowia publicznego i małoletnich, oraz poważnych negatywnych skutków dla fizycznego i psychicznego dobrostanu osoby⁶⁷.

20. Aby osiągnąć wspomniane cele, niezbędne było, zdaniem Komisji, **usunięcie przeszkód i zapobieganie pojawianiu się nowych** w prowadzeniu działalności gospodarczej on-line. Jedną z głównych przeszkód wynikała z różnic w sposobie, w jaki opracowywane są przepisy krajowe, oraz tego, że wiele państw członkowskich przyjęło lub zamierza przyjąć przepisy dotyczące takich kwestii, jak: usuwanie nielegalnych treści w internecie, należyta staranność, procedury zgłaszania i działania oraz przejrzystość. W celu zapewnienia spójności, w kontekście realizacji zasady skuteczności prawa unijnego⁶⁸, w rozporządzeniu przewidziano ramy dla regulacji instytucjonalnej w zakresie nadzoru nad usługami cyfrowymi oraz przepisy dotyczące współpracy między organami na szczeblu unijnym, które mają na celu zwiększenie poziomu zaufania, innowacji i rozwoju na rynku wewnętrznym, ale przede wszystkim jednolitości i skuteczności stosowania⁶⁹.

21. Rozbieżne przepisy, jak podkreślono w motywie 2 DSA, biorąc pod uwagę z natury transgraniczny charakter internetu, który jest powszechnie wykorzystywany w celu świadczenia tych usług, mają negatywny **wpływ na rynek wewnętrzny**, który zgodnie z art. 26 ust. 2 TFUE obejmuje obszar bez granic wewnętrznych, w którym jest zapewniony swobodny przepływ towarów i usług oraz swoboda przedsiębiorczości. Z tym względów podstawą wydania aktu o usługach cyfrowych jest art. 114 ust. 1 w zw. z art. 26 TFUE zawierający regulację kompetencji ogólnej związanej z urzeczywistnianiem rynku wewnętrznego. Jest to także element kluczowy związany z budową **jednolitego rynku cyfrowego w UE**⁷⁰ i **strategii cyfrowej UE**, której elementami są umożliwienie prężnej społeczności innowacyjnych i szybko rozwijających się przedsiębiorstw typu start-up i MŚP uzyskania dostępu do finansowania i ekspansji działalności, wzmocnienie odpowiedzialności platform internetowych w zaproponowanym akcie prawnym o usługach cyfrowych oraz wyjaśnienie zasad

⁶⁷ Zob. szerzej komentarz do art. 34 DSA.

⁶⁸ Zob. pkt III.1 poniżej.

⁶⁹ Zob. też R. Müller-Terpitz [w:] *Digital Services Act: Gesetz über digitale Dienste: Kommentar*, red. R. Müller-Terpitz, M. Köhler, München 2024, s. 3; M. Grochowski [w:] *Rynek cyfrowy...*, red. M. Grochowski, s. 79.

⁷⁰ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Strategia jednolitego rynku cyfrowego dla Europy, COM(2015) 0192 final.

dotyczących usług online, zadbanie, by przepisy UE były adekwatne do celów gospodarki cyfrowej, zapewnienie uczciwej konkurencji dla wszystkich przedsiębiorstw w Europie, zwiększenie dostępu do wysokiej jakości danych przy jednoczesnym zapewnieniu ochrony danych osobowych i danych wrażliwych⁷¹. W ramach jej realizacji w komunikacie pt. „Kształtowanie cyfrowej przyszłości Europy” Komisja zobowiązała się do aktualizacji przepisów horyzontalnych, w których określono zadania i obowiązki dostawców usług cyfrowych, w szczególności platform internetowych, dostrzegając ich wpływ na rynek wewnętrzny i jednolity rynek cyfrowy⁷². Co ostatecznie urzeczywistniono w szczególności aktem o usługach cyfrowych⁷³, podkreślając w motywie 4 DSA, że ustanowią się w nim zestaw jednolitych, skutecznych i proporcjonalnych obowiązkowych zasad na poziomie Unii w celu ochrony rynku wewnętrznego i poprawienia jego funkcjonowania.

22. **Wspieranie innowacji, wzrostu i konkurencyjności na jednolitym rynku europejskim** jest drugim z zasadniczych celów regulacji aktu o usługach cyfrowych⁷⁴. Osiągnięcie tego celu, co wynika *expressis verbis* z art. 1 ust. 1 DSA, realizowane jest przez ustanowienie zharmonizowanych przepisów dotyczących bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego. Tak skonstruowane ramy prawne mają bowiem ułatwiać innowacje. Jak słusznie podnosi się w doktrynie, choć cele te mają charakter równorzędny i autonomiczny, to ich realizacja może prowadzić do konfliktów⁷⁵. Ma temu jednak przeciwdziałać m.in. przyjęta koncepcja regulacyjna neutralności technologicznej, która ma być stymulatorem rozwoju technologii i innowacji⁷⁶.

3. Podmioty chronione

23. Przepisy rozporządzenia należy **interpretować i stosować z uwzględnieniem praw podstawowych uznanych w Karcie praw podstawowych Unii Europejskiej oraz praw podstawowych stanowiących ogólne zasady prawa Unii**. Prawa podstawowe, do których referuje prawodawca unijny, obejmują m.in. prawo do wolności wypowiedzi i informacji, w tym wolności i pluralizmu mediów⁷⁷, prawo do poszanowania życia prywatnego i rodzinnego⁷⁸, prawo do ochrony danych osobowych⁷⁹, ochrony konsumentów⁸⁰, prawo

⁷¹ Zob. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_pl#dokumenty (dostęp: 2.01.2024 r.).

⁷² Zob. https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf (dostęp: 2.01.2024 r.).

⁷³ Na temat innych aktów wchodzących w skład pakietu cyfrowego zob. pkt I.1 teza 3 powyżej.

⁷⁴ R. Müller-Terpitz [w:] *Digital Services Act...*, red. R. Müller-Terpitz, M. Köhler, s. 5–6.

⁷⁵ M. Grochowski [w:] *Rynek cyfrowy...*, red. M. Grochowski, s. 80.

⁷⁶ Motyw 4 *in fine* DSA. Na temat relewantności innowacji w kontekście klauzuli rynku wewnętrznego zob. opinia Rzecznika Generalnego H. Saugmandsgaarda Øe w sprawie C-401/19, Rzeczpospolita Polska przeciwko Parlamentowi Europejskiemu i Radzie Unii Europejskiej, EU:C:2021:613, pkt 113.

⁷⁷ Zob. art. 11 KPP UE.

⁷⁸ Zob. art. 7 KPP UE.

⁷⁹ Zob. art. 8 KPP UE.

⁸⁰ Zob. art. 38 KPP UE.

do niedyskryminacji⁸¹ oraz prawo do skutecznego środka prawnego⁸², ale i wolność prowadzenia działalności gospodarczej⁸³, w tym swobodę zawierania umów, a także prawo do godności ludzkiej⁸⁴, prawa dziecka⁸⁵, prawo do ochrony własności, w tym własności intelektualnej.

Wykonując uprawnienia określone w rozporządzeniu, wszystkie zaangażowane organy publiczne powinny dążyć w sytuacjach, w których występuje konflikt odpowiednich praw podstawowych, do osiągnięcia właściwej równowagi między danymi prawami zgodnie z **zasadą proporcjonalności**. W tym kontekście pomocne mogą być kryteria zapewnienia koegzystencji kolidujących praw wypracowane w orzecznictwie zarówno Trybunału Sprawiedliwości, jak i – a może zwłaszcza – Europejskiego Trybunału Praw Człowieka⁸⁶.

Ryzyko naruszenia praw podstawowych wskazane zostało również jako ryzyko systemowe, stając się podstawą obowiązków analitycznych nałożonych na dostawców VLOP i VLOSE na mocy art. 34 ust. 1 lit. b DSA. *Notabene* konstrukcja tych obowiązków jest jednym z przejawów przyjętego w akcie o usługach cyfrowych, znanego z ogólnego rozporządzenia o ochronie danych, podejścia opartego na ryzyku (ang. *risk-based approach*)⁸⁷. Dzięki podejściu opartemu na ryzyku możliwe jest w konsekwencji niuansowanie środków mitygujących ryzyko w sposób zależny od intensywności i zakresu negatywnego wpływu lub zagrożeń w konkretnych przypadkach. Pozwala ono bowiem konstrukcyjnie na elastyczne technologicznie ogniskowanie uwagi na prawach i wolnościach jednostki⁸⁸.

⁸¹ Zob. art. 21 KPP UE.

⁸² Zob. art. 47 KPP UE.

⁸³ Zob. art. 16 KPP UE.

⁸⁴ Zob. art. 1 KPP UE.

⁸⁵ Zob. art. 24 KPP UE.

⁸⁶ Zob. rozstrzygnięcia ETPCz: z 23.07.2009 r., skarga nr 12268/03, Hachette Filipacchi Associés (ICI PARIS) przeciwko Francji, HUDOC, § 41; z 8.12.2015 r., skarga nr 28999/03, Timciuc przeciwko Rumunii, HUDOC, § 144, oraz z 10.05.2011 r., skarga nr 48009/08, Mosley przeciwko Zjednoczonemu Królestwu, HUDOC, § 111; wyroki ETPCz: z 28.07.2005 r., skarga nr 59320/00, Von Hannover przeciwko Niemcom, HUDOC, § 28.04.2009 r., skarga nr 39311/05, Karakó przeciwko Węgrom, HUDOC, § 26; z 25.11.2008 r., skarga nr 36919/02, Armonienė przeciwko Litwie, HUDOC, § 39; z 25.11.2008 r., skarga nr 23373/03, Biriuk przeciwko Litwie, HUDOC, § 38; z 7.02.2012 r., skarga nr 39954/08, Axel Springer AG przeciwko Niemcom, HUDOC, § 89 i n.; z 27.06.2017 r., skarga nr 931/13, Satakunnan Markkinapörssi Oy i Satamedia Oy przeciwko Finlandii, HUDOC, § 125, a także wyroki TS opierające się przy interpretacji na orzecznictwie ETPCz, zgodnie z 52 ust. 3 KPP UE: z 8.04.2014 r., C-293/12 i C-594/12, Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in., EU:C:2014:238, pkt 54 i 55; z 3.09.2015 r., C-398/13 P, Inuit Tapiriit Kanatami i in. przeciwko Komisji Europejskiej, EU:C:2015:535, pkt 46; z 14.03.2017 r., C-157/15, Samira Achbita i Centrum voor gelijkheid van kansen en voor racismebestrijding przeciwko G4S Secure Solutions NV, EU:C:2017:203, pkt 27; z 15.03.2017 r., C-528/15, Policie ČR, Krajské ředitelství policie Ústeckého kraje, odbor cizinecké policie przeciwko Salah Al Chodor i in., EU:C:2017:213, pkt 37 i 38.

⁸⁷ M. Grochowski [w:] *Rynek cyfrowy...*, red. M. Grochowski, s. 79.

⁸⁸ Szerzej na temat podejścia opartego na ryzyku jako modelu regulacyjnego zob. m.in. D. Lubasz, E. Bielak-Jomaa, *Analiza ryzyka jako element systemu ochrony danych osobowych w kancelariach prawnych* [w:] *Analiza ryzyka i bezpieczeństwo danych w kancelariach prawnych*, red. D. Lubasz, Warszawa 2022, s. 28–30; *Ochrona danych osobowych. Ocena ryzyka i skutków. Metody i praktyczne przykłady*, red. M. Gumularz, T. Izydorczyk, Warszawa 2021.

24. Szeroki zakres odnośnych praw podstawowych, które mają być chronione środkami przewidzianymi w rozporządzeniu, **implikuje zakres podmiotowy ochrony, obejmując nim wszystkich użytkowników usług cyfrowych, ale także innych uczestników obrotu**, których prawa mogą być naruszone. Nie ma znaczenia kwalifikacja podmiotowa, w szczególności regulacji aktu o usługach cyfrowych nie można upatrywać jako *strictae* regulacji konsumenckiej, choć i konsumenci są podmiotami chronionymi, zwłaszcza w kontekście regulacji art. 30–33 DSA.
25. Jak podkreśliła Komisja, akt o usługach cyfrowych ma na celu stworzenie bezpieczniejszego środowiska internetowego dla konsumentów i przedsiębiorstw, wprowadzając zestaw przepisów, których zadaniem jest: skuteczniejsza **ochrona konsumentów** i ich praw podstawowych, **określenie jasnych obowiązków** dla platform internetowych i mediów społecznościowych, **zwalczanie nielegalnych treści lub produktów**, mowy nienawiści i dezinformacji, **osiągnięcie większej przejrzystości** poprzez lepszą sprawozdawczość i nadzór oraz **wspieranie innowacji, wzrostu i konkurencyjności** na rynku wewnętrznym UE.
26. **Podmiotami chronionymi mają być wszystkie zainteresowane strony**, w szczególności obywatele UE, przez: **zwalczanie nielegalnych treści online, w tym towarów** i usług, **wzmocnienie pozycji użytkowników** i społeczeństwa obywatelskiego, mechanizmy oceny i ograniczenia ryzyka systemowego oraz **wzmocnienie nadzoru i egzekwowania** w odniesieniu do dostawców usług pośrednich, w tym nadanie ważnej roli koordynatorom ds. usług cyfrowych w każdym państwie członkowskim UE oraz Europejskiej Radzie ds. Usług Cyfrowych. Ponadto Komisja Europejska ma posiadać dodatkowe uprawnienia nadzorcze w odniesieniu do dostawców VLOP i VLOSE.
27. **Podmiotami chronionymi są również odbiorcy usługi**, tj. podmioty korzystające z usługi pośredniej, w szczególności w celu poszukiwania informacji lub udostępnienia jej, niezależnie, czy czynią to w związku czy bez związku z działalnością gospodarczą⁸⁹. Prawodawca unijny wyraźnie podkreśla to w motywie 2 DSA, wskazując, że do celów rozporządzenia za odbiorców usługi uważa się użytkowników biznesowych, **konsumentów** i innych użytkowników. Pojęcie odbiorcy usługi **ma kluczowe znaczenie z perspektywy zastosowania** m.in.: art. 12–23 DSA, tj. wyłączeń odpowiedzialności pośredników, moderowania treści, procedury zgłaszania i działania, art. 24 i n. DSA, tj. obowiązków nałożonych na platformy internetowe, art. 33 i n. DSA, tj. obowiązków nałożonych na bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe.

⁸⁹ Szerzej na temat pojęcia odbiorcy usługi zob. komentarz do art. 3 DSA.

4. Zakres zastosowania

28. W akcie u usługach cyfrowych wprowadzono zharmonizowane przepisy dotyczące świadczenia **usług pośrednich na rynku wewnętrznym**, ustanawiając w szczególności:
- a) ramy warunkowego wyłączenia odpowiedzialności dostawców usług pośrednich;
 - b) przepisy dotyczące szczególnych obowiązków w zakresie należytej staranności dostosowane do określonych szczególnych kategorii dostawców usług pośrednich;
 - c) przepisy dotyczące wdrażania i egzekwowania rozporządzenia, w tym w odniesieniu do współpracy i koordynacji między właściwymi organami.
29. Kluczowym pojęciem wyznaczającym zarówno zakres przedmiotowy, jak i podmiotowy regulacji rozporządzenia jest **pojęcie usług pośrednich**, zdefiniowane w art. 3 lit. g DSA jako usługa zwykłego przekazu, usługa cachingu i usługa hostingu **będące** usługami społeczeństwa informacyjnego, tj. zgodnie z definicją zawartą w dyrektywie 2015/1535 usługami normalnie świadczonymi za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy⁹⁰.

Dla pełnej analizy zasięgu definicji pojęcia „usługa pośrednia” należy jednak sięgnąć jeszcze do definicji **pojęcia platformy internetowej**⁹¹, która jest jednym z podtypów usług hostingu oraz **wyszukiwarki internetowej**, która jest usługą pośrednią, ale definicyjnie niekoniecznie usługą hostingu⁹². Podtypami usług platform internetowych i wyszukiwarek internetowych są **bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe**, czyli takie których średnia miesięczna liczba aktywnych odbiorców usługi w Unii wynosi co najmniej 45 mln i które zostały wskazane przez Komisję⁹³. Kwalifikacje te mają znaczenie z perspektywy regulacyjnego różnicowania nakładanych obowiązków na podmioty należące do poszczególnych ww. kategorii.

Skoncentrowanie uwagi prawodawcy na **podmiotach świadczących usługi pośrednie** wynika m.in., jak wskazuje się w motywie 5 DSA, z wykładniczego wzrostu korzystania z tych usług, głównie we wszelkiego rodzaju zgodnych z prawem i użytecznych społecznie

⁹⁰ Szerzej zob. komentarz do art. 3 lit. a i g DSA.

⁹¹ Zob. art. 3 lit. i DSA.

⁹² Zob. art. 3 lit. j DSA. Szerzej zob. pkt III.3 komentarza do art. 16 DSA.

⁹³ Zob. art. 33 DSA. Dokument Komisji wydany na podstawie art. 33 ust. 4 DSA, PUB/2023/821: Bardzo duże platformy internetowe i bardzo duże wyszukiwarki wskazane na podstawie art. 33 ust. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych) – 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.U. L 277 z 27.10.2022, s. 1), 2023/C 249/02. Zob. także https://ec.europa.eu/commission/presscorner/detail/pl/ip_23_2413 (dostęp: 2.01.2024 r.): Bardzo duże platformy internetowe: Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando. Bardzo duże wyszukiwarki internetowe: Bing i Google Search.

celach, przy równoczesnym zwiększeniu ich roli w pośrednictwie w zakresie niezgodnych z prawem lub w inny sposób szkodliwych informacji i działań oraz ich rozpowszechnianiu, czemu regulacja rozporządzenia ma przeciwdziałać.

30. Prawodawca unijny zwraca również uwagę **na sytuacje graniczne**, wskazując, że w praktyce niektórzy dostawcy usług pośrednich pośredniczą w zakresie usług, które mogą, ale nie muszą być świadczone drogą elektroniczną, takich jak zdalne usługi technologii informacyjnej, transport, zakwaterowanie lub usługi doręczeń. Usługi takie nie będą objęte regulacją rozporządzenia, a zakres jego zastosowania powinien się ograniczać wyłącznie do usług pośrednich. Rozporządzenie nie powinno mieć wpływu na wymogi określone w prawie Unii lub prawie krajowym dotyczące produktów lub usług, których świadczenie odbywa się poprzez usługi pośrednie, w tym w sytuacjach, gdzie usługa pośrednia stanowi integralną część innej usługi, niebędącej usługą pośrednią⁹⁴.
31. Warto także wskazać, że w przepisach rozporządzenia co do niektórych obowiązków dostawców usług pośrednich przewidziano wyłączenie dla **mikro- i małych przedsiębiorców** w zakresie dotyczącym dodatkowych przepisów mających zastosowanie do platform internetowych⁹⁵ i dodatkowych przepisów dotyczących dostawców platform internetowych umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość⁹⁶ – odpowiednio w art. 19 i 29 DSA.
32. Zawarte w art. 1 ust. 2 DSA **wyliczenie przedmiotu regulacji ma charakter przykładowy**.
33. **Terytorialny zakres zastosowania** rozporządzenia oraz wyłączenia są natomiast przedmiotem regulacji art. 2 DSA.

5. Wyłączenia odpowiedzialności dostawców usług pośrednich

34. Zgodnie z art. 1 ust. 2 lit. a DSA przedmiotem regulacji rozporządzenia są ramy warunkowego **wyłączenia odpowiedzialności dostawców usług pośrednich**. W motywie 16 DSA uzasadniając konieczność objęcia regulacją horyzontalnych ram warunkowych wyłączeń odpowiedzialności dostawców usług pośrednich, ustanowionych w dyrektywie 2000/31/WE i doceniając równocześnie ich znaczenie w kontekście wpływu na rynek wewnętrzny, wskazuje się, że jest to konieczne z uwagi na rozbieżności w transpozycji i stosowaniu odpowiednich przepisów na poziomie krajowym oraz w celu zapewnienia jasności i spójności.

Przepisy rozporządzenia zastępują w tym obszarze regulacyjnym przepisy art. 12–15 dyrektywy 2000/31/WE, jednak nie następuje tu zmiana paradygmatów leżących u podstaw

⁹⁴ Zob. motyw 6 DSA.

⁹⁵ Zob. rozdział III sekcja 3 DSA.

⁹⁶ Zob. rozdział III sekcja 4 DSA.

dotychczasowej regulacji⁹⁷. Kluczowe jest przeniesienie przepisów do stosowanego jednolite i bezpośrednio w całej Unii rozporządzenia. Równocześnie w stosunku do regulacji art. 14 u.s.u.d.e., implementującego do polskiego porządku prawnego art. 14 dyrektywy 2000/31/WE, modyfikacje te są jednak istotniejsze z uwagi na odmienności wprowadzone przez polskiego ustawodawcę w procesie implementacji⁹⁸. Istotną nowością jest natomiast przewidziany w art. 16 DSA mechanizm zgłaszania i działania, który nie był przewidziany ani w dyrektywie 2000/31/WE, ani w ustawie o świadczeniu usług drogą elektroniczną, a który stanowi jeden z istotnych elementów systemu zwalczania nielegalnych treści.

35. **Horyzontalne ramy warunkowych wyłączeń** odpowiedzialności dostawców usług pośrednich, ustanowionych w dyrektywie 2000/31/WE, miały na celu zrównoważenie postulatów rozwoju handlu elektronicznego z zapewnieniem pewności obrotu i zwalczaniem rozpowszechniania nielegalnych treści. Jak podkreśla się w motywie 16 DSA, pozwoliły one na wprowadzenie wielu nowych usług na całym rynku wewnętrznym i zwiększenie ich skali. Cele te nie uległy zasadniczej zmianie, dlatego należało zdaniem Komisji regulację tę utrzymać.
36. Warunkowe wyłączenia odpowiedzialności nie zapewniają immunitetu w zakresie odpowiedzialności za naruszenie przepisów rozporządzenia, w szczególności w zakresie dochowania należytej staranności i wykonania szczegółowych obowiązków nałożonych na poszczególne kategorie dostawców usług pośrednich. Podstawą dla takiej odpowiedzialności będzie bowiem art. 54 DSA uzupełniony odpowiednią regulacją krajową. Nałożenie takich obowiązków związane jest z dostrzeżeniem roli, jaką odgrywają ci dostawcy, uprzywilejowani w zakresie odpowiedzialności, w zakresie pośrednictwa niezgodnego z prawem.

6. Szczególne obowiązki w zakresie należytej staranności dostosowane do określonych szczególnych kategorii dostawców usług pośrednich

37. Zgodnie z art. 1 ust. 2 lit. b DSA przedmiotem regulacji rozporządzenia są **szczególne obowiązki w zakresie należytej staranności dostosowane do określonych szczególnych kategorii dostawców usług pośrednich**. Należyta staranność jest kluczową wartością wyrażoną w rozporządzeniu i jest ona rozumiana jako wymóg właściwego podejścia

⁹⁷ F. Hofmann [w:] *Digital Services Act: Gesetz über digitale Dienste*, red. F. Hofmann, B. Raue, Baden-Baden 2023, s. 53; W. Chomiczewski, *Zasady wyłączeń odpowiedzialności dostawców usług pośrednich w projekcie rozporządzenia Akt o usługach cyfrowych (cz. I)*, PNT 2021/2, s. 22. W doktrynie niemieckiej zmiany określa się wręcz jedynie jako redakcyjne: F. Hofmann [w:] *Digital Services Act...*, red. F. Hofmann, B. Raue, s. 157.

⁹⁸ Zob. szerzej W. Chomiczewski [w:] *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, red. D. Lubasz, M. Namysłowska, Warszawa 2011, s. 225 i n.; X. Konarski, *Komentarz do ustawy o świadczeniu usług drogą elektroniczną*, Warszawa 2004, s. 139 i n.; D. Lubasz, *Handel elektroniczny. Bariery prawne*, Warszawa 2013, s. 359 i n.; M. Piech, *Treści oczywiście bezprawne* [w:] M. Piech, *Pośrednicy internetowi w prawie Unii Europejskiej. Rola i obowiązki wobec treści użytkowników*, Warszawa 2019, s. 177.

przez dostawców usług pośrednich do problemu nielegalnych treści, dezinformacji online i innych zagrożeń społecznych. Jak podkreśla prawodawca unijny w motywie 3 DSA, działanie z należytą starannością dostawców usług pośrednich ma zasadnicze znaczenie dla bezpiecznego, przewidywalnego i godnego zaufania środowiska internetowego oraz umożliwienia obywatelom Unii i innym osobom korzystania z przysługujących im praw.

Z kolei w motywie 40 DSA wskazuje się, że aby osiągnąć cele określone w rozporządzeniu, w szczególności poprawić funkcjonowanie rynku wewnętrznego oraz zapewnić bezpieczne i przejrzyste środowisko internetowe, należy ustanowić jasny, skuteczny, przewidywalny i wyważony zestaw zharmonizowanych obowiązków w zakresie należytej staranności dla dostawców usług pośrednich. Celem tych obowiązków powinno być przede wszystkim zagwarantowanie osiągnięcia różnych celów polityki publicznej, takich jak bezpieczeństwo i zaufanie odbiorców usługi, w tym konsumentów, małoletnich i użytkowników szczególnie narażonych na ryzyko stania się ofiarą nawoływania do nienawiści, molestowania seksualnego lub innych dyskryminujących działań, ochrona odpowiednich praw podstawowych zapisanych w KPP UE, **zapewnienie rzeczywistej rozliczalności tych dostawców** oraz wzmocnienie pozycji odbiorców i innych zainteresowanych stron przy jednoczesnym ułatwieniu niezbędnego nadzoru przez właściwe organy.

38. W związku z tym istotne jest, aby **obowiązki w zakresie należytej staranności były dostosowane do rodzaju, wielkości i charakteru danej usługi pośredniej**⁹⁹. Ponadto obowiązki w zakresie należytej staranności, które powinny być rozsądne i niearbitralne, są potrzebne, aby zaradzić identyfikowanym obawom dotyczącym porządku publicznego, takim jak ochrona prawnie uzasadnionych interesów odbiorców usługi, zwalczanie nielegalnych praktyk i ochrona praw podstawowych zapisanych w KPP UE. Obowiązki w zakresie należytej staranności są niezależne od kwestii odpowiedzialności dostawców usług pośrednich, należy je zatem oceniać oddzielnie¹⁰⁰.

39. **Obowiązki w zakresie należytej staranności** zostały ujęte w ramy rozdziału III DSA i dostosowane do poszczególnych kategorii dostawców usług pośrednich, zależnie od rodzaju, wielkości i charakteru świadczonych przez nich usług. Należą do nich:

- obowiązki mające zastosowanie do wszystkich dostawców usług pośrednich¹⁰¹, dotyczące ustanowienia punktów kontaktowych, przedstawicieli prawnych, formułowania warunków korzystania z usług i obowiązków sprawozdawczych;
- dodatkowe obowiązki dostawców usług hostingu, w tym platform internetowych¹⁰², dotyczące obowiązku wdrożenia mechanizmu zgłaszania i działania, uzasadnienia decyzji o zastosowaniu ograniczeń oraz obowiązku zawiadomienia o podejrzeniu popełnienia przestępstwa;

⁹⁹ Motyw 41 DSA.

¹⁰⁰ Motyw 41 *in fine* DSA.

¹⁰¹ Zob. art. 11–15 DSA.

¹⁰² Zob. art. 16–18 DSA.

- dodatkowe obowiązki dostawców platform internetowych¹⁰³ dotyczące wdrożenia wewnętrznego systemu rozpoznawania skarg, umożliwienia odbiorcom usług i podmiotom zgłaszającym w mechanizmie *notice and action* pozasądowego rozstrzygania sporów, odnoszące się do zaufanych podmiotów sygnalizujących, sprawozdawczości w zakresie przejrzystości, projektowania interfejsów internetowych wraz z zakazem *deceptive designs*, a także do reklamy oraz systemów rekomendacji i ochrony małoletnich;
- dodatkowe obowiązki dostawców platform internetowych umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość¹⁰⁴, obejmujące obowiązek zapewnienia identyfikowalności przedsiębiorców zawierających umowy z konsumentami za pośrednictwem platformy, *compliance-by-design*, obowiązki informacyjnych o usługach lub produktach nielegalnych będących przedmiotem transakcji;
- dodatkowe obowiązki spoczywające na dostawcach bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych w zakresie zarządzania ryzykiem systemowym¹⁰⁵, w tym: obowiązek przeprowadzenia oceny ryzyka systemowego i podjęcie działań zmierzających do zmitigowania stwierdzonego ryzyka, obowiązek poddania się mechanizmowi reagowania kryzysowego wdrożonego przez Komisję oraz raz na rok poddania się niezależnemu audytowi pod kątem realizacji zobowiązań, obowiązki w zakresie dodatkowej przejrzystości reklam, systemów rekomendacji, umożliwienia dostępu do danych, a także sprawozdawczość w zakresie przejrzystości.

40. Ukształtowanie kaskadowe obowiązków powoduje, że np. dostawcy bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych są zobowiązani wykonać nie tylko zobowiązania z sekcji 5 rozdziału III DSA, które są *expressis verbis* adresatami, lecz także, jako że kwalifikowani są jako dostawcy usług pośrednich, obowiązki wskazane w poprzedzających sekcjach rozdziału III DSA, z zastrzeżeniem adekwatności, zwłaszcza z perspektywy sekcji 4 odnoszącej się jedynie do platform umożliwiających zawieranie umów z konsumentami. Sekcja 1 zawiera zatem przepisy ogólne odnoszące się do wszystkich dostawców usług pośrednich, natomiast kolejne sekcje – do szczegółowych typów lub kategorii świadczonych przez nie usług. Powoduje to, że konkretny usługodawca, zależnie od kwalifikacji, będzie podlegał regulacji sekcji 1 oraz może podlegać dodatkowo regulacji zawartej w jednej lub kilku sekcjach 2–5 rozdziału III DSA.

¹⁰³ Zob. art. 20–28 DSA.

¹⁰⁴ Zob. art. 30–32 DSA.

¹⁰⁵ Zob. art. 34–42 DSA.

7. Przepisy dotyczące wdrażania i egzekwowania niniejszego rozporządzenia, w tym w odniesieniu do współpracy i koordynacji między właściwymi organami

41. Przedmiotem rozporządzenia jest również regulacja dotycząca **wdrażania i egzekwowania rozporządzenia**, w tym w odniesieniu do współpracy i koordynacji między właściwymi organami¹⁰⁶. O ile do państw członkowskich należy wyznaczenie organów właściwych oraz opracowanie przepisów proceduralnych odnoszących się do postępowań skargowych oraz takich, których celem jest stwierdzenie naruszenia przepisów rozporządzenia i nałożenie sankcji, o tyle w rozporządzeniu określono ramy dla tych obszarów regulacyjnych. Stanowi to przedmiot regulacji rozdziału IV DSA wskazującego na konieczność powołania organów właściwych, w tym koordynatorów ds. usług cyfrowych, wymogi dotyczące tychże organów i ich uprawnienia, kompetencje, skoordynowane czynności sprawdzające i mechanizmy spójności. Ponadto w rozdziale IV DSA uregulowane są kwestie odnoszące się do ustanowienia i zakresu kompetencji Europejskiej Radu ds. Usług Cyfrowych oraz egzekwowania rozporządzenia w stosunku do dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych.

IV. Korelacje z innymi przepisami

42. Relacje aktu o usługach cyfrowych do innych aktów prawnych wyznacza art. 2 ust. 3–4 DSA. W pierwszej kolejności wskazuje on, że rozporządzenie nie ma wpływu na stosowanie dyrektywy 2000/31/WE o **handlu elektronicznym** w zakresie, w którym pozostaje ona w mocy¹⁰⁷, a zatem przede wszystkim w zakresie klauzuli rynku wewnętrznego – tzw. zasady państwa pochodzenia¹⁰⁸, informacji handlowej¹⁰⁹, obowiązków informacyjnych¹¹⁰ i zasad dotyczących kontraktowania¹¹¹.
43. Ponadto stosownie do art. 2 ust. 4 DSA akt o usługach cyfrowych pozostaje bez uszczerbku dla przepisów ustanowionych w innych aktach prawnych Unii regulujących inne aspekty **świadczenia usług pośrednich** na rynku wewnętrznym lub określających i uzupełniających komentowane rozporządzenie, w szczególności dla:

¹⁰⁶ Zob. art. 1 ust. 2 lit. c DSA.

¹⁰⁷ Przepisem art. 89 ust. 1 DSA uchylone zostają przepisy art. 12–15 dyrektywy 2000/31/WE, w związku z wprowadzeniem regulacji art. 4, 5, 6, 8 DSA.

¹⁰⁸ Zob. art. 3 DSA.

¹⁰⁹ Zob. art. 6–8 DSA.

¹¹⁰ Zob. art. 5 DSA.

¹¹¹ Zob. art. 9–11 DSA. Szerzej zob. D. Lubasz [w:] *Świadczenie usług...*, red. D. Lubasz, M. Namysłowska, s. 80 i n.; X. Konarski, *Komentarz do ustawy o świadczeniu...*, s. 139 i n.; D. Lubasz, *Handel elektroniczny...*, s. 112 i n.; D. Kot, *Dyrektywa Unii Europejskiej o handlu elektronicznym i jej implikacje dla prawa cywilnego*, KPP 2001/1, s. 89; S. Freytag, *Harmonisierung der Providerhaftung* [w:] *Electronic Business in Europa*, red. M. Lehmann, Wien 2002, s. 113; S. Freytag, *Providerhaftung im Binnenmarkt. Verantwortlichkeit für rechtswidrige Inhalte nach der E-Commerce-Richtlinie*, „Computer und Recht” 2000/9, s. 604; F. Maennel, *Die Europäische Richtlinie zum Electronic Commerce* [w:] *Electronic...*, red. M. Lehmann, s. 64.

- dyrektywy 2019/790 w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym;
- rozporządzenia 2019/1150 w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (rozporządzenie *platform-to-business*);
- rozporządzenia 2021/784 w sprawie przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym;
- prawa Unii w dziedzinie ochrony konsumentów i bezpieczeństwa produktów, w tym rozporządzeń 2017/2394 i 2019/1020 oraz dyrektyw 2001/95/WE i 2013/11/UE;
- prawa Unii w dziedzinie ochrony danych osobowych, w szczególności RODO i dyrektywy 2002/58/WE.

V. Perspektywy

1. Akty delegowane

44. W rozporządzeniu przewidziano powierzenie Komisji uprawnień do przyjęcia **aktów delegowanych** na warunkach określonych w art. 87 DSA¹¹². Mogą być one przyjmowane w następujących obszarach:
- kryteria identyfikacji bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych¹¹³,
 - etapy procedury, metodyki audytowe i wzory sprawozdań w odniesieniu do audytów¹¹⁴,
 - specyfikacje techniczne dotyczące wniosków o dostęp do danych dostawców bardzo dużych platform internetowych lub bardzo dużych wyszukiwarek internetowych¹¹⁵,
 - szczegółowe metodyki i procedury określania opłaty nadzorczej¹¹⁶.
45. Zgodnie z art. 290 ust. 2 lit. b TFUE akt delegowany może wejść w życie tylko wtedy, gdy Parlament Europejski lub Rada **nie wyrażą wobec niego sprzeciwu**. Jak podkreśla się w motywie 152 DSA, ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodne z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z 13.04.2016 r. w sprawie lepszego stanowienia prawa. Aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, Komisja jest zobowiązana przekazywać tym instytucjom wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą

¹¹² Zob. komentarz do art. 87 DSA.

¹¹³ Zob. art. 24 ust. 2, art. 33 ust. 2 i 3 DSA.

¹¹⁴ Zob. art. 37 ust. 7 DSA.

¹¹⁵ Zob. art. 40 ust. 13 DSA.

¹¹⁶ Zob. art. 43 ust. 3, 4 i 5 DSA. Szerzej zob. komentarz do art. 87 DSA.

systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych¹¹⁷.

46. Na podstawie art. 43 ust. 4 DSA Komisja **wydała rozporządzenie delegowane** (UE) 2023/1127 z 2.03.2023 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 o szczegółową metodykę i procedury dotyczące opłat nadzorczych pobieranych przez Komisję od dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych.
47. Komisja przedstawiła również **projekt rozporządzenia delegowanego** ustanawiającego na podstawie art. 37 ust. 7 DSA zasady przeprowadzania audytów bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych¹¹⁸.

2. Akty wykonawcze

48. Komisji w rozporządzeniu powierzono **uprawnienia wykonawcze** w odniesieniu do następujących obszarów:
- ustanowienia wzorów określających formę, treść i inne szczegóły sprawozdań dotyczących moderowania treści¹¹⁹;
 - określenia kwoty rocznej opłaty nadzorczej pobieranej od dostawców bardzo dużych platform internetowych oraz bardzo dużych wyszukiwarek internetowych¹²⁰;
 - ustanawiania praktycznych ustaleń dotyczących postępowania, wysłuchania i wynegocjowanego ujawnienia informacji w kontekście nadzoru, dochodzenia, egzekwowania i monitorowania w odniesieniu do dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych¹²¹;
 - określenia praktycznych i operacyjnych ustaleń na potrzeby funkcjonowania systemu wymiany informacji i jego interoperacyjności z pozostałymi odpowiednimi systemami¹²².
49. Uprawnienia są wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 z 16.02.2011 r. **ustanawiającym przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję**.
50. Przyjmowanie aktów wykonawczych przez Komisję odbywa się w **procedurze doradczej**, o której mowa w art. 88 DSA (procedura komitetowa)¹²³.

¹¹⁷ Motyw 152 DSA.

¹¹⁸ Document Ares(2023)3171302.

¹¹⁹ Zob. art. 15 ust. 3, art. 24 ust. 6 DSA.

¹²⁰ Zob. art. 43 ust. 3 DSA.

¹²¹ Zob. art. 83 DSA.

¹²² Zob. art. 85 ust. 3 oraz motyw 151 DSA.

¹²³ Szerzej zob. komentarz do art. 88 DSA.

51. Na podstawie wskazanego przepisu art. 83 DSA Komisja przyjęła rozporządzenie wykonawcze (UE) 2023/1201 z 21.06.2023 r. w sprawie szczegółowych zasad dotyczących prowadzenia przez Komisję niektórych postępowań na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 (akt o usługach cyfrowych).

3. Akty krajowe

52. Zgodnie z motywem 9 DSA akt o usługach cyfrowych **w pełni harmonizuje** przepisy mające zastosowanie do usług pośrednich na rynku wewnętrznym. Państwa członkowskie **nie mogą zatem przyjmować lub utrzymywać w mocy dodatkowych wymogów krajowych w odniesieniu do spraw objętych zakresem rozporządzenia**, chyba że w rozporządzeniu przewidziano stosowne wyjątki. Miałoby to wpływ na bezpośrednie i jednolite stosowanie w pełni zharmonizowanych przepisów mających zastosowanie do dostawców usług pośrednich zgodnie z jego celami. Nie powinno to jednak wykluczać możliwości stosowania innych przepisów krajowych mających zastosowanie do dostawców usług pośrednich, zgodnie z prawem Unii, w tym dyrektywy 2000/31/WE, w szczególności z jej art. 3, w przypadku gdy przepisy prawa krajowego służą realizacji uzasadnionych celów leżących w interesie publicznym, innych niż cele rozporządzenia.
53. W konsekwencji zakres swobody legislacyjnej państw członkowskich ograniczony został, w obszarze harmonizowanym, do przypadków określonych w rozporządzeniu lub wynikających z generalnego zakresu zastosowania przez Unię. W rozporządzeniu zawarto m.in. następujące **klauzule kompetencyjne**:
- art. 9 ust. 2 DSA, na podstawie którego państwa członkowskie zostały upoważnione do przyjęcia przepisów stanowiących podstawę nakładania i egzekwowania nakazów **podjęcia działań przeciwko nielegalnym treściom**, a także wprowadzenia dodatkowych warunków wydawania takich nakazów. W tym zakresie prawo krajowe powinno być zgodne, na co wskazuje wprost art. 9 ust. 2 DSA, z prawem Unii, w tym KPP UE i postanowieniami TFUE dotyczącymi swobody przedsiębiorczości i swobody świadczenia usług wewnątrz Unii, w szczególności w odniesieniu do usług gier hazardowych i zakładów¹²⁴;
 - art. 10 ust. 2 DSA stanowiący zobowiązanie dla państw członkowskich, by w przepisach stanowiących podstawę do wydawania nakazu udzielenia informacji określone zostały wskazane w tym przepisie **minimalne warunki takich nakazów**. Warunki i wymogi ustanowione mają jednak pozostać bez uszczerbku dla krajowego prawa cywilnego procesowego i krajowego prawa karnego procesowego;
 - art. 21 ust. 6 DSA uprawniający państwa członkowskie do **ustanowienia organów pozasądowego rozstrzygania sporów**;
 - art. 49 ust. 1 i 2 DSA zobowiązujący państwa członkowskie do wyznaczenia co najmniej jednego właściwego **organu odpowiedzialnego za nadzorowanie dostawców**

¹²⁴ Zob. również motyw 32 DSA.