KATARZYNA KLAFKOWSKA-WAŚNIOWSKA
MIŁOSZ MALAGA
IGOR B. NESTORUK

PRAWA UŻYTKOWNIKÓW NA JEDNOLITYM RYNKU CYFROWYM

RIGHTS OF USERS IN THE DIGITAL SINGLE MARKET

HANDBOOK

WYDAWNICTWO NAUKOWE UAM

PRAWA UŻYTKOWNIKÓW
NA JEDNOLITYM RYNKU CYFROWYM

Handbook

RIGHTS OF USERS
IN THE DIGITAL SINGLE MARKET

UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

Katarzyna Klafkowska-Waśniowska
Miłosz Malaga
Igor B. Nestoruk

PRAWA UŻYTKOWNIKÓW NA JEDNOLITYM RYNKU CYFROWYM

Handbook

RIGHTS OF USERS IN THE DIGITAL SINGLE MARKET

WYDAWNICTWO NAUKOWE

POZNAŃ 2025

Recenzenci/Revievers:
dr hab. Magdalena Słok-Wódkowska, prof. UW
prof. Maria Lillà Montagnani

Projekt/Project: 101084833 — dig_INFlow — ERASMUS-JMO-2022-HEI-TCH-RSCH.

Dofinansowane przez Unię Europejską

Sfinansowane ze środków UE. Wyrażone poglądy i opinie są jedynie opiniami autora lub autorów i niekoniecznie odzwierciedlają poglądy i opinie Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Unia Europejska ani EACEA nie ponoszą za nie odpowiedzialności.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Projekt okładki / Cover design: K. & S. Szurpit
Redaktor / Copy Editor: Marzena Urbańczyk
Korekta (w jęz. angielskim) /Proofreader (English version): Rob Pagett
Redakcja techniczna i DTP / Production Editor and DTP: Reginaldo Cammarano

Autorzy rysunków / Figures prepared by: Jakub Bąchor (7), Jakub Drąg (3), Krzysztof Jeromin (1, 2, 4), Wiktor Kępiński (6), Weronika Łomako (1, 2, 4), Marianna Zawal (5)

Opracowanie graficzne rysunków / Graphic design of Figures: Daria Słomowicz

ISBN 978-83-232-4438-7 (PDF)
DOI: 10.14746/amup.9788323244387

WYDAWNICTWO NAUKOWE UNIWERSYTETU IM. ADAMA MICKIEWICZA W POZNANIU
61-701 POZNAŃ, UL. FREDRY 10
www.press.amu.edu.pl
Sekretariat: tel. 61 829 46 46, faks 61 829 46 47, e-mail: wydnauk@amu.edu.pl
Dział Promocji i Sprzedaży: tel. 61 829 46 40, e-mail: press@amu.edu.pl

Wydanie I. Ark. wyd. 16,5. Ark. druk. 14,75

DRUK I OPRAWA: VOLUMINA.PL SP. Z O.O., SZCZECIN, UL. KS. WITOLDA 7–9

Spis treści

Contents

Abbreviations

Wykaz skrótów

AVMSD	–	Audiovisual Media Services Directive (Dyrektywa o audiowizualnych usługach medialnych)
B2B	–	business-to-business (przedsiębiorca–przedsiębiorca)
B2C	–	business-to-consumer (przedsiębiorca–konsument)
C2C	–	consumer-to-consumer (konsument–konsument)
CDA	–	Communications Decency Act
CDSM	–	Directive on Copyright in the Digital Single Market (Dyrektywa o prawie autorskim na jednolitym rynku cyfrowym)
CFREU	–	Charter of Fundamental Rights of the European Union
CJEU	–	Court of Justice of the European Union
CSS	–	comparison shopping services („porównywarki" zakupów online)
DEI	–	Digital Evolution Index (indeks cyfrowej ewolucji)
DMA	–	Digital Markets Act (Akt o rynkach cyfrowych)
DSA	–	Digital Services Act (Akt o usługach cyfrowych)
DSC	–	Digital Services Coordinator (koordynator ds. usług cyfrowych)
Dz. Urz. UE	–	Dziennik Urzędowy Unii Europejskiej
EBDS	–	European Board for Digital Services (Europejska Rada ds. Usług Cyfrowych)
ECD	–	E-commerce Directive (Dyrektywa o handlu elektronicznym)
EESC	–	European Economic and Social Committee
EKES	–	Europejski Komitet Ekonomiczno-Społeczny
FRAND	–	fair, reasonable, and non-discriminatory (uczciwe, rozsądne i niedyskryminujące)
GDPR	–	General Data Protection Regulation
ISP	–	intermediary service providers (dostawca usług pośrednich)
ISS	–	information society services
JRC	–	jednolity rynek cyfrowy
KPP UE	–	Karta praw podstawowych Unii Europejskiej
KYBC	–	know your business customer (znaj swojego klienta biznesowego)
MFN	–	most favoured nation (klauzula najwyższego uprzywilejowania)

NI-ICS – number-independent interpersonal communication services (usługi komunikacji interpersonalnej niewykorzystujące numerów)
OCSSP – online content-sharing service providers (dostawcy usług platform udostępniania)
ODS – out-of- court dispute settlement (pozasądowe organy rozpatrywania sporów)
OJ – Official Journal of the European Union
P2B – platform-to-business (platforma–przedsiębiorca)
P2C – platform-to-consumer (platforma–konsument)
RODO – rozporządzenie o ochronie danych osobowych
TEC – Treaty establishing the European Community
TFEU – Treaty on the Functioning of the European Union
TFUE – Traktat o funkcjonowaniu Unii Europejskiej
TSUE – Trybunał Sprawiedliwości Unii Europejskiej
TWE – Traktat ustanawiający Wspólnotę Europejską
T&C – terms and conditions (regulamin)
UKE – Urząd Komunikacji Elektronicznej
UOKiK – Urząd Ochrony Konkurencji i Konsumentów (Office of Competition and Consumer Protection)
VLOP – very large online platform (bardzo duża platforma internetowa)
VLOSE – very large online search engine (bardzo duża wyszukiwarka internetowa)
VSP – video-sharing platform (platforma udostępniania wideo)

PRAWA UŻYTKOWNIKÓW NA JEDNOLITYM RYNKU CYFROWYM

Handbook

Wprowadzenie

Celem niniejszej publikacji jest wyjaśnienie oraz poddanie krytycznej analizie zagadnień związanych z prawną pozycją użytkowników oraz z samymi prawami użytkowników na jednolitym rynku cyfrowym.

Od 2020 r. katalog unijnych rozporządzeń, dyrektyw, jak również dokumentów typu *soft law*, obejmujących swoim zakresem różnorodną problematykę jednolitego rynku cyfrowego, powiększył się w sposób znaczący. Przykładowo na prawa użytkowników wskazuje Akt w sprawie danych. Z kolei logika identyfikowania oraz wspierania praw użytkowników jest obecna na gruncie rozporządzenia o ochronie danych osobowych (RODO). W ramach tego coraz bardziej złożonego zbioru instrumentów regulacyjnych uwaga koncentruje się na Akcie o usługach cyfrowych (Digital Services Act, DSA) oraz na Akcie o rynkach cyfrowych (Digital Markets Act, DMA).

Te dwa ostatnie rozporządzenia UE, zaproponowane pierwotnie w postaci tzw. pakietu usług cyfrowych, konkretyzują obowiązki nakładane na dostawców usług pośrednich, w celu zapewnienia ich odpowiedzialnej działalności (ang. *responsibility*), należytej staranności i zagwarantowania uczciwości i kontestowalności rynków cyfrowych. Formułując cel DSA, wprost wskazano na potrzebę „przewidywalnego i budzącego zaufanie środowiska internetowego", w którym skutecznie chronione są prawa podstawowe. Z kolei DMA ma służyć zapewnieniu „kontestowalnych i uczciwych rynków w sektorze cyfrowym" z korzyścią dla użytkowników biznesowych i użytkowników końcowych.

Użytkownicy, czyli odbiorcy usług, konsumenci, użytkownicy biznesowi oraz końcowi, pozostają w rezultacie w samym centrum ram regulacyjnych dla jednolitego rynku cyfrowego. Stąd też publikację rozpoczyna omówienie samej koncepcji, a także rozwoju tych ram regulacyjnych (rozdział I), by w dalszej kolejności główną uwagę poświęcić analizie kolejno trzech kluczowych zagadnień: (1) wzmocnieniu ochrony praw podstawowych użytkowników w obszarze moderacji treści na tle przepisów DSA (rozdział II), (2) mapowaniu korzyści dla konsumentów na gruncie przepisów DSA (rozdział III) oraz (3) zakresowi praw przyznanych uczestnikom rynków cyfrowych na gruncie regulacji DMA (rozdział IV).

W tych rozdziałach na pierwszy plan wysunięto następujące pytania: Czy DMA oraz DSA przyznają użytkownikom jakiekolwiek nowe prawa? W jaki sposób dotychczasowe uprawnienia użytkowników mogą zostać wzmocnione w rezultacie

zastosowania nowych narzędzi prawnych? Wskazano przy tym na duże oczekiwania, jakie towarzyszyły omawianemu pakietowi regulacyjnemu, szczególnie jeśli wziąć pod uwagę potrzebę zapewnienia „skutecznej ochrony" oraz „korzyści" dla użytkowników. To, na ile okażą się one jedynie pustymi deklaracjami, wydaje się zależeć od szeregu czynników – w szczególności od tego, czy DSA i DMA są w stanie sprostać dynamice przemian technologicznych, ponadto od tego, czy relacje tych rozporządzeń z dotychczasowymi, nadal obowiązującymi przepisami prawa UE okażą się jasne i spójne, wreszcie od tego, w jakich ramach możliwe będzie egzekwowanie obowiązków nałożonych na dostawców usług pośrednich. Stąd też ostatni rozdział poświęcono zagadnieniu prywatno- oraz publicznoprawnych narzędzi egzekwowania przepisów DSA i DMA (rozdział V). W tym obszarze można obserwować dopiero wstępną fazę kształtowania się ram dla nadzoru, egzekwowania czy monitorowania, co pozwala jednocześnie prześledzić przykłady synergii oraz różnic w podejściu przyjętych w obu rozporządzeniach. Kluczowe są więc pytania o to, czego w zasadzie użytkownik może oczekiwać na polu stosowania instrumentów *public enforcement*, oraz o to, kiedy indywidualne roszczenia oraz skargi powinny stanowić realnie dostępną opcję ochrony interesów użytkowników.

Niniejszy Handbook jest efektem prac w zespole Katedry Jean Monnet Chair Digital Single Market and the Free Flow of Information (2022–2025). W ramach projektu współpracowaliśmy również z doktorantami i studentami, czego rezultatem są towarzyszące rozdziałom grafiki. Za ich przygotowanie chcielibyśmy podziękować następującym osobom: Jakubowi Bąchorowi, Jakubowi Drągowi, Krzysztofowi Jerominowi, Wiktorowi Kępińskiemu, Weronice Łomako, Darii Słomowicz oraz Mariannie Zawal.

Rozdział I

Jednolity rynek cyfrowy i ochrona użytkowników – ramy prawne

1.1. Pojęcie jednolitego rynku cyfrowego – wprowadzenie

Koncepcje „społeczeństwa informacyjnego" i gospodarki opartej na wiedzy były przedmiotem dyskusji jako cele strategiczne UE od późnych lat 90. XX w., tj. od początku intensywnego rozwoju internetu i nowych możliwości komunikacyjnych. Termin „jednolity rynek cyfrowy" (JRC) został przybliżony w Komunikacie Komisji Europejskiej z 2015 r.[1] Określono w nim, że JRC „to przestrzeń, w której zapewniony jest swobodny przepływ towarów, osób, usług i kapitału, a obywatele i przedsiębiorstwa mogą bez przeszkód i na zasadach uczciwej konkurencji uzyskać dostęp do usług online lub je świadczyć". Osiągnięciu tego celu miał służyć pakiet reform zaproponowany w strategii z 2015 r. i kontynuowany w ramach strategicznego priorytetu „Cyfrowa Europa"[2]. W 2015 r. według indeksu cyfrowej ewolucji (Digital Evolution Index, DEI)[3] 8 krajów Unii rozwijało się dobrze, ale groziło im ryzyko „przegapienia" kluczowego momentu, 7 krajów, w tym Polska, znalazło się w kategorii „uwaga" na możliwość utraty okazji, a tylko 2 zostały określone jako „wyróżniające się" w zakresie cyfrowego rozwoju. DEI wskazuje na różnice między państwami UE, które mogły przeszkodzić w osiągnięciu jednolitego rynku[4].

Harmonizacja zapoczątkowana w tym okresie zmierzała do poprawy infrastruktury cyfrowej oraz do poprawy jej dostępności dla konsumentów i przedsiębiorców wraz z wzrostem bezpieczeństwa w sieci i ochrony przed nielegalnymi treściami.

[1] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Strategia jednolitego rynku cyfrowego dla Europy*, COM/2015/0192 final.

[2] Komisja Europejska, *Shaping Europe's Digital Future*, Luxembourg 2020, https://eufordigital.eu/wp-content/uploads/2020/04/communication-shaping-europes-digital-future-feb2020_en_4.pdf (dostęp: 3.04.2025).

[3] Digital Evolution Index został opracowany przez zespół z Fletcher School, Tufts University; B. Chakravorti, Ch. Tunnard, R.S. Chaturvedi, *Where the Digital Economy is Moving Fastest,* Harvard Business Review, Analytic Services, 9.02.2015, https://hbr.org/2015/02/where-the-digital-economy-is-moving-the-fastest (dostęp: 3.04.2025).

[4] Osiągnięcie celów priorytetowych w zakresie transformacji cyfrowej mierzone jest w UE indeksem DESI (Digital Economy and Society Index), https://ec.europa.eu/newsroom/dae/redirection/document/106717 (dostęp: 3.04.2025).

Przyjęto w tym okresie akty prawne dotyczące geoblokowania, swobodnego przepływu danych nieosobowych, przenoszenia usług w zakresie treści oraz harmonizacji w zakresie prawa autorskiego i prawa mediów. Przełomowe rozporządzenie o ochronie danych osobowych, RODO[5], wskazywało dwa główne cele: swobodny przepływ danych i ochronę prawa do danych osobowych jako prawa podstawowego. Uwidacznia to istotną cechę prawa rynku cyfrowego, czyli dążenie do realizacji swobód gospodarczych przy jednoczesnym wzmacnianiu ochrony praw podstawowych. Jest to szczególnie widoczne w przypadku nie tylko RODO, przyjętego na podstawie art. 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE)[6], lecz także Aktu o usługach cyfrowych opartego na art. 114 TFUE.

Analiza zakresu przeprowadzonej harmonizacji prowadzi do wniosku, że na prawo jednolitego rynku cyfrowego należy patrzeć z różnych perspektyw: (1) ułatwiania internetowej działalności gospodarczej przy wsparciu zdrowej konkurencji, (2) regulowania kluczowych zasobów, jakimi są dane i informacje, oraz (3) ochrony wartości wyrażonych w Karcie praw podstawowych UE (KPP UE)[7]. Trzonem JRC pozostaje swoboda świadczenia usług, w szczególności usług społeczeństwa informacyjnego.

1.2. Pakiet o usługach cyfrowych a priorytety legislacyjne dla „Cyfrowej Europy"

Strategie i inicjatywy wspomniane powyżej zaowocowały licznymi krokami legislacyjnymi, podjętymi w odniesieniu do sektora cyfrowego. W 2019 r. Parlament Europejski wraz z Radą przyjęły tzw. rozporządzenie Platform-to-Business (P2B)[8]. Stanowiło ono pierwszy krok w zakresie regulowania praktyk platform (pośredników) względem użytkowników biznesowych. Istotnie, perspektywa użytkownika dominuje w motywach preambuły, w których zaznacza się, że wielu konsumentów (użytkowników końcowych) korzysta z platform internetowych w Unii Europejskiej i w związku z tym są „kluczowymi czynnikami wspierającymi przedsiębiorczość i nowe modele biznesowe, handel oraz innowacje, które mogą również przyczynić się do poprawy dobrobytu konsumentów", jak również „mogą mieć zasadnicze znaczenie dla sukcesu komercyjnego przedsiębiorstw korzystających z takich usług w celu dotarcia do konsumentów" (motywy 1 i 2 rozporządzenia P2B).

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119, 4.05.2016, s. 1–88).

[6] Traktat o funkcjonowaniu Unii Europejskiej z dnia 13 grudnia 2007 r. – wersja skonsolidowana (Dz. Urz. UE C 202, 7.06.2016, s. 47–360).

[7] Dz. Urz. UE C 326, 26.10.2012, s. 391–407.

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1150 z dnia 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz. Urz. UE L 186, 11.07.2019, s. 57–79).

Komunikat Komisji z 2020 r.[9] proponował zarówno odpowiedzi na wyzwania, jak i możliwości, jakie stwarza transformacja cyfrowa. Podkreślono w nim, że obywatele (czy też po prostu „ludzie") pozostają centralnym punktem prowadzonych rozważań. Komisja wskazała, że celem regulacyjnym jest „technologia przynosząca korzyści ludziom" i „uczciwa konkurencyjna gospodarka", w której zapewnione są równe warunki konkurencji dla przedsiębiorstw różnej wielkości i w różnych sektorach; konsumentom, w tym najbardziej zagrożonym, zapewnia się odpowiednią ochronę; a pełniący funkcję „prywatnych strażników dostępu do rynków, klientów i informacji" podlegają odpowiednim regulacjom. Pozostałe kluczowe cele wskazane w Komunikacie obejmowały zagwarantowanie otwartego, demokratycznego i zrównoważonego społeczeństwa oraz jednolitego rynku dla danych.

Po wydaniu Komunikatu Komisja prowadziła liczne konsultacje publiczne, w których między innymi zamierzała zweryfikować potrzebę wprowadzenia nowego rozporządzenia w zakresie usług cyfrowych, bazującego na podstawach z dyrektywy o handlu elektronicznym. W ramach podjętej inicjatywy odnoszono się nie tylko do swobody świadczenia usług cyfrowych, ale również do ochrony bezpieczeństwa użytkowników i poszanowania ich praw podstawowych. Założenia wyrażone w Komunikacie zostały również potwierdzone podczas pracy nad nowym narzędziem dotyczącym konkurencji, które wyraźnie było poświęcone największym platformom, jako strażnikom dostępu na rynkach cyfrowych, i zmierzało do odnowienia równowagi pomiędzy największymi platformami i ich użytkownikami biznesowymi, a w perspektywie – do zapewnienia jak największego wyboru konsumentom[10].

Działania te skutkowały przedłożeniem projektów DSA[11] i DMA[12]. Od początku były one pomyślane jako jeden zestaw reguł mający dwa główne cele. Po pierwsze, by stworzyć bezpieczniejszą przestrzeń internetową, umożliwiającą obywatelom Unii i innym osobom korzystanie z przysługujących im praw podstawowych, w tym z wysokiego poziomu ochrony konsumentów[13]. Po drugie, by wyrównać warunki konkurencji w sektorze cyfrowym i tym samym przywrócić równowagę rynkową między uczestnikami rynku, włączając w to użytkowników biznesowych[14].

---

[9] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Kształtowanie cyfrowej przyszłości Europy", COM(2020) 67 final (sekcja B), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52020DC0067 (dostęp: 3.04.2025).

[10] Komisja Europejska: Dyrekcja Generalna ds. Konkurencji i H. Schweitzer, *The New Competition Tool: Its Institutional Set Up and Procedural Design: Expert Study*, Brussels 2020, https://data.europa.eu/doi/10.2763/060011 (dostęp: 3.04.2025).

[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (Akt o usługach cyfrowych) (Dz. Urz. UE L 277, 27.10.2022, s. 1–102).

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 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, 12.10.2022, s. 1–66).

[13] Motyw 3 i art. 1 ust. 1 DSA.

[14] Zob. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

1.3. Od dyrektywy w sprawie handlu elektronicznego do Aktu o usługach cyfrowych

1.3.1. Swoboda przepływu usług społeczeństwa informacyjnego

Dyrektywa o handlu elektronicznym (E-commerce directive, ECD) z 2000 r.[15] była pierwszym krokiem w kierunku zapewnienia swobody przepływu usług społeczeństwa informacyjnego (USI). Do wprowadzania regulacji w tym obszarze podchodzono z ostrożnością, ponieważ USI mogą stanowić wyraz ogólniejszej zasady, jaką jest wolność wyrażania się i opinii[16]. Pojęcie „usługi społeczeństwa informacyjnego" zdefiniowane w dyrektywie 2015/1535[17] stanowi podstawowy element budowania prawnych definicji usług na rynku cyfrowym, np. definicji „usługi pośredniej" w DSA czy definicji „usługi platformy udostępniania wideo" w dyrektywie o audiowizualnych usługach medialnych (Audiovisual Media Services Directive, AVMSD)[18]. Zakresem USI objęta jest szeroka gama usług online, takich jak sprzedaż towarów, rozpowszechnianie informacji oraz przekazów handlowych (promocyjnych) czy oferowanie narzędzi wyszukiwania[19]. Pojęcie USI obejmuje każdą usługę świadczoną zwykle za wynagrodzeniem, na odległość, za pomocą środków komunikacji elektronicznej i na indywidualne żądanie odbiorcy. USI są często darmowe dla odbiorcy, ale finansowane z reklam.

Wspieranie swobody świadczenia usług wymagało usunięcia przeszkód wynikających z braku pewności prawnej oraz różnic w prawie krajowym. Z uwagi na to harmonizację w dyrektywie o handlu elektronicznym przeprowadzono w wybranych obszarach, wskazanych w art. 1 ust. 2 ECD[20]. Szczególnie istotne są **trzy fundamenty swobody świadczenia USI**: klauzula rynku wewnętrznego i zakaz uprzedniego zezwolenia (art. 3–4); wyłączenie odpowiedzialności (art. 12–14); oraz zakaz nakładania obowiązku ogólnego monitorowania treści (art. 15). Zgodnie z tzw. klau-

[15] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (Dz. Urz. UE L 178, 17.7.2000, s. 1–16).

[16] Motyw 9 ECD.

[17] Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz. Urz. UE L 241, 17.09.2015, s. 1–15).

[18] Dyrektywa Parlamentu Europejskiego i Rady 2010/13/UE z dnia 10 marca 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, 15.04.2010, s. 1–24).

[19] Motyw 18 ECD.

[20] W art. 1 ust. 22 wskazano przepisy odnoszące się do: rynku wewnętrznego, siedzib usługodawców, informacji handlowych, umów zawieranych drogą elektroniczną, odpowiedzialności pośredników, kodeksów postępowania, pozasądowych dróg rozstrzygania sporów, dochodzenia praw przed sądem oraz współpracy między państwami członkowskimi.

zulą rynku wewnętrznego czy z zasadą państwa pochodzenia dostawcy USI muszą spełniać wymogi ustanowione w prawie państwa ich siedziby (ang. *establishment*), chyba że w dyrektywie dopuszczono odstępstwa zgodnie z art. 3 ust. 4. Zasada ta znajduje zastosowanie jedynie w „dziedzinach koordynowanych" dyrektywą o handlu elektronicznym[21]. Poza zakresem ECD pozostawiono np. prawo autorskie lub prawo mediów. Państwom członkowskim nie wolno wprowadzać wymogu uzyskania zezwolenia na prowadzenie działalności objętej definicją USI. Nie wolno im również nakładać obowiązku ogólnego monitorowania (filtrowania) przekazywanych treści, co znajduje zastosowanie do usług pośredników zapewniających tzw. zwykły przekaz, caching i hosting. Zakaz ten jest przedmiotem szerokiej dyskusji w literaturze i w orzecznictwie[22].

1.3.2. Wyłączenia odpowiedzialności w dyrektywie o handlu elektronicznym

Tak zwane **bezpieczne zatoki**, czyli horyzontalne wyłączenia odpowiedzialności, zostały wprowadzone, aby zapewnić niezakłócony rozwój infrastruktury internetowej. Jak skrótowo, lecz trafnie, ujął to Graeme B. Dinwoodie, dyrektywa o handlu elektronicznym wprowadziła „immunitet" dla tych pośredników, którzy jedynie pasywnie i neutralnie przekazują materiał nielegalny stworzony i komunikowany przez innych (art. 12), dla tych, którzy oferują „caching" tymczasowych kopii nielegalnych danych innych podmiotów (art. 13), oraz dla tych, którzy przechowują nielegalne materiały innych podmiotów i nie mają wiedzy lub informacji o bezprawnej działalności ani świadomości dotyczącej faktów i okoliczności, z których by to w sposób oczywisty wynikało (art. 14)[23]. Rozwiązania te stworzyły neutralne technologiczne otoczenie regulacyjne pozwalające na rozwój platform internetowych, niemających w 2000 r. właściwości i skali, jakie mają dzisiaj[24]. Rozwój platform internetowych znalazł swoje odbicie w licznych pytaniach do Trybunału Sprawiedliwości Unii Europejskiej (TSUE) o wykładnię postanowień dyrektywy o handlu elektronicznym.

Jak zauważył Rzecznik Generalny Maciej Szpunar w sprawie *Uber*, „każda działalność gospodarcza obejmuje elementy świadczone drogą elektroniczną, jak:

[21] Art. 2 lit. h ECD.

[22] Sprawy: C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) przeciwko Netlog NV* (ECLI:EU:C:2012:85); C-18/18, *Eva Glawischnig-Piesczek przeciwko Facebook Ireland Limited* (ECLI:EU:C:2019:821).

[23] G.B. Dinwoodie, *A Comparative Analysis of the Secondary Liability of Online Service Provoders*, w: G.B. Dinwoodie (red.), *Secondary Liability of Internet Service Providers*, Cham 2017, s. 34.

[24] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Platformy internetowe i jednolity rynek cyfrowy. Szanse i wyzwania dla Europy, COM(2016) 288 final, s. 9.

informacje dotyczące produktów, rezerwacja, umawianie spotkań czy zapłata", nie każdej jednak powinna dotyczyć liberalizacja z dyrektywy ECD[25]. TSUE uznał usługi pośrednictwa, takie jak oferowane przez Uber, za nierozerwalnie związane z działalnością offline i w związku z tym za wchodzące w zakres usług transportowych, a nie usług społeczeństwa informacyjnego[26]. Z kolei w sprawie *Airbnb*, TSUE uznał, że usługa pośrednictwa umożliwiająca za pomocą platformy elektronicznej kontakty pomiędzy potencjalnymi najemcami a oferującymi usługę krótkoterminowego zakwaterowania, „czemu towarzyszy świadczenie również szeregu usług dodatkowych", stanowi USI[27]. Star Taxi App, usługa pośrednictwa służąca łączeniu pasażerów i kierowców taksówek, również została uznana za USI[28]. Jako USI kwalifikuje się również oferowanie lokalnej, bezpłatnej sieci wi-fi, jeśli odbywa się w celach promocji sprzedawanych towarów i usług[29].

Obszar naruszeń praw własności intelektualnej zrodził szczególne wyzwania dla stosowania wyłączeń od odpowiedzialności w obszarze hostingu. W przełomowych sprawach *Google France* i *L'Oréal* TSUE wskazał, że dostawca usług pośrednich (ang. *intermediary service providers*, ISP) może skorzystać z wyłączenia odpowiedzialności z art. 14, jeżeli nie odgrywa czynnej roli, wskutek której zyskałby wiedzę o przechowywanych informacjach lub kontrolę nad nimi[30]. W sprawie *L'Oréal* TSUE dodał, że platforma sprzedażowa nie może uchylić się od odpowiedzialności, jeśli usługodawca „wiedział o stanie faktycznym lub okolicznościach, na podstawie których przedsiębiorca wykazujący należytą staranność powinien stwierdzić bezprawność danych ofert sprzedaży, i w przypadku posiadania takiej wiedzy nie podjął niezwłocznie działań"[31]. Aspekt należytej staranności w działaniach dostawcy usługi hostingu został rozwinięty w sprawie *YouTube*. TSUE wskazał, że jeżeli taki przedsiębiorca „wie lub powinien wiedzieć, że co do zasady użytkownicy jego platformy bezprawnie podają do publicznej wiadomości treści chronione za jej pośrednictwem", można od należycie starannego operatora oczekiwać wdrożenia odpowiednich rozwiązań

[25] Opinia Rzecznika Generalnego Macieja Szpunara z dnia 11 maja 2017 r., sprawa C-434/15, *Asociación Profesional Elite Taxi przeciwko Uber Systems Spain, SL* (ECLI:EU:C:2017:364), pkt 37.

[26] Wyrok TSUE z dnia 20 grudnia 2017 r. , sprawa C-434/15, *Asociación Profesional* Élite *Taxi przeciwko Uber Systems Spain, SL* (ECLI:EU:C:2017:981).

[27] Wyrok TSUE z dnia 19 grudnia 2019 r., sprawa C-390/18, *postępowanie karne przeciwko X* (ECLI:EU:C:2019:1112).

[28] Wyrok TSUE z dnia 3 grudnia 2020 r., sprawa C-62/19, *Star Taxi App SRL przeciwko Unitatea Administrativ Teritorială Municipiul Bucureşti prin Primar General and Consiliul General al Municipiului Bucureştisrl* (ECLI:EU:C:2020:980).

[29] Wyrok TSUE z dnia 15 września 2016 r., sprawa C-484/14, *Tobias Mc Fadden przeciwko Sony Music Entertainment Germany GmbHMcFadden* (ECLI:EU:C:2016:689).

[30] Wyrok TSUE z dnia 23 marca 2010 r., połączone sprawy C-236/08–C-238/08, *Google France SARL i Google Inc. przeciwko Louis Vuitton Malletier SA (C-236/08), Google France SARL przeciwko Viaticum SA i Luteciel SARL (C-237/08) i Google France SARL przeciwko Centre national de recherche en relations humaines (CNRRH) SARL i pozostałym (C-238/08)* (ECLI:EU:C:2010:159), pkt 120.

[31] Wyrok TSUE z dnia 12 lipca 2011 r., sprawa C-324/09, *L'Oréal SA i inni przeciwko eBay International AG i pozostałym* (ECLI:EU:C:2011:474), pkt 122–124.

technicznych zapobiegających naruszeniom[32]. Orzeczenie to poprzedza wydanie DSA, w którym bezpośrednio na dostawców usług nałożono określone obowiązki w zakresie należytej staranności. W świetle orzecznictwa szereg pytań o zakres pojęcia USI, o standard należytej staranności[33] i o „rozliczalność" ISP[34], jak również o zakres obowiązków niezależnych od ponoszonej odpowiedzialności[35] pozostało otwartych.

1.3.3. Regulacja działalności platform internetowych – droga do DSA

Najistotniejszym zagadnieniem w sferze regulacji platform internetowych była kwestia, jak zapewnić, żeby „odpowiedzialnie" zaangażowały się one w zwalczanie nielegalnych treści, a ich działania nie zakłócały konkurencji ani nie skutkowały dodatkowym ryzykiem dla konsumentów. Rozważanie te zostały ujęte w Komunikacie Komisji dotyczącym platform internetowych[36] i rozwinięte w ramach pakietu propozycji legislacyjnych zmian w prawie autorskim, w dyrektywie o audiowizualnych usługach medialnych, w rozporządzeniu w sprawie zwalczania treści terrorystycznych czy w rozporządzeniu w sprawie zapewnienia transparentności i uczciwości dla użytkowników biznesowych. W Zaleceniu w sprawie zwalczania nielegalnych treści online[37] zaproponowano niewiążące i horyzontalne wytyczne dotyczące odpowiedzialności platform i zachęt do proaktywnego zwalczania nielegalnych treści, włączając w to wykorzystanie automatycznych środków wykrywania nielegalnych treści. Ich stosowanie powinno być jednak ograniczone do działań, które są „odpowiednie i proporcjonalne, poddane odpowiednim zabezpieczeniom" (motyw 3). Dyrektywa o prawie autorskim na jednolitym rynku cyfrowym (Digital Single Market Directive, CDSM) z 2019 r.[38] i nowelizacja AVMSD z 2018 r.[39] stanowią przykłady odmiennego podejścia do odpowiedzialności platform. W dyrektywie

[32] Wyrok TSUE z dnia 22 czerwca 2021 r., połaczone sprawy C-682/18 i C-683/18, *Frank Peterson przeciwko Google LLC i pozostałym oraz Elsevier Inc. przeciwko Cyando AG* (EU:C:2021:503), pkt 83.

[33] Ch. Angelopoulos, *European Intermediary Liability in Copyright: A Tort Based Analysis*, rozprawa doktorska, Universiteit van Amsterdam 2016, https://hdl.handle.net/11245/1.527223, s. 251 i n.

[34] M. Husovec, *Accountable, Not Liable: Injunctions Against Intermediaries*, „TILEC Discussion Paper" 2016, no. 2016-012, http://dx.doi.org/10.2139/ssrn.2773768.

[35] G. Dinwoodie, op. cit., s. 38.

[36] COM (2016) 288 final.

[37] Zalecenie Komisji (UE) 2018/334 z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w internecie, C/2018/1177 (Dz. Urz. UE L 63, 6.03.2018, s. 50–61).

[38] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 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, 17.05.2019, s. 92–125).

[39] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1808 z dnia 14 listopada 2018 r. zmieniająca dyrektywę 2010/13/UE w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych) ze względu na zmianę sytuacji na rynku (Dz. Urz. UE L 303, 28.11.2018, s. 69–92).

CDSM wprowadzono szczególny reżim wyłączenia odpowiedzialności dla platform udostępniania treści (art. 17), podnosząc standard działań oczekiwanych od platform. Z kolei w dyrektywie AVMSD wprowadzono dodatkowe obowiązki dla platform udostępniania wideo, uzupełniając reżim wyłączenia odpowiedzialności z dyrektywy ECD, poddane kontroli krajowych organów regulacyjnych w sferze mediów (art. 28b). Celem zmian było stworzenie odpowiedniego otoczenia regulacyjnego dla gospodarki cyfrowej i dla zrównoważonego rozwoju biznesowego modelu platform[40]. Przyjęcie DSA jako horyzontalnej regulacji usług pośredników internetowych zainicjowano w komunikacie dotyczącym kształtowania cyfrowej przyszłości Europy z 2020 r. w ramach strategicznego celu, jakim jest budowanie otwartego, zrównoważonego i demokratycznego społeczeństwa[41]. W tym kontekście DSA jawi się jako akt prawny dotyczący przede wszystkim wzmocnienia pozycji obywateli i budowania godnego zaufania środowiska internetowego, a mniej – kwestii gospodarczych. W uzasadnieniu projektu DSA podkreślono, że nie wszystkie cele ECD zostały osiągnięte[42]. Celem DSA jest wsparcie swobody świadczenia usług pośredników internetowych[43], w oparciu o kluczowe zasady ECD, i doprecyzowanie kwestii ich odpowiedzialności i obowiązków[44]. Wyłączenia odpowiedzialności i zakaz ogólnego obowiązku monitorowania są przedmiotem jednolitych rozwiązań (rozdz. 2 DSA), a regulację dopełnia nałożenie obowiązków w zakresie należytej staranności (rozdz. 3 DSA).

1.4. Unijna polityka ochrony konsumentów wobec transformacji cyfrowej

Punktem wyjścia do ustaleń, w jakim zakresie DSA wpływa na prawną sytuację konsumentów, powinno być wyjaśnienie, czy i w jaki sposób prowadzona od blisko 50 lat wspólnotowa polityka w dziedzinie ochrony konsumentów odnosi się do rozwoju technologii cyfrowych, czy szerzej – do kształtowania się społeczeństwa informacyjnego. Przy czym już na wstępie obraz sytuacji, który wyłania się z dokonanego poniżej przeglądu wybranych źródeł, można sprowadzić do hasła: „co jest nielegalne offline powinno być nielegalne online" (rys. 1).

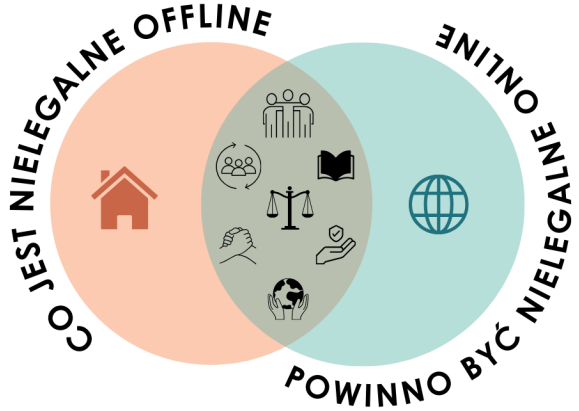
[40] COM (2016) 88 final.

[41] COM (2020) 67 final, s. 12.

[42] Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) i zmieniające dyrektywę 2000/31/WE (COM/2020/825 final, Bruksela, 15.12.2020), s. 7.

[43] Pojęcie zdefiniowane w art. 3 lit. g DSA.

[44] F. Wilman, *The Digital Services Act (DSA) – An Overview*, 16.12.2022, http://dx.doi.org/10.2139/ssrn.4304586.



Rysunek 1. Polityka ochrony konsumentów w środowisku cyfrowym

Rysunek 1 wskazuje, że obie sfery (online – offline) traktowane są równoważnie oraz pozostają w relacji (częściowego) wzajemnego przenikania. Umieszczone w części wspólnej ikonki mają symbolizować katalog podstawowych praw konsumenta. Poza tą wspólną przestrzenią wciąż pozostają obszary rozłączne, wskazujące na specyfikę i odrębności każdej ze sfer.

Kluczowym elementem do odczytania tej formuły jest koncepcja „konsumenta" przyjęta w jednym z pierwszych dokumentów określających niewiążące założenia regulacyjne (*soft law*)[45] w obszarze ochrony konsumentów. W tzw. pierwszym programie polityki ochrony i informowania konsumentów z 1975 r. Rada EWG uznała, że „konsument nie jest już postrzegany jedynie jako nabywający lub użytkujący towary lub usługi dla zaspokojenia potrzeb osobistych, rodzinnych lub zbiorowych, ale także jako osoba zainteresowana różnymi aspektami życia społecznego, które mogą oddziaływać na nią jako konsumenta w sposób pośredni lub bezpośredni"[46]. Koncepcja ta w charakterystyczny sposób łączy wymiar ekonomiczny i społeczny. Przy czym ten pierwszy, sprowadzający konsumenta do roli biernego uczestnika transakcji rynkowej, został (już wówczas!) uznany za niewystarczający. Wymagał on bowiem uzupełnienia o wymiar społeczny ujmowany bardzo szeroko – łączący pojęcie konsumenta z pojęciem obywatela.

[45] Europejskie *soft law* stanowi specyficzny element uwzględniany w dyskusji na temat źródeł prawa UE – por. J. Köndgen, *Die Rechtsquellen des Europäischen Privatrechts*, w: K. Riesenhuber (red.), *Europäische Methodenlehre: Handbuch für Ausbildung und Praxis*, Berlin 2006, s. 155.

[46] Rezolucja Rady z dnia 14 kwietnia 1975 r. w sprawie wstępnego programu Europejskiej Wspólnoty Gospodarczej dotyczącego ochrony konsumentów i polityki informacyjnej (Dz. Urz. WE C 92, s. 1–16), załącznik, pkt 3. Rezolucja, podobnie jak inne dokumenty nienormatywne przyjęte przed datą akcesji Polski do UE, nie występuje w obiegu prawnym w oficjalnej polskiej wersji językowej. Tytuł rezolucji został przetłumaczony na potrzeby niniejszej publikacji.

To z kolei, biorąc pod uwagę przebieg procesów integracyjnych stanowiących o obecnym kształcie UE, może uzasadniać sięganie po koncepcję obywatela rynku (ang. *market citizen*, niem. *Marktbürger*)[47].

Dopiero po takim „zdefiniowaniu" pojęcia konsumenta Rada WE wyznaczyła główne kierunki polityki służącej ochronie interesów konsumentów. Wyrażono je w postaci katalogu pięciu „podstawowych praw" dotyczących kolejno zdrowia i bezpieczeństwa, ochrony interesów gospodarczych, naprawienia szkody, informacji i edukacji oraz reprezentacji (bycia wysłuchanym)[48]. Katalog ten pozostaje aktualny właściwie w niezmienionej postaci, chociaż przez kolejne dekady polityki konsumenckiej można obserwować jego transformację, przesuwanie akcentów w obrębie jego składowych, uwzględniające zmiany dokonujące się w otoczeniu społeczno-ekonomicznym.

W połowie lat 90., w ślad za rozpowszechnieniem się technologii informacyjnych wśród priorytetów wspólnotowej polityki konsumenckiej pojawiają się działania umożliwiające konsumentom skorzystanie z możliwości stwarzanych przez społeczeństwo informacyjne. Charakterystyczna jest wówczas orientacja tej polityki na zapewnienie konsumentom dostępu do tworzącego się systemu informacyjnego (ang. *accessibility*) w połączeniu z dostrzeżeniem konieczności budowania nowych umiejętności (ang. *skills*) użytkownika, w tym poprzez edukację[49]. Choć jednocześnie w dokumentach określających plany reagowania na cyfrową rewolucję na poziomie wspólnotowym nawiązania do praw konsumentów były bardzo skromne[50].

W kontekście podstawowych praw jednostki dokumenty te dostrzegają konieczność ochrony prywatności, przy czym nie jest ona wprost łączona z klasycznym katalogiem praw konsumentów. Dopiero przyjęta w 1999 r. rezolucja Rady w sprawie konsumenckiego wymiaru społeczeństwa informacyjnego[51] sygnalizuje reorientację w dotychczasowej polityce Wspólnot. Samo pojęcie

---

[47] Por. J. Köndgen, op. cit., s. 138; S. Weatherill, *Law and Values in the European Union*, Oxford 2016, s. 390 i n. Akceptacja takiej terminologicznej hybrydy może być poddana krytyce jako próba przekształcenia relacji międzyludzkich w formy rynkowej wymiany (A. Aldridge, *Konsumpcja*, tłum. M. Żakowski, Warszawa 2006, s. 114).

[48] Rezolucja Rady z 14 kwietnia1975 r., załącznik, pkt 3.

[49] Komunikat Komisji, Priorytety polityki ochrony konsumentów na lata 1996–1998 (COM(95) 519 final, Bruksela, 31.10.1995), s. 8. Zob. uwaga w przypisie 46.

[50] Por. Komisja Europejska, Droga Europy do społeczeństwa informacyjnego. Plan działania. Komunikat Komisji do Rady, Parlamentu Europejskiego, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów (COM(94) 347 final, Bruksela, 19.07.1994), s. 3–4; Komisja Europejska, Komunikat Komisji do Rady, Parlamentu Europejskiego, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Europa w czołówce globalnego społeczeństwa informacyjnego: Kroczący plan działania (COM(96) 607 final, Bruksela, 27.11.1996), s. 6. Zob. uwaga w przypisie 46.

[51] Rezolucja Rady UE z dnia 19 stycznia 1999 r. w sprawie konsumenckiego wymiaru społeczeństwa informacyjnego (Dz. Urz. UE 1999/C 23/01). Zob. uwaga w przypisie 46.

społeczeństwa informacyjnego nie jest w niej zdefiniowane. Posłużono się za to formułą „nowych technologii przesyłania i przechowywania informacji […], które mają głęboki wpływ na całe społeczeństwo”[52]. Rada wylicza aż 11 kwestii szczególnie istotnych z perspektywy interesów konsumentów, wśród nich między innymi transparentność odnośnie do ilości oraz jakości informacji, ochronę dzieci oraz prywatność i ochronę danych osobowych (motyw 4), podkreślając jednocześnie, że warunkiem wstępnym do zaakceptowania przez konsumentów społeczeństwa informacyjnego i ich uczestnictwa w nim jest zaufanie[53] (motyw 5). Z kolei budowa tego społeczeństwa, zgodnie z rezolucją (motyw 6), wymaga zapewnienia konsumentom ochrony odnośnie do nowych technologii „na poziomie odpowiadającym temu, który jest dostępny w tradycyjnych transakcjach z udziałem konsumentów przy zastosowaniu istniejących zasad polityki konsumenckiej wobec nowych produktów i usług społeczeństwa informacyjnego”. To stanowisko wydaje się mieć kluczowe znaczenie dla rozumienia kierunku, jaki prezentowana rezolucja wytyczała dla polityki konsumenckiej w tworzącym się środowisku cyfrowym[54].

Mimo upływu 25 lat od daty przyjęcia powyższej rezolucji pozostaje ona nadal aktualna. Potwierdzają to przykłady najnowszych unijnych dokumentów w zakresie zarówno konsumenckiego *soft law*, jak i szerzej – cyfrowego środowiska. Poniżej w porządku chronologicznym wskazano trzy źródła mające wyraźny związek z unijnymi ramami regulacyjnymi dla społeczeństwa informacyjnego, w których centralne miejsce zajmuje również instrument prawny w postaci DSA.

Jeszcze w trakcie prac nad DSA, na etapie wstępnego porozumienia politycznego między Radą a Parlamentem Europejskim w jednym z komunikatów prasowych relacjonujących stanowisko Rady skorzystano z tej formuły, podkreślając w zwięzły sposób, że „nowym przepisom przyświeca zasada, że co jest nielegalne offline, powinno też być nielegalne online”[55].

---

[52] Ibidem, pkt 1.

[53] Rola zaufania w środowisku cyfrowym może być oceniana odmiennie zależnie od tego, czy istniejące w nim relacje będziemy oceniali w kontekście komunikacyjnym czy też w komercyjnym (por. R. Hardin, *Trust*, Cambridge 2006, s. 100 i n.).

[54] W komentarzach towarzyszących temu dokumentowi sygnalizowano jednocześnie potrzebę zachowania ostrożności w prostym implementowaniu znanych dotąd zasad do środowiska online: M. de Cock Buning et al., *Consumer@Protection.EU: An Analysis of European Consumer Legislation in the Information Society*, „Journal of Consumer Policy” 2001, t. 24, s. 329. Na tym tle jeszcze w pierwszej dekadzie XXI w. zaobserwowano, że choć głównym zadaniem Internetu „jest stworzenie sieci internetowych, które byłyby równie intensywne jak te, które istnieją *offline*”, to jednak „jak dotąd, Internet […], w niewielkim stopniu odwzorowuje bogate i złożone relacje w realu” – R. Hardin, op. cit., s. 116.

[55] Rada UE, Komunikat prasowy z 25 listopada 2021 r., https://www.consilium.europa.eu/pl/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act/ (dostęp: 3.06.2024).

Kolejnego przykładu dostarcza Nowy program na rzecz konsumentów[56] określający główne kierunki polityki konsumenckiej realizowanej w latach 2020–2025. Komisja Europejska oparła go na strukturze złożonej z pięciu kluczowych obszarów priorytetowych. Po transformacji ekologicznej drugie miejsce na liście tych obszarów zajmuje transformacja cyfrowa[57]. W rozwinięciu tego elementu programu znajdujemy szereg odniesień do pojedynczych działań Komisji, w tym jedno dotyczące przygotowywanego już wówczas przez Komisję projektu DSA. W akapicie poświęconym temu wnioskowi Komisja stwierdza wprost, że DSA „zapewni konsumentom skuteczną ochronę przed niezgodnymi z prawem produktami, treściami i działaniami na platformach internetowych równoważną ochronie przysługującej im poza Internetem"[58]. W aktualnym programie polityki konsumenckiej podobne sformułowanie pojawia się również w kilku innych jego fragmentach[59].

Wreszcie w treści Europejskiej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie z 2022 r.[60], już w rozdziale 1 (Ukierunkowanie transformacji cyfrowej na człowieka) znajdujemy zobowiązanie do „wprowadzenia niezbędnych środków, aby zapewnić poszanowanie w Internecie oraz poza Internetem uznanych w prawie Unii wartości Unii i praw jednostek"[61]. Choć zbieżność tego sformułowania z tym cytowanym za treścią rezolucji Rady z 1999 r. nie jest tak widoczna jak w przypadku obu wcześniejszych źródeł, to samo zestawienie obu sfer (offline i online) wydaje się charakterystyczne. Nawet jeśli w Deklaracji o samych konsumentach nie ma mowy (sięgnięto po szerszą formułę użytkowników), to nietrudno wskazać w niej widoczne nawiązania do klasycznych konsumenckich praw (np. bezpieczeństwa, swobody wyboru, partycypacji). Pozwala to odczytywać ten dokument w kontekście nowoczesnej polityki konsumenckiej.

Tytułem podsumowania rysunek 2 prezentuje zestawienie centralnych zagadnień wyrażonych w wyżej przywołanych dokumentach z 1975, z 1999 oraz z 2022 r.

Wobec trwającej aktualnie cyfrowej ofensywy regulacyjnej UE polityka konsumencka zajmuje konsekwentne stanowisko, inkorporując do klasycznego katalogu praw konsumenta zagadnienia specyficzne dla społeczeństwa informacyjnego. Było to widoczne już na etapie pierwszych działań podejmowanych na płaszczyźnie wspólnotowej w reakcji na rozwój technologii informacyjnych. Tendencja ta[62] jest

[56] Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego i Rady, Nowy program na rzecz konsumentów. Poprawa odporności konsumentów na potrzeby trwałej odbudowy, COM(2020) 696 final, Bruksela, 13.11.2020.

[57] Ibidem, s. 2.

[58] Ibidem, s. 13.

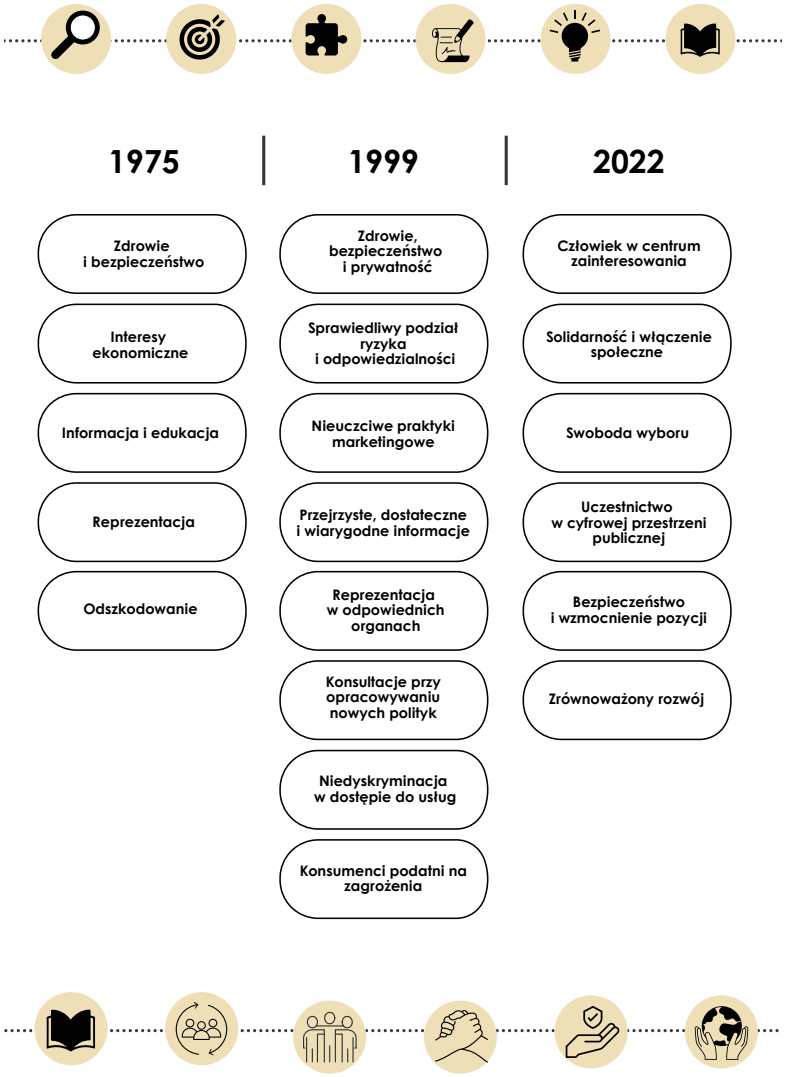
[59] W tym również na samym wstępie do pkt 3.2 poświęconego kluczowemu obszarowi priorytetowemu, jaki stanowi transformacja cyfrowa: ibidem, s. 12.

[60] Europejska deklaracja praw i zasad cyfrowych w cyfrowej dekadzie (Dz. Urz. UE C 23, 23.01.2023, s. 1–7).

[61] Ibidem, s. 2.

[62] Nawet jeżeli jest związana z ryzykiem fragmentaryzacji prawa konsumenckiego – zob. F. de Elizalde, *Fragmenting Consumer Law Through Data Protection and Digital Market Regulations: The DMA, the DSA,*

zauważalna również na tle ostatnich inicjatyw legislacyjnych dotykających środowiska cyfrowego, w tym DSA oraz DMA.



Rysunek 2. Ewolucja polityki ochrony konsumentów w środowisku cyfrowym

W rozdziale III, koncentrując się na mapowaniu praw konsumentów, wskazano szereg skonkretyzowanych nawiązań do zidentyfikowanego powyżej hasła wyznaczającego kierunek unijnej polityki konsumenckiej w środowisku cyfrowym.

the GDPR, and EU Consumer Law, „Journal of Consumer Policy" 2025, https://doi.org/10.1007/s10603-025-09584-3.

1.5. Od prawa konkurencji do Aktu o rynkach cyfrowych

1.5.1. Relacja między prawem konkurencji UE a Aktem o rynkach cyfrowych

Prawo konkurencji ustanawia ramy regulacyjne pozwalające reagować na działania przedsiębiorstw, które podważają wspólny rynek i zakłócają konkurencję. Praktyka decyzyjna Komisji Europejskiej dowodzi w ostatnich latach, że wobec większości przedstawicieli branży big tech stwierdzono naruszenie zakazu nadużywania pozycji dominującej w rozumieniu art. 102 TFUE. Rzeczywiście – przepis ten był stosowany konsekwentnie względem praktyk antykonkurencyjnych pochodzących od takich podmiotów jak Google[63], Amazon[64], Facebook (obecnie Meta)[65] czy Apple[66].

Można jednak wskazać na cechy unijnego prawa konkurencji, które sprawiają, że jest ono mniej adekwatne czy skuteczne w reagowaniu na wyzwania charakterystyczne dla rynków cyfrowych. Cechy te dotyczą przede wszystkim przedmiotu ochrony, egzekwowania oraz ogólnej charakterystyki prawa konkurencji[67].

Po pierwsze, prawo konkurencji jest materialnie ograniczone do przypadków porozumień ograniczających konkurencję (art. 101 TFUE), nadużywania pozycji dominującej (art. 102 TFUE) oraz kontroli koncentracji (na podstawie unijnego rozporządzenia ws. kontroli koncentracji). W konsekwencji dana praktyka rynkowa powinna być objęta zakresem którejś z powołanych kategorii, aby mogła zostać uznana za naruszenie prawa konkurencji. W odniesieniu do omawianych zagadnień najczęściej stosowany jest zakaz nadużywania pozycji dominującej. Wymaga to jednak ustalenia, że dane przedsiębiorstwo rzeczywiście posiada pozycję dominującą na danym rynku oraz że jego określone zachowanie można uznać za konkretny rodzaj nadużycia owej pozycji dominującej. W związku z tym istnieje ryzyko, że niektóre nieuczciwe czy szkodliwe praktyki nie zostałyby objęte zakresem zastosowania prawa konkurencji tak długo, jak nie są podejmowane przez przedsiębiorstwa zajmujące pozycję dominującą w rozumieniu art. 102 TFUE.

Po drugie, w większości przypadków analiza zgodności działania z prawem konkurencji musi być dokonana przez zainteresowane przedsiębiorstwo, natomiast

[63] Zob. decyzje Komisji: z dnia 2 czerwca 2017 r., Google Search (Shopping) (sprawa AT.39740); z dnia 18 lipca 2018 r., Google Android (sprawa AT.40099); z dnia 14 lipca 2016 r., Google Search (AdSense) (sprawa AT.40411).

[64] Zob. decyzje Komisji: z dnia 4 maja 2017 r., E-books (Amazon) (sprawa AT.40153); z dnia 2 marca 2023 r., Amazon Marketplace (sprawa AT.40462); z dnia 2 marca 2023r., Amazon – Buy Box (sprawa AT.40703).

[65] Zob. decyzja Komisji z dnia 14 listopada 2024 r., Facebook Marketplace (sprawa AT.40684).

[66] Zob. następujące decyzje Komisji: z dnia 4 marca 2024 r., Apple – App Store Practices (music streaming) (sprawa AT.40437); z dnia 22 listopada 2024 r., Apple – App Store Practices (e-books/audiobooks) (sprawa AT.40652) i z dnia 24 czerwca 2024 r., Apple – App Store Practices (other applications) (sprawa AT.40716).

[67] Motyw 5 DMA.

właściwe egzekwowanie tych reguł odbywa się na zasadzie *ex post* i wymaga przeprowadzenia, często bardzo złożonego, postępowania. Zatem to uczestnicy rynku na własne ryzyko oceniają zgodność podejmowanej praktyki z unijnym prawem konkurencji. W razie wystąpienia naruszenia musi zostać ono zidentyfikowane przez Komisję Europejską (lub krajowy organ konkurencji). Wówczas Komisja może wszcząć postępowanie, w którym szczegółowo bada daną praktykę rynkową i podejmuje pogłębione badanie rynku. Wszystkie te aspekty sprawiają, że od podjęcia praktyki naruszającej konkurencję do wydania przez Komisję decyzji stwierdzającej owo naruszenie i nakazującej jego zaprzestanie może minąć kilka lat. Tak długi czas może być szczególnie problematyczny w odniesieniu do rynków cyfrowych z uwagi na ich intensywną dynamikę i panujący na nich krajobraz konkurencji.

Po trzecie, z systemowej perspektywy, „tradycyjne" prawo konkurencji nie odnosi się do systemowej zawodności rynku, wynikającej z praktyk podejmowanych przez strażników dostępu[68]. Jest to konsekwencją, omówionych wyżej, ograniczonych narzędzi, jakimi dysponuje prawo konkurencji, a także jego celów i natury. Te bowiem skupiają się na reakcji na konkretne działania ograniczające konkurencję, a nie na zmianie struktury rynku czy uzdrowieniu ogólnych jego zawodności.

Dlatego prawodawca unijny dostrzegł potrzebę wprowadzenia szczególnych narzędzi pozwalających na skuteczne udzielenie odpowiedzi na praktyki strażników dostępu oraz na zapewnienie kontestowalności i uczciwości rynków cyfrowych[69]. Reguły te zostały ustanowione w ramach DMA.

Chociaż DMA stanowi element prawa rynku wewnętrznego, rozporządzenie to jest istotnie inspirowane prawem konkurencji, w tym jego celami, systematyką oraz praktyką egzekwowania jego reguł względem przedstawicieli branży big tech. Zostało ono również opracowane w celu zaradzenia ograniczeniom wynikającym z egzekwowania art. 102 TFUE na rynkach cyfrowych[70].

Wejście w życie DMA oraz jego pełne stosowanie pozostają bez uszczerbku dla stosowania prawa konkurencji do praktyk podejmowanych przez strażników dostępu, pod warunkiem że praktyki te ograniczają konkurencję w rozumieniu art. 101–102 TFUE[71]. Jak potwierdzono w preambule DMA, rozporządzenie to jest komplementarne względem prawa konkurencji i nie zmierza do kolizji z tym porządkiem prawnym. Brak kolizji zdaje się znajdować potwierdzenie w tym, że prawo konkurencji i DMA mają nieco odmienne cele. O ile to pierwsze skupia się

[68] Dokument roboczy Komisji: Ocena skutków towarzysząca wnioskowi dotyczącemu rozporządzenia w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (Akt o rynkach cyfrowych), SWD(2020) 363 final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020SC0363, pkt 68 i nast., 119.

[69] Jak wspomniano w Sekcji dotyczącej Pakietu dla Usług Cyfrowych jako elementu strategii Cyfrowej Europy, pierwotnie narzędzie to było określane jako „nowe narzędzie konkurencji" (ang. *the New Competition Tool*).

[70] F. Bostoen, *Understanding the Digital Markets Act*, "Antitrust Bulletin" 2023, t. 68, nr 2, s. 265.

[71] Art. 1 ust. 6 DMA.

na ochronie niezakłóconej konkurencji na jakimkolwiek rynku właściwym, o tyle DMA zmierza do zapewnienia, że warunki na rynkach doświadczających obecności strażników dostępu pozostaną lub staną się uczciwe i kontestowalne[72].

Jednocześnie w odniesieniu do egzekwowania Komisja i organy krajowe powinny respektować zasadę *ne bis in idem* i w konsekwencji koordynować prowadzone przez siebie postępowania w celu uniknięcia nakładania równoległych sankcji za tę samą praktykę z perspektywy naruszenia prawa konkurencji oraz DMA[73].

1.5.2. Ogólna charakterystyka rynków cyfrowych oraz cele DMA

Pełna wersja tytułu DMA odnosi się do *kontestowalnych* i *uczciwych* rynków w sektorze cyfrowym. Rzeczywiście – rozporządzenie to przede wszystkim zmierza do zapewnienia tych cech na rynkach cyfrowych. Można stwierdzić, że dany rynek jest kontestowalny, nawet jeśli jest na nim tylko jeden uczestnik rynku lub jest ich niewielu, a podmioty te nadal nie są w stanie ograniczyć konkurencji, np. przez sztuczne podwyższenie cen. Scenariusz taki może mieć miejsce, gdy na rynkach nie występują żadne lub wysokie bariery wejścia, przez co podmioty „zasiedziałe" na rynku są ograniczone w swoich działaniach przez presję konkurencyjną wywieraną przez potencjalne wejścia na rynek nowych podmiotów. Stąd – w przeciwieństwie do modeli monopolu – przedsiębiorstwa działające na rynkach kontestowalnych nie będą w stanie podejmować decyzji niezależnie od swoich klientów czy dostawców, a w konsekwencji nie będą w stanie podejmować działań ograniczających konkurencję.

Obecnie występujące cechy rynków cyfrowych sprawiają, że rzeczywiście rynki te nie są kontestowalne ani nie panują na nich uczciwe warunki. Do cech tych zaliczyć można: rosnącą koncentrację (przekładająca się na mniejszą liczbę dostawców usług platformowych); pionową i cyfrową integrację platform internetowych; ekstremalnie duże korzyści skali (dzięki czemu dodatkowi użytkownicy biznesowi czy końcowi pozyskiwani są przy niemal zerowych kosztach); bardzo silne efekty sieciowe (im więcej użytkowników ma platforma, tym większa jest jej zdolność do przyciągnięcia pozostałej części popytu); zdolność do łączenia wielu użytkowników biznesowych z wieloma użytkownikami końcowymi dzięki wielostronności tych usług; efekty uzależnienia od jednego dostawcy (*lock-in effects*, tj. gdy użytkownicy muszą włożyć istotny wysiłek lub ponieść istotne koszty, aby zmienić aktualnego dostawcę usług na jego konkurenta) oraz brak możliwości korzystania przez użytkowników końcowych z wielu platform (tzw. *multi-homing*, tj. skłonność użytkowników zarówno biznesowych, jak i końcowych do równoległego korzystania z kilku konkurencyjnych platform)[74].

[72] Motyw 11 DMA.
[73] Motyw 86 DMA.
[74] Motyw 2 DMA.

W takim środowisku rynkowym trudno jest racjonalnie oczekiwać pojawienia się nowych dostawców usług platformowych. Nawet jeśli hipotetycznie Google obniżyłoby jakość swojej usługi wyszukiwania online (np. przez korzystanie z algorytmów skutecznie promujących określony rodzaj treści lub stron internetowych) albo Meta zaczęłaby pobierać określone opłaty od użytkowników Facebooka czy Instagrama, trudno byłoby nowym uczestnikom rynku z powodzeniem objąć satysfakcjonującą część rynku wyszukiwarek internetowych czy mediów społecznościowych.

W konsekwencji najwięksi dostawcy podstawowych usług platformowych zaczęli być postrzegani jako tzw. strażnicy dostępu. Zgodnie z motywem 6 DMA, strażnicy dostępu wywierają znaczący wpływ na rynek wewnętrzny, gdyż zapewniają dużej liczbie użytkowników biznesowych punkty dostępu umożliwiające im docieranie do użytkowników końcowych w dowolnym miejscu w Unii i na różnych rynkach. Tradycyjnie bowiem handel odbywałby się na wielu różnych, niezależnych od siebie rynkach czy forach. Jednakże rosnąca tendencja do przekształcania go w handel elektroniczny na platformach internetowych oznacza, że platformy stały się obszarami handlowymi, przez co zyskały wpływ na kształtowanie warunków i struktury rynków.

Stanowi to szczególne wyzwanie, gdy dana platforma jest zintegrowana pionowo i w konsekwencji jednocześnie jest obecna na rynku wyższego rzędu (np. internetowa platforma handlowa) oraz na rynku niższego rzędu (działając jako konkurent innych użytkowników biznesowych platformy, np. sklep Amazon konkurujący z innymi sprzedawcami na własnej platformie przy prowadzeniu sprzedaży książek). W takim przypadku strażnik dostępu ma dodatkową motywację, żeby traktować swoich użytkowników biznesowych (będących jednocześnie konkurentami na rynku niższego rzędu) w sposób nieuczciwy, z korzyścią dla własnej usługi oferowanej na rynku niższego rzędu.

Dlatego celem DMA jest odbudowa równowagi miedzy uczestnikami rynków cyfrowych: największymi platformami (czyli strażnikami dostępu) oraz ich użytkownikami: zarówno biznesowymi, jak i końcowymi. DMA ustanawia zatem ochronę prawną przeciwko nieuczciwym praktykom podejmowanym przez strażników dostępu. W szerszym ujęciu wprowadzenie DMA wynika z dostrzeżenia określonych, strukturalnych zawodności rynku i potrzeby poprawy funkcjonowania rynku wewnętrznego przez eliminację jego rozdrobnienia mającego miejsce w sektorze cyfrowym[75].

1.6. Podsumowanie

W niniejszym rozdziale w szerszym kontekście ujęto wprowadzenie pakietu legislacyjnego w zakresie usług cyfrowych. Skupiono uwagę przede wszystkim na tych obszarach regulacji, które są rozwijane w kolejnych rozdziałach publikacji:

[75] Motyw 7 DMA.

na wprowadzeniu obowiązków w zakresie należytej staranności jako odpowiedzi na niedostatki dyrektywy o handlu elektronicznym, na zapewnieniu skutecznej ochrony konsumenta i na przyjęciu podejścia *ex ante* w odniesieniu do praktyk strażników dostępu w celu dopełnienia istniejących reguł konkurencji. Głównym wątkiem analizy jest działalność platform internetowych i potrzeba wzmocnienia ochrony ich użytkowników.

Z perspektywy regulacyjnej istotne jest podkreślenie, że rolą platform internetowych jest nie tylko przechowywanie informacji, jak w przypadku zwykłych usług hostingu, ale również rozpowszechnianie informacji należących do różnych kategorii. DSA i DMA bazują na założeniu, że funkcjonowanie platform wiąże się z różnorodnymi relacjami pomiędzy nimi, użytkownikami i przedsiębiorcami. Relacje te skrótowo ujmuje się jako: C2C (ang. *consumer-to-consumer*, konsument–konsument), B2C (ang. *business-to-consumer*, przedsiębiorca–konsument), B2B (ang. *business-to-business*, przedsiębiorca–przedsiębiorca), P2C (ang. *platform-to-consumer*, platforma–konsument) czy P2B (ang. *platform-to-business*, platforma–przedsiębiorca). W związku z tym omawiane rozporządzenia dotyczą szeregu aspektów relacji platform z użytkownikami biznesowymi, praktyk dotyczących konsumentów, użytkowników końcowych czy innych działań odbiorców usług. Użytkownicy korzystają z platform, aby szukać informacji i dzielić się nimi, kupować i sprzedawać, budować swoją markę, kształcić się czy korzystać z rozrywek. Możliwości dla użytkowników wydają się nieskończone.

Koncepcja „użytkownika" wynikająca z Europejskiej deklaracji praw i zasad cyfrowych odzwierciedla aktualne stanowisko wskazujące, że należy przyjąć perspektywę szerszą niż ograniczoną do perspektywy rynkowej. Najlepiej oddaje to następujące sformułowanie: „technologia powinna służyć i przynosić korzyści wszystkim ludziom mieszkającym w UE oraz umożliwiać im w pełni bezpieczną realizację ich aspiracji przy jednoczesnym poszanowaniu ich praw podstawowych". Cele DSA i DMA służą realizacji wizji „bezpiecznego środowiska internetowego"[76], co zostało poddane krytycznej analizie w niniejszej publikacji.

[76] Art. 1.1, 10, 11 Europejskiej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie.

Rozdział II

Moderowanie treści i prawa użytkowników w Akcie o usługach cyfrowych – wzmacniane czy zaniedbane?

2.1. Wprowadzenie

DSA stanowi regulacyjną odpowiedź na problemy podnoszone w długiej dyskusji o odpowiedzialności pośredników, naruszeniach, zagrożeniach i szkodach występujących wskutek ułatwienia komunikacji przez platformy internetowe. Obowiązki w zakresie należytej staranności, wprowadzone w rozdziale 3 DSA, dotyczą przede wszystkim moderowania treści i wzmacniania ochrony konsumenta[1]. Zakres tych obowiązków różni się w zależności od kategorii, do której należy pośrednik. W sekcjach 1–5 przyjęto stopniowalne podejście: od podstawowych obowiązków nakładanych na wszystkich pośredników do obowiązków, którym podlegają jedynie bardzo duże platformy (ang. *very large online platform*, VLOP) i bardzo duże wyszukiwarki internetowe (ang. *very large online search engine*, VLOSE). Zakresem DSA objęte są trzy kategorie pośredników, oferujących: zwykły przesył (*mere conduit*), caching i hosting[2]. Im bardziej pośrednik jest zaangażowany w rozpowszechnianie informacji, tym więcej obowiązków na niego nałożono. Zaangażowanie, o którym mowa, może przybierać postać przechowywania informacji (hosting, sekcja 2) przechowywania i rozpowszechniania informacji (platformy internetowe, sekcja 3) czy przechowywania i rozpowszechniania przy potencjalnie istotnym wpływie na bardzo szeroki krąg odbiorców (czyli VLOP czy VLOSE)[3]. W niniejszym rozdziale uwaga skupiona jest na obowiązkach platform internetowych, z uwagi na znaczenie ich roli w rozpowszechnianiu informacji dla wolności wypowiedzi.

Jednolite obowiązki w zakresie należytej staranności mają służyć realizacji określonych celów polityki publicznej, takich jak budowanie bezpieczeństwa i zaufania odbiorców usług, ochrona praw podstawowych czy zapewnienie rozliczalności usługodawców i wzmacnianie użytkowników[4]. Do obowiązków w zakresie należytej

[1] W zakresie postanowień dotyczących interfejsów internetowych, reklam czy informacji o produktach i usługach dostępnych na platformach.

[2] Art. 3 lit. g Aktu o usługach cyfrowych (DSA) (Dz. Urz. UE L 277, 27.10.2022, s. 1–102).

[3] Zgodnie z definicją z art. 3 lit. e i art. 33 ust. 1 DSA, próg wyznaczono jako 45 mln aktywnych użytkowników miesięcznie.

[4] Motyw 40 DSA.

staranności należą: ustanowienie mechanizmów moderowania treści, obowiązki w zakresie informowania konsumentów, raportowania czy udostępniania danych dotyczących usługi. Odbiorca usług znajduje się wyraźnie w centrum regulacji – jako ten, którego należy wzmacniać i którego prawa podstawowe wymagają ochrony. Użytkownik, jako odbiorca informacji[5], wymaga ochrony przed szkodą, nękaniem czy przed obrażaniem. Moderowanie treści, jako narzędzie takiej ochrony, zgodnie z DSA obejmuje działania, których celem jest wykrywanie, identyfikowanie i zwalczanie nielegalnych treści lub informacji niezgodnych z warunkami świadczenia usług, za pomocą całej gamy środków ograniczających dostępność czy widoczność informacji[6]. Moderowanie treści może jednak również ograniczać swobodę rozpowszechniania informacji. Ryzyko, jakie moderowanie treści przez platformy rodzi dla praw podstawowych, było przedmiotem analiz i opracowań na poziomie międzynarodowym i regionalnym, w ramach których sformułowano pierwsze wnioski i zalecenia. Zidentyfikowano trzy podstawowe sfery ryzyka: (1) delegowanie platformom funkcji sądowniczych w zakresie oceny nielegalności treści; (2) brak transparentności, szczególnie w zakresie decyzji podejmowanych na platformach, stosowania zautomatyzowanych narzędzi oraz podstaw decyzji moderujących; (3) brak skutecznych i odpowiednich środków ochrony prawnej[7].

DSA jest w Europie kluczowym aktem określającym, jak pośrednicy tworzą i utrzymują cyfrową infrastrukturę dla komunikacji i przepływów informacji. Istnieje wyraźne oczekiwanie, że platformy podchodzą do tego zadania odpowiedzialnie i wzmacniają nasze bezpieczeństwo. Domyślnym imperatywem jest zasada, że platformy, jako przedsiębiorcy, zapewniają poszanowanie praw podstawowych[8]. Z tej perspektywy w niniejszym rozdziale poddano analizie prawa użytkowników, które mogą stanowić korelat obowiązków w zakresie należytej staranności nałożonych na platformy internetowe w obszarze moderowania treści. Rozdział rozpoczynają rozważania na temat ryzyka dla wolności wypowiedzi, dalej omówione zostają wybrane postanowienia DSA, tak by w konkluzji odpowiedzieć, w jaki sposób wzmocniono pozycję użytkowników platform.

---

[5] Art 3 lit. b DSA.

[6] Art. 3 lit. t DSA.

[7] Na podstawie oceny zagrożeń wskazanej w: D. Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Geneva2018, s. 10–14; *Side-stepping Rights: Regulating Speech by Contract: Policy Brief*, London 2018, s. 14–18, https://www.article19.org/wp-content/uploads/2018/06/Regulating-speech-by-contract-WEB.pdf (dostęp: 3.04.2025); E. Pírková, J. Pallero, *26 Recommendation on Content Governance: A Guide for Lawmakers, Regulators and Company Policy Makers*, Access Now, 2020, s. 14–18, https://www.accessnow.org/guide/guide-how-to-protect-human-rights-in-content-governance/ (dostęp: 3.04.2025).

[8] Zgodnie z wytycznymi w zakresie poszanowania praw człowieka przez przedsiębiorców: *Guiding Principles on Business and Human Rights, Implementing the UN Protect-Respect-Remedy Framework*, New York–Geneva 2011, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf (dostęp: 3.04.2025).

2.2. Wzmocnienie pozycji użytkowników w zakresie moderowania treści

Organizacje pozarządowe wspierające prawa obywatelskie rekomendują minimum moderowania treści. Z perspektywy wolności rozpowszechniania i otrzymywania informacji wydaje się, że im mniej moderowania, tym lepiej. Zachęcanie do moderowania może łatwo skutkować nadmiernym ograniczaniem dostępności treści, tzw. *over-blocking* czy *over-moderation*[9].

Ciekawym przykładem zdecydowanego ograniczania moderowania treści jest działalność platformy Twitter. Zmieniając nazwę platformy na X, zmieniono także jej misję – w stronę platformy „wszystko w jednym" dla użytkownika. W mediach szeroko komentowano pomysły Elona Muska o platformie jako otwartym „miejskim rynku" czy jego oczekiwania utopijnej wolności słowa[10]. W dyskusji podniesiono, że aby naprawdę zapewnić wolność słowa, potrzebujemy moderowania treści[11]. Platforma X obrała jednak inny kierunek – ograniczyła liczbę moderatorów, co wzbudziło pytania o to, jak poradzi sobie z napływem mowy nienawiści czy dezinformacji[12]. To podejście zostało w praktyce poddane testom w październiku 2023 r., w momencie ataku Hamasu na Izrael. Ponieważ obowiązywał już DSA[13], a X jest jednym z VLOP, Komisja Europejska zażądała informacji, jak platforma zwalcza nielegalne treści, w szczególności o charakterze terrorystycznym, przemoc i mowę nienawiści oraz jak ogranicza ryzyko wynikające z masowego rozpowszechniania takich treści[14]. W raporcie transparentności opublikowanym przez X podkreślono wartość wolności wypowiedzi oraz zadeklarowano zapewnienie zarówno jej, jak

[9] N. Elkin-Koren, M. Peerel, G. de Gregorio, *Social Media as Contractual Networks: A Bottom-up Check on Content Moderation*, „Iowa Law Review" 2022, t. 107, s. 989–994, https://ilr.law.uiowa.edu/sites/ilr.law.uiowa.edu/files/2023-02/A2_ElkinKoren_DeGregio_Perel.pdf; O.L. Haimson et al., *Disproportionate Removals and Differing Content Moderation Experiences for Conservative, Transgender, and Black Social Media Users: Marginalization and Moderation Gray Areas*, „Proceedings of the ACM on Human-Computer Interaction" 2021, t. 5, nr CSCW2, artykuł 466, https://doi.org/10.1145/3479610.

[10] Elon Musk talks about his plans for Twitter at TED, YouTube, 14.04.2022, https://www.youtube.com/watch?v=WrH-CTRrj_I (dostęp: 3.04.2025).

[11] E. Dworkin, *Elon Musk Wants a Free Speech Utopia: Technologists Clap Back*, The Washington Post, 18.4.2022, https://www.washingtonpost.com/technology/2022/04/18/musk-twitter-free-speech/ (dostęp: 3.04.2025).

[12] B. Ortutay, M. O'Brien, The Associated Press, *Elon Musk Fires Outsourced Content Moderators Who Track Hate and Harmful Posts on Twitter*, Fortune, 14.11.2022, https://fortune.com/2022/11/13/twitter-elon-musk-fires-outsourced-content-moderators-track-hate-harmful/ (dostęp: 3.04.2025); X Safety, *Freedom of Speech, Not Reach: An Update on our Enforcement Philosophy*, Blog X, 17.04.2023, https://blog.twitter.com/en_us/topics/product/2023/freedom-of-speech-not-reach-an-update-on-our-enforcement-philosophy (dostęp: 3.04.2025).

[13] Rozporządzenie stosuje się w pełni od lutego 2024 r., natomiast część postanowień odnoszących się do VLOP znalazła zastosowanie od listopada 2022 r., zob. art. 93 DSA.

[14] The Commission send request for information to X, European Union, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4953 (dostęp: 3.04.2025).

i bezpieczeństwa, zgodnie z DSA[15]. W grudniu 2023 r. Komisja zdecydowała się jednak otworzyć formalne dochodzenie przeciwko X[16], a X zdecydował o zwiększeniu inwestycji w moderowanie treści[17]. Komisja kontynuuje procedurę, kierując do platformy X żądanie udostępnienia dodatkowych informacji między innymi na temat systemów rekomendowania informacji oraz pozwalających na ustalenie faktów dotyczących moderowania treści[18]. Przykład ten jasno pokazuje, że trudno wyobrazić sobie funkcjonowanie platform bez moderowania treści.

2.2.1. Zachęcanie do moderowania na platformach

Jak wskazano już na wczesnym etapie dyskusji o odpowiedzialności platform, moderowanie treści jest ich inherentną cechą, nieodłącznym elementem funkcjonowania platform[19]. Kiedy proponowano DSA, dobrowolne moderowanie treści było już ugruntowaną praktyką na platformach internetowych o globalnym zasięgu. Mimo tego DSA nadal podlega krytyce jako regulacja prowadząca do intensyfikowania moderowania treści. Obejmuje ona również wykorzystywanie w coraz szerszym zakresie algorytmów do zwalczania treści nielegalnych i szkodliwych[20].

Krytyka ta po pierwsze może wynikać z podstawowego celu, jaki wyznacza DSA. Jest nim „stanowienie zharmonizowanych przepisów dotyczących bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego […], w którym skutecznie chronione są prawa podstawowe". Sformułowanie użyte w art. 1 DSA wskazuje na pierwszoplanową rolę „bezpieczeństwa" w środowisku internetowym. Pozostaje to zgodne z szerszą perspektywą, w której celem jest nacisk na

[15] X transparency report, https://transparency.twitter.com/dsa-transparency-report.html (dostęp: 3.04.2025).

[16] Komisja rozpoczęła dochodzenie w sprawie potencjalnego naruszenia art. 34 ust. 1, 34 ust. 2 i 35 ust. 1, 16 ust. 5 i 16 ust. 6, 25 ust. 1, 39 i 40 ust. 12 DSA – *Commission opens formal proceedings against X under the Digital Services Act*, European Union, 18.12.2023, https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6709 (dostęp: 3.04.2025).

[17] Raporty przedłożone Komisji Europejskiej wskazywały, że liczba moderatorów na platformie X jest wyraźnie mniejsza niż na innych platformach, S. Dang, *Musk's X Aims to Hire 100 Content Moderators in Austin by End of Year*, Reuters, 27.01.2024, https://www.reuters.com/technology/musks-x-aims-hire-100-content-moderators-austin-by-end-year-2024-01-27/ (dostęp: 3.04.2025).

[18] Komunikat prasowy z 17 stycznia 2025 r., *Commission addresses additional investigatory measures to X in the ongoing proceedings under the Digital Services Act*, https://digital-strategy.ec.europa.eu/en/news/commission-addresses-additional-investigatory-measures-x-ongoing-proceedings-under-digital-services (dostęp: 3.04.2025).

[19] T. Gillespie, *Custodians of the Internet. Platforms, Content Moderation and the Hidden Decisions That Shape Social Media*, New Haven–London 2018, s. 21.

[20] M.L. Montagnani, *Virtues and Perils of Algorithmic Enforcement and Content Regulation in the EU-A Toolkit for A Balanced Algorithmic Copyright Enforcement*, „Case Western Reserve Journal of Law, Technology and Internet" 2019–2020, t. 11, nr 1, s. 11, https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=3767008 (dostęp: 3.04.2025).

odpowiedzialne zaangażowanie platform w ochronę wartości Unii Europejskiej. Zamierzeniem jest współpraca z platformami bez przekraczania czerwonej linii, jaką jest powierzenie platformom roli regulatora w zakresie dostępności treści.

Po drugie, platformy mogą być niejako „zachęcane" do dobrowolnego moderowania treści poprzez kształt postanowień o wyłączeniach odpowiedzialności. Zgodnie z art. 7 DSA, ISP nie tracą możliwości powołania się na wyłączenie odpowiedzialności (z art. 4–6 DSA), jeśli z własnej inicjatywy, w dobrej wierze i z należytą starannością prowadzą dobrowolne czynności sprawdzające lub podejmują inne środki „mające na celu wykrycie, identyfikację i usunięcie nielegalnych treści lub uniemożliwienie do nich dostępu". Postanowienie to określa się mianem „klauzuli dobrego Samarytanina"[21], co wywodzi się z interpretacji art. 230 CDA[22] w prawie amerykańskim. Dyrektywa ECD nie zawierała podobnego rozwiązania, a w jej świetle jedynie „bierni" pośrednicy, np. dostawcy usługi hosting, mogli korzystać z wyłączenia odpowiedzialności[23]. DSA odnosi się do koncepcji raczej „neutralnego" niż „biernego" świadczenia usług. Preambuła DSA zawiera wskazówki, jak rozumieć „neutralność" usługodawcy. Działania pośrednika powinny ograniczać się do czysto technicznego i automatycznego przetwarzania informacji przekazanych przez odbiorcę usług; ułatwianie nielegalnych działań nie jest głównym celem usługi, a jej dostawca nie jest w żaden sposób redakcyjnie odpowiedzialny za przekazywane treści[24]. Co więcej, pośrednicy pozostają „neutralni", jeśli wdrażają różne narzędzia moderowania treści, by usuwać nielegalne treści, co stanowi element ich obowiązków z zakresu należytej staranności. Działania z własnej inicjatywy platform, co do zasady opierają się na warunkach świadczenia usługi i w praktyce odnoszą się zarówno do działań nielegalnych, jak i do działań niezgodnych z polityką platformy. Rozumienie „neutralności" w kategoriach charakterystyki działań platform budzi zatem wątpliwości. Zgodnie z danymi statystycznymi, większość decyzji dotyczących moderowania treści jest podejmowana na podstawie „polityki platform"[25]. Można więc zastanawiać się, na ile platformy są „neutralne" w zakresie moderowania komunikacji internetowej.

Po trzecie, DSA pozostaje bez uszczerbku dla moderowania treści, które wynikają z wcześniejszej harmonizacji, nie ogranicza również zachęt do moderowania.

---

[21] F. Wilman, *Between Preservation and Qualification: The Evolution of the DSA's Liability Rules in Light of the CJEU's Case Law*, w: J. van Hoboken et al. (red.), *Putting the DSA into Practice: Enforcement, Access to Justice and Global Implications*, Berlin 2023, s. 37, https://www.ivir.nl/publicaties/download/vHoboken-et-al_Putting-the-DSA-into-Practice.pdf (dostęp: 3.04.2025).

[22] Communications Decency Act z 1995 r., Congress.gov, https://www.congress.gov/bill/104th-congress/senate-bill/314 (dostęp: 3.04.2025).

[23] M. Piech, *Pośrednicy internetowi w prawie Unii Europejskiej. Rola i obowiązki wobec treści użytkowników*, Warszawa 2019.

[24] Motywy 18–21 DSA.

[25] *DSA Transparency Database*, European Union, https://transparency.dsa.ec.europa.eu/ (dostęp: 3.04.2025).

Artykułem 17 dyrektywy CDSM wprowadzono szczególny reżim odpowiedzialności dla dostawców usług platform udostępniania (ang. *online content-sharing service providers*, OCSSPs). Dominuje opinia, że OCSSP są skłaniani do moderowania treści, ponieważ – zgodnie z art. 17 – jeśli nie uzyskają odpowiedniego zezwolenia na udostępnianie danych treści na swojej platformie, mimo „dołożenia najwyższych starań", muszą dołożyć wszelkich starań, zgodnie z wysokimi standardami rzetelności zawodowej, aby zapewnić, że określone utwory (lub inne przedmioty chronione), co do których podmioty uprawnione dostarczyły informacje wymagane dyrektywą, będą niedostępne na platformie. Wymagają tego warunki wyłączenia odpowiedzialności dla OCSSP. Artykuł 17 dyrektywy CDSM pozostaje *lex specialis* w stosunku do DSA. Zdecydowanie wyłącza to stosowanie art. 6 DSA, w miejsce czego stosowane są postanowienia art. 17 ust. 4 CDSM. Nie zostało jednak w pełni wyjaśnione, czy stosowanie art. 7 jest również wyłączone w odniesieniu do OCSSP. Wydaje się, że w świetle art. 17 ust. 4 wszystkie działania podejmowane przez OCSSP, by zapewnić niedostępność treści naruszających prawa autorskie i pokrewne, jak i przeciwdziałać ich kolejnym udostępnieniom, są formalnie „dobrowolne". Pozostają jednak prawnym warunkiem wyłączenia odpowiedzialności, w związku z czym pojawiają się głosy, że art. 17 ust. 4 pozostawia bardzo mało miejsca na dobrowolne działania. W związku z tym możliwość zastosowania art. 7 DSA nie powinna być wyłączona, chociaż może mieć ograniczone znaczenie w praktyce[26]. Odpowiedzialność prawno-autorska jest ewidentnym przykładem faktycznego nacisku na platformy, aby moderowały treści.

DSA nie wprowadza wyraźnego obowiązku moderowania treści, a wyraźnie zakazuje nakładania ogólnego obowiązku monitorowania informacji. Równocześnie nie budzi wątpliwości, że platformy mają obowiązek podejmowania działań na podstawie nakazów od właściwych organów krajowych (art. 9 i 10) i podejmowania działań na podstawie zgłoszeń nielegalnych treści (art. 16). Artykuł 7 z kolei potwierdza podejście przychylne dla własnych inicjatyw w zakresie moderowania.

DSA nakłada wyraźny obowiązek wprowadzenia mechanizmów moderowania treści. Biorąc pod uwagę obowiązek odpowiadania na zgłoszenia naruszeń, nie ma wątpliwości co do konieczności moderowania treści, jeśli przedstawiono uzasadnione zgłoszenie. Zgłoszenia spełniające warunki określone w art. 16 ust. 2 skutkują uzyskaniem wiedzy przez usługodawcę, co ma znaczenie w kontekście potencjalnego wyłączenia odpowiedzialności. Jeśli pośrednik nie zareaguje niezwłocznie i nie usunie treści lub nie ograniczy jej dostępności, nie będzie mógł skorzystać z wyłą-

[26] J.P. Quintais, S. Schwemer, *The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?*, „European Journal of Risk Regulation" 2022, t. 13, nr 2, s. 207, https://doi.org/10.1017/err.2022.1; E. Rosati, *The Digital Services Act and Copyright Enforcement: The Case of Article 17 of the DSM Directive*, w: M. Cappello (red.), *Unravelling the Digital Services Actpackage*, Strasbourg 2021, s. 76, https://rm.coe.int/iris-special-2021-01en-dsa-package/1680a43e45. Artykuł 17 ust. 3 dyrektywy CDSM wskazuje, że art. 14 ust. 1 dyrektywy ECD (uchylony przez DSA) nie znajduje zastosowania, jeśli OCSSP dokonują komunikowania publicznie zgodnie z art. 17 ust. 1 CDSM.

czenia odpowiedzialności za jej rozpowszechnianie, niezależnie od podstaw takiej odpowiedzialności (cywilnej, karnej czy administracyjnej). Postanowienia DSA, zapewniające, że na usługodawców nie jest nakładany obowiązek ogólnego monitorowania informacji ani aktywnego ustalania faktów lub okoliczności wskazujących na nielegalną działalność, potwierdzają, że platformy mają działać na zasadzie reakcji. Natomiast ich proaktywne działania wydają się pożądane w świetle art. 7 DSA i jego celów, dopóki działania te nie będą stanowić „uprzedniej cenzury", a platformy nie postawią się w roli ostatecznych sędziów w zakresie dopuszczalności informacji.

2.2.2. „Prawo" do zgłaszania treści

Organizacja Bits of Freedom podjęła próbę naświetlenia „praw użytkowników" na podstawie DSA. Wyjaśniając prawa w zakresie moderowania treści, wskazano, że platformy muszą ułatwić zgłaszanie treści, które użytkownik uzna za nielegalne[27]. Pojawia się pytanie: czy można to rozpatrywać w kontekście „prawa" do zgłaszania? Użytkownicy, w tym przypadku jakakolwiek osoba, jakikolwiek podmiot, uzyskują możliwość skorzystania z funkcji, jaką oferują platformy, z określonego „przycisku", często pod ikonką „zgłoś naruszenie". Użytkownicy mają pełne prawo oczekiwać jasnych wskazówek, jak uzyskać dostęp do elektronicznego formularza, który mogą w prosty sposób wypełnić, aby zgłosić treść nielegalną. Jeśli takiej możliwości nie ma, „usługobiorca", ale również jakakolwiek organizacja, podmiot bądź zrzeszenie upoważnione do wykonywania w ich imieniu praw przyznanych w DSA, może złożyć skargę do koordynatora usług cyfrowych (ang. *digital services coordinator*, DSC)[28]. Można zauważyć, że o ile funkcja zgłaszania ma być dostępna dla wszystkich, o tyle skarga może zostać złożona tylko przez odbiorcę usługi bądź przez podmiot wskazany w art. 53 DSA.

„Prawo" zgłaszania nielegalnych treści powinno być odczytywane przez pryzmat Europejskiej deklaracji praw i zasad cyfrowych. Zgodnie z zasadami dotyczącymi „chronionego, bezpiecznego i pewnego środowiska cyfrowego", podkreślono że „każdy powinien mieć dostęp do technologii, produktów i usług cyfrowych, które z założenia są bezpieczne i chronione". W tym świetle instytucje UE zobowiązują się do przeciwdziałania i rozliczania działań promujących przemoc i nienawiść drogą cyfrową[29]. Brakuje oczywiście pełnej synergii pomiędzy tym postanowieniem z zakresu *soft law* a DSA. DSA ma jednocześnie węższy zakres, dotyczy funkcjonalności zgłaszania treści w celu zapewnienia bezpieczeństwa, i szerszy, jako że obejmuje zwalczanie wszelkich nielegalnych treści, a nie jedynie przemocy i nienawiści. Z badań przeprowadzanych dla UE wynika, że w 2018 r.

[27] *Stay Loud. Know Your Rights*, Bits of Freedom, 17.04.2024, https://www.jouwplatformrechten.nl/en/rights/moderation (dostęp: 3.04.2025).

[28] Art. 53 DSA.

[29] Art. 16 lit. b Europejskiej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie.

65% respondentów nie uznawało Internetu za bezpieczny. Z 61% ankietowanych, aktywnych w Internecie, tylko 1 osoba na 5 informowała dostawcę usługi o nielegalnych treściach, jakie napotykała[30]. DSA zdecydowanie zmierza zarówno do poprawy bezpieczeństwa, jak i do wzmocnienia użytkowników i ich aktywnego udziału w tworzeniu bezpiecznej przestrzeni. Jak wskazano w motywach DSA, obowiązki i warunki określone w art. 16 mają na celu „zapewnić terminowe i niearbitralne przetwarzanie zgłoszeń z zachowaniem należytej staranności", zapewniając „solidne gwarancje" w szczególności dla ochrony praw podstawowych zagwarantowanych w KPP UE[31]. Do działań przeciwdziałających nadmiernemu blokowaniu treści, godzącemu w zasadę wolności wypowiedzi, można zaliczyć postanowienie, zgodnie z którym ISP uzyskuje „faktyczną wiedzę" lub świadomość naruszeń w rozumieniu art. 6 DSA, jeśli zgłoszenie pozwala należycie starannemu usługodawcy „stwierdzenie – bez szczegółowej analizy prawnej – nielegalnego charakteru danej działalności lub informacji"[32]. Zatem jeśli usługodawca zdecyduje, że taki sam system zgłoszeń wprowadza dla treści co prawda legalnych, ale niezgodnych z T&C (ang. *terms and conditions*, pol. regulamin), za pożądane należy uznać podobne rozwiązania, jak w przypadku treści nielegalnych[33], szczególnie jeśli w praktyce T&C odnoszą się do jednocześnie do treści nielegalnych i niezgodnych z polityką platformy.

Zobowiązując wyraźnie pośredników do zapewnienia prostej możliwości zgłaszania nielegalnych treści, DSA idzie o krok dalej niż rozwiązania w zakresie moderowania treści istniejące wcześniej w ramach prawa wtórnego UE. W AVMSD zapewnienie użytkownikom transparentnych i przyjaznych w obsłudze mechanizmów zgłaszania bądź oflagowywania materiałów wideo, stanowiących nawoływanie do nienawiści lub przemocy bądź przestępstwo w świetle prawa UE, znalazło się na liście środków, jakie platformy udostępniania wideo (ang. *video-sharing platforms*, VSP) **mogą** stosować, by zwalczać nielegalne treści. Krajowe organy regulacyjne powinny jednak uznać zapewnienie takiej funkcji za niezbędne, gdyż w innym przypadku prowadzi to do konfliktu z przepisami zakazującymi środków ogólnego monitorowania treści *ex ante*[34]. Jak wskazano w uzasadnieniu projektu, postanowienia DSA mają uzupełniać AVMSD, zapewniając bardziej szczegółowe wymagania dotyczące przejrzystości i skarg użytkowników[35]. W świetle DSA użytkownicy zawsze muszą mieć możliwość zgłoszenia treści nielegalnych.

---

[30] *Flash Eurobarometer 469. Report. Illegal Content Online*, European Union, 4.06.2018, https://europa.eu/eurobarometer/surveys/detail/2201 (dostęp: 3.04.2025).

[31] Motyw 52 DSA.

[32] Art. 16 ust. 3 DSA.

[33] Art. 16 ust. 3 DSA mógłby być może znaleźć zastosowanie *per analogiam*.

[34] Art. 28b AVMSD.

[35] Komisja Europejska, Ocena skutków Aktu o usługach cyfrowych (SWD (2020) 348 final, n.d.), § 290.

Zastosowanie art. 16 DSA w sferze praw autorskich wzbudziło szereg wątpliwości, ponieważ dyrektywa CDSM ustanawia szczególny reżim odpowiedzialności[36]. To podmioty uprawnione są predestynowane do zgłaszania naruszeń prawa autorskiego i stanowią podkategorię „użytkowników platform". Zgodnie z dyrektywą CDSM, dostawcy usług platform powinni nie dopuścić do udostępniania materiałów naruszających prawo autorskie[37]. W tym obszarze postanowienia dyrektywy CDSM stanowią *lex specialis* w stosunku do DSA. Obawy z perspektywy wolności wypowiedzi budzi dobrowolne stosowanie tzw. *upload filters*[38]. Stosowanie takich mechanizmów jest ograniczane wynikającymi z orzecznictwa TSUE założeniami, że muszą one być w stanie rozróżnić treści rozpowszechniane zgodnie i niezgodnie z prawem, inaczej ich stosowanie będzie naruszeniem wolności wypowiedzi[39]. Poza tym zgłoszenia, w świetle dyrektywy CDSM, są składane w sytuacjach, gdy mimo współpracy z podmiotami uprawnionymi bądź w sytuacji braku takiej współpracy treści naruszające prawo autorskie jednak pojawią się na platformie. Stosowanie wówczas art. 16 ust. 1–2 zapewnia ustanowienie odpowiednich funkcji dla zgłaszania treści.

Jak zauważono, przed przyjęciem DSA zharmonizowane mechanizmy *notice and action* powinny uzupełniać ramy egzekwowania praw autorskich[40]. Co więcej, zastosowanie art. 16 ust. 2 pozwoli w ujednolicony sposób oceniać, kiedy zgłoszenia są wystarczająco uzasadnione, wskazując przy tym wyraźnie na wymóg podania URL. Wreszcie – stosowanie art. 16 ust. 3, nawet jeśli wydaje się on formalnie powiązany z art. 6 DSA, jest zgodne z orzecznictwem TSUE. Informacje podawane przez zgłaszających są źródłem faktycznej wiedzy[41] tylko wtedy, gdy treści są w oczywisty sposób bezprawne, tzn. usługodawca jest w stanie ocenić je bez szczegółowej analizy prawnej[42]. Niezależnie od wzmacniania pozycji użytkowników art. 16 DSA ustanawia również wymogi dotyczące zgłoszeń, które służą ochronie przed nadmiernym moderowaniem. Ochrona praw podstawowych użytkowników jest istotna również w sferze IP. Co więcej, DSA ustanawia szczególne warunki egzekwowania obowiązków w zakresie należytej staranności, co pozwoli na złożenie skargi, gdy właściwe mechanizmy zgłaszania nie zostaną wprowadzone, jak również w innych przypadkach naruszeń art. 16[43].

[36] E. Rosati, op. cit.; J.P Quintais, S.F. Schwemer, op. cit.

[37] Art. 17 ust. 4 lit. a– b CDSM.

[38] E. Rosati, op. cit., s. 75.

[39] Wyrok TSUE z dnia 26 kwietnia 2022, sprawa C-401/09, *Rzeczpospolita Polska przeciwko Parlamentowi Europejskiemu oraz Radzie Unii Europejskiej* (ECLI:EU:C:2022:297), pkt 90.

[40] Komisja Europejska, Ocena skutków Aktu o usługach cyfrowych, § 291.

[41] W przypadku gdy usługodawca miał faktyczną wiedzę o nielegalnych treściach, nie może powoływać się na zwolnienie z odpowiedzialności (art. 6 DSA). W świetle szczególnego reżimu art. 17 ust. 4, jeśli OCCSP nie podjął szybkich działań w oparciu o wystarczająco uzasadnione zawiadomienie, ponosi odpowiedzialność za publiczne udostępnienie tych treści.

[42] Sprawa C-401/09, *Rzeczpospolita Polska przeciwko Parlamentowi Europejskiemu oraz Radzie Unii Europejskiej*, pkt 91.

[43] Art. 53 DSA.

2.3. Transparentność moderowania dla użytkowników: prawo do bycia poinformowanym

Oczekiwanie większej transparentności stanowiło istotny punkt w debacie nad regulacją platform. Dyskusja toczyła się wokół dwóch zasadniczych zagadnień: transparentności dla użytkowników i przejrzystości powiązanej z publiczną rozliczalnością działania platform. Drugi z wymienionych aspektów jest powiązany z zakresem informacji przekazywanych władzom publicznym, publikowanych online i dostępnych dla opinii publicznej oraz udzielanych wybranym podmiotom działającym w interesie publicznym, np. zweryfikowanym badaczom. Organizacje pozarządowe rekomendowały wysoki standard transparentności[44], szczególnie w odniesieniu do automatycznego moderowania treści, tak aby ograniczyć nieprzewidywalność nakładania ograniczeń w zakresie treści[45].

Raporty transparentności zaczęły być szerzej publikowane około 2013 r. Poczynając od Google, coraz więcej platform dobrowolnie przekazywała swoim użytkownikom uzasadnienia podjętych decyzji[46]. Praktyki te zostały poddane badaniom i analizie, tak aby uzyskać wgląd w to, czego dowiadujemy się z danych udostępnianych przez platformy[47], czy też w jaki sposób informacje te wpływają na zachowania użytkowników[48]. Badania te w istotnym zakresie pochodzą z USA, gdzie zadawano ciekawe pytania, jak oceniać otoczenie regulacyjne, tak aby transparentność miała rzeczywiste znaczenie (ang. *meaningful transparency*)[49]. Pytania te można streścić następująco: jakich informacji oczekujemy, jakich potrzebujemy i jakie decyzje będą na ich podstawie podejmowane?[50] Istotne dla analizy jest to, jakie wnioski możemy wyprowadzić z przekazywanych danych i w jaki sposób pomogą one ulepszyć środowisko platform.

---

[44] E. Pírková, J., Pallero, op. cit., s. 33; Santa Clara Principles on content moderation 2.0, https://santaclaraprinciples.org/ (dostęp: 3.04.2025).

[45] Rada Europy, *Content Moderation: Best Practices Towards Effective Legal and Procedural. Frameworks for Self-Regulatory and Co-regulatory Mechanisms of Content Moderation, Guidance Note Adopted by the Steering Committee for Media and Information Society (CDMSI) at Its 19th Plenary Meeting, 19–21 May 2021*, 2021, s. 42, https://edoc.coe.int/en/internet/10198-content-moderation-guidance-note.html (dostęp: 3.04.2025); D. Kaye, op. cit., rekomendacje 69 i 71, s. 20.

[46] Zob. https://www.tspa.org/curriculum/ts-fundamentals/transparency-report/history-transparency-reports/ (dostęp: 3.04.2025).

[47] E. Goldman, *Content Moderation and Remedies*, „Michigan Technology Law Review" 2021, t. 28, nr 1, artykuł 2, s. 57, https://doi.org/10.36645/mtlr.28.1.content.

[48] S. Jhaver, A. Bruckman, E. Gilbert, *Does Transparency in Moderation Really Matter?: User Behavior After Content Removal Explanations on Reddit*, „Proceedings of the ACM on Human-Computer Interaction" 2019, t. 3, nr CSCW, artykuł 150, s. 152, https://doi.org/10.1145/3359252.

[49] N.P. Suzor et al., *What do We Mean When We Talk about Transparency? Toward Meaningful Transparency in Commercial Content Moderation*, „International Journal of Communication" 2019, t. 13, s. 1527.

[50] E. Goldman, op. cit., s. 58.

DSA zmierza do wprowadzenia ram regulacyjnych, w których transparentność jest kluczowa dla ustanowienia środowiska, w którym prawa podstawowe są skutecznie ochronione. Transparentność stanowi trzon obowiązków w zakresie należytej staranności. Służyć ma przewidywalności decyzji, a to z kolei ma przeciwdziałać ryzyku niejasnych reguł i ryzyku zbyt szerokiego marginesu swobody moderowania treści. Aby lepiej ukazać prawa użytkowników, obowiązki w zakresie transparentności mogą być podzielone na trzy grupy:

a) Prawa użytkowników jako odbiorców usługi do bycia poinformowanym o zasadach moderowania treści (art. 14 DSA).

b) Prawa użytkowników do bycia poinformowanym w sytuacji potencjalnego ograniczenia ich wolności rozpowszechniania informacji (art. 17 DSA).

c) Ogólny dostęp do raportów platform dotyczących moderowania treści (art. 15, 22, 42 DSA).

Ad a) Warunki świadczenia usługi

W AVMSD, jako pierwszej próbie harmonizacji działań platform w zakresie zwalczania nielegalnych treści, nacisk położono na informowanie użytkowników o nielegalnych i szkodliwych treściach[51], których rozpowszechnianie na platformie będzie ograniczane[52]. Podejście to ewoluowało[53] i aktualnie DSA wymaga, aby każdy dostawca usługi hostingu informował w swoich warunkach świadczenia usług o wszelkich restrykcjach w zakresie korzystania z usługi w odniesieniu do informacji, które użytkownik chce zamieszczać, w tym o **wszelkich politykach, procedurach, środkach i narzędziach wykorzystywanych na potrzeby moderowania treści**. Informacje te muszą uwzględniać informację o algorytmicznie podejmowanych decyzjach i ich przeglądzie dokonywanym przez człowieka oraz o wewnętrznym systemie rozpatrywania skarg.

Ogólne informacje o „jakichkolwiek ograniczeniach" można odnieść do wskazania na profil usługi, wskazując rodzaj treści, dla których jest przeznaczona. Informacje te powinny również zawierać wyjaśnienia o zakazie rozpowszechniania treści nielegalnych. Z art. 14 DSA wynika, że użytkownik ma prawo być poinformowany szczegółowo o polityce w zakresie rozpowszechniania treści, w szczególności o treściach, które są nie tyle nielegalne, ile niezgodne z polityką platformy. Polityka platformy może przybrać postać „wytycznych dla społeczności", w których *de facto* łączą się odniesienia do treści nielegalnych i niepożądanych. Użytkownik powinien także zostać poinformowany o stosowanych środkach i narzędziach moderowania

[51] Jak wskazano w art. 28b ust. 1 AVMSD.

[52] Art. 28b ust. 3 lit. a.

[53] Wskazuje się, że art. 5 ust. 1 Rozporządzenia 2021/784 stanowił bezpośrednią inspirację dla DSA – J.P. Quintais et al., *Enforcement of Terms of Service*, „German Law Journal" 2023, t. 24, nr 5, s. 890, https://doi.org/10.1017/glj.2023.53.

treści. Obejmują one zwykle te środki, które zostały wymienione w definicji moderowania treści, takie jak: depozycjonowanie, demonetyzacja, uniemożliwienie dostępu lub usunięcie treści (art. 3 lit. t DSA). W świetle regulacji jest wyraźnie widoczne, że użytkownik powinien móc dowiedzieć się, jakie treści będą ograniczane i jaki zakres środków moderowania może być zastosowany. Informacje te powinny być przekazane jasno, jednoznacznie i prostym językiem[54]. W praktyce warunki świadczenia usług i regulaminy mogą być kompleksowymi dokumentami. W związku z tym VLOP i VLOSE dodatkowo muszą opublikować T&C w językach urzędowych wszystkich państw, i zapewnić „zwięzłe, łatwo dostępne i nadające się do odczytu maszynowego streszczenie warunków korzystania z usług" (art. 14 ust. 5 DSA).

Poziom szczegółowości oczekiwany od T&C można wywnioskować również z art. 17 ust. 3 DSA dotyczącego uzasadnień decyzji o moderowaniu. Informacja przekazywana *ex ante*, zanim jakiekolwiek treści zostaną udostępnione, powinna uprzedzać, co może się wydarzyć po opublikowaniu treści stanowiących naruszenie prawa oraz warunków świadczenia usługi. W idealnym układzie zasadnienie decyzji powinno pozwolić użytkownikowi „połączyć kropki" i zrozumieć, do jakiego naruszenia doszło w konkretnej sytuacji.

DSA nie wskazuje wyraźnie, że platformy internetowe powinny dostosować polityki w ramach swoich usług do międzynarodowego standardu ochrony praw człowieka. Standardy te powinny jednak odgrywać pierwszoplanową rolę w sferze moderowania treści[55]. DSA obliguje jednakże platformy internetowe do „działania z należytą starannością, w sposób obiektywny i proporcjonalny oraz z należytym uwzględnieniem praw i prawnie uzasadnionych interesów wszystkich zaangażowanych stron, w tym zapisanych w Karcie praw podstawowych odbiorców usługi" (art.14 ust. 4 DSA). Uzasadnione jest zatem oczekiwanie, że ograniczenia i polityka moderowania treści muszą być przygotowane w zgodzie ze standardem ochrony praw podstawowych w UE i w tym zakresie powinny podlegać ewaluacji.

W zakresie wolności wypowiedzi i prawa autorskiego bardziej szczegółowe postanowienia dyrektywy CDSM wymagają od OCSSP informowania użytkowników, w zapisach T&C, że mogą korzystać oni z utworów i innych przedmiotów chronionych, w ramach ograniczeń i wyjątków przewidzianych w prawie Unii Europejskiej (art. 17 ust. 9 *in fine*). Jest to przykład istotnej informacji, która powinna być udzielana na podstawie prawa krajowego, implementującego dyrektywę. Aby informacja ta była rzeczywiście istotna, powinna iść w parze z możliwością publikowania treści zawierających cytaty czy będących parodią, niezależnie od ryzyka, jakie może to tworzyć dla platform. W przeciwnym razie ogólna informacja o możliwości skorzystania z wyjątków i ograniczeń może pozostać pustą obietnicą.

[54] Komisja powinna wspierać standardy w zakresie norm dotyczących szablonów, projektowania i przetwarzania na potrzeby komunikacji z odbiorcami usługi w sposób przyjazny dla użytkownika w zakresie ograniczeń wynikających z warunków korzystania z usług i zmian do tych warunków, art. 44 ust. 1 lit. b DSA.

[55] J.P. Quintais et al., op. cit., s. 881–882.

Ad b) Uzasadnienie nałożonych ograniczeń

W celu zapewnienia transparentności decyzji w zakresie moderowania treści dostawcy usług platform internetowych mają obowiązek przekazywania informacji zarówno tym użytkownikom, którzy zgłosili nielegalne treści, jak i tym, których dotyczy decyzja w zakresie ograniczenia widoczności lub dostępności treści. Zgodnie z art. 16 ust. 4–6 DSA, zgłaszający użytkownik powinien najpierw otrzymać informację potwierdzającą przyjęcie zgłoszenia, a następnie informację o decyzji dostawcy usługi hostingu, włączając w to informację o ewentualnym stosowaniu zautomatyzowanych środków na potrzeby takiego rozpatrywania lub podejmowania decyzji i o możliwościach odwołania. Odbiorca usługi, którego dotyczy decyzja o nałożeniu ograniczeń wskazanych w art. 17 ust. 1 lit. a–d[56], powinien otrzymać jasne i konkretne uzasadnienie nałożonych ograniczeń, niezależnie od tego, czy decyzja motywowana była nielegalnością treści czy ich niezgodnością z warunkami świadczenia usług. Obowiązek podania uzasadnienia nie dotyczy moderowania treści w oparciu o „zakazy" z art. 9 DSA ani informacji stanowiących „wprowadzające w błąd treści handlowe o dużej objętości"[57]. Obowiązek dostawcy jest też ograniczony do przypadków, gdy usługodawca zna elektroniczne dane kontaktowe użytkownika.

Uzasadnienie nałożonych ograniczeń musi zawierać, po pierwsze, informacje o rodzaju nałożonych ograniczeń, a po drugie, wyjaśnienie okoliczności i faktów leżących u podstaw podejmowanej decyzji. Dla użytkownika powinno być jasne, czy treści zostały usunięte, czy dostęp do nich został ograniczony, czy zostały „zdepozycjonowane", czy też zostały nałożone inne ograniczenia, jak tzw. *shadow ban*. Nadto, powinno być wiadomo, czy ograniczono możliwości monetyzowania treści oraz czy zawieszono konto użytkownika bądź zakończono świadczenie wobec niego usługi.

Choć nie zostało to jednoznacznie wymienione w DSA, jako element „okoliczności i faktów" leżących u podstaw decyzji należy traktować wyjaśnienie, których dokładnie treści ograniczenie dotyczy. Dostawca hostingu powinien również, w stosownych przypadkach, informować o tym, czy decyzja wynika ze zgłoszenia czy z własnych czynności sprawdzających usługodawcy. Ograniczenie tego obowiązku do niejasno określonych „stosownych przypadków" zasługuje na krytykę. Ryzyko dla ograniczenia praw podstawowych związane z moderowaniem podkreślane jest w szczególności w zakresie dobrowolnych działań platform, poza tym informacja ta jest istotna w kontekście korzystania ze ścieżki odwoławczej. Jako że art. 24 ust. 5 DSA obliguje platformy do przekazywania uzasadnień do publikacji w otwartej bazie

[56] W praktyce zawęża to kategorię użytkowników usługi do tych, którzy udostępniają informacje, a nie jedynie „poszukują informacji", chyba że można racjonalnie uznać, że poszukiwanie informacji może pociągać za sobą zawieszenie konta lub zakończenie świadczenia usługi. Postanowienie to znajduje zastosowanie przede wszystkim do zarejestrowanych użytkowników, jako że tworzą konto, podając swoje dane kontaktowe. Nie ma jednak wyraźnego wymogu, aby był to zarejestrowany użytkownik.

[57] Potocznie nazywanych „spamem".

danych[58], w celu wspierania „rozliczalności" platform można uznać, że ograniczenia nakładane przez platformy internetowe są zawsze „stosownym przypadkiem"[59]. Jeśli decyzja oparta jest na stwierdzeniu nielegalności treści, uzasadnienie musi zawierać wskazanie podstawy prawnej, wraz z uzasadnieniem takiej oceny. Jeśli decyzja była oparta na niezgodności z warunkami świadczenia usług, odpowiednie podstawy kontraktowe powinny być wskazane i wyjaśnione. Przegląd przykładowych decyzji publikowanych w bazie Komisji wskazuje na braki w zakresie przekazywania informacji naprawdę istotnych dla użytkowników. Przykładowo, pod hasłem „fakty i okoliczności" oraz w ramach wyjaśnienia, dlaczego treści uznane są za niezgodne z warunkami świadczenia usługi, mogą znaleźć się dokładnie te same informacje. Ponadto, widoczna jest praktyka wskazywania w sposób ogólny kilka możliwych podstaw uznania treści za naruszające T&C[60]. Z analizowanego przykładowego zgłoszenia nie wynikają żadne szczegóły wyjaśniające, dlaczego konkretne treści zostały usunięte w przypadku automatycznego wykrywania i częściowo zautomatyzowanego podejmowania decyzji. Informacje o stosowaniu zautomatyzowanych środków w procesie identyfikowania treści i wydania decyzji powinny być przedstawiane „w stosownych przypadkach". Postanowienie to należy interpretować zgodnie z wysokimi standardami transparentności w obszarze zagrożeń dla praw podstawowych: „stosownym przypadkiem" powinien być każdy przypadek użycia zautomatyzowanych środków do moderowania treści. Spełnianie minimalnych wymogów z DSA na razie w praktyce oznacza odpowiedź „tak" lub „nie" na pytanie, czy takie środki są stosowane, i „tak", „nie", „częściowo" w przypadkach automatyzacji procesu podejmowania decyzji. Informacje te są istotne nie tylko dla publicznej rozliczalności platform, lecz także w związku ze składaniem odwołań od decyzji. Przekazywanie w sposób jasny i przyjazny dla użytkownika informacji o możliwościach odwołania stanowi ostatni obligatoryjny element uzasadnienia. Obowiązek przekazania uzasadnienia aktualizuje się w dniu nałożenia ograniczenia, chociaż nie wskazano terminu, do jakiego należy takie uzasadnienie przekazać. W praktyce powinno się to dziać automatycznie z moderowaniem treści, w innym przypadku ograniczy to możliwość składania odwołań.

Ad c) Obowiązki w zakresie raportowania

Jak już wskazano, uzasadnienia decyzji platform internetowych są publikowane w internetowej bazie *transparency database*, wraz z ich wstępną analizą i statystykami. Rozwiązanie to wpisuje się w obowiązki w zakresie przejrzystości, powiązane z publiczną rozliczalnością, oraz wspiera badania i analizę systemów moderowania na podstawie danych. W tym samych duchu utworzono bazę warunków świadcze-

[58] *DSA Transparency Database*, op. cit.

[59] „Stosownym przypadkiem" mogłyby nie być działania dostawców hostingu niepowiązane z publicznym rozpowszechnianiem informacji.

[60] Zob. https://transparency.dsa.ec.europa.eu/statement/17541329612 (dostęp: 3.04.2025).

nia usług[61], a elementem ram ustanowionych przez DSA dla transparentności są obowiązki w zakresie raportowania.

Podstawowe obowiązki w zakresie raportowania ustanowiono w art. 15 DSA, dodatkowe wymagania dla platform zawiera art. 23, a szczególne obowiązki VLOP i VLOSE uregulowano w art. 42. Głównym narzędziem są regularnie składane i publicznie dostępne raporty przedstawiane na wzorach stanowiących załącznik do rozporządzenia Komisji[62]. Raporty te są dostępne dla wszystkich zainteresowanych użytkowników. Ich znaczenie leży w umożliwieniu szerszego, systemowego ujęcia mechanizmów moderowania treści. Wszyscy dostawcy usług pośrednich są zobowiązani do przedstawiania rocznych, jasnych, łatwo zrozumiałych i publicznie dostępnych raportów na temat wszelkiego prowadzonego moderowania treści (art. 15 ust. 1). Istotną część raportów stanowi informowanie o liczbach: liczbie nakazów otrzymanych od organów państwowych, liczbie zgłoszeń na podstawie art. 16 ust. 1, liczbie zgłoszeń procedowanych w sposób zautomatyzowany czy liczbie odwołań składanych za pośrednictwem wewnętrznych mechanizmów składania skarg. Platformy internetowe muszą dodatkowo raportować o liczbie sporów przedstawionych pozasądowym organom rozpatrywania sporów (ang. *out-of-court dispute settlement*, ODS) i o zawieszeniu świadczenia usług w stosunku do podmiotów często rozpowszechniających oczywiście bezprawne treści bądź składających oczywiście bezzasadne zgłoszenia czy odwołania[63].

Liczby dostarczają informacji o skali fenomenu moderowania treści i wykorzystywania, dostosowanych do wymogów DSA, mechanizmów zgłaszania treści. Jednakże nawet podstawowe wymogi w zakresie raportowania wykraczają poza przekazywanie liczb. Wymagane są na przykład informacje o wszelkich przypadkach „wykorzystania zautomatyzowanych środków do celów moderowania treści, w tym opis jakościowy, wyszczególnienie konkretnych celów, wskaźniki dokładności i ewentualny poziom błędu zautomatyzowanych środków wykorzystanych w osiąganiu tych celów oraz zastosowane zabezpieczenia" (art. 15 ust. 1 lit. e). Dostawcy VLOP i VLOSE powinni udzielać szczegółowych informacji o moderatorach, o ich kwalifikacjach, znajomości języków, szkoleniach i udzielanym im wsparciu (art. 42 ust. 1 DSA). Zapewnienie, że ogromne ilości danych raportowanych przez platformy są przedstawiane w sposób spójny, umożliwiający badania analityczne i ich porównywanie, stanowi spore wyzwanie. Zunifikowany wzorzec raportu służy temu celowi, jednak może też rodzić ryzyko nadmiernych uproszczeń. Dobrym przykładem są wskaźniki dokładności i poziomu błędu w zakresie automatycznego moderowania treści przez

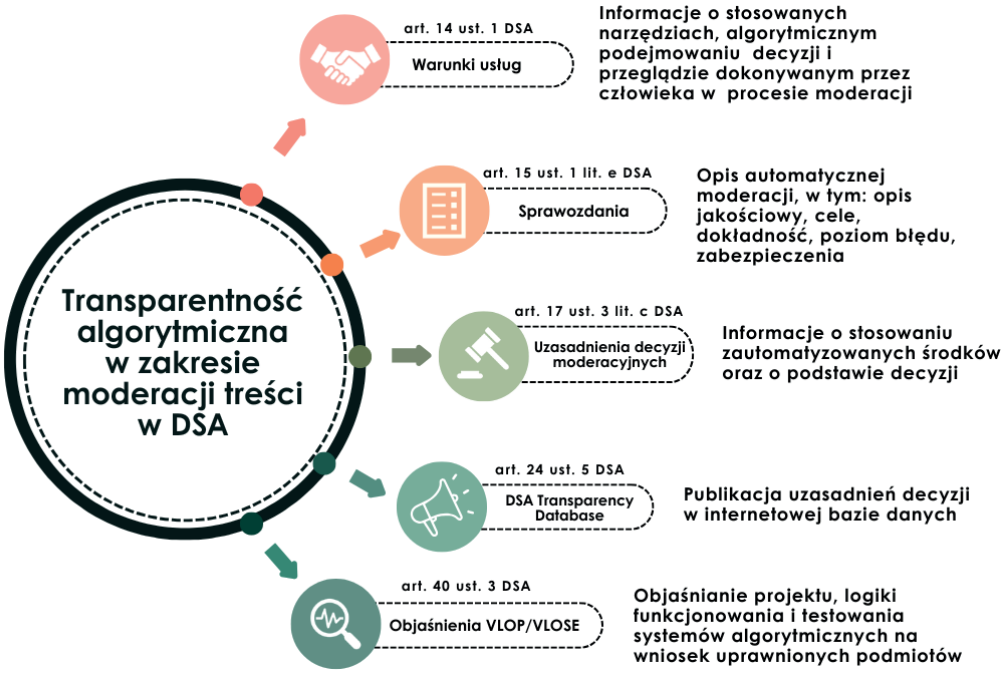
[61] Zob. https://platform-contracts.digital-strategy.ec.europa.eu/ (dostęp: 3.04.2025).

[62] Rozporządzenie wykonawcze Komisji (UE) 2024/2835 z dnia 4 listopada 2024 r. ustanawiające wzory związane z wypełnianiem obowiązków sprawozdawczych w zakresie przejrzystości spoczywających na dostawcach usług pośrednich i dostawcach platform internetowych na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 (Dz. Urz. UE L, 2024/2835, 5.11.2024).

[63] Dodatkowe obowiązki związane z przeciwdziałaniem nadużyciom związanym z korzystaniem z usług zawiera art. 23 DSA.

VLOP. Należałoby oczekiwać, że użytkownicy dowiedzą się więcej na temat tego, jak platformy określają dokładność i trafność działania algorytmów oraz jak mierzą ich poziom błędu. Przyjęty wzorzec raportu uwzględnia wymóg udzielania „informacji kontekstowych", a nie tylko liczbowych, co może być wstępem do uporządkowania informacji o moderowaniu jako „masowym zarządzaniu wypowiedziami"[64].

Sprowadza to prowadzoną analizę do niezwykle istotnego pytania: kto będzie analizował dane na temat moderowania treści i jak to wpłynie na ocenę zgodności działań platform z obowiązkami w zakresie należytej staranności? Celem nadrzędnym DSA jest przy tym zapewnienie skutecznej ochrony praw podstawowych, w tym wolności wypowiedzi.



Rysunek 3. Algorytmy w moderacji – obowiązki informacyjne

Po pierwsze zatem, transparentność służy wykazaniu zgodności z ramami dla należytej staranności ustanowionymi w DSA, a egzekwowanie tych obowiązków należy do DSC i Komisji[65]. Wymogi w zakresie transparentności mają nadto służyć indywidualnym użytkownikom, jako źródło informacji niezbędnej w celu dochodzenia roszczeń. Z kolei w zakresie rozliczalności platform DSA ujmuje funkcjonowanie systemów moderowania treści na liście czynników systemowego ryzyka w kontek-

[64] Ang. *mass speech administration*; E. Douek, *Content Moderation as Systems Thinking*, „Harvard Law Review" 2022, t. 136, nr 2, s. 528.

[65] Zagadnienie szczegółowo omówione w rozdziale V.

ście działalności VLOP (art. 34 ust. 2 lit. b). Ryzyko, że dobrowolne moderowanie treści wpływa na zakres wolności rozpowszechniania i otrzymywania informacji, poprzez tzw. *over-blocking* i automatyczne usuwanie treści zgodnych z prawem, należy rozpatrywać w kategoriach systemowego ryzyka. W DSA wskazuje się nie tylko na ryzyko rozpowszechniania treści nielegalnych lub na negatywny wpływ na procesy wyborcze, ale również na „ryzyko wystąpienia faktycznych lub przewidywalnych negatywnych skutków dla wykonywania praw podstawowych". W ramach uwzględniania ryzyka systemowego[66] zagrożenia te powinny być zidentyfikowane przez VLOP, co powinno prowadzić do zastosowania środków ograniczających to ryzyko. Wady systemów moderowania mogą zostać odkryte również w raportach z audytów dotyczących zgodności działań VLOP z wymogami DSA (art. 37 ust. 1).

Komisja i DSC powinny brać pod uwagę ryzyko dla wolności wypowiedzi w trakcie analizy przekazywanych im danych. Wskazuje się, że część danych może *de facto* „przykrywać" poważne problemy, na przykład niski wskaźnik w zakresie odwołań od decyzji platformy, w tym sporów kierowanych do organów ODS, może błędnie sugerować brak problemów po stronie użytkowników[67]. Zadaniem Komisji i DSC jest nadzorowanie przestrzegania DSA i promowanie najlepszych praktyk, w tym w formie kodeksów postępowania, co ma wspomóc zwalczanie systemowego ryzyka. Opinia publiczna powinna być informowana, na podstawie informacji dostępnych publicznie i dostępnych dla zweryfikowanych badaczy, o ryzykach wynikających z funkcjonowania platform. Ostatecznie to użytkownik może teoretycznie podjąć decyzję, że nie będzie korzystał z danej usługi. Jest to zgodne z założeniami Deklaracji w sprawie praw i zasad cyfrowych: „Każdy powinien mieć możliwość skutecznego i swobodnego wyboru – w oparciu o obiektywne, przejrzyste, łatwo dostępne i wiarygodne informacje – usług online, z których chce korzystać"[68]. Wydaje się to jednak utopijnym założeniem w świecie, gdzie usługi platform docierające do globalnej publiczności stanowią podstawową infrastrukturę komunikacyjną współczesnego społeczeństwa.

2.4. Podsumowanie

Sformułowanie konkluzji wymaga powrotu następującego pytania: rozwiązanie jakiego głównego problemu postawiono sobie za cel w DSA? Czy jest nim zapewnienie, że przestrzeń cyfrowa jest bezpieczna i wolna od nielegalnych i szkodliwych treści? Czy też jest nim nadmierna swoboda platform w moderowaniu rozpowszechnianych

[66] Zgodnie z art. 34 DSA.

[67] M. Senftleben, *Guardians of the UGC Galaxy – Human Rights Obligations of Online Platforms, Copyright Holders, Member States and the European Commission Under the CDSM Directive and the Digital Services Act*, „Journal of Intellectual Property, Information Technology and E-Commerce Law" 2023, t. 14, nr 3, s. 436–437, https://ssrn.com/abstract=4683206.

[68] Art. 10 Europejskiej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie.

informacji? Zapewnienie bezpieczeństwa i przewidywalności jest zdecydowanie podstawowym zamierzeniem (art. 1 DSA). Ochrona praw podstawowych, również wyraźna w celach DSA, jest ujęta szeroko: od ochrony przed nielegalnymi treściami, by zapewnić brak naruszeń w sferze godności ludzkiej, po ochronę prywatności i wolności wypowiedzi. Aby wzmocnić użytkowników, platformy zostały zobowiązane do zapewnienia określonych funkcji: ułatwiania zgłaszania nielegalnych treści, co zostało omówione w ramach „prawa" do zgłaszania treści, jak również umożliwiania prostej ścieżki składania odwołań od decyzji platformy. Elementem wspierania bezpieczeństwa w środowisku platform jest ustanowienie ram prawnych, które sprzyjają dobrowolnemu moderowaniu treści. Nie ma wątpliwości, że DSA wpływa na wzmożenie moderowania, jednocześnie zwiększając kontrolę nad tymi mechanizmami, w tym stosowanymi dobrowolnie przez platformy.

Ponieważ ryzyka dla wolności wypowiedzi zostały zidentyfikowane szczególnie w sferze moderowania treści niezgodnych z polityką platform[69], zabezpieczenia wprowadzane w przypadku moderowania treści nielegalnych powinny znaleźć zastosowanie do moderowania w przypadku niezgodności treści z warunkami świadczenia usług. Aby zminimalizować ryzyko nadużyć, wymogi dotyczące przedstawiania „wystarczająco uzasadnionego wyjaśnienia powodów" zgłoszenia i obowiązek powiadomienia użytkownika, który zamieścił kwestionowaną treść, powinny znaleźć zastosowanie również w przypadku zgłoszeń wskazujących na niezgodność z warunkami świadczenia usług. Należy podkreślić, że platformy w szerokim zakresie opierają się w przypadku moderowania na swojej wewnętrznej polityce, gdyż, poza może treściami w sposób oczywisty nielegalnymi[70], ocena bezprawności treści jest trudna, szczególnie biorąc pod uwagę obszary niezharmonizowane i współistnienie porządków prawnych 27 państw członkowskich. Przykładem może być naruszenie dóbr osobistych czy treści szkodliwe dla małoletnich.

Odpowiedzią na ryzyko nadmiernego moderowania jest przyznanie w DSA użytkownikom prawa do informacji, niezależnie od tego, czy decyzje oparte są na nielegalności treści czy ich niezgodności z T&C. Prawo do bycia poinformowanym można wywodzić z praw konsumenckich, ale w DSA znajduje ono zastosowanie również do użytkowników biznesowych i potencjalnie do innych zainteresowanych podmiotów (art. 17 ust. 1). Ogólnie ujęte prawo do informacji przekłada się w DSA na obowiązki w zakresie informowania o polityce moderowania treści, o działaniach, które mogą wpłynąć na wolność rozpowszechniania i otrzymywania informacji, w formie uzasadnienia ograniczeń. Wykładnia obowiązków w zakresie udzielania informacji powinna zapewnić, że użytkownicy mogą się skutecznie odwołać od decyzji bądź złożyć uzasadnioną skargę do DSC. Istotne zatem, aby użytkownicy mogli się dowiedzieć, jak dana treść została ograniczona, dlaczego uznano, że

[69] Ten rodzaj moderowania jest nieobowiązkowy z perspektywy prawa UE, wydaje się jednak być pożądany.

[70] Jak np. pornografia dziecięca.

narusza warunki usługi i czy decyzja została podjęta po weryfikacji przez człowieka. Postanowienia DSA interpretowane w świetle celu, jakim jest wzmocnienie użytkowników w zakresie ochrony ich praw podstawowych, obligują platformy do udzielania konkretnych informacji. Trudno jednakże jednoznacznie określić, jakich informacji platformy powinny udzielać w odniesieniu do algorytmicznego moderowania i do weryfikacji przez człowieka w indywidualnym przypadku. W tej sferze nie tyle wzmacnia się indywidualną pozycję użytkowników, ile oczekuje się od nich zaufania do organów nadzorujących platformy, które mają zapewniony szerszy dostęp do informacji o moderowaniu treści.

Rozdział III

Zasada ochrony praw konsumentów w Akcie o usługach cyfrowych – mapowanie korzyści dla konsumentów

3.1. DSA a unijne prawo konsumenckie

Konsumencki wymiar celu i przedmiotu DSA (por. uwagi dotyczące art. 1 ust. 1 DSA oraz motywu 3 preambuły DSA w rozdziale I) nietrudno jest dostrzec na gruncie współczesnego prawa UE. Wystarczy w tym celu uwzględnić przynajmniej jeden kluczowy w tym kontekście element traktatowych zasad prawa UE. Jest nim zawarta w art. 12 TFUE tzw. klauzula horyzontalna, zgodnie z którą wymogi ochrony konsumentów są uwzględniane przy określaniu i urzeczywistnianiu innych polityk i działań Unii[1]. W efekcie ostatniej rewizji prawa traktowego z 2009 r. przepis ten – poprzednio jako art. 153 ust. 2 Traktatu ustanawiającego Wspólnotę Europejską (TWE)[2] – został przeniesiony do części pierwszej TFUE i umieszczony wśród zasad Unii Europejskiej. Tą zmianę lokalizacji należy odczytywać wprost jako wyraz podwyższenia rangi i samodzielności obszaru polityki ochrony konsumentów[3]. Dodatkowego potwierdzenia tej zasadniczej zmiany dostarcza również KPP UE, gdzie zasada ochrony konsumentów (art. 38 KPP UE) zamyka katalog przepisów tworzących Tytuł IV KPP UE (Solidarność), nie czyniąc jednak z ochrony konsumentów prawa podstawowego w rozumieniu art. 52 KPP UE[4].

Ten niewątpliwy awans zasady ochrony konsumentów, co nie bez przesady można określić jako przejaw „konstytucjonalizacji", stanowi dzisiaj pewien standard w unijnym porządku prawnym. Również DSA można poddać ocenie w kontekście jego wypełnienia. Zadanie to unijny prawodawca w zasadzie ułatwił w opisie celu

[1] W literaturze słusznie w kontekście klauzul horyzontalnych wskazuje się, że ich konstrukcja z natury nieostra, w sposób zbiorczy odnosząca się do chronionych interesów może okazać się trudna w przypadku próby wyegzekwowania w konkretnym przypadku wobec braku możliwości prostego jej przełożenia na prawnie umocowane roszczenia – por. S. Weatherill, *Law and Values in the European Union*, Oxford 2016, s. 135 i n.

[2] Wersja skonsolidowana 2002 (Dz. Urz. UE C 325, 24.12.2002, s. 33–184).

[3] S. Weatherill, *Consumer Policy*, w: P. Craig, G. de Búrca (red.), *The Evolution of EU Law*, 3 wyd., Oxford 2021, s. 875.

[4] I. Benöhr, *EU Consumer Law and Human Rights*, Oxford 2013, s. 63; N. Reich, H.-W. Micklitz, *Economic Law, Consumer Interests and EU Integration*, w: N. Reich et al. (red.), *European Consumer Law*, 2 wyd., Cambridge–Antwerp–Portland 2014, s. 14; S. Weatherill, *Law and Values*…, s. 136 i n.

DSA, precyzując, czemu (a tym samym komu) służyć ma regulacja bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego. Ma być to przestrzeń, która „ułatwi innowacje" i w której „skutecznie chronione są prawa podstawowe zapisane w Karcie, w tym zasada ochrony konsumentów" (art. 1 ust. 1 DSA). W preambule DSA (motywy 1 i 4) podkreślono owo specyficzne połączenie wątku proinnowacyjnego (stymulowanie innowacji, wprowadzanie innowacyjnych usług cyfrowych) z wątkiem proobywatelskim, wyrażającym się odniesieniem do praw podstawowych zagwarantowanych w KPP UE.

Ten drugi ze wspomnianych wątków jest szeroki, ponieważ obok zasady ochrony konsumentów przywołanej wprost w art. 1 ust. 1 DSA obejmuje również wolność wypowiedzi i informacji, wolność prowadzenia działalności gospodarczej oraz prawa do niedyskryminacji (motyw 3 preambuły DSA). Wszystkie łącznie będą pomocne w odczytaniu formuły „bezpiecznego, przewidywalnego i godnego zaufania środowiska internetowego". Prawa konsumentów (por. art. 169 ust. 1 TFUE) nie stanowią w tym ujęciu wyizolowanego elementu tej regulacji, lecz powinny być traktowane jako jeden z wielu punktów odniesienia dla przepisów DSA, zarówno tych, które do zagadnienia ochrony konsumentów odnoszą się bezpośrednio, jak i tych pozostałych, które często jedynie w pośredni, aczkolwiek widoczny sposób wpływają na prawny status konsumenta usług cyfrowych.

***Relacja między DSA a konsumenckim* acquis.** Art. 2 ust. 4 lit. f DSA stwierdza, że rozporządzenie pozostaje bez uszczerbku dla „prawa Unii w dziedzinie ochrony konsumentów i bezpieczeństwa produktów". W otwartym katalogu wymienia w kontekście konsumenckim dwa unijne rozporządzenia oraz dwie dyrektywy, spośród których rozporządzenie (UE) 2017/2394[5] oraz dyrektywa 2013/11/UE[6] są szczególnie istotne z perspektywy egzekwowania praw konsumentów, podczas gdy dwa pozostałe akty prawne dotyczą kwestii bezpieczeństwa produktów[7]. Relacja DSA do konkretnych przepisów prawa konsumenckiego UE jest dynamiczna. Pozwala ona oddzielić od DSA takie przepisy, które regulują inne aspekty świadczenia usług pośrednich na rynku wewnętrznym (np. umowy o dostarczanie treści cyfrowych i usług cyfrowych w kontekście dyrektywy (UE) 2019/770[8]). Uzasadnia również

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2394 z dnia 12 grudnia 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, 27.12.2017, s. 1–26).

[6] Dyrektywa Parlamentu Europejskiego i Rady 2013/11/UE z dnia 21 maja 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, 18.06.2013, s. 63–79).

[7] Przy czym przywołana w tym przepisie dyrektywa 2001/95/WE (Dz. Urz. UE L 11, 15.01.2002, s. 4–17) została uchylona w związku z wejściem w życie rozporządzenia (UE) 2023/988 (Dz. Urz. UE L 135, 23.05.2023, s. 1–51).

[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych (Dz. Urz. UE L 136, 22.05.2019, s. 1–27).

wzięcie pod uwagę takich regulacji, które będą dookreślały i uzupełniały niniejsze rozporządzenie. Taką rolę można przypisać choćby dyrektywie 2005/29/WE[9] czy wyżej wymienionym przepisom z zakresu egzekwowania praw konsumentów. Dynamikę tej relacji ilustrują poszczególne przepisy DSA, które omówiono w punktach 3.3 i 3.4 poniżej. Poprzedza je punkt 3.2, który poświęcono podstawowym pojęciom odnoszącym się do podmiotów uwikłanych w ramy regulacyjne DSA. W centrum uwagi postawiono konsumenta.

3.2. Konsument jako podmiot w DSA

DSA jako rozporządzenie ramowo harmonizujące warunki świadczenia usług pośrednich stanowi wyraz nowego podejścia w stosunku do rozwiązań przyjętych jeszcze na początku ery cyfrowej w dyrektywie 2000/31/WE[10]. Oba akty prawne przewidują szereg obowiązków adresowanych do podmiotów profesjonalnych – dostawców usług społeczeństwa informacyjnego, skupiając się przy tym na kategorii usługodawców będących pośrednikami. Przy czym istotnym *novum*, jakie wprowadzono w tym zakresie w DSA, jest zróżnicowanie obowiązków nakładanych na pośredników w zależności od ich znaczenia dla środowiska cyfrowego, w szczególności stopnia oddziaływania mierzonego liczbą aktywnych odbiorców usługi (zob. art. 3 lit. p i q DSA oraz motyw 77 preambuły DSA). Wyraża się to rozróżnieniem standardów należytej staranności dla podmiotów profesjonalnych objętych przepisami poszczególnych sekcji rozdziału 3 DSA (art. 11–48). Otwiera ją lista obowiązków mających zastosowanie do wszystkich dostawców usług pośrednich (sekcja 1), a kolejne sekcje wprowadzają dodatkowe przepisy odnoszące się do kolejnych podkategorii podmiotów.

Architektura DSA. Taki sposób ujęcia zasadniczych przepisów rozporządzenia można porównać do układu centrycznego składającego się z wielu przylegających płaszczyzn lub zbiorów obejmujących przepisy kształtujące obowiązki danej grupy przedsiębiorców. Punktem wyjścia (jądro, centrum) dla tego układu stanowią obowiązki dotyczące wszystkich dostawców usług pośrednich. Kolejne płaszczyzny, zmierzając w kierunku od centrum na zewnątrz, tworzą kolejne przepisy mające zastosowanie do dostawców usług hostingu, następnie do dostawców platform internetowych, platform internetowych umożliwiających zawieranie umów B2C,

[9] Dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z dnia 11 maja 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, 11.06.2005, s. 22–39).

[10] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (Dz. Urz. UE L 178, 17.07.2000, s. 1–16).

aż po dodatkowe przepisy adresowane do dostawców bardzo dużych platform internetowych (VLOP) i bardzo dużych wyszukiwarek internetowych (VLOSE).

Zorientowanie tych przepisów na profesjonalnych aktorów rynku jest oczywiste. Pozwala jednocześnie poszczególne płaszczyzny tak sformułowanych obowiązków odczytywać z perspektywy pozostałych podmiotów tworzących środowisko internetowe, a mianowicie pojemnej kategorii **„odbiorców usługi"** (ang. *recipient of the service*, niem. *Nutzer*). Pojęcie to zdefiniowano na potrzeby DSA w art. 3 lit. b DSA oraz wyjaśniono w motywie 2 jego preambuły. Tam właśnie wskazano, że za odbiorców usługi uważa się „użytkowników biznesowych, konsumentów i innych użytkowników". Takie ujęcie, znacznie bardziej niż definicja legalna, uwydatnia zróżnicowany charakter podmiotów, które zgodnie z DSA mają stanowić odbiorców usługi (użytkowników). Odpowiada ono specyfice trójstronnych modeli biznesowych typowych dla współcześnie działających platform internetowych. Jednocześnie umieszczenie w tej grupie podmiotów konsumentów obok użytkowników biznesowych[11] sprawia, że obie podgrupy należy traktować jako funkcjonalnie powiązane z uwagi na ich wzajemne relacje oraz pozycję wobec pośrednika, w szczególności platformy internetowej.

W przepisach szczegółowych DSA skorzystano oczywiście z rozróżnienia konsumentów od innych odbiorców usług, co uwzględniono poniżej, odrębnie omawiając przepisy adresowane do konsumentów (pkt 3) oraz te, które dotyczą ich pośrednio (pkt 4). Niniejszą próbę zmapowania korzyści dla konsumentów oparto na założeniu korelacji obowiązków nakładanych na pośredników z uprawnieniami odbiorców usług, w szczególności konsumentów. Owo sprzężenie między obowiązkiem a prawem jest typowe dla stosunków cywilnoprawnych w klasycznym ujęciu, chociaż wymaga uwzględnienia specyfiki relacji trójstronnych występujących w środowisku platform internetowych. Przykładem, który ilustruje konieczność zindywidualizowanego podejścia przy identyfikacji odbiorców usługi, może być sytuacja występująca na jednej z bardzo dużych platform internetowych (serwis LinkedIn)[12]. Jest ona wykorzystywana przez osoby fizyczne, niemniej przeważnie w celach, które są związane z ich działalnością zawodową. Tym samym na tle przesłanek definicji legalnej z art. 3 lit. c DSA przepisy rozporządzenia, które adresowane są wyłącznie do konsumentów (głównie w relacji B2C), mogą nie znaleźć zastosowania wobec tej usługi. Nadal stosowane będą jednak przepisy służące interesom pozostałych odbiorców usług, niezawężone wyłącznie do ich podgrupy obejmującej wyłącznie konsumentów.

[11] DSA nie definiuje tego pojęcia, ale czyni to rozporządzenie (UE) 2019/1150 (Dz. Urz. UE L 186, 11.07.2019, s. 57–79), które w ślad za art. 2 ust. 4 DSA, można potraktować jako uzupełniające DSA w tym względzie. W tym kontekście warto zwrócić uwagę na pojęcia „użytkownik biznesowy" oraz „użytkownik końcowy" zdefiniowane w art. 2 DMA (zob. rozdział IV pkt 4.4).

[12] Ich aktualizowaną listę opublikowano na stronie https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (dostęp: 3.04.2025).

Definicja pojęcia „konsument". Brzmienie art. 3 lit. c DSA nie odbiega od definicji znanych z klasycznych regulacji z zakresu unijnego prawa ochrony konsumentów (np. dyrektywy 2011/83/UE[13], dyrektywy 2005/29/WE czy rozporządzenia (UE) 2017/2394). Zbieżność nie jest przy tym zaskakująca, pozwala bowiem na konsekwentne rozgraniczenie tej grupy podmiotów, dla której prawo unijne przewiduje szczególny reżim ochronny. W ten sposób możliwa jest realizacja dyrektywy unijnej polityki konsumenckiej – „co jest nielegalne offline, powinno być nielegalne online" (por. rozdział I).

W kilku przypadkach omówionych poniżej (por. pkt 3.3) DSA zawiera przepisy wyraźne odnoszące się do konsumentów. Należy jednak z całą mocą podkreślić: nie oznacza to, że tylko takie przepisy będą stanowiły pole stosowania konsumenckiego *acquis*. Wszędzie bowiem tam, gdzie DSA odnosi się do „odbiorców usługi" bez wyraźnej delimitacji, o którą z podkategorii użytkowników chodzi, każdorazowy stan faktyczny będzie wymagał uważnej oceny strony podmiotowej, tak by rozstrzygnąć, czy daje on podstawę do sięgnięcia po reżim konsumencki. Funkcjonalne powiązanie kilku podkategorii użytkowników, a także potencjalne interakcje między nimi mogą przełożyć się również na ukształtowanie unijnego standardu ochrony odbiorcy usług społeczeństwa informacyjnego. Przy ewolucji takiego standardu znaczącą rolę odegrać może założenie wysokiego poziomu ochrony praw konsumentów realizowane konsekwentnie przez Unię Europejską.

Uwzględniając definicję legalną z DSA, konsument pozostaje *homo economicus passivus*. Pozwala to odróżnić go od pozostałych użytkowników (odbiorców usług), w szczególności biznesowych, ale także tych, którzy w środowisku internetowym realizują cele niewpisujące się w kontekst gospodarczy (działalność polityczna, charytatywna itp.). Dalsze zniuansowanie tego pojęcia z uwagi choćby na dynamikę i zmienność funkcji, jakie mogą pełnić odbiorcy usług społeczeństwa informacyjnego, pozostanie rolą orzecznictwa. Istniejący w tym zakresie dorobek TSUE[14] może stanowić pewien punkt odniesienia. Nie ulega wątpliwości, że w znacznej mierze dopiero praktyka stosowania DSA pokaże, na ile szczególna architektura tego aktu, w tym specyficzne relacje między podmiotami wchodzącymi w interakcje na rynku usług cyfrowych, powinny zostać odzwierciedlone w kontekście ochrony konsumenta.

---

[13] Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z dnia 25 października 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, 22.11.2011, s. 64–88).

[14] Por. wyrok TSUE z dnia 25 stycznia 2018 r. w sprawie C-498/16, *Maximilian Schrems przeciwko Facebook Ireland Limited* (ECLI:EU:C:2018:37), dotyczący oceny statusu prawnego użytkownika prywatnego konta na portalu społecznościowym w kontekście jurysdykcyjnym, oraz wyrok TSUE z dnia 8 czerwca 2023 r. w sprawie C-570/21, *I.S., K.S. przeciwko YYY*, odnoszący się do przesłanek pojęcia konsumenta w szczególnym kontekście kontraktowym (umowy o podwójnym charakterze).

Charakterystyczna dla DSA perspektywa łączenia zasady ochrony konsumentów z prawami podstawowymi zdecydowanie skłania do intensyfikacji trwającej już dyskusji nad potrzebą rekonceptualizacji pojęcia konsumenta z uwzględnieniem specyficznych warunków środowiska cyfrowego[15], w tym jego wymiaru obywatelskiego[16] zawartego w formule społeczeństwa informacyjnego.

3.3. Konsument jako podmiot w DSA na platformach B2C

3.3.1. Wyjątek konsumencki przy odpowiedzialności za usługi hostingu

Obok zupełnie nowych przepisów dotyczących świadczenia usług pośrednich, w DSA pojawiają się również takie, które stanowią modernizację dotychczasowych rozwiązań. Ma to miejsce w przypadku standardu odpowiedzialności dostawców usług pośrednich, który pierwotnie został ukształtowany w odniesieniu do handlu elektronicznego przez dyrektywę 2000/31/WE. Część jej przepisów w zmodernizowanej wersji została inkorporowana do DSA w postaci art. 4–6 i art. 8. Ich odpowiedniki z dyrektywy 2000/31/WE zostały natomiast uchylone na mocy art. 89 DSA[17]. Sprzyja to niewątpliwie ukształtowaniu jednolitego standardu regulacyjnego w całej UE.

Przesłanki towarzyszące wyłączeniu odpowiedzialności dostawców usług pośrednich przewidziane w DSA w większości stanowią powtórzenie rozwiązań przewidzianych w dyrektywie 2000/31/WE. Jednak w przypadku art. 6 DSA, który odnosi się do wyłączenia odpowiedzialności dostawcy usługi hostingu, wprowadzono nowy przepis uwzględniający interesy konsumentów, w tym ich prawo do skutecznej ochrony interesów gospodarczych oraz prawo do informacji zawarte w formule transparentności i bezpieczeństwa środowiska internetowego akcentowanej w DSA. To nowe rozwiązanie zawarte w art. 6 ust. 3 DSA w kaskadowej strukturze tego przepisu zajmuje szczególne miejsce. Ustęp 1 określa bowiem przesłanki wyłączenia (ang. *exemption*) odpowiedzialności dostawcy usługi hostingu, podczas gdy ust. 2–3 wprowadzają wyłączenie na drugim poziomie (ang. *counter-exception*), wskazując na przypadki, kiedy to właśnie wyłączenie z ust. 1 nie ma zastosowania, a zatem możliwa jest odpowiedzialność dostawcy.

---

[15] S. Umit Kucuk, *Consumerism in the Digital Age*, „Journal of Consumer Affairs" 2016, t. 50, nr 3, s. 533, https://doi.org/10.1111/joca.12101.

[16] I. Benöhr, op. cit., s. 173; N. Helberger et al., *Digital Consumers and the Law: Towards a Cohesive European Framework*, Alphen aan den Rijn, 2013, s. 8 i n.; L. McShane, C. Sabadoz, *Rethinking the Concept of Consumer Empowerment: Recognizing Consumers as Citizens*, „International Journal of Consumer Studies" 2015, t. 39, nr 5, s. 547, https://doi.org/10.1111/ijcs.12186.

[17] W konsekwencji również właściwe przepisy przyjęte w ramach transpozycji tej dyrektywy w państwach członkowskich UE przestały obowiązywać, a w ich miejsce weszły stosowane bezpośrednio w prawie krajowym przepisy DSA.

Skutkiem zastosowania wyjątku konsumenckiego z art. 6 ust. 3 DSA będzie odpowiedzialność dostawcy usług pośrednich, chociaż jednocześnie nie każdej kategorii takiego podmiotu, lecz jedynie – jak wyraźnie wskazano w tym przepisie – dostawców platform internetowych umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość (tzw. platformy B2C). Z perspektywy obecnego kształtu przepisów dotyczących odpowiedzialności dostawców cyfrowych art. 6 ust. 3 DSA można ocenić jako ukłon w kierunku konsumentów korzystających z tego typu platform. Tam bowiem występuje największe ryzyko naruszenia ich interesów, a zatem również potrzeba jego minimalizowania. Jednocześnie w swoim ogólnym założeniu przepis ten nawiązuje do obowiązków platform B2C, którym w DSA poświęcono odrębne przepisy, w szczególności dotyczące identyfikowalności przedsiębiorców (zob. pkt 3.3.2 poniżej). Przypisanie bowiem odpowiedzialności platformie B2C będzie możliwe po spełnieniu przesłanek wynikających z art. 6 ust. 3 DSA, wśród których istotne znaczenie ma sposób, w jaki platforma B2C „przedstawia określoną informację lub w inny sposób umożliwia zawarcie danej transakcji".

***Wpływ konsumenckiego* case law.** Sam mechanizm ponoszenia odpowiedzialności przez pośrednika, który wyłania się na tle brzmienia tego przepisu, nie jest w pełni nowy. Odpowiada bowiem rozwiązaniom wypracowanym jeszcze na gruncie znacznie wcześniejszych niż DSA unijnych przepisów dotyczących praw konsumenta przy sprzedaży towarów konsumpcyjnych[18]. W sprawie C-149/15 (*Wathelet*)[19] dotyczącej sprzedaży konsumentowi używanego samochodu w wyroku z 2016 r. TSUE, orzekając na podstawie wówczas obowiązujących przepisów dyrektywy 1999/44/WE[20], uznał, że odpowiedzialność sprzedawcy powinna być rozciągnięta na pośrednika-przedsiębiorcę, który nie poinformował konsumenta w należyty sposób o tym, że właścicielem sprzedawanego towaru jest osoba fizyczna. Wyrok ten jest aktualnie przywoływany[21] jako rozwiązanie modelowe, które wykorzystano w środowisku cyfrowym pod rządami DSA. Ponownie potwierdza to podążanie przez UE w kierunku obranym w polityce konsumenckiej wyrażonym formułą „co jest nielegalne offline, powinno być nielegalne online".

Wzorzec „przeciętnego konsumenta". Ocena działań platformy B2C na gruncie art. 6 ust. 3 DSA odbywa się przy zastosowaniu kryterium „przeciętnego konsu-

[18] Por. M. Dregelies, *Verbraucherschutz im Digital Services Act*, „Verbraucher und Recht" 2023, nr 5, s. 176.

[19] Wyrok TSUE z dnia 9 listopada 2016 r., *Sabrina Wathelet przeciwko Garage Bietheres & Fils SPRL* (ECLI:EU:C:2016:840).

[20] Uchylonej na mocy przepisów dyrektywy (UE) 2019/771, tzw. dyrektywy Omnibus (Dz. Urz. UE L 136, 22.05.2019, s. 28–50), której przyjęcie z kolei służyło w znacznej mierze realizacji unijnej strategii jednolitego rynku cyfrowego.

[21] H. Schulte-Nölke, *The EU Digital Services Act and EU Consumer Law*, w: A. de Franceschi, R. Schulze (red.), *Harmonizing Digital Contract Law: The Impact of EU Directives 2019/770 and 2019/771 and the Regulation of Online Platforms: A Handbook*, Baden-Baden 2023, s. 708.

menta". To z jego perspektywy dokonywana będzie weryfikacja transparentności transakcji na platformie oraz identyfikowalności podmiotów zaangażowanych w nią od strony profesjonalnej. Przekonanie takiego konsumenta, że przedmiotowe informacje zostały przekazane przez samą platformę internetową albo przez przedsiębiorców (odbiorców usługi) działających z jej upoważnienia lub pod jej kontrolą, będzie rozstrzygało o przypisaniu odpowiedzialności właśnie platformie, a nie przedsiębiorcy pozostającemu w relacji B2C z konsumentem. Pojęcie „przeciętnego konsumenta" wywodzi się z orzecznictwa TSUE, skąd na poziomie legislacyjnym zostało zakotwiczone w dyrektywie 2005/29/WE jako punkt odniesienia dla stosowania zakazu nieuczciwych praktyk handlowych. Przeniesienie go na grunt DSA oznacza poszerzenie zakresu jego zastosowania w obrębie działalności dostawców usług pośrednich, uzasadniając tym samym przypisywany mu w literaturze walor „wzorca wszelkich rzeczy"[22]. Jednocześnie stanowić może impuls do dalszego rozwoju tego kryterium właśnie z uwzględnieniem specyfiki środowiska internetowego, a w szczególności relacji, w których w tym środowisku występują konsumenci.

3.3.2. Należyta staranność platform B2C wobec konsumentów

W strukturze rozdziału 3 DSA, określającego obowiązki dostawców usług pośrednich w zakresie należytej staranności, w odrębnej sekcji (sekcja 4) przewidziano dodatkowe przepisy (art. 29–32 DSA) dotyczące dostawców platform internetowych umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość, czyli platform internetowych B2C[23].

Artykuł 29 DSA przewiduje wyłączenie stosowania przepisów zawartych w tej sekcji wobec określonych kategorii przedsiębiorców: mikroprzedsiębiorstw i małych przedsiębiorstw[24]. Takie rozwiązanie nie jest spotykane w klasycznych przepisach prawa konsumenckiego UE, w których sama idea harmonizacji pewnych aspektów funkcjonowania rynku, w tym jednolitego rynku cyfrowego przy zachowaniu wysokiego poziomu ochrony konsumentów, oznacza rozwiązanie korzystne dla przedsiębiorców, w szczególności w sektorze małych i średnich przedsiębiorstw[25].

[22] H.-W. Micklitz, *Unfair Commercial Practices and Misleading Advertising*, w: N. Reich et al. (red.), *European Consumer Law*, op. cit., s. 94. W kontekście stosowania tych przepisów wobec platform określanych jako *social media*, zob.: M. Dregelies, op. cit., s. 178.

[23] W kontekście terminologicznym w obrębie unijnego prawa konsumenckiego warto wskazać na pojęcie „internetowa platforma handlowa" wprowadzone przez wyżej przywołaną dyrektywę Omnibus do dyrektywy 2005/29/WE. Obejmuje ono zarówno platformy internetowe B2C, jak i C2C. Jest tym samym szersze od tego użytego w DSA, choć jednocześnie w omawianym tutaj rozporządzeniu nie znajdziemy definicji legalnej pojęcia „platforma internetowa B2C", a jedynie definicję terminu „platforma internetowa" (art. 3 lit. i DSA). Por. również pojęcie „dostawca internetowej platformy handlowej" z art. 3 pkt 14 rozporządzenia (UE) 2023/988 (Dz. Urz. UE L 135, 23.05.2023, s. 1–51).

[24] Analogicznie wyłączenie przewidziano w ramach sekcji 3 rozdziału 3 – zob. art. 19 DSA.

[25] Por. motywy 3 i 10 dyrektywy (UE) 2019/771.

DSA z kolei uzasadnia takie wyłączenie potrzebą uniknięcia nieproporcjonalnych obciążeń, jednocześnie podkreślając (w motywie 57 preambuły), że dostawcy usług, którzy korzystają z tego wyłączenia, obowiązki tej sekcji mogą wypełniać na zasadzie dobrowolności. Można w tym miejscu wyrazić wątpliwość, na ile mechanizm rynkowej konkurencji będzie generował dostateczną presję na dostosowanie się do wyższych (bardziej przyjaznych konsumentom) standardów, co pozwoliłoby zniwelować różnice w traktowaniu konsumentów, które wyłaniają się z obecnej konstrukcji przepisów DSA.

Rysunek 4. Nowe reguły należytej staranności platform internetowych B2C

Zasadnicze obowiązki platform internetowych B2C sformułowano w art. 30–32 DSA. Z perspektywy systematyki można mówić o trzech nowych regułach należytej staranności, których zwięzłe określenie towarzyszy każdemu ze wspomnianych przepisów zilustrowanych łącznie na rys. 4. W obszarze wspólnym, stanowiącym centrum i główny punkt ciężkości tych przepisów, znajduje się konsument, stąd odnosząc się do nich poniżej, wskazano, w jaki sposób wpływają one na sytuację prawną konsumenta w środowisku internetowym.

Identyfikowalność przedsiębiorców. Artykuł 30 DSA wpisuje się bezpośrednio w realizację celu przejrzystości środowiska internetowego. Ma on w pierwszej kolejności zapewniać, aby przedsiębiorcy mogli korzystać z platform internetowych B2C „jedynie w celu propagowania wiadomości o produktach lub usługach lub oferowania usług lub produktów konsumentom znajdującym się w Unii", niejako wykluczając używanie platform B2C w innych celach, wykraczających poza dosyć płynne granice transakcji rynkowej[26].

[26] Do zjawisk występujących poza tym obszarem można zaliczyć reklamę polityczną, która od niedawna w UE podlega przepisom rozporządzenia (UE) 2024/900 (Dz. Urz. UE L, 2024/900, 20.03.2024).

Przepis ten dotyczy przede wszystkim relacji między platformami a działającymi na nich przedsiębiorcami (P2B), od tych pierwszych wymagając, by uzyskali informacje o tych przedsiębiorcach (służące ich identyfikacji i ujęte w postaci wyliczenia w art. 30 ust. 1 lit. a–d DSA), a dodatkowo dołożyli „wszelkich starań", żeby te informacje zweryfikować jako wiarygodne i pełne (art. 30 ust. 2 DSA). W tych obu ustępach można dostrzec niewątpliwe pogłębienie reguły „znaj swojego klienta biznesowego" (ang. *know your business customer*, KYBC), wskazanej wcześniej w przepisach dyrektywy 2000/31/WE. Ich odpowiednikiem w obrocie B2C są wymogi informacyjne przewidziane w dyrektywie 2011/83/UE czy w dyrektywie 2005/29/WE, ale oczywiście bez jednoczesnego obowiązku ich weryfikacji, który występuje wyłącznie w relacji P2B. Dodać należy, że opisywany tutaj wymóg należytej staranności ma być realizowany na wczesnym etapie, a mianowicie przed skorzystaniem przez przedsiębiorcę z usług dostawcy platformy[27].

Konstrukcja identyfikowalności przedsiębiorców na platformach B2C jest wzmocniona poprzez mechanizm egzekwowania w zakresie terminowego dostarczania, a także prawidłowości wymaganych informacji. Przybiera on postać odmowy zezwolenia na korzystanie z platformy, żądania usunięcia uchybień oraz zawieszenia świadczenia usług na rzecz takiego przedsiębiorcy, jednocześnie przyznając przedsiębiorcom swoiste prawo obrony ich interesów poprzez korzystanie z procedur wnoszenia skarg przewidzianych w art. 20–21 DSA dla odbiorców usług.

Unijny konsument jest pośrednim beneficjentem opisanego wyżej mechanizmu[28]. Uzyskuje dzięki niemu dodatkową płaszczyznę (relacja P2B) weryfikacji informacji, które mają istotne znaczenie na przedpolu transakcji B2C na platformie, niezależnie od wymogów informacyjnych, które przedsiębiorcy zobowiązani są wypełniać w relacji B2C. Niewątpliwie służy to ochronie jego interesów w razie potencjalnego sporu z przedsiębiorcą. Jednocześnie obowiązek przechowywania takich informacji przez dostawcę platformy internetowej, ograniczony do okresu 6 miesięcy po zakończeniu stosunku umownego P2B, nie osłabia istotnie prokonsumenckiego charakteru art. 30 DSA, ponieważ jak wskazano na wstępie (pkt 3.3.1) obowiązuje on bez uszczerbku dla pozostałych przepisów unijnego prawa konsumentów[29].

Zgodność w fazie projektowania. Znaczenie właśnie tych przepisów z obszaru prawa konsumentów, ale także unijnych reguł bezpieczeństwa produktów, podkreśla również obowiązek wynikający z art. 31 DSA. Analogicznie jak w przypadku identyfikowalności przedsiębiorców przepis ten dotyczy relacji P2B, wymagając od

[27] Dla przedsiębiorców, którzy korzystają już z usług platform internetowych B2C, w art. 30 ust. 2 akapit 2 DSA przewidziano termin na dostosowanie się do nowych obowiązków, który upływa po 12 miesiącach od dnia rozpoczęcia stosowania DSA, tj. od 17 lutego 2024 r.

[28] Jedynie część informacji o danym przedsiębiorcy, które uzyskuje dostawca platformy internetowej, podlega udostępnieniu bezpośrednio odbiorcom „co najmniej na interfejsie platformy" (art. 30 ust. 7 DSA).

[29] Komplementarne obowiązki przedsiębiorców dotyczące identyfikowalności wprowadza rozporządzenie (UE) 2023/988 – por. motyw 58 jego preambuły.

platform internetowych zaprojektowania i organizacji swojego interfejsu internetowego w taki sposób, aby umożliwić przedsiębiorcom działającym na platformie wypełnianie spoczywających na nich obowiązków informacyjnych o charakterze przedkontraktowym wynikających z prawa UE. DSA wymienia tutaj przykładowo rozporządzenie (EU) 2019/1020[30], jak również inne akty prawne (zob. motyw 74 preambuły). Ich listę aktualnie uzupełnia rozporządzenie (UE) 2023/988.

Jednocześnie w art. 31 ust. 2 DSA wskazano minimalne wymogi dotyczące kilku kategorii informacji (np. znaki identyfikujące przedsiębiorcę czy informacje dotyczące etykietowania i oznakowania produktów). W żadnym jednak przypadku konsekwencją zgodności w fazie projektowania nie jest ogólny obowiązek monitorowania produktów lub usług przez platformy internetowe B2C, co koresponduje choćby z art. 8 DSA. Platformy internetowe B2C mają dokładać jedynie „rozsądnych starań" (art. 31 ust. 3 DSA) w zakresie sprawdzenia, czy oferowane za ich pośrednictwem produkty lub usługi zostały zidentyfikowane jako nielegalne. Źródłem takich ustaleń może być przykładowo zmodyfikowany Unijny System Szybkiej Informacji, którego skróconą nazwę „RAPEX" na mocy rozporządzenia (UE) 2023/988 przemianowano na „Safety Gate"[31].

Obowiązek zapewnienia zgodności w fazie projektowania ma konstrukcję zasadniczo zbliżoną (nieco mniej rozbudowaną) w stosunku do pierwszego z obowiązków (identyfikowalność przedsiębiorców) przewidzianych w sekcji 4 rozdziału 3 DSA. Z perspektywy konsumentów jego niewątpliwym walorem jest wzmocnienie przepisów Unii, które konkretyzują prawa konsumenta do określonych informacji, a także chronią ich zdrowie czy życie w zakresie bezpieczeństwa produktów[32]. Projekt i organizacja technologii (software) wyrażone konkretnym interfejsem internetowym tworzącym architekturę samej platformy ma tym samym, wedle art. 31 DSA, służyć wzmocnieniu skuteczności przepisów prawa powszechnie obowiązującego. Uzasadnione jest rozpatrywanie tej regulacji w połączeniu z pozostałymi przepisami DSA odnoszącymi się do kwestii projektowania i organizacji interfejsów internetowych oraz usług świadczonych przez dostawców platform przy ich użyciu (art. 25, 28, 34–35 DSA).

Prawo do informacji. Katalog reguł należytej staranności adresowanych do platform internetowych B2C zamyka art. 32 DSA. Formułuje on skonkretyzowany obowiązek reagowania przez dostawcę platformy, który „poweźmie wiadomość […] o nielegalnym produkcie lub usłudze oferowanych […] za jego pośrednictwem" (art. 32 ust. 1 DSA). Taka reakcja polegać ma na przekazywaniu konsumentom,

[30] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 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. L 169, 25.06.2019, s. 1–44).

[31] Obowiązek korzystania z tego portalu w odniesieniu do bezpieczeństwa produktów wprowadzono na podstawie art. 22 rozporządzenia (UE) 2023/988.

[32] M. Dregelies, op. cit., s. 179.

którzy nabyli nielegalny produkt lub usługę, trzech rodzajów informacji: o tym, że produkt lub usługa są nielegalne, o tożsamości przedsiębiorcy oraz wszelkich odpowiednich środkach odwoławczych. Obowiązek ten podlega realizacji *ex post*, co różni go od mechanizmów przewidzianych w art. 30 i 31 DSA. Dodatkowo jego warunkiem jest to, aby dostawca platformy B2C posiadał dane kontaktowe konsumentów. Jeżeli jednak takowych nie posiada, aktualny staje się wariant tego obowiązku w postaci podania wyżej wymienionych informacji do wiadomości publicznej i w łatwo dostępny sposób na interfejsie internetowym danej platformy B2C (art. 32 ust. 2 DSA).

Tak skonstruowany obowiązek można uznać za skorelowany z prawem do informacji, które ma realizować się w relacji P2C. W odróżnieniu od dwóch wyżej omówionych reguł staranności na platformach B2C ten ostatni przepis stwarza dla konsumentów najbardziej bezpośredni instrument realizacji ich praw do informacji oraz ochrony przed nielegalnymi towarami lub usługami, które mogą między innymi godzić w ich interesy ekonomiczne. Znaczenie tego obowiązku można ocenić w obrębie DSA jako istotne uzupełnienie narzędzi służących zwalczaniu nielegalnych treści[33]. Ich pojęcie, zdefiniowane w art. 3 lit. h DSA, jak wskazano w motywie 12 preambuły DSA, powinno „w szerokim zakresie odzwierciedlać istniejące przepisy w środowisku pozainternetowym", co można odczytywać wprost jako realizację dyrektywy określonej w unijnej polityce konsumenckiej (zob. rozdział I pkt 1.4). Przykłady informacji dotyczących nielegalnych treści, produktów, usług i działań wymieniono w wyżej przywołanym motywie preambuły DSA. Prawo do informacji w rozumieniu art. 32 DSA jest też istotnym uzupełnieniem, a tym samym wzmocnieniem istniejących, głównie publicznoprawnych, instrumentów informacyjnych dotyczących bezpieczeństwa produktu, w szczególności tych najnowszych poświęconych działalności platform internetowych[34].

3.4. Wybrane przepisy DSA z perspektywy konsumenckiej

Uwzględniając strukturę DSA, w tym w szczególności przepisy określające obowiązki dostawców usług pośrednich (zob. pkt 3.2) – wszędzie tam, gdzie beneficjentami tych obowiązków będą odbiorcy usług, również konsumenci będą korzystali z takich mechanizmów służących przejrzystemu i bezpiecznemu środowisku internetowemu. W poprzednim punkcie dokonano przeglądu takich mechanizmów wprost przeznaczonych dla konsumentów. W tym miejscu skoncentrowano się na wybranych

[33] Ibidem, s. 180 – autor krytycznie wskazuje zarówno na trudności w zakresie badania stanu wiedzy dostawcy platformy internetowej B2C w zakresie nielegalności produktu czy usługi, jak i na czasowe ograniczenie związania platformy omawianym obowiązkiem (zob. art. 32 ust. 1 akapit 2 DSA).

[34] Por. art. 35 rozporządzenia (UE) 2023/988.

przepisach DSA, które kręgu beneficjentów przewidzianych w nich rozwiązań nie zawężają do konsumentów, ale pośrednio służą również ich interesom. Podstawą tego wyboru jest w głównej mierze możliwość powiązania omawianych poniżej przepisów z typowymi źródłami prawa konsumenckiego (przepisy dotyczące klauzul umownych czy reklamy), w tym wrażliwości na potrzeby szczególnej grupy konsumentów (ochrona małoletnich).

3.4.1. Warunki korzystania z usług

Instrument, z jednej strony ingerujący w swobodę umów zawieranych przez dostawców usług pośrednich, a z drugiej będący wyrazem poszukiwania skuteczniejszej ochrony użytkowników, szczególnie w zakresie przysługującej im wolności wypowiedzi w środowisku cyfrowym, sformułowano w art. 14 DSA. Ma on postać szczególnego standardu informowania o ograniczeniach w korzystaniu z tych usług.

Jego centralnym elementem jest obowiązek informowania na temat wszelkich polityk, procedur, środków i narzędzi wykorzystywanych na potrzeby moderowania treści (art. 14 ust. 1 zd. 2 DSA), co należy odczytywać w połączeniu z bardzo szeroko zakreśloną definicją legalną moderowania treści z art. 3 lit. t DSA. Przy czym merytoryczną warstwę tego obowiązku uzupełnia druga warstwa – wymóg formułowania takich informacji w określony sposób, w tym jasno i w sposób prosty, zrozumiały, przyjazny dla użytkownika i jednoznaczny (art. 14 ust. 1 zd. 3 DSA).

Nie jest celem niniejszych uwag prezentowanie całości tego rozbudowanego przepisu ani tym bardziej jego powiązań zarówno z innymi przepisami DSA, jak i z innymi aktami prawa UE. Zasadne jest natomiast podkreślenie znaczenia tej regulacji jako próby równoważenia interesów poszczególnych aktorów społeczeństwa informacyjnego. Jego wymiar „obywatelski" jest szczególnie ewidentny na tle zawartego w art. 14 ust. 4 DSA odesłania do praw i prawnie uzasadnionych interesów wszystkich zaangażowanych stron, w tym zapisanych w KPP UE i odnoszących się do odbiorców usługi. Spoglądając na niego z nieco węższej perspektywy prawa konsumenckiego uzasadnione jest odniesienie się do kilku kwestii.

„Przyjazny dla użytkownika". Po pierwsze, art. 14 DSA w zw. z art. 3 lit. u DSA, w którym zdefiniowano „warunki korzystania z usług", wprowadza w obszarze ochrony odbiorców usług, a tym samym również konsumentów, nowe przesłanki przy ocenie obowiązków informacyjnych służących kompensowaniu asymetrii informacyjnej typowej dla relacji B2C[35]. W wielu starszych, ale również w nowszych

[35] M. Husovec, *Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules*, „Berkeley Technology Law Journal" 2023, t. 38, nr 3, s. 918, https://doi.org/10.15779/Z38M902431.

przepisach dotyczących umów konsumenckich (np. w dyrektywie 93/13/EWG[36] czy w dyrektywie 2011/83/UE)[37], powtarza się wymóg wyrażania określonych informacji „w prostym, zrozumiałym języku"[38]. Jednak formuła użyta w DSA jest znacznie bardziej rozbudowana. Szczególną uwagę zwraca w niej przesłanka „przyjazności dla użytkownika", odnosząca się do języka, w którym formułowane mają być wymagane informacje. Pojawia się ona obok art. 14 DSA w wielu innych przepisach rozporządzenia (por. art. 12 ust. 1, art. 16 ust. 1, art. 41 ust. 1 DSA), ale również poza nim w unijnych przepisach tworzących ramy prawne funkcjonowania społeczeństwa cyfrowego[39]. Specyficzny zakres zastosowania tej przesłanki czyni z art. 14 DSA *lex specialis* wobec analogicznych przepisów prawa UE. Jednocześnie użycie jej obok pozostałych, tradycyjnych przesłanek wskazuje na odmienne znaczenie, które w kontekście relacji użytkownik–platforma można odczytywać jako potrzebę dopasowania formy językowej komunikacji czy jej zgodności z oczekiwaniami użytkownika w potocznym rozumieniu. W ujęciu dogmatycznym można tutaj dostrzec wyraz obowiązywania ogólnej zasady dobrej wiary, którą można wiązać z zasadą zaufania, również akcentowaną w DSA.

Kontrola klauzul. Po drugie, ustanowione przez dostawców usług pośrednich klauzule dotyczące ograniczeń nakładanych w związku z korzystaniem z ich usług będą podlegały ocenie przez pryzmat przepisów służących eliminowaniu nieuczciwych warunków w umowach konsumenckich, które w prawie państw członkowskich UE są efektem implementacji przepisów dyrektywy 93/13/EWG. Będzie to szczególnie istotne w kontekście zmian warunków korzystania z usług, o których wspomina art. 14 ust. 2 DSA, a które to zmiany dotyczyć mogą przecież również ograniczeń związanych z moderowaniem treści. Naruszenie zasad przejrzystości, które ustanawia DSA w omawianym zakresie, w kontekście ochrony konsumentów będzie mogło być egzekwowane właśnie na gruncie reżimu przewidzianego dla nieuczciwych warunków umów[40], który w szczególności pozwala na stwierdzenie, że dana klauzula nie jest wiążąca dla konsumenta (por. art. 6 dyrektywy 93/13/EWG). Takie rozstrzygnięcie w konsekwencji będzie mogło prowadzić do istotnych różnic

[36] Dyrektywa Rady 93/13/EWG z dnia 5 kwietnia 1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich (Dz. Urz. UE L 95, 21.04.1993, s. 29–34).

[37] Poza obszarem prawa konsumenckiego warto zwrócić uwagę na zastosowanie zasady transparentności w obszarze ochrony danych osobowych – por. motyw 58 rozporządzenia (UE) 2016/679 (Dz.Urz. UE L 119, 4.05.2016, s. 1–88).

[38] Standard „prostoty" i „zrozumiałości" jest przy tym wiązany z zasadą transparentności rozumianą jako subkategoria dobrej wiary – por. uwagi na tle dyrektywy 93/13/EWG: H.-W. Micklitz, *Unfair Terms in Consumer Contracts*, w: N. Reich et al. (red.), *European Consumer Law*, s. 143. Współcześnie warto w tym kontekście zwrócić uwagę na dobrowolny standard ISO dla prostego języka opublikowany 23 czerwca 2023 r. jako ISO 24495-1:2023 „Plain language Part 1: Governing principles and guidelines".

[39] Por. art. 1 pkt 5, 44–45 rozporządzenia (UE) 2024/1183 (Dz. Urz. UE L, 2024/1183, 30.04.2024) oraz motywy 7 i 52 rozporządzenia (UE) 2022/868 (Dz. Urz. UE L 152, 3.06.2022, s. 1–44).

[40] H. Schulte-Nölke, op. cit., s. 710 i n., autor zwraca uwagę na zmiany w brzmieniu omawianego przepisu proponowane w trakcie prac legislacyjnych nad projektem DSA.

w sytuacji prawnej konsumentów i pozostałych grup odbiorców usług, których interesom służyć ma art. 14 DSA.

Odnośnie do ochrony małoletnich, o których wspomina art. 14 ust. 3 DSA, zob. uwagi w pkt 3.4.3 poniżej.

3.4.2. Reklama internetowa

Szeroka definicja terminu „reklama" z art. 3 lit. r DSA pozostaje spójna z podejściem do usług społeczeństwa informacyjnego, które nie zamykają się jedynie w paradygmacie rynkowym („niezależnie od tego, czy w celach komercyjnych czy niekomercyjnych…"). Ten pierwszy był dominujący w dyrektywie 2000/31/WE, co ilustruje choćby porównanie definicji pojęcia „informacja handlowa" z art. 2 lit. f tejże (por. art. 3 lit. w DSA) z szerokim rozumieniem „reklamy" na gruncie DSA (por. motywy 68–69 preambuły DSA). DSA poświęca przy tym zjawisku reklamy znacznie więcej uwagi niż wspomniana dyrektywa, co dowodzi pewnej dojrzałości omawianej regulacji, szczególnie jeśli rozpatrywać ją łącznie z przepisami DMA dotyczącymi internetowych usług reklamowych[41].

Z perspektywy przejrzystości komunikacji w środowisku internetowym dla konsumenta niezwykle ważna jest adresowana do platform internetowych regulacja określająca obowiązki identyfikowania określonych informacji jako reklama lub informacja handlowa (art. 26 ust. 1 i 2 DSA). Połączono ją z zakazem reklamy opartej na profilowaniu z wykorzystaniem danych wrażliwych (art. 26 ust. 3 DSA). Szczególnie ten ostatni przepis doskonale ilustruje, jak silnie we współczesnym środowisku komunikacji elektronicznej skorelowane są reżimy dotyczące ochrony interesów ekonomicznych konsumentów jako aktorów rynku oraz ochrony danych osobowych.

W przypadku dostawców bardzo dużych platform internetowych i bardzo dużych wyszukiwarek internetowych DSA idzie dalej, formułując w art. 39 jeszcze wyższy standard przejrzystości praktyk reklamowych. Jest on wyrażony między innymi obowiązkiem ustanowienia i udostępnienia szczególnego zasobu w postaci repozytorium (ang. *repository*, niem. *Archiv*, fr. *registre*) minimalnych informacji odnoszących się do udostępnianych reklam. Jednocześnie systemy reklamowe stosowane przez tę szczególną kategorię dostawców usług pośrednich stanowią odrębny czynnik brany pod uwagę przy ocenie czy zmniejszaniu ryzyka systemowego stosownie do art. 34–35 DSA (por. motyw 79 i n. preambuły DSA).

Na tle obecnie szeroko rozbudowanego konsumenckiego prawa reklamy w UE[42], w obrębie którego można wyróżnić przepisy o charakterze ogólnym (dyrektywa

[41] Zob. rozdział IV pkt 4.4.3.

[42] Jego początków szukać można we wspólnotowym *case law* rozwijanym na tle swobód traktatowych, identyfikowanym w unijnej terminologii pod klasycznymi formułami (np. *Cassis de Dijon*, *Keck*, *Mars*).

2005/29/WE) oraz rozdrobnione, nierzadko fragmentaryczne sektorowe regulacje[43], można stwierdzić, że DSA stanowi istotne uzupełnienie obecnego reżimu w kontekście zjawiska reklamy internetowej. Zważywszy na wielorakie funkcje reklamy, jako narzędzia informacyjnego oraz perswazyjnego służącego wpływaniu na zachowania odbiorców, w środowisku cyfrowym przepisy te słusznie zlokalizowano obok zakazu zwodniczych interfejsów (ang. *dark patterns*) z art. 25 DSA[44] oraz regulacji dotyczącej stosowania systemów rekomendacji przez platformy internetowe z art. 27 DSA.

Nawet jeśli DSA jako regulacja o horyzontalnym zakresie oddziaływania na pośredników internetowych ogranicza pojęcie reklamy do informacji prezentowanych „przez platformę internetową na jej interfejsie internetowym" (art. 3 lit. r DSA), a tym samym nie reguluje zjawiska reklamy w Internecie w sposób zupełny, to zważywszy na pozycję platform w środowisku cyfrowym, szczególnie tych wskazanych jako VLOP, wskazane przepisy DSA mają do spełnienia istotną funkcję. Zakres ich stosowania nie będzie obejmował przedsiębiorców wyraźnie wyłączonych na mocy art. 19 DSA, co jest z kolei rozwiązaniem generującym ryzyko ukształtowania się odmiennych standardów należytej staranności w zakresie praktyk reklamowych. Wątpliwości na tym tle wydają się analogiczne do tych zasygnalizowanych powyżej na gruncie art. 29 DSA (por. pkt 3.3.2 powyżej).

3.4.3. Ochrona małoletnich

Kolejny poruszany na tle DSA wątek konsumencki wynika ze szczególnego potraktowania jednej grupy odbiorców usług, a mianowicie małoletnich. Można go odczytywać jako dowód realizacji wytycznych polityki konsumenckiej formułowanych zarówno na wczesnym etapie rozwoju ram regulacyjnych społeczeństwa informacyjnego[45], jak i we współczesnych unijnych dokumentach typu *soft law*[46].

[43] Dotyczą one specyficznych produktów (np. żywności, produktów leczniczych), środków rozpowszechniania (np. audiowizualnych usług medialnych) czy konkretnych treści. W tej ostatniej kategorii mieszczą się przepisy rozporządzenia (UE) 2024/900 dotyczące reklamy politycznej oraz proponowane przepisy w zakresie marketingu ekologicznego (zob. Komisja Europejska, Wniosek dotyczący dyrektywy w sprawie oświadczeń środowiskowych, COM(2023) 166 final, Bruksela, 22.03.2023).

[44] Przepis ten odnosi się do projektowania i organizacji interfejsów internetowych, co pozwala łączyć go z omówionym wcześniej art. 31 DSA, adresowanym do platform internetowych typu B2C (zob. pkt 3.3.2). Jednocześnie w art. 25 ust. 2 DSA wyraźnie odseparowano zakaz z ust. 1 od przepisów dyrektywy 2005/29/WE oraz rozporządzenia (UE) 2016/679 (por. motywy 67–68 preambuły DSA).

[45] Zob. motyw 4 rezolucji Rady z 19 stycznia 1999 r. (Dz. Urz. UE 1999/C 23/01), akcentujący potrzebę „ochrony dzieci przeciwko nieodpowiednim treściom".

[46] Zob. Komisja Europejska, Nowy program na rzecz konsumentów, op. cit., s. 21–22, w którym interesy dzieci i osób małoletnich ujęto w obrębie grup konsumentów szczególnie podatnych na zagrożenia.

Jednocześnie jest to wyraz większej uwagi, jaką UE poświęca prawom dziecka[47], również w szczególnym kontekście cyfrowej transformacji[48].

Przepisy DSA odnoszące się do tej grupy użytkowników usług społeczeństwa informacyjnego charakteryzuje podwyższenie standardu należytej staranności oczekiwanej od dostawców usług pośrednich. Ilustruje to art. 14 ust. 3 DSA, który skierowany jest do wszystkich dostawców usług pośrednich (zob. uwagi w pkt 3.4.1). Przewidziany w art. 14 ust. 1 DSA standard transparentności został zaostrzony przez wprowadzenie wymogu „wyjaśniania" warunków i ograniczeń połączonego z wymogiem zrozumiałości takich wyjaśnień dostosowanym do odbiorców, jakimi są właśnie małoletni. Pomijając brak definicji terminu „małoletni" w prawie UE[49], obowiązek z art. 14 ust. 3 DSA nie jest jednak dostatecznie precyzyjny, głównie z uwagi na sformułowanie mające służyć identyfikacji usługi pośredniej, której ma dotyczyć. Będzie on bowiem aktualny wyłącznie wówczas, kiedy taka usługa „jest skierowana przede wszystkim do małoletnich lub gdy korzystają z niej w głównej mierze małoletni", co jedynie bardzo zdawkowo objaśnia motyw 46 preambuły DSA.

Znacznie bardziej czytelną formułą posłużono się w art. 28 DSA, który jest jednym z przepisów adresowanych do „dostawców platform internetowych dostępnych dla małoletnich". Niemniej przepis ten, podobnie jak art. 14 ust. 3 DSA, można ocenić jako stosunkowo ogólny. Obowiązek zapewnienia wysokiego poziomu prywatności, bezpieczeństwa i ochrony małoletnich nie odbiega przecież od założenia wysokiego poziomu ochrony konsumentów od dawna wynikającego z art. 169 ust. 1 TFUE czy z art. 38 KPP UE. Z kolei wymóg realizacji tego celu przez platformy internetowe w drodze „wprowadzenia odpowiednich i proporcjonalnych środków", na co wskazuje art. 28 ust. 1 DSA, pozostawia im szeroki margines swobody. Jej granice jedynie potencjalnie będą ograniczane przez wytyczne Komisji wymienione w art. 28 ust. 4 DSA.

Analogicznie jak w przypadku relacji między art. 14 ust. 1 i ust. 3 DSA w odniesieniu do małoletnich w kontekście reklamy na platformach, zakres zakazu prezentowania reklam opartych na profilowaniu z art. 26 ust. 3 DSA został zaostrzony na gruncie art. 28 ust. 2 DSA. Wynika to z braku ograniczenia w postaci przesłanki wykorzystywania szczególnych kategorii danych osobowych. Niestety ostrze tego rygoru ulega „rozwodnieniu" w kontekście ustalania statusu odbiorcy usługi jako małoletniego, kiedy wymaganie od platformy internetowej wiedzy „z wystarczającą pewnością", że odbiorca usługi jest małoletni (art. 28 ust. 2 DSA), należy rozpatrywać

[47] Zob. Komisja Europejska, Strategia UE na rzecz praw dziecka (COM(2021) 142 final, Bruksela, 24.03.2021), s. 19, w której ówczesny projekt DSA został przywołany wprost.

[48] W treści Europejskiej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie konieczność ochrony i wzmacniania pozycji dzieci i młodzieży w internecie została podkreślona w ramach rozdziału 5 – Bezpieczeństwo, ochrona i wzmocnienie pozycji, w szczególności w art. 20–22.

[49] Rada Europy, Agencja Praw Podstawowych Unii Europejskiej, *Handbook on European Law Relating to the Rights of the Child*, Luxembourg 2022, s. 19, https://data.europa.eu/doi/10.2811/610564 (dostęp: 3.04.2025).

w połączeniu z brakiem obowiązku przetwarzania dodatkowych danych osobowych w celu oceny, czy odbiorca usługi jest małoletni (art. 28 ust. 3 DSA).

Biorąc pod uwagę powyższe krytyczne uwagi, ale również i to, że wskazane przepisy nie wyczerpują bynajmniej odesłań do kwestii ochrony małoletnich zawartych w DSA[50], uzasadnione jest sformułowanie stanowiska, że w swoim podejściu do problemu ochrony tej grupy szczególnie podatnej na ryzyka środowiska cyfrowego DSA stanowi ważny krok naprzód. Jednocześnie, oceniając w sposób ogólny podejście regulacyjne DSA w zakresie ochrony małoletnich, może ono się wydawać podobne do tego, jakie oferuje unijny reżim w zakresie ochrony danych osobowych (por. przede wszystkim rozporządzenie (UE) 2016/679). DSA bowiem nie ogranicza się do traktowania małoletnich wyłącznie w kontekście rynkowym jako konsumentów. Jest to oczywistą konsekwencją celu zakreślonego w art. 1 DSA, co wiąże się między innymi z tym, że oba rozporządzenia nie stanowią klasycznych aktów z zakresu prawa ochrony konsumentów (por. uwagi w pkt 3.1).

W kontekście ochrony wrażliwych grup konsumentów DSA pozostawia jednak istotny niedosyt, ponieważ akcentuje w sposób uzasadniony potrzebę ochrony małoletnich, ale niemalże[51] pomija w szczególności interesy odbiorców usług, którzy z uwagi na wiek (osoby starsze) są również narażeni na szczególne ryzyka, a w efekcie postępującej gwałtownie cyfryzacji powinni również móc liczyć na wsparcie ze strony unijnego prawodawcy w realizacji spójnej wizji społeczeństwa informacyjnego.

3.5. Podsumowanie

DSA, jako instrument prawny będący niewątpliwie odpowiedzią na wyzwania współczesnego społeczeństwa informacyjnego w ramach gospodarki platform cyfrowych, w której kluczową rolę odgrywają dostawcy usług pośrednich, unowocześnia dotychczasowe unijne przepisy odnoszące się do handlu elektronicznego, dostrzegając interesy konsumentów wyróżnionych w obrębie odbiorców usług pośrednich. Nie kreuje jednak przy tym nowego pojęcia konsumenta, lecz opiera się na dotychczasowym unijnym *acquis* w obszarze ochrony konsumentów, w szczególności na wyrażonym w prawie pierwotnym UE dążeniu do zapewnienia wysokiego poziomu ochrony konsumentów na rynku wewnętrznym.

[50] Wyraźne odesłania dotyczące tej grupy odbiorców usług zawarto w przepisach adresowanych do dostawców VLOP i VLOSE dotyczących oceny i zmniejszania ryzyka systemowego – zob. art. 34–35 DSA. Por. również kampanię informacyjną prowadzoną w ramach unijnego Programu „Cyfrowa Europa" (DIGITAL), https://www.betterinternetforkids.eu/policy/digitalservicesact (dostęp: 3.04.2025).

[51] Zob. uwagi na temat przesłanki „przeciętny konsument" użytej w art. 6 ust. 3 DSA, który to przepis precyzuje granice odpowiedzialności platform internetowych (rozdział III pkt 3.3.1).

Nakładane na dostawców usług pośrednich obowiązki wymagają każdorazowo skorelowania z prawami, wśród których z perspektywy ochrony konsumentów na czoło wysuwa się prawo do bezpieczeństwa oraz prawo do informacji (przejrzystości) realizowane w postaci różnych przepisów tworzących swoistą architekturę DSA. W tym sensie DSA przyczynia się do wzmocnienia interesów konsumentów podobnie jak i pozostałych odbiorców usług.

Poszczególne przepisy DSA, zarówno te adresowane wprost do konsumentów na platformach internetowych B2C, jak i te odnoszące się do wszystkich odbiorców usług, a przez to kreujące pewne korzyści również dla konsumentów, potwierdzają nierzadko bardzo wyraźnie realizację dyrektywy unijnej polityki konsumenckiej wyrażoną w formule „co jest nielegalne offline, powinno być nielegalne online". W konsekwencji konieczne jest dostrzeżenie wielostronnych relacji łączących DSA z dotychczasowym *acquis consummateur*. Nie czyni to jednocześnie z DSA typowej regulacji z zakresu prawa ochrony konsumentów, lecz raczej uzasadnia potrzebę nowego spojrzenia na sytuację prawną konsumentów w środowisku cyfrowym, którego ramy prawne podlegają coraz szerszej oraz intensywnej rozbudowie w UE.

Rozdział IV

Uprawnienia przyznane uczestnikom rynków cyfrowych przez Akt o rynkach cyfrowych

4.1. Wprowadzenie

Jak wskazano w rozdziale I, DMA istotnie opiera się na unijnym prawie konkurencji pod względem charakteru regulacji oraz stopnia, w jakim materialne postanowienia DMA wynikają z wcześniejszej praktyki decyzyjnej Komisji w zakresie stosowania art. 102 TFUE. Wyjaśniono również, że w toku prac nad wprowadzeniem DSA Komisja pierwotnie odwoływała się do DMA jako do „nowego instrumentu prawa konkurencji", który z jednej strony miał opierać się na podobnych założeniach regulacyjnych, a z drugiej – być kierowany jedynie do największych przedstawicieli rynków cyfrowych.

Jednocześnie DMA i unijne prawo konkurencji istotnie się różnią pod wieloma względami. Zidentyfikowanie tych różnic pozwala w lepszym zrozumieniu, w jaki sposób obowiązki nałożone przez DMA na branżę big tech mogą być postrzegane jako źródło uprawnień przyznanych użytkownikom usług platformowych świadczonych przez te przedsiębiorstwa.

4.2. Kluczowe podobieństwa i różnice między DMA a prawem konkurencji

Pierwsza różnica dotyczy przedmiotu regulacji i zakresu zastosowania. Prawo konkurencji stosuje się do określonych praktyk podejmowanych na jakimkolwiek rynku. Stąd jego zakres zastosowania ma charakter horyzontalny (ogólny) i nie jest ograniczony do określonego rodzaju działalności czy obszaru prawnego.

Rynki cyfrowe. Z kolei przepisy DMA można uznać za sektorowe w tym sensie, że znajdują one zastosowanie do praktyk podejmowanych na rynkach cyfrowych, tj. w sektorze produktów dostarczanych i usług świadczonych przy użyciu lub za pośrednictwem usług społeczeństwa informacyjnego[1]. W istocie DMA znajduje

[1] Art. 2 pkt 4 DMA.

zastosowanie do podstawowych usług platformowych[2], świadczonych przez strażników dostępu.

Po drugie, prawo konkurencji znajduje zastosowanie do przedsiębiorstw[3], a w przypadku art. 102 TFUE – do przedsiębiorstw zajmujących pozycję dominującą na danym rynku właściwym. Pozycja dominująca definiowana jest jako „pozycja ekonomiczna przedsiębiorstwa, która umożliwia mu utrudnianie skutecznej konkurencji na rynku właściwym, poprzez możliwość przejawiania zachowań w znacznym stopniu niezależnych od innych konkurentów, klientów, a w końcu także od konsumentów"[4]. Pozycję dominującą ustala się przez określenie siły rynkowej i udziałów rynkowych danego przedsiębiorstwa oraz jego konkurentów[5].

Strażnicy dostępu. DMA znajduje z kolei zastosowanie do ściśle określonego rodzaju przedsiębiorstw, tj. do strażników dostępu. Artykuł 2 pkt 1 oraz art. 3 DMA stanowią, że są to przedsiębiorstwa świadczące podstawowe usługi platformowe i wskazane jako strażnicy dostępu w odpowiednim postępowaniu. Przedsiębiorstwo jest określane jako strażnik dostępu, jeśli spełnia łącznie następujące warunki[6]:

– wywiera znaczący wpływ na rynek wewnętrzny[7];

– świadczy podstawową usługę platformową będącą ważnym punktem dostępu, za pośrednictwem którego użytkownicy biznesowi docierają do użytkowników końcowych[8]; oraz

---

[2] Definicja podstawowych usług platformowych została zawarta w art. 2 pkt 2 DMA i zawiera: usługi pośrednictwa internetowego; wyszukiwarki internetowe; internetowe serwisy społecznościowe; usługi platformy udostępniania wideo; usługi łączności interpersonalnej niewykorzystujące numerów; systemy operacyjne; przeglądarki internetowe; wirtualnych asystentów; usługi przetwarzania w chmurze; internetowe usługi reklamowe.

[3] Czyli jakikolwiek podmiot prowadzący działalność gospodarczą niezależnie od formy prawnej czy źródeł finansowania, zob. wyrok TSUE z dnia 23 kwietnia 1991 r., sprawa C-41/90, *Klaus Höfner i Fritz Elser przeciwko Macrotron GmbH* (ECLI:EU:C:1991:161); R. Whish, D. Bailey, *Competition Law*, Oxford 2021, s. 85.

[4] Wyroki TSUE: z dnia 14 lutego 1978 r., sprawa 27/76, *United Brands Company i United Brands Continentaal BV przeciwko Komisji Wspólnot Europejskich* (ECLI:EU:C:1978:22), pkt 65; z dnia 13 lutego 1979, sprawa 85/76, *Hoffmann-La Roche & Co. AG przeciwko Komisji Wspólnot Europejskich* (ECLI:EU:C:1979:36) oraz z dnia 3 lipca 1991 r., sprawa C-62/86, *AKZO Chemie BV przeciwko Komisji Wspólnot Europejskich* (ECLI:EU:C:1991:286).

[5] Zob. szerzej: Komunikat Komisji, Wytyczne w sprawie priorytetów, którymi Komisja będzie się kierować przy stosowaniu art. 82 Traktatu WE w odniesieniu do szkodliwych działań o charakterze praktyki wyłączającej, podejmowanych przez przedsiębiorstwa dominujące (Dz. Urz. UE C 45, 24.02.2009, s. 7–20), pkt 9 i n.

[6] Art. 3 ust. 1–2 DMA.

[7] To kryterium odnosi się do wyników finansowych uzyskiwanych przez dane przedsiębiorstwo. Próg uznania za strażnika dostępu wynosi 7,5 mld EUR obrotu uzyskanego w Unii w każdym z ostatnich trzech lat obrotowych lub jeżeli jego średnia kapitalizacja rynkowa lub równoważna rzeczywista wartość rynkowa wynosiła co najmniej 75 mld EUR w ostatnim roku obrotowym. Dodatkowo dla uznania znaczącego wpływu na rynek wewnętrzny konieczne jest świadczenie przez strażnika dostępu podstawowych usług platformowych w przynajmniej trzech państwach członkowskich.

[8] Omawiane kryterium przekłada się na co najmniej 45 mln aktywnych miesięcznie użytkowników końcowych mających siedzibę lub miejsce pobytu w Unii oraz co najmniej 10 000 aktywnych rocznie użytkowników biznesowych z siedzibą w Unii.

– zajmuje ugruntowaną i trwałą pozycję w zakresie prowadzonej przez siebie działalności lub można przewidzieć, że zajmie taką pozycję w niedalekiej przyszłości[9].

Po trzecie, unijne prawo konkurencji zawiera ogólne zakazy, przede wszystkim dotyczące porozumień ograniczających konkurencję oraz nadużycia pozycji dominującej. Pojęcia te zostały doprecyzowane w katalogach otwartych określających praktyki antymonopolowe, zawartych w art. 101–102 TFUE. Jednocześnie prawo konkurencji cechuje pewna elastyczność przy ustalaniu w indywidualnych sprawach, czy dane działanie wchodzi w zakres danego zakazu. Podejście to niewątpliwie ma istotne zalety (w tym zdolność do identyfikowania nowych form naruszenia prawa konkurencji), jednakże wiążą się z tym istotne implikacje dla terminowości i dynamiki postępowań, w których każda praktyka musi zostać indywidualnie oceniona na podstawie ogólnych kryteriów naruszenia.

***Ściśle określone obowiązki i zakazy*.** Natomiast art. 5–7 DMA wprowadzają zamknięty katalog precyzyjnie określonych obowiązków i zakazów kierowanych do strażników dostępu. Niektóre z nich bezpośrednio wynikają z decyzji Komisji, wydawanych na podstawie art. 102 TFUE, w których stwierdzano antykonkurencyjne skutki takich praktyk jak korzystniejsze traktowanie własnych usług na platformie (self-preferencing) czy nieuczciwe wykorzystywanie danych przez platformy internetowe.

DMA między innymi zakazuje strażnikom dostępu zbierania, przetwarzania i udostępniania danych osobowych użytkowników końcowych platform. Żeby uniknąć efektów uzależnienia użytkowników, strażnicy dostępu nie mogą także uniemożliwiać użytkownikom biznesowym oferowania tych samych produktów lub usług użytkownikom końcowym po cenach lub na warunkach innych niż na platformach prowadzonych przez strażników dostępu. Są to jedynie niektóre przykłady ściśle określonych obowiązków i zakazów zawartych w DMA. Szersze omówienie wszystkich obowiązków (oraz tego, jak przekładają się one na uprawnienia użytkowników platform) przedstawiono w pkt 4.5 niniejszego rozdziału.

Po czwarte, prawo konkurencji egzekwowane jest *ex post*, co wymaga przeprowadzenia przez Komisję złożonego postępowania w celu stwierdzenia, czy doszło do naruszenia.

***Egzekwowanie* ex ante.** W DMA przyjęto odmienne podejście i wprowadzono mechanizmy egzekwowania *ex ante*. Jak wynika z art. 8 ust. 1 DMA, to na strażnikach dostępu ciąży obowiązek zapewnienia i wykazania zgodności ich działań z materialnymi obowiązkami wprowadzonymi przez omawiane rozporządzenie. Ponadto, zgodnie z art. 11 DMA, strażnicy dostępu składają Komisji sprawozdania opisujące środki wdrożone w celu zapewnienia zgodności działań strażników

[9] Kryterium trwałości zostaje spełnione, jeśli progi dotyczące liczby użytkowników zostały osiągnięte w każdym z ostatnich trzech lat obrotowych.

z postanowieniami DMA. Dodatkowo art. 15 DMA zobowiązuje strażników dostępu do przedstawiania raportów przygotowanych przez niezależnych audytorów, zawierających opis stosowanych technik profilowania konsumentów.

Komisja nadzoruje stosowanie się przez strażników dostępu do obowiązków wynikających z DMA. Kwestia ta została szerzej omówiona w rozdziale V, dotyczącym egzekwowania przepisów DSA i DMA.

Niekiedy podnosi się, że materialny zakres DMA nie wnosi wiele nowego w porównaniu do prawa konkurencji: w tym względzie przepisy DMA stanowić mają raczej swego rodzaju kodyfikację i doprecyzowanie praktyki decyzyjnej Komisji i krajowych organów ochrony konkurencji, funkcjonujących na podstawie unijnego i krajowego prawa konkurencji. Przyznaje się w tym kontekście, że zasadnicza wartość dodana wnoszona przez DMA wynika z aspektów proceduralnych rozporządzenia. Jak wspomniano, DMA daje nowe narzędzia egzekwowania prawa, pozwalające na przezwyciężenie ograniczeń wynikających ze stosowania prawa konkurencji[10].

4.3. Akt o rynkach cyfrowych jako źródło uprawnień użytkowników platform

4.3.1. Bezpośredni skutek prawa konkurencji UE

Odpowiadając na pytanie, czy dany akt prawa unijnego, pierwotnego czy wtórnego, może stanowić źródło uprawnień przyznanych jednostkom, w istocie dążymy do ustalenia, czy ów akt jest bezpośrednio skuteczny. Zagadnienie to było przedmiotem wątpliwości zwłaszcza na początku obowiązywania prawa unijnego, gdy zastanawiano się, czy Traktaty (oraz akty przyjęte na ich podstawie) stanowią źródła praw i obowiązków nałożonych jedynie na państwa członkowskie (jak to ma miejsce w przypadku prawa międzynarodowego publicznego, do którego porządku należą Traktaty), czy też jednostki również mogą być adresatami tych przepisów. Stąd zasada bezpośredniego skutku oznacza, że jednostki mogą wywodzić uprawnienia z prawa UE i powoływać się na te prawa bezpośrednio w postępowaniach przed sądami krajowymi[11].

Zasada ta bywa utożsamiana z cechą bezpośredniego stosowania, która oznacza, że określone akty prawa unijnego są stosowane w krajowych porządkach prawnych dokładnie w takim samym zakresie, w jakim zostały przyjęte przez unijnego prawodawcę. Jednocześnie akty bezpośrednio stosowane są co do zasady bezpośrednio

[10] O. Andriychuk, *Do DMA Obligations for Gatekeepers Create Entitlements for Business Users?*, „Journal of Antitrust Enforcement" 2023, t. 11, nr 1, s. 126.

[11] Zob. wyrok TSUE z dnia 5 lutego 1963 r., sprawa 26/62, *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos przecwko Netherlands Inland Revenue Administration* (ECLI:EU:C:1963:1), oraz wynikającą z niego linię orzeczniczą dotyczącą zasady bezpośredniego skutku.

skuteczne, pod warunkiem że przyznają uprawnienia w sposób jasny, precyzyjny i bezwarunkowy.

Bezpośredni skutek unijnego prawa konkurencji został potwierdzony w ustalonym orzecznictwie TSUE[12]. Nie budzi zatem wątpliwości, że podstawowe przepisy prawa konkurencji są bezpośrednio skuteczne w relacjach horyzontalnych (między jednostkami) i w konsekwencji strony postępowań przed sądami krajowymi mogą z tych przepisów wywodzić swoje żądania i roszczenia. Do żądań tych zaliczyć można przykładowo stwierdzenie nieważności porozumienia ograniczającego konkurencję czy powództwo o odszkodowanie za szkodę poniesioną w związku ze stosowaniem wygórowanych cen przez uczestnika takiego antykonkurencyjnego porozumienia.

4.3.2. Bezpośredni skutek DMA

Ustalenia wymaga, czy DMA przyznaje jakiekolwiek uprawnienia (prawa podmiotowe) użytkownikom biznesowym i końcowym platform. Z jednej strony, według niektórych autorów, omawiane rozporządzenie nie może być postrzegane jako źródło uprawnień, ponieważ nie przyznaje ich bezpośrednio i w sposób pozytywny[13]. Z drugiej – wątpliwość ta może być rozstrzygnięta z perspektywy zasady ogólnej bezpośredniego skutku prawa UE.

Nie budzi wątpliwości, że DMA, jako unijne rozporządzenie, jest bezpośrednio stosowany, a także bezpośrednio skuteczny[14]. Dlatego stanowi źródło uprawnień przyznanych jednostkom (w tym wypadku użytkownikom końcowym i biznesowym), które to uprawnienia mogą być powoływane bezpośrednio przed sądami krajowymi. Co więcej, motyw 42 DMA stanowi, że z perspektywy osiągnięcia celów DMA (dotyczących uczciwości i kontestowalności rynków cyfrowych) istotne jest, aby zabezpieczyć prawo użytkowników biznesowych i użytkowników końcowych do zgłaszania obaw dotyczących nieuczciwych praktyk strażników dostępu przez zwracanie uwagi odpowiednich organów administracyjnych lub innych organów publicznych, w tym sądów krajowych.

[12] Wyroki TSUE: z dnia 30 stycznia 1974 r., sprawa 127/73, *Belgische Radio en Televisie and société belge des auteurs, compositeurs et éditeurs przeciwko SV SABAM i NV Fonior* (ECLI:EU:C:1974:6); z dnia 20 września 2001 r., sprawa C-453/99, *Courage Ltd przeciwko Bernard Crehan i Bernard Crehan przeciwko Courage Ltd i innym* (ECLI:EU:C:2001:465).

[13] O. Andriychuk, op. cit., s. 129.

[14] A. Komninos, *Private Enforcement of the DMA Rules before the National Courts*, 5.04.2024, s. 5, http://dx.doi.org/10.2139/ssrn.4791499; F. Bostoen, *Understanding the Digital Markets Act*, „Antitrust Bulletin" 2023, t. 68, nr 2, s. 303; D. Geradin, *Ensuring DMA Compliance: What Are the Business Users' Options?*, The Platform Law Blog, 28.11.2023, https://theplatformlaw.blog/2023/11/28/ensuring-dma-compliance-what-are-the-business-users-options/ (dostęp: 3.04.2025); K. Bania, D. Geradin, S. Huijts, *7 March Is DMA D-Day: What Does This Mean?*, The Platform Law Blog, 7.03.2024, https://theplatformlaw.blog/2024/03/07/7-march-is-dma-d-day-what-does-this-mean/ (dostęp: 3.04.2025).

Bezpośredni skutek omawianego rozporządzenia znajduje także potwierdzenie w systemie bliskiej współpracy między Komisją (główną instytucją odpowiedzialną za egzekwowanie DMA) a sądami krajowymi, przyjętej w art. 39 DMA.

Z uwagi na bardzo dobre rozeznanie Komisji w sposobie funkcjonowania rynków cyfrowych (co wynika z otrzymywanych raportów zgodności, raportów audytorów, postępowań ws. badania rynku oraz informacji zawartych w skargach otrzymywanych prawdopodobnie od innych uczestników rynku), na podstawie art. 39 ust. 1 DMA sądy krajowe mogą zwrócić się do Komisji z prośbą o przekazanie posiadanych przez nią informacji bądź o opinię w konkretnej sprawie. Zakres tego postanowienia będzie jeszcze weryfikowany w praktyce jego stosowania (np. z uwagi na poufny charakter przekazywanych informacji), jednakże obowiązