

AKT O USŁUGACH CYFROWYCH

Komentarz

redakcja naukowa Mirosław Gumularz

Katarzyna Araczewska, Agata Domańska, Mateusz Franke
Agnieszka Grzelak, Mirosław Gumularz, Tomasz Izydorec
Artur Piechocki, Natalia Polańska, Martyna Popiołek-Dębska
Mirosław Wróblewski, Jan Ząbczyk

AKT O USŁUGACH CYFROWYCH

Komentarz

redakcja naukowa Mirosław Gumularz

Katarzyna Araczewska, Agata Domańska, Mateusz Franke
Agnieszka Grzelak, Mirosław Gumularz, Tomasz Izydorczyk
Artur Piechocki, Natalia Polańska, Martyna Popiołek-Dębska
Mirosław Wróblewski, Jan Ząbczyk

Stan prawny na 25 stycznia 2024 r.

Recenzent

Dr hab. Paweł Fajgielski, prof. Katolickiego Uniwersytetu Lubelskiego Jana Pawła II

Wydawczyni

Monika Pawłowska

Redaktorka prowadząca

Joanna Cybulska

Opracowanie redakcyjne

Trzy Kropki Joanna Maż

Projekt okładek serii

Wojtek Janikowski, Przemek Dębowski

Komentarze do poszczególnych przepisów napisali:

Katarzyna Araczeńska: art. 25

Agata Domańska: art. 29–30

Mateusz Franke: art. 21, 26–27, 31–32, 38–39

Agnieszka Grzelak, Mirosław Wróblewski: art. 49–63

Mirosław Gumularz: art. 1–20 (z wyjątkiem pkt 4.3 komentarza do art. 1
i art. 3 lit. m), art. 22–24, 28, 44–48, 64–67, 70–73, 86–93

Tomasz Izydorczyk: załącznik

Artur Piechocki: pkt 4.3 do art. 1

Natalia Polańska: art. 68–69

Martyna Popiołek-Dębska: art. 74–85

Jan Ząbczyk: art. 3 lit. m, 33–37, 40–43

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

ISBN 978-83-8358-323-5

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@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

Wykaz skrótów	33
Przedmowa	41
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)	43
Rozdział I	
Przepisy ogólne	115
Artykuł 1. Przedmiot i zakres stosowania	115
1. Kwestie wstępne	115
1.1. DSA w kontekście dyrektywy 2000/31	115
1.2. Zmiana podejścia regulacyjnego	116
2. DSA a dyrektywa 2000/31 i ustawa o świadczeniu usług drogą elektroniczną	119
2.1. DSA a dyrektywa 2000/31	119
2.2. DSA a ustawa o świadczeniu usług drogą elektroniczną – przegląd wymogów	120
2.3. DSA a ustawa o świadczeniu usług drogą elektroniczną w zakresie kluczowych pojęć	124
2.4. Konsekwencje braku stosowania ustawy o świadczeniu usług drogą elektroniczną	125
3. Przepisy DSA a różne kategorie dostawców usług pośrednich	126
3.1. Struktura piramidy	126
3.2. Przekrój regulacji	126
4. Kwestie szczegółowe	136
4.1. Kwestia neutralności technologicznej	136
4.2. <i>Shadow banning</i> (ukryte blokowanie)	138
4.3. System nazw domen internetowych jako usługa pośrednia	140

Artykuł 2. Zakres stosowania	144
1. Zakres regulacji	145
1.1. Zasięg terytorialny DSA	145
1.2. Zakres przedmiotowy	147
1.3. Zakres podmiotowy	147
1.4. Paradoks stosowania DSA	147
2. Brak wpływu na stosowanie dyrektywy 2000/31	148
3. Przepisy ustanowione w innych aktach prawnych UE regulujących inne aspekty świadczenia usług pośrednich na rynku wewnętrznym lub określających i uzupełniających DSA – wybrane problemy	149
3.1. Rozporządzenie 2021/784	149
3.1.1. Zakres	149
3.1.2. Treści terrorystyczne	149
3.1.3. Dostawcy usług hostingowych	150
3.2. Prawo autorskie	152
3.3. Przepisy prawa UE w dziedzinie ochrony danych osobowych, w szczególności RODO i dyrektywy 2002/58	154
3.3.1. Wzajemne odesłania RODO i DSA	154
3.3.2. Dostawca jako administrator/współadministrator danych lub podmiot przetwarzający	155
Artykuł 3. Definicje	156
a) „usługa społeczeństwa informacyjnego”	156
1. Usługa społeczeństwa informacyjnego – kontekst regulacyjny	156
1.1. Pojęcie usługi społeczeństwa informacyjnego w rozumieniu dyrektywy 2015/1535	156
1.1.1. Świadczenie usługi na odległość	156
1.1.2. Świadczenie usługi drogą elektroniczną	157
1.1.3. Świadczenie usługi na indywidualne żądanie odbiorcy usług	157
1.2. Problemy szczególne	158
1.2.1. Problem wynagrodzenia (uzyskiwanej korzyści)	158
1.2.2. Elektroniczny charakter na przykładzie platform pośrednictwa	159
1.2.2.1. Sprawa Ubera	159
1.2.2.2. Sprawa Airbnb	161
1.2.3. Sektor publiczny a usługi społeczeństwa informacyjnego	162
2. Usługa społeczeństwa informacyjnego a usługa świadczona drogą elektroniczną	163
2.1. Siatka pojęciowa	163
2.2. Usługi „mieszane”	167

b)	„odbiorca usługi”	167
1.	Kwestie ogólne	167
2.	Problemy szczególne	168
2.1.	Relacja umowna czy pozaumowna?	168
2.2.	Usługobiorca a role w ramach ochrony danych osobowych	170
c)	„konsument”	170
1.	Zagadnienia wstępne	170
1.1.	Elementy definicji i szerszy kontekst regulacyjny	170
1.2.	Relatywizacja ochrony	171
2.	Podwójny cel	172
d)	„oferować usługi w Unii”	172
1.	Kontekst regulacyjny	172
2.	Istotne powiązania	173
e)	„istotne powiązanie z Unią”	173
f)	„przedsiębiorca”	174
g)	„usługa pośrednia”	175
1.	Usługa pośrednia i węższe kategorie	175
2.	Usługa pośrednia a platforma pośrednictwa	176
2.1.	Przykłady platform pośrednictwa	176
2.2.	Definicja usługi pośrednictwa w rozporządzeniu 2019/1150	177
2.3.	Dostawca usługi pośredniej a dostawca usługi pośrednictwa internetowego	178
2.4.	Pośrednictwo w DSA	179
3.	Definicja usługi pośredniej a kwestia przesłanek odpowiedzialności	179
4.	Kwestia przechowywania informacji	180
5.	Inne przykłady usług pośrednich	181
h)	„nielegalne treści”	182
1.	Kontekst regulacyjny	182
2.	Motywy DSA	185
3.	Stanowisko Komisji Europejskiej odnośnie do treści nielegalnych	186
4.	Kwestia dezinformacji	187
5.	Różnice między państwami członkowskimi i ich konsekwencje	187
5.1.	Konfiguracje możliwych konfliktów	187
5.2.	Ograniczenie arbitralności	188
5.3.	Stanowisko Komisji Europejskiej i praktyczne konsekwencje	188
5.4.	Przykłady kategorii treści nielegalnych lub naruszających warunki umowy	191
5.5.	Swoboda określania treści naruszających warunki umowy	192
i)	„platforma internetowa”	192
1.	Kontekst regulacyjny	192
2.	Rozumienie platform internetowych – ujęcie szerokie i kontekst DSA	193
3.	Motywy DSA	194

j) „wyszukiwarka internetowa”	195
1. Kontekst regulacyjny	196
2. Cechy wyszukiwarki internetowej	196
k) „publiczne rozpowszechnianie”	197
1. Kontekst regulacyjny	197
2. Znaczenie	197
l) „umowa zawierana na odległość”	198
1. Kontekst regulacyjny	198
2. Pojęcie umowy zawieranej na odległość na gruncie dyrektywy 2011/83	199
3. Pojęcie konsumenta	199
4. Zakres dyrektywy a regulacja DSA	200
m) „interfejs internetowy”	200
n) „koordynator ds. usług cyfrowych właściwy dla miejsca siedziby”	201
o) „koordynator ds. usług cyfrowych właściwy dla miejsca przeznaczenia”	201
1. Motywy DSA	201
2. Kontekst regulacyjny	202
p) „aktywny odbiorca platformy internetowej”	203
q) „aktywny odbiorca wyszukiwarki internetowej”	203
1. Kontekst regulacyjny	203
2. Wyjaśnienie motywów DSA (motyw 77 DSA)	204
r) „reklama”	204
1. Kontekst regulacji	204
2. Pojęcie reklamy	205
s) „system rekomendacji”	205
1. Kontekst regulacji	205
2. System rekomendacji	205
t) „moderowanie treści”	206
1. Kontekst regulacyjny	206
2. Cel wprowadzenia pojęcia	207
3. Moderowanie treści w kontekście informacji niezgodnych z warunkami korzystania z ich usług	208
4. Cele i środki moderowania treści	209
5. Automatyzacja moderacji	210
u) „warunki korzystania z usług”	211
1. Kontekst regulacyjny	211
2. Kwestia umowy	213
v) „osoby z niepełnosprawnościami”	213
1. Definicja wynikająca z dyrektywy 2019/882	213
2. Kontekst regulacyjny	214
w) „informacja handlowa”	214
1. Definicja i motywy dyrektywy 2000/31	214

2. Kontekst regulacyjny	215
x) „obrót”	215
1. Odesłanie do rozporządzenia 139/2004	215
2. Kontekst regulacyjny	217
Rozdział II	
Odpowiedzialność dostawców usług pośrednich	219
1. Dostawca	219
1.1. Pojęcie dostawcy usługi pośredniej	219
1.2. Kwestia pasywności a neutralności – między kryteriami kwalifikacji a kryteriami braku odpowiedzialności dostawcy	220
1.3. Złożoność problemu regulacji odpowiedzialności dostawcy	223
2. Mechanizm wyłączenia odpowiedzialności	223
2.1. Horyzontalny charakter wyłączenia	223
2.2. Kogo chroni wyłączenie	224
2.3. Odpowiedzialność dostawcy RODO	224
2.4. Przesłanki odpowiedzialności dostawcy	224
2.5. Możliwe podstawy roszczeń (na gruncie prawa polskiego) względem usługodawcy, które wejdą w grę, gdy nie znajdzie zastosowania art. 4–6 DSA, tj. mechanizm wyłączenia odpowiedzialności	228
2.6. Ciężar dowodu na przykładzie ochrony danych osobowych i relacji między art. 82 RODO i art. 24 k.c.	229
2.7. Section 230 (amerykańska regulacja dotycząca odpowiedzialności dostawców)	230
2.8. Kwestia dochodzenia roszczeń w przypadku treści naruszających warunki umowy	231
2.9. Naruszenie DSA – podstawa odpowiedzialności cywilnoprawnej	232
2.10. Rozliczalność	232
Artykuł 4. „Zwykły przekaz”	233
1. Kwestie ogólne	233
1.1. Pojęcie zwykłego przekazu	233
1.2. Mechanizm wyłączenia odpowiedzialności na gruncie dyrektywy 2000/31 i orzecznictwa	234
1.2.1. Dyrektywa 2000/31	234
1.2.2. Motywy dyrektywy 2000/31	234
1.2.3. Pojęcie zwykłego przekazu na gruncie orzecznictwa TSUE	235
1.2.4. Dyrektywa 2000/31 a kontekst DSA	238
1.3. Przykłady i kwestie budzące wątpliwości	239
1.3.1. Przykłady wskazane w DSA	239
1.3.2. Kwestia nr IP	240

2. Przesłanki wyłączenia odpowiedzialności	240
2.1. Przesłanki	240
2.2. Sieć telekomunikacyjna	241
2.3. Kwestia modyfikacji informacji zawartych w transmisji	241
2.4. Filtrowanie i wyłączenie odpowiedzialności	242
Artykuł 5. „Caching”	242
1. Kwestie ogólne	243
1.1. Pojęcie cachingu	243
1.2. Mechanizm wyłączenia odpowiedzialności na gruncie dyrektywy 2000/31	243
1.2.1. Dyrektywa 2000/31	243
1.2.2. Motywy dyrektywy 2000/31	244
1.2.3. Dyrektywa 2000/31 a kontekst DSA	244
1.2.4. Przykłady w DSA	245
2. Przesłanki wyłączenia odpowiedzialności	246
2.1. Podejście na gruncie dyrektywy 2000/31	246
2.2. Przesłanki wyłączenia odpowiedzialności na gruncie DSA	246
Artykuł 6. Hosting	247
1. Kwestie ogólne	248
1.1. Pojęcie hostingu na gruncie DSA	248
1.1.1. Informacje przekazane przez odbiorcę usługi	248
1.1.2. Przykłady w DSA	250
1.1.3. Komentowany przepis a inne przepisy DSA	250
1.1.4. Przesłanki wyłączenia odpowiedzialności a przepisy szczególne	251
1.2. Mechanizm wyłączenia odpowiedzialności na gruncie dyrektywy 2000/31 i orzecznictwa	251
1.2.1. Dyrektywa 2000/31	251
1.2.2. Orzecznictwo TSUE na gruncie dyrektywy 2000/31	251
1.2.3. Orzecznictwo sądów polskich na gruncie ustawy o świadczeniu usług drogą elektroniczną – pojęcie hostingu	252
2. Przesłanki wyłączenia odpowiedzialności na gruncie DSA	254
2.1. Motyw 22 DSA	254
2.2. Hosting a pomocnictwo	254
2.3. Ciężar dowodu wiedzy usługodawcy	255
2.4. Wiedza dostawcy w orzecznictwie sądów polskich oraz TSUE	256
2.5. Wiedza z DSA a wiedza o naruszeniu z RODO	259
3. Wymagana reakcja dostawcy	259
3.1. Wymagana reakcja i źródło wiedzy	259
3.2. Reakcja na gruncie art. 6 DSA a działanie w przypadku żądania właściwego organu	260

3.3. Zablokowanie czy usunięcie treści	261
3.4. Pochopna reakcja dostawcy i jej konsekwencja	263
4. Wyłączenie względem platform internetowych umożliwiających zawieranie umów	263
4.1. Zakres wyłączenia	263
4.2. Przesłanki wyłączenia odpowiedzialności	264
4.3. Platformy internetowe a platformy pośrednictwa	264
Artykuł 7. Dobrowolne czynności sprawdzające prowadzone z własnej inicjatywy i zgodność z prawem	266
1. Zakres i cel regulacji	266
1.1. Cel regulacji	266
1.2. Monitorowanie treści niezgodnych z warunkami umowy	268
1.3. Zakres czynności sprawdzających	271
1.4. Monitorowanie a uzyskanie wiedzy	272
1.5. Uprzednia weryfikacja treści nielegalnych i naruszających warunki umowy	272
1.6. Działanie w dobrej wierze i z zachowaniem należytej staranności	273
1.7. Przekroczenie zakresu art. 7 DSA	274
1.8. Adresat czynności	275
2. Monitorowanie a RODO	275
2.1. Filtrowanie treści a RODO	275
2.2. Możliwe podejścia do problemu kwalifikacyjnego	276
Artykuł 8. Brak ogólnych obowiązków w zakresie monitorowania lub aktywnego ustalania faktów	278
1. Zagadnienia ogólne	278
1.1. Cel regulacji	278
1.2. Zakres	279
2. Dyrektywa 2000/31	279
2.1. Orzecznictwo TSUE na gruncie dyrektywy 2000/31	280
2.1.1. Przykładowa matryca	282
2.1.2. Przegląd poszczególnych (wybranych) spraw	282
2.1.3. Podsumowanie	287
2.2. Przykłady orzeczeń sądów polskich	288
3. Monitorowanie treści zgodnie z art. 8 DSA a kwestia oceny ryzyka	288
Artykuł 9. Nakaz podjęcia działań przeciwko nielegalnym treściom	289
1. Cel i zakres regulacji	291
1.1. Funkcja regulacji	291
1.2. Zakres obowiązków – podsumowanie	293
1.3. Zakres zastosowania i problem odesłania	294
1.4. Kwestia terytorialna	295

2. Kwestie szczegółowe	295
2.1. Termin	295
2.2. Potencjalne naruszenia DSA, które nie dotyczą dostawców	295
2.3. Obowiązki dostawcy względem odbiorców usługi	296
2.4. Kwestia przepisów szczególnych krajowych i unijnych	297
Artykuł 10. Nakazy udzielenia informacji	298
1. Cel i zakres regulacji	300
1.1. Funkcja regulacji	300
1.2. Zakres obowiązków – podsumowanie	301
1.3. Odwołanie do art. 9 DSA	301
 Rozdział III	
Obowiązki w zakresie należytej staranności na potrzeby przejrzystego i bezpiecznego środowiska internetowego	303
 Sekcja 1	
Obowiązki mające zastosowanie do wszystkich dostawców usług pośrednich	303
Artykuł 11. Punkty kontaktowe dla organów państw członkowskich, Komisji i Rady Usług Cyfrowych	303
1. Zakres i cel regulacji	304
1.1. Typy punktów kontaktowych	304
1.2. Cele regulacji	305
1.3. Zakres regulacji	305
2. Kwestie szczegółowe	305
2.1. Kontekst innych przepisów	305
2.2. Kto może skorzystać z punktu kontaktowego	305
2.3. Obowiązki informacyjne	306
2.4. Kwestia języków	306
Artykuł 12. Punkty kontaktowe dla odbiorców usług	307
1. Kwestie ogólne	307
1.1. Cel i zakres regulacji	307
1.2. Sposób komunikacji	307
1.3. Uzupełnienie wymogów dyrektywy 2000/31	308
Artykuł 13. Przedstawiciele prawni	309
1. Cel i zakres regulacji	310
1.1. Cel regulacji	310
1.2. Zakres podmiotowy regulacji	311
1.3. Kwestie wątpliwe dotyczące zakresu stosowania przepisu	311
1.3.1. Siedziba dostawcy	311
1.3.2. Oferowanie usługi	311
1.4. Miejsce zamieszkania lub siedziba przedstawiciela	312
1.5. Kompetencje merytoryczne przedstawiciela	312

2. Obowiązki i odpowiedzialność dostawcy i przedstawiciela	313
2.1. Przedstawiciel	313
2.2. Dostawca – przegląd obowiązków	313
2.3. Obowiązek informacyjny dostawcy	315
Artykuł 14. Warunki korzystania z usług	315
1. Cel i zakres regulacji	316
1.1. Kwestie ogólne	316
1.2. Zakres zastosowania	316
1.3. Kwestie konsumenckie	318
1.4. Inne regulacje a DSA	319
1.5. Odbiorca	320
1.6. Wpływ na swobodę kontraktowania	320
1.7. Obowiązki informacyjne – czego brakuje?	321
2. Zakres obowiązków	322
2.1. Wszelkie ograniczenia względem informacji przekazywanych przez odbiorców usługi	322
2.2. Ograniczenia a aktywne filtrowanie treści	325
2.3. Informacje o istotnych zmianach warunków	326
2.4. Małoletni	326
2.5. Stosowanie i egzekwowanie ograniczeń	328
2.6. Ograniczenia z art. 14 ust. 4 DSA a inne typy ograniczeń	329
2.7. Elementy warunków umowy – podsumowanie	329
Artykuł 15. Obowiązki sprawozdawcze w zakresie przejrzystości spoczywające na dostawcach usług pośrednich	332
1. Kwestie wstępne	333
1.1. Zakres	333
1.2. Pojęcie mikro- i małego przedsiębiorstwa	334
1.3. Sposób i zawartość publikacji	334
2. Treść sprawozdania	334
Sekcja 2	
Dodatkowe przepisy mające zastosowanie do dostawców usług hostingu, w tym platform internetowych	340
Artykuł 16. Mechanizmy zgłaszania i działania	340
1. Zakres i cel regulacji	341
1.1. Cel regulacji – mechanizm zgłoszenia i działania	341
1.2. Zakres podmiotowy	342
1.3. Zakres przedmiotowy – kategoria treści	343
1.4. Zakres obowiązków	343
2. Kwestie szczegółowe	344
2.1. Elementy zgłoszenia	344
2.2. Anonimowość a etap przyjęcia zgłoszenia	345

3. Reakcja na zgłoszenie	347
3.1. Standard staranności (art. 16 ust. 6 DSA)	347
3.2. Terminowość po stronie dostawcy na gruncie komentowanego przepisu	348
3.3. Powiązanie z art. 6 DSA	349
3.4. Nadużycia po stronie zgłaszającego	350
3.5. Informacja zwrotna	350
Artykuł 17. Uzasadnienie	351
1. Zakres i cel regulacji	352
1.1. Zakres regulacji	352
1.2. Cel regulacji	353
1.3. Wyłączenia	354
1.4. Relacja do art. 6 DSA	354
2. Uzasadnienie	355
2.1. Kryteria prawidłowego sformułowania uzasadnienia	355
2.2. Moment przekazania informacji	355
2.3. Sposób przekazania informacji i problem etykietowania	356
2.4. Dane kontaktowe	358
2.5. Elementy uzasadnienia	358
Artykuł 18. Zawiadomienie o podejrzeniu popełnienia przestępstwa	359
1. Cel i zakres regulacji	359
1.1. Motywy regulacji	359
1.2. Dostawca usług	360
1.3. Pojęcie przestępstwa zagrażającego życiu lub bezpieczeństwu osoby lub osób	360
2. Obowiązki	361
2.1. Adresat informacji	361
2.2. Kwestia aktywnego przeszukiwania treści	362
2.3. Inne obowiązki	362
2.4. Sankcje	363
Sekcja 3	
Dodatkowe przepisy mające zastosowanie do platform internetowych	363
Artykuł 19. Wyłączenie dotyczące mikroprzedsiębiorstw i małych przedsiębiorstw	363
Artykuł 20. Wewnętrzny system rozpatrywania skarg	364
1. Zakres i cel regulacji	365
1.1. Cel regulacji	365
1.2. Zakres regulacji – podmioty odpowiedzialne	366
1.3. Zakres regulacji – podmioty uprawnione	366
1.4. Zakres regulacji – przedmiot skargi	367
2. Procedura	369
2.1. Wstrzymanie wykonania decyzji	369

2.2. Termin wniesienia skargi	369
2.3. Dostępność procedur	369
2.4. Kwalifikacje personelu i automatyczne decyzje	369
2.5. Uzasadnienie a skarga	370
2.6. Kryteria prawidłowego działania	370
2.7. Obowiązek działania po stronie dostawcy w przypadku zasadności skargi	371
2.8. Odpowiedzialność	371
Artykuł 21. Pozasądowe rozstrzyganie sporów	372
1. Kwestie wstępne	375
1.1. Adresaci normy	375
1.2. Cel i przedmiot regulacji	375
2. Pozasądowe rozstrzyganie sporów w DSA – zagadnienia ogólne	376
2.1. Uprawnieni do skorzystania z pozasądowego rozstrzygnięcia sporu	376
2.2. Przedmiot postępowania	377
2.3. Wybór organu pozasądowego rozstrzygania sporów przez odbiorców usług i zgłaszających	378
2.4. Obowiązek informacyjny	379
2.5. Pozasądowe rozstrzyganie sporów a prawo do sądu	379
2.6. Postępowanie w sprawie pozasądowego rozstrzygnięcia sporu a przedawnienie	380
2.7. Współpraca z organem pozasądowego rozstrzygania sporów	381
2.8. Obowiązek dostawcy platformy udziału w postępowaniu	382
2.9. Niewiążący charakter rozstrzygnięcia	383
2.10. Prawo właściwe	385
3. Certyfikacja organów pozasądowego rozstrzygania sporów	389
3.1. Ogólne zasady	389
3.2. Warunki certyfikacji	389
3.2.1. Bezstronność i niezależność	390
3.2.2. Niezbędna wiedza ekspercka	390
3.2.3. Wynagrodzenie członków niepowiązane z wynikiem	391
3.2.4. Łatwa dostępność	391
3.2.5. Szybkość, skuteczność i oszczędność oraz język postępowania	392
3.2.6. Jasny i sprawiedliwy regulamin wewnętrzny	393
3.3. Certyfikat	394
3.4. Sprawozdanie organu pozasądowego rozstrzygania sporów	394
3.5. Sprawozdanie koordynatora ds. usług cyfrowych	395
4. Termin rozstrzygnięcia sprawy	395

5. Opłaty i wydatki	396
5.1. Rozstrzygnięcie na korzyść odbiorcy usługi	396
5.2. Rozstrzygnięcie na korzyść dostawcy platformy internetowej	397
5.3. Wysokość opłat	397
5.4. Krytyka	399
6. Publiczne organy pozasądowego rozstrzygania sporów	399
7. Cofnięcie certyfikacji	400
8. Zgłoszenie Komisji	400
9. Stosunek do innych regulacji unijnych z zakresu pozasądowego rozstrzygania sporów	401
9.1. Stosunek do dyrektywy 2013/11	401
9.2. Stosunek do rozporządzenia 2019/1150	402
9.3. Stosunek do dyrektywy 2019/790	403
9.4. Stosunek do dyrektywy 2010/13	405
10. Wejście w życie i stosowanie	406
Artykuł 22. Zaufane podmioty sygnalizujące	407
1. Zakres i cel regulacji	408
1.1. Motywy DSA	408
1.2. Korzyści i ryzyka	409
1.3. Zakres dostawców, których dotyczą (dodatkowe) obowiązki	409
1.4. Zaufane podmioty sygnalizujące a sygnaliści w rozumieniu dyrektywy 2019/1937	410
2. Kwestie szczegółowe	411
2.1. Status zaufanego podmiotu sygnalizującego	411
2.2. Obowiązki dostawców	413
2.3. Obowiązki zaufanych podmiotów sygnalizujących	415
Artykuł 23. Środki podejmowane przeciwko nadużywaniu i ochrona przed nim	415
1. Zakres i cel regulacji	416
1.1. Zakres i cel regulacji	416
1.2. Motywy DSA i cele regulacji	417
1.3. Dwa przypadki nadużycia	417
1.4. Pojęcie oczywiście nielegalnych treści, a także zgłoszeń lub skarg	418
1.5. Przykład RODO	418
2. Realizacja wymogów	419
2.1. Uprawnienie czy obowiązek?	419
2.2. Intensywność reakcji	419
2.3. Zakres swobody i dalej idące środki	420
2.4. Naruszenie wymogów art. 23 DSA – scenariusze	421
2.5. Konsekwencje reakcji dostawcy	421
2.6. Odpowiedzialność nadużywającego	422
3. Podsumowanie	422

Artykuł 24. Obowiązki sprawozdawcze w zakresie przejrzystości spoczywające na dostawcach platform internetowych	423
1. Zakres i cel regulacji	424
1.1. Cel regulacji	424
1.2. Zakres regulacji	424
1.3. Dodatkowe obowiązki sprawozdawcze	425
Artykuł 25. Projekt i organizacja interfejsów internetowych	426
1. Uwagi ogólne	426
2. Definicja praktyk typu dark patterns	428
2.1. Interfejs internetowy	429
2.2. Negatywny wpływ na zdolność odbiorców usługi do podejmowania wolnych i świadomych decyzji	430
2.3. Sposoby ograniczania wolnych i świadomych wyborów	433
2.4. Dopuszczalność stosowania perswazji	435
2.5. Intencjonalność i skuteczność zwodniczych interfejsów	435
3. Kategorie i przykłady	436
4. Zakres zakazu	439
5. Relacje z przepisami z zakresu ochrony konsumentów i ochrony danych	440
Artykuł 26. Reklamy na platformach internetowych	442
1. Kwestie wstępne	442
1.1. Adresaci normy	442
1.2. Cel i przedmiot regulacji	443
2. Reklama	444
2.1. Wynagrodzenie	444
2.2. Prezentowanie na interfejsie internetowym	445
2.3. Propagowanie	446
2.4. Reklama a informacja handlowa	447
3. Informacje dotyczące reklamy	448
3.1. Zakres informacji	449
3.1.1. Oznaczenie reklamy	449
3.1.2. Wskazanie reklamodawcy	449
3.1.3. Wskazanie płatnika	450
3.1.4. Główne parametry wykorzystywane do określenia odbiorcy	450
3.1.5. Źródło informacji dotyczących reklamy	453
3.1.6. Obowiązki dostawcy platformy a jego rola w ekosystemie reklamie internetowej	453
4. Zgłaszanie i oznaczanie informacji handlowych	454
5. Zakaz reklamy opartej na profilowaniu na podstawie szczególnych kategorii danych	456
5.1. Profilowanie	456

5.2. Szczególne kategorie danych	457
5.3. Krytyka i kontrowersje	458
6. Art. 26 DSA a inne regulacje	460
6.1. Relacja do art. 27 i 38 DSA	460
6.2. RODO	460
6.3. Dyrektywa 2002/58	461
6.4. Dyrektywa 2010/13	462
6.5. Dyrektywa 2005/29	462
6.6. Dyrektywa 2000/31	462
7. Normy i kodeksy postępowania	463
8. Wejście w życie i stosowanie	463
Artykuł 27. Przejrzystość systemu rekomendacji	464
1. Kwestie wstępne	464
1.1. Adresaci normy	464
1.2. Cel i przedmiot regulacji	466
2. System rekomendacji	468
2.1. Definicja	468
2.2. Systemy algorytmiczne	469
2.2.1. Systemy rekomendacji oparte na treści (zawartości)	469
2.2.2. Systemy rekomendacji oparte na filtrowaniu kolaboratywnym	470
2.2.3. Hybrydowe systemy rekomendacji	470
2.3. Sugerowanie i szeregowanie prezentowanych informacji w interfejsie internetowym	470
3. Obowiązki informacyjne dotyczące systemów rekomendacji	471
3.1. Warunki korzystania z usług	471
3.2. Prosty i przystępny język	472
3.3. Szczegółowość informacji	474
3.4. Główne parametry	474
3.5. Opcje zmieniania głównych parametrów lub wpływania na nie	475
3.6. Funkcjonalność wyboru i zmiany głównych parametrów	478
3.7. Wyjaśnienie głównych parametrów	478
4. Art. 27 DSA a inne regulacje	480
4.1. Rozporządzenie 2019/1150	480
4.2. Dyrektywa 2019/2161	482
4.2.1. Dyrektywa 2005/29	482
4.2.2. Dyrektywa 2011/83	484
4.3. DMA	484
4.4. Krytyka	485
5. Inne przepisy DSA dotyczące systemów rekomendacji	485
6. Wejście w życie i stosowanie	486

Artykuł 28. Ochrona małoletnich w internecie	486
1. Kwestie ogólne	486
1.1. Zakres regulacji	486
1.2. Małoletni	487
2. Kwestie szczegółowe	488
2.1. Kwestia minimalizacji	488
2.2. Obowiązki dostawcy	489
2.3. Profilowanie	492
Sekcja 4	
Dodatkowe przepisy dotyczące dostawców platform internetowych umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość	494
Artykuł 29. Wyłączenie dotyczące mikroprzedsiębiorstw i małych przedsiębiorstw	494
1. Uwagi ogólne	494
2. Definicje mikroprzedsiębiorstwa i małego przedsiębiorstwa	495
3. Definicja bardzo dużej platformy internetowej	496
Artykuł 30. Identyfikowalność przedsiębiorców	497
1. Informacje ogólne	499
2. Obowiązek pozyskania informacji pozwalających na identyfikację przedsiębiorcy	500
3. Weryfikowanie wiarygodności udzielonych przez przedsiębiorcę informacji	502
4. Zawieszenie świadczenia usług i tryb odwoławczy	503
5. Obowiązek przechowywania informacji identyfikujących przedsiębiorcę	505
6. Ujawnienie informacji o przedsiębiorcach osobom trzecim	505
7. Udostępnianie informacji o przedsiębiorcach	506
Artykuł 31. Zgodność w fazie projektowania	507
1. Kwestie wstępne	508
1.1. Adresaci normy	508
1.2. Wyłączenie dotyczące mikro- i małych przedsiębiorstw	509
1.3. Cel i przedmiot regulacji	509
2. Sposób zaprojektowania i organizacji interfejsu	511
2.1. Informacje o podmiocie gospodarczym	511
2.2. Informacje przedkontraktowe	512
2.3. Zgodność	513
2.4. Bezpieczeństwo produktów	517
2.5. Zgodność i bezpieczeństwo produktów a interfejs internetowej platformy handlowej	518
2.6. Minimalny zakres informacji	519
2.7. Rozporządzenie 2023/988 a internetowe platformy handlowe	520

3. Obowiązek weryfikacji	522
3.1. Weryfikacja uprzednia	522
3.2. Weryfikacja następcza	524
3.2.1. Bazy danych i interfejsy w aktualnym stanie prawnym	525
3.2.2. System Safety Gate	527
4. Pozostałe uwagi	527
4.1. Fotokody lub tokeny	527
4.2. Konsekwencje niewykonania obowiązków dostawcy internetowej platformy handlowej	527
5. Wejście w życie i stosowanie	529
Artykuł 32. Prawo do informacji	529
1. Kwestie wstępne	530
1.1. Adresaci normy	530
1.2. Wyłączenie dotyczące mikro- i małych przedsiębiorstw	530
1.3. Cel i przedmiot regulacji	531
1.4. Stosunek do rozporządzenia 2023/988	532
2. Powzięcie wiadomości o nielegalnym produkcie lub nielegalnej usłudze	532
2.1. Powzięcie wiadomości	532
2.2. Nielegalność	534
3. Informacja dla konsumentów	534
3.1. Zakres informacji	534
3.2. Ramy czasowe	535
3.3. Przechowywanie danych	535
4. Brak danych kontaktowych	536
5. Wejście w życie i stosowanie	536
Sekcja 5	
Dodatkowe obowiązki spoczywające na dostawcach bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych w zakresie zarządzania ryzykiem systemowym	537
Artykuł 33. Bardzo duże platformy internetowe i bardzo duże wyszukiwarki internetowe	537
1. Uwagi ogólne dotyczące regulacji bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych	539
1.1. Cel regulacji	539
1.2. Zakres podmiotowy regulacji	540
1.3. Zakres przedmiotowy i metoda regulacji	541
2. Kryteria kwalifikacji określonych podmiotów jako dostawców bardzo dużych platform internetowych lub dostawców bardzo dużych wyszukiwarek internetowych	541

3. Kryterium minimalnej średniej liczby miesięcznie aktywnych odbiorców usługi w Unii	542
3.1. Minimalna średnia liczba miesięcznie aktywnych odbiorców usługi w Unii i jej zmiany	542
3.2. Okres, za jaki powinna być mierzona średnia liczba miesięcznie aktywnych odbiorców usługi w Unii oraz częstotliwość pomiarów	543
3.3. Rozumienie pojęcia aktywnego odbiorcy usługi w Unii	544
3.4. Techniczny sposób mierzenia rzeczywistej liczby aktywnych odbiorców usług w Unii	546
3.5. Metodyka obliczania średniej liczby aktywnych miesięcznie odbiorców usług w Unii	547
4. Postępowanie Komisji w celu uznania danego podmiotu za dostawcę bardzo dużej platformy internetowej lub dostawcę bardzo dużej wyszukiwarki internetowej	547
4.1. Uwagi ogólne	547
4.2. Wszczęcie i przebieg postępowania	548
4.3. Postępowanie sporne	549
4.4. Publikacja decyzji i termin rozpoczęcia wykonywania obowiązków	550
4.5. Dotychczas opublikowane informacje i podjęte decyzje	551
5. Postępowanie Komisji w celu zniesienia wskazania danego podmiotu jako dostawcę bardzo dużej platformy internetowej lub dostawcę bardzo dużej wyszukiwarki internetowej	553
5.1. Przestanki	553
5.2. Publikacja decyzji i termin ustania stosowania obowiązków	553
Artykuł 34. Ocena ryzyka	554
1. Uwagi ogólne	555
1.1. Cel regulacji	555
1.2. Zakres podmiotowy regulacji	556
1.3. Zakres przedmiotowy regulacji	557
1.4. Metoda regulacji zarządzania ryzykiem w DSA	557
2. Zasady ogólne przeprowadzania oceny ryzyka	558
2.1. Zakres przedmiotowy oceny ryzyka	558
2.2. Przypadki i terminy przeprowadzania oceny ryzyka	560
2.3. Forma oceny ryzyka i przechowywanie dokumentacji	561
2.4. Procedura zarządzania ryzykiem	562
3. Metoda przeprowadzania oceny ryzyka	562
3.1. Wymóg zachowania należytej staranności	562
3.2. Identyfikacja, analiza i ocena ryzyka	564
3.3. Kategorie ryzyka systemowego	565
3.4. Czynniki mające wpływ na ryzyko	567

3.5. Aspekty regionalne lub językowe	568
3.6. Ciągłość procesów oceny ryzyka	568
4. Audyty w zakresie oceny ryzyka	569
5. Pierwsze postępowanie w związku z naruszeniem m.in. art. 34 ust. 1 i 2 DSA	569
Artykuł 35. Zmniejszanie ryzyka	570
1. Uwagi ogólne	571
1.1. Przedmiot i cel regulacji	571
1.2. Zakres podmiotowy	573
2. Zasady wprowadzania środków zmniejszających ryzyko	573
2.1. Uwagi ogólne	573
2.2. Przykładowe środki zmniejszające ryzyko systemowe wskazane w DSA	575
2.3. Wpływ na prawa podstawowe	578
2.4. Audyty w zakresie wprowadzenia środków zmniejszających ryzyko	579
3. Sprawozdania Rady Usług Cyfrowych	580
3.1. Uwagi ogólne	580
3.2. Identyfikacja ryzyka	581
3.3. Najlepsze praktyki	582
3.4. Aspekt krajowy	582
4. Wytyczne Komisji	583
4.1. Uwagi ogólne	583
4.2. Zakres wytycznych	583
5. Pierwsze postępowanie w związku z naruszeniem m.in. art. 35 ust. 1 DSA	584
Artykuł 36. Mechanizm reagowania kryzysowego	584
1. Uwagi ogólne	586
1.1. Przedmiot i cel regulacji	586
1.2. Zakres podmiotowy	588
2. Przestanki wydania decyzji w ramach mechanizmu reagowania kryzysowego	588
3. Treść decyzji wydanej w ramach mechanizmu reagowania kryzysowego	590
3.1. Zobowiązania, które mogą zostać nałożone na dostawców w ramach decyzji	590
3.2. Ograniczenia w zakresie zobowiązań, które mogą zostać nałożone na dostawców	592
4. Postępowanie w celu wydania decyzji	592
4.1. Wszczęcie postępowania	592
4.2. Charakter prawny zaleceń Rady Usług Cyfrowych	593
4.3. Przebieg postępowania	594

4.4. Publikacja decyzji	595
5. Działania następcze	595
5.1. Uwagi ogólne	595
5.2. Dialog z dostawcami	596
5.3. Monitorowanie stosowania szczególnych środków	596
6. Postępowanie w celu zmiany (w tym cofnięcia) decyzji	597
6.1. Uwagi ogólne	597
6.2. Rodzaje możliwych zmian	598
7. Sprawozdanie ze stosowania szczególnych środków	599
8. Ocena przestrzegania przez dostawców obowiązków z art. 36 DSA	599
Artykuł 37. Niezależny audyt	600
1. Uwagi ogólne	603
1.1. Przedmiot i cel regulacji	603
1.2. Zakres podmiotowy	604
2. Przedmiot i zakres audytów	605
2.1. Uwagi ogólne	605
2.2. Ocena wypełniania obowiązków określonych w rozdziale III DSA	605
2.3. Szczegółowy zakres przedmiotowy oceny wypełniania niektórych obowiązków określonych w rozdziale III DSA	606
2.4. Ocena wypełniania zobowiązań podjętych na podstawie kodeksów postępowania oraz protokołów kryzysowych	607
3. Zasady przeprowadzania audytów	609
3.1. Zasady ogólne	609
3.2. Wymogi dla organizacji audytującej i wybór takiej organizacji przez danego dostawcę	610
3.3. Umowa między audytowanym dostawcą a organizacją audytującą	612
3.4. Współpraca i pomoc między audytowanym dostawcą a organizacją audytującą	613
4. Sprawozdania z audytu	615
4.1. Uwagi ogólne	615
4.2. Elementy sprawozdania z audytu	615
4.3. Brak możliwości przeprowadzenia „pełnego” audytu	617
4.4. Wzór sprawozdania z audytu	617
4.5. Sprawozdanie z audytu inne niż „pozytywne”	617
4.6. Obowiązki sprawozdawcze w zakresie przejrzystości	618
5. Kontrola zgodności z art. 37 DSA	618
Artykuł 38. System rekomendacji	619
1. Kwestie wstępne	619
1.1. Adresaci normy	619
1.2. Cel i przedmiot regulacji	620

2. Opcje rekomendacji nieoparte na profilowaniu	621
2.1. Profilowanie	621
2.2. Opcje nieoparte na profilowaniu	621
2.3. Dostępność opcji nieopartych na profilowaniu	623
3. Problem bardzo dużych wyszukiwarek internetowych	624
3.1. Systemy rekomendacji a wyszukiwarki internetowe	624
3.2. Definicja systemu rekomendacji	624
3.3. Przebieg procesu legislacyjnego	625
3.4. Konsekwencje błędu w procesie legislacyjnym	627
3.5. Stosowanie art. 27 DSA do bardzo dużych wyszukiwarek internetowych	628
4. Dobrowolne normy	629
5. Pozostałe uwagi	629
6. Wejście w życie i stosowanie	630
Artykuł 39. Dodatkowa przejrzystość reklam internetowych	630
1. Kwestie wstępne	631
1.1. Adresaci normy	631
1.2. Cel i przedmiot regulacji	632
1.3. Dostawcy bardzo dużych wyszukiwarek internetowych	632
2. Repozytorium	633
2.1. Umiejscowienie repozytorium i wyszukiwanie, niezawodność	633
2.2. API	634
2.3. Okres przechowywania	634
2.4. Brak danych osobowych	634
2.5. Prawdziwość i kompletność informacji	635
3. Zawartość repozytorium	636
3.1. Treść reklamy	636
3.2. Reklamodawca i finansujący	637
3.3. Okres prezentowania reklamy	637
3.4. Dopasowane reklamy	637
3.5. Informacje handlowe	639
3.6. Liczba odbiorców	641
4. Wyjątki	642
5. Wytyczne i dobrowolne normy	643
6. Pozostałe uwagi	643
7. Wejście w życie i stosowanie	643
Artykuł 40. Dostęp do danych i kontrola danych	644
1. Uwagi ogólne	647
1.1. Przedmiot i cel regulacji	647
1.2. Zakres podmiotowy regulacji	648
2. Dostęp do danych zapewniany koordynatorom ds. usług cyfrowych i Komisji	649

2.1. Zakres udostępnianych danych i sposób ich wykorzystania	649
2.2. Procedura uzyskiwania dostępu i sposób zapewnienia dostępu	650
3. Dostęp do danych zapewniany zweryfikowanym badaczom	651
3.1. Uwagi ogólne	651
3.2. Uzasadniony wniosek badacza	651
3.3. Udzielenie dostępu do danych przez dostawców	653
4. Dostęp do danych dla pozostałych badaczy	653
5. Akty delegowane określające warunki techniczne w zakresie udostępniania danych	654
Artykuł 41. Komórka nadzoru przestrzegania niniejszego rozporządzenia	655
1. Uwagi ogólne	657
1.1. Przedmiot i cel regulacji	657
1.2. Zakres podmiotowy regulacji	657
2. Komórka nadzoru przestrzegania przepisów DSA	658
2.1. Komórka nadzoru jako element drugiej linii obrony	658
2.2. Niezależności komórki nadzoru	658
2.3. Uprawnienia i zasoby komórki nadzoru	660
2.4. Dostęp komórki nadzoru do organu zarządzającego	662
2.5. Skład komórki nadzoru	662
2.6. Kierownik komórki nadzoru	663
2.7. Kompetencje i zadania pracowników komórki nadzoru	664
3. Rola organu zarządzającego w zakresie zarządzania ryzykiem określona w art. 41 DSA	666
Artykuł 42. Obowiązki sprawozdawcze w zakresie przejrzystości	667
1. Uwagi ogólne	668
1.1. Przedmiot i cel regulacji	668
1.2. Zakres podmiotowy regulacji	669
2. Sprawozdania dotyczące moderowania treści	669
2.1. Uwagi ogólne	669
2.2. Elementy dodatkowe sprawozdań dostawców bardzo dużych platform internetowych	669
2.3. Elementy dodatkowe sprawozdań dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych	670
2.4. Forma sprawozdań	670
2.5. Terminy publikowania sprawozdań	671
2.6. Sprawozdania dotyczące moderowania treści jako element badań poprzedzających wszczęcie postępowania w związku z uchybieniami obowiązków DSA	671
3. Sprawozdania dotyczące zarządzania ryzykiem systemowym	672
3.1. Uwagi ogólne	672

3.2. Treść sprawozdań	672
3.3. Przekazywanie sprawozdań i ich publikacja	672
3.4. Usuwanie informacji z publicznie dostępnych sprawozdań	673
Artykuł 43. Opłata nadzorcza	673
1. Uwagi ogólne	675
1.1. Przedmiot i cel regulacji	675
1.2. Zakres podmiotowy regulacji	675
2. Zasady dotyczące ponoszenia opłaty nadzorczej uregulowane w DSA	676
2.1. Zasady obliczania całkowitej kwoty rocznych opłat nadzorczych oraz indywidualnych opłat nadzorczych	676
2.2. Rozporządzenie delegowane	677
3. Szczegółowe zasady dotyczące ponoszenia opłaty nadzorczej uregulowane w rozporządzeniu 2023/1127	678
3.1. Sposób obliczania wysokości indywidualnej opłaty nadzorczej	678
3.2. Procedura płatności	681
 Sekcja 6	
Inne przepisy dotyczące obowiązków w zakresie należytej staranności	681
Artykuł 44. Normy	681
Artykuł 45. Kodeksy postępowania	683
Artykuł 46. Kodeksy postępowania w odniesieniu do reklam internetowych	684
Artykuł 47. Kodeksy postępowania w odniesieniu do dostępności	684
1. Cel i zakres regulacji	685
1.1. Cel regulacji	685
1.2. Typy kodeksów	686
1.3. Cel przyjmowania kodeksów	686
1.4. Kodeksy w przepisach DSA	686
2. Kwestie szczegółowe	687
2.1. Odwołanie do konkretnych kodeksów	687
2.2. Dobrowolność a decyzje KE	688
Artykuł 48. Protokoły kryzysowe	688
1. Kwestie ogólne	690
1.1. Cel regulacji	690
1.2. Praktyczne konsekwencje przyjęcia protokołów	690
 Rozdział IV	
Wdrażanie, współpraca, sankcje i egzekwowanie	692
 Sekcja 1	
Właściwe organy i krajowi koordynatorzy ds. usług cyfrowych	692
Artykuł 49. Właściwe organy i koordynatorzy ds. usług cyfrowych	692
1. Cel i zakres regulacji	693

1.1. Cel i zakres rozdziału IV DSA	693
1.2. Cel art. 49 DSA	694
2. Wyznaczenie właściwego organu	695
3. Koordynator do spraw usług cyfrowych	696
3.1. Wyznaczenie koordynatora	696
3.2. Zadania koordynatora	698
Artykuł 50. Wymogi dotyczące koordynatorów ds. usług cyfrowych	699
1. Cel i zakres regulacji	700
2. Wymóg niezależności koordynatora	701
3. Wymóg zapewnienia koordynatorowi niezbędnych zasobów	703
4. Wymóg zapewnienia niezależności organom właściwym	703
Artykuł 51. Uprawnienia koordynatorów ds. usług cyfrowych	703
1. Cel i zakres regulacji	707
2. Uprawnienia koordynatora ds. usług cyfrowych w zakresie czynności sprawdzających	707
3. Uprawnienia koordynatora ds. usług cyfrowych w odniesieniu do egzekwowania przepisów DSA wobec dostawców	709
4. Uprawnienia koordynatora ds. usług cyfrowych o charakterze <i>ultima ratio</i>	710
5. Regulacja krajowa	711
Artykuł 52. Sankcje	713
1. Zakres i cel przepisu	714
2. Rodzaj i charakter sankcji	715
3. Maksymalna wysokość grzywny	716
4. Okresowa kara pieniężna	716
5. Obowiązek informacyjny państw członkowskich	716
6. Zakres regulacji krajowej	717
Artykuł 53. Prawo do wniesienia skargi	718
1. Cel i zakres przepisu	718
2. Podmioty uprawnione do wniesienia skargi	719
3. Przedmiot skargi	720
4. Właściwość koordynatora	720
5. Ocena skargi	720
6. Współpraca transgraniczna	721
7. Prawo do bycia wysłuchanym i otrzymania informacji	721
Artykuł 54. Odszkodowanie	722
1. Cel i zakres przepisu	722
2. Zasady odpowiedzialności odszkodowawczej	722
3. Założenia rozwiązań polskich	723
Artykuł 55. Sprawozdania z działalności	723
1. Cel i zakres przepisu	724
2. Obowiązki sprawozdawcze	724

3. Odbiorcy sprawozdania	724
4. Treść sprawozdania	725
Sekcja 2	
Kompetencje, skoordynowane czynności sprawdzające i mechanizmy spójności	726
Artykuł 56. Kompetencje	726
1. Cel i zakres przepisu	727
2. Właściwość państw członkowskich	728
3. Właściwość Komisji	729
4. Współpraca państw i Komisji	729
Artykuł 57. Wzajemna pomoc	730
1. Cel i zakres przepisu	731
2. Wymiana informacji	731
3. Wymiana informacji na potrzeby czynności sprawdzających	732
Artykuł 58. Współpraca transgraniczna między koordynatorami ds. usług cyfrowych	733
1. Cel i zakres przepisu	734
2. Wnioski kierowane do koordynatora właściwego dla miejsca siedziby	735
3. Uzasadnienie wniosku	735
4. Działania podejmowane przez koordynatora właściwego dla miejsca siedziby	736
Artykuł 59. Skierowanie sprawy do Komisji	736
1. Cel i znaczenie przepisu	737
2. Skierowanie sprawy do Komisji przez Radę Usług Cyfrowych	737
3. Postępowanie Komisji	738
4. Obowiązki koordynatora	738
Artykuł 60. Wspólne czynności sprawdzające	739
1. Cel i zakres przepisu	740
2. Przestanki dla podjęcia wspólnych czynności sprawdzających	741
3. Tryb podejmowania i prowadzenia wspólnych czynności sprawdzających oraz wymóg współpracy	742
4. Zakończenie wspólnych czynności sprawdzających	743
5. Możliwość przekazania sprawy Komisji	743
Sekcja 3	
Europejska Rada ds. Usług Cyfrowych	743
Artykuł 61. Europejska Rada ds. Usług Cyfrowych	743
1. Cel i zakres przepisu	744
2. Skład Rady Usług Cyfrowych, charakter i adresaci działań Rady	744
3. Niezależność Rady Usług Cyfrowych	745
4. Cele działania Rady Usług Cyfrowych	745

Artykuł 62. Struktura Rady Usług Cyfrowych	746
1. Cel i zakres przepisu	747
2. Skład Rady Usług Cyfrowych	748
3. Posiedzenia Rady Usług Cyfrowych	748
Artykuł 63. Zadania Rady Usług Cyfrowych	749
1. Cel i zakres przepisu	750
2. Zadania Rady Usług Cyfrowych	750
3. Obowiązki związane z działaniami koordynatorów niezgodnymi ze stanowiskiem Rady Usług Cyfrowych	752
Sekcja 4	
Nadzór, czynności sprawdzające, egzekwowanie i monitorowanie w odniesieniu do dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych	752
Artykuł 64. Rozwój wiedzy eksperckiej i zdolności	752
Artykuł 65. Egzekwowanie obowiązków dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych	753
Artykuł 66. Wszczęcie postępowania przez Komisję i współpraca w ramach czynności sprawdzających	754
Artykuł 67. Wnioski o udzielenie informacji	756
Artykuł 68. Uprawnienie do odbierania wyjaśnień i przyjmowania oświadczeń	758
1. Uwagi ogólne	758
2. Warunki skorzystania z uprawnień Komisji	759
2.1. Zakres podmiotowy	759
2.2. Zakres przedmiotowy	759
2.3. Inne obowiązki (konieczność poinformowania koordynatora ds. usług cyfrowych)	760
2.4. Sposób przeprowadzenia przesłuchania	760
2.5. Sankcje	760
3. Uprawnienie do rejestrowania wyjaśnień	760
Artykuł 69. Uprawnienia do przeprowadzania kontroli	761
1. Uwagi ogólne	764
2. Zakres podmiotowy	764
3. Kontrola Komisji Europejskiej – forma prawna	765
4. Uprawnienia Komisji Europejskiej w toku kontroli	765
5. Gwarancje procesowe kontrolowanego	768
5.1. Ochrona prawna tajemnicy komunikacji z zewnętrznym prawnikiem (ang. <i>legal professional privilege</i> , LPP)	768
5.2. Udział zewnętrznego prawnika w toku kontroli	769
5.3. Przywilej dotyczący zakazu samooskarżania	770
5.4. Możliwość zaskarżenia decyzji Komisji Europejskiej związanych z kontrolą	770

6. Rola audytorów i ekspertów w toku kontroli	771
7. Współpraca Komisji Europejskiej z koordynatorami ds. usług cyfrowych oraz innymi właściwymi organami państwa członkowskiego	771
8. Sankcje	772
Artykuł 70. Środki tymczasowe	772
Artykuł 71. Zobowiązania	773
Artykuł 72. Działania z zakresu monitorowania	774
Artykuł 73. Nieprzestrzeganie przepisów	775
1. Zakres regulacji	776
2. Środki	776
3. Przypadki naruszenia DSA	776
Artykuł 74. Grzywny	777
1. Cel regulacji	778
1.1. Charakter grzywien	778
1.2. Fakultatywny charakter kar grzywny	779
2. Kary	779
2.1. Kara w wysokości 6%	779
2.2. Kara w wysokości 1%	780
3. Przedstawienie wstępnych ustaleń przez Komisję przed wydaniem decyzji	781
4. Przesłanki nałożenia kary finansowej	781
Artykuł 75. Wzmoczony nadzór nad środkami zaradczymi w celu wyeliminowania naruszeń obowiązków ustanowionych w rozdziale III sekcja 5	782
1. Cel regulacji i informacje wstępne	783
2. Stosowanie systemu wzmoczonego nadzoru	784
3. Środki wystarczające do zaprzestania lub usunięcia stwierdzonego naruszenia	784
4. Uzgadnianie planu działania	785
5. Monitorowanie wdrażania planu działania	785
Artykuł 76. Okresowe kary pieniężne	786
1. Cel regulacji	787
2. Działanie zagrożone karą	788
3. Fakultatywny charakter kary	788
4. Ustalenie wysokości kary	788
5. Łagodzenie sankcji	789
6. Funkcje kary	789
Artykuł 77. Termin przedawnienia dotyczący nakładania sankcji	789
1. Cel regulacji i wprowadzenie	790
2. Przedawnienie orzekania	791
3. Przerwanie terminu biegu przedawnienia orzekania	791

4. Bieg terminu przedawnienia po jego przerwaniu	791
5. Zawieszenie terminu przedawnienia	792
Artykuł 78. Termin przedawnienia dotyczący wykonania sankcji	792
1. Cel regulacji i wprowadzenie	792
2. Przedawnienie wykonania sankcji	793
3. Przerwanie biegu terminu przedawnienia	794
4. Bieg terminu przedawnienia po jego przerwaniu	794
5. Zawieszenie terminu przedawnienia	794
Artykuł 79. Prawo do bycia wysłuchanym i prawo dostępu do akt	794
1. Informacje ogólne	795
2. Zakres podmiotowy i przedmiotowy prawa do wysłuchania	796
3. Prawo dostępu do akt	797
4. Informacje zebrane w sprawie	798
Artykuł 80. Publikacja decyzji	798
1. Informacje ogólne	798
2. Obowiązek publikacji decyzji	799
3. Informacje poufne	800
4. Charakter publikacji	800
Artykuł 81. Kontrola przez Trybunał Sprawiedliwości Unii Europejskiej	800
1. Informacje ogólne	800
2. Rola Trybunału Sprawiedliwości	801
Artykuł 82. Wnioski dotyczące ograniczeń dostępu i współpraca z sądami krajowymi	801
1. Informacje ogólne	802
2. Zastosowanie środków dodatkowych	802
3. Dyrektywy orzekania	804
Artykuł 83. Akty wykonawcze dotyczące interwencji Komisji	804
1. Informacje ogólne	805
2. Przedmiot aktów wykonawczych	805
3. Sposób procedowania Komisji	805
Sekcja 5	
Wspólne przepisy dotyczące egzekwowania	806
Artykuł 84. Tajemnica zawodowa	806
1. Informacje ogólne	806
2. Pojęcie informacji poufnych na gruncie rozporządzenia	806
3. Podmioty objęte obowiązkiem zachowania tajemnicy	807
4. Ochrona tajemnicy zawodowej	807
5. Czas trwania obowiązku zachowania poufności	807
Artykuł 85. System wymiany informacji	808
1. Informacje ogólne	808
2. Działanie systemu wymiany informacji	809

3. Akty wykonawcze Komisji	809
Artykuł 86. Przedstawicielstwo	810
1. Zagadnienia ogólne	810
2. Obowiązki związane z przyjmowaniem skarg	811
Sekcja 6	
Akty delegowane i wykonawcze	811
Artykuł 87. Wykonywanie przekazanych uprawnień	811
Artykuł 88. Procedura komitetowa	812
Rozdział V	
Przepisy końcowe	814
Artykuł 89. Zmiany dyrektywy 2000/31/WE	814
Artykuł 90. Zmiany dyrektywy (UE) 2020/1828	814
Artykuł 91. Przegląd	814
Artykuł 92. Wcześniejsze stosowanie w stosunku do dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych	815
Artykuł 93. Wejście w życie i stosowanie	816
1. Kwestia dyrektywy 2000/31 (art. 89 DSA)	816
2. Zmiany dyrektywy 2020/1828 (art. 90 DSA)	816
3. Przeglądy KE (art. 91 DSA)	817
4. Wcześniejsze stosowanie (art. 92 DSA)	817
5. Wejście w życie i stosowanie (art. 93 DSA)	818
Załącznik	819
1. Usługa społeczeństwa informacyjnego	819
2. Istota usług społeczeństwa informacyjnego z perspektywy technicznej	820
3. Usługi społeczeństwa informacyjnego świadczone przez podmioty prywatne i publiczne	822
4. Ryzyka naruszenia praw lub wolności związane z implementacją wybranych przepisów DSA w kontekście stosowania RODO	822
5. Elementy usług opartych na algorytmach sztucznej inteligencji (AI) a DSA	839
5.1. Wstęp	839
5.2. Przykład analizy usługi cyfrowej i jej składowych elementów z wykorzystaniem sztucznej inteligencji	840
Bibliografia	843
Autorzy	853

WYKAZ SKRÓTÓW

Akty prawne

- DMA – 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 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)
- dyrektywa CRD – 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 i firmami inwestycyjnymi, 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 98/6 – 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, ze zm.)
- dyrektywa 2000/31 – 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) (2000/31/WE) (Dz.Urz. UE L 178, s. 1)
- dyrektywa 2001/29 – 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 2001/95 – dyrektywa 2001/95/WE Parlamentu Europejskiego i Rady z 3.12.2001 r. w sprawie ogólnego bezpieczeństwa produktów (Dz.Urz. UE L 11, s. 4, ze zm.)

- dyrektywa 2002/58 – 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 – 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 – 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 2010/13 – 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) (wersja ujednolicona) (Dz.Urz. UE L 95, s. 1, ze zm.)
- dyrektywa 2011/83 – 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 – 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, ze sprost.)
- dyrektywa 2013/11, dyrektywa ADR – 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 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 (ujednoczenie) (Dz.Urz. UE L 241, s. 1)

- 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, ze sprost.)
- 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 2019/1937 – dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23.10.2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz.Urz. UE L 305, s. 17, ze zm.)
- dyrektywa 2019/2161 – dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/2161 z 27.11.2019 r. zmieniająca dyrektywę Rady 93/13/EWG i dyrektywy 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.)
- EKPC – Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4.11.1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.)
- k.c. – ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2023 r. poz. 1610 ze zm.)
- k.k. – 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.)
- KPP – Karta praw podstawowych Unii Europejskiej (Dz.Urz. UE C 303 z 2007 r., s. 1, ze zm.)
- pr. aut. – ustawa z 4.02.1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2022 r. poz. 2509 ze zm.)
- pr. energ. – ustawa z 10.04.1997 r. – Prawo energetyczne (Dz.U. z 2022 r. poz. 1385 ze zm.)

- pr. pras. – ustawa z 26.01.1984 r. – Prawo prasowe (Dz.U. z 2018 r. poz. 1914 ze zm.)
- 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, ze sprost.)
- 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, ze zm.)
- rozporządzenie Rzym II – rozporządzenie (WE) nr 864/2007 Parlamentu Europejskiego i Rady z 11.07.2007 r. dotyczące prawa właściwego dla zobowiązań pozaumownych (Rzym II) (Dz.Urz. UE L 199, s. 40)
- rozporządzenie 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 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 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 1215/2012 – 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 524/2013 – rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 524/2013 z 21.05.2013 r. w sprawie internetowego systemu rozstrzygania sporów konsumenckich oraz zmiany rozporządzenia (WE) nr 2006/2004 i dyrektywy 2009/22/WE (rozporządzenie w sprawie ODR w sporach konsumenckich) (Dz.Urz. UE L 165, s. 1)
- rozporządzenie 910/2014 – 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)

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)
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 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 2023/988	– 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 2023/1127	– 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 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 (wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 47)
TUE	– Traktat o Unii Europejskiej (wersja skonsolidowana Dz.Urz. UE C 83 z 2010 r., s. 13)
u.g.h.	– ustawa z 19.11.2009 r. o grach hazardowych (Dz.U. z 2023 r. poz. 227)
u.i.c.t.u.	– ustawa z 9.05.2014 r. o informowaniu o cenach towarów i usług (Dz.U. z 2023 r. poz. 168)
u.o.b.d.	– ustawa z 27.07.2001 r. o ochronie baz danych (Dz.U. z 2021 r. poz. 386)

u.o.b.p.	– ustawa z 12.12.2003 r. o ogólnym bezpieczeństwie produktów (Dz.U. z 2021 r. poz. 222)
u.o.d.o.	– ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781)
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.r.r.p.r.f.	– ustawa z 5.08.2015 r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego Rzeczniku Finansowym i o Funduszu Edukacji Finansowej (Dz.U. z 2023 r. poz. 1809 ze zm.)
u.r.t.	– ustawa z 29.12.1992 r. o radiofonii i telewizji (Dz.U. z 2022 r. poz. 1722)
u.ś.u.d.e.	– ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344)
zalecenie 2003/361	– Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422) (Dz.Urz. UE L 124, s. 36)

Czasopisma

MoP	– Monitor Prawniczy
OSNC	– Orzecnictwo Sądu Najwyższego. Izba Cywilna
OSNC-ZD	– Orzecnictwo Sądu Najwyższego. Izba Cywilna – zbiór dodatkowy
PNT	– Prawo Nowych Technologii
RPEiS	– Ruch Prawniczy, Ekonomiczny i Socjologiczny
ZNUJ	– Zeszyty Naukowe Uniwersytetu Jagiellońskiego

Inne

ADR	– pozasądowe rozstrzyganie sporów (ang. <i>alternative dispute resolution</i>)
CIT	– podatek dochodowy od osób prawnych
DNS	– <i>Domain Name System</i>
EIOD	– Europejski Inspektor Ochrony Danych
EROD	– Europejska Rada Ochrony Danych
ETPC	– Europejski Trybunał Praw Człowieka
GUS	– Główny Urząd Statystyczny

KE, Komisja	– Komisja Europejska
KRRiT	– Krajowa Rada Radiofonii i Telewizji
MŚP	– małe lub średnie przedsiębiorstwo
ODR	– internetowe rozstrzyganie sporów (ang. <i>online dispute resolution</i>)
PIT	– podatek dochodowy od osób fizycznych
RPO	– Rzecznik Praw Obywatelskich
SA	– sąd apelacyjny
SN	– Sąd Najwyższy
TS, TSUE	– Trybunał Sprawiedliwości Unii Sprawiedliwości
UE	– Unia Europejska
UKE	– Urząd Komunikacji Elektronicznej
UOKiK	– Urząd Ochrony Konkurencji i Konsumentów

PRZEDMOWA

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) to kompleksowa regulacja dotycząca różnych aspektów usług świadczonych drogą elektroniczną (usług społeczeństwa informacyjnego). Wskazane przepisy potocznie nazywane są „konstytucją internetu”, ponieważ odnoszą się do kluczowych aspektów jego funkcjonowania i problemów, które go dotyczą, jak np. kwestia odpowiedzialności dostawców za przechowywanie treści nielegalnych, procedury dotyczące zgłaszania i działania w zakresie treści nielegalnych, moderowania treści, reklamy, zwodniczych interfejsów, systemów rekomendacji czy usług dostępnych dla małoletnich.

Oznacza to, że prawodawca unijny uwzględnił najbardziej aktualne kwestie i wyzwania, które dotyczą regulowania nowych technologii. Zwraca na to zresztą uwagę samo DSA, podkreślając w preambule, że minęło ponad dwadzieścia lat po przyjęciu obowiązujących ram prawnych regulujących usługi online, które zostały ustanowione w dyrektywie 2000/31, a w międzyczasie pojawiły się nowe i innowacyjne modele biznesowe i usługi, takie jak internetowe serwisy społecznościowe i internetowe platformy umożliwiające konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość, które pozwoliły użytkownikom biznesowym i konsumentom na przekazywanie i uzyskiwanie dostępu do informacji oraz zawieranie transakcji na nowe sposoby.

DSA to rozporządzenie nie tylko kompleksowo uwzględniające różne aspekty funkcjonowania dostawców usług w internecie, ale jednocześnie obejmujące także różne obszary regulacyjne, jak prawo konsumenckie, ochronę danych osobowych, prawo własności intelektualnej itd. Dotyczy zarówno kwestii prywatnoprawnych, jak i publicznoprawnych. Dlatego wykładnia przepisów przedmiotowego rozporządzenia wymaga rozumienia powiązań zachodzących nie tylko wewnątrz samego DSA, lecz także zachodzących między DSA a innymi aktami prawnymi, w tym RODO czy ustawą o świadczeniu usług drogą elektroniczną, która nawet po wejściu w życie DSA (i rozpoczęciu jego stosowania) w dużej mierze pozostanie w mocy.

DSA nie tylko dotyczy różnych obszarów regulacji prawnych, lecz także ma charakter interdyscyplinarny w tym sensie, że dotyczy kwestii prawnych i technicznych, a znajomość tych przepisów jest istotna nie tylko dla prawników (np. radców prawnych i adwokatów), ale także np. inspektorów ochrony danych, na co zwróciła uwagę 16.01.2024 r. Europejska Rada Ochrony Danych w dokumencie dotyczącym pozycji prawnej inspektorów ochrony danych, podkreślając wagę rozumienia przez inspektorów m.in. wymogów DSA¹.

Biorąc pod uwagę powyższe kwestie, istotnym celem, jaki przyświecał autorom komentarza, było przedstawienie omawianych zagadnień w możliwie praktyczny sposób. Z pewnością wiele z zaprezentowanych podglądów będzie poddanych weryfikacji, m.in. w ramach konkretnych spraw sądowych. Zależało nam jednak na tym, aby czytelnik rozumiał, które kwestie budzą największe wątpliwości i jakie – w ramach tych zagadnień – można zaprezentować warianty interpretacyjne. W szczególności po to, aby był w stanie przewidzieć kierunek rozstrzygania konkretnych spraw. Przy tym autorzy nie uchylali się od zajęcia w ramach tych wątpliwości swojego stanowiska. Zawsze jednak wskazywali argumenty, które przemawiały za takim, a nie innym podejściem i jakie są możliwe inne rozstrzygnięcia.

DSA weszło w życie 16.11.2022 r., natomiast jego pełne stosowanie nastąpi 17.02.2024 r. (w stosunku do wszystkich podmiotów wskazanych w rozporządzeniu). W międzyczasie (czyli jeszcze przed 17.02.2024 r.) DSA znalazło zastosowanie odnośnie do kilkunastu dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych wskazanych zgodnie z art. 33 ust. 4 DSA. Pozwoliło to (na tej niewielkiej podmiotowej „próbie”) obserwować (w toku prac nad komentarzem) praktykę pierwszego okresu stosowania rozporządzenia i wyciągnąć pierwsze praktyczne wnioski co do problemów, z jakimi przy wdrożeniu tych przepisów będą się zderzać dostawcy.

Pragnę w tym miejscu serdecznie podziękować autorom poszczególnych części komentarza za ich wytrwałość i wysiłek włożony w przygotowanie swoich stanowisk. Jednocześnie należy podkreślić, że w przypadku autorów piastujących funkcje publiczne zaprezentowane stanowiska są wyrazem ich osobistych poglądów. Dziękuję także prof. Pawłowi Fajgielskiemu za pozytywną recenzję i uwagi, które zostały uwzględnione i podniosły merytoryczną wartość publikacji.

Kraków, 20.01.2024 r.

Dr Mirosław Gumularz

¹ Zob. https://edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf (dostęp: 20.01.2024 r.).

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 właściwości 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 podróbionych, 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 nierozzerwalnie 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 rozstrzygnięcie 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,

przedstawiciele 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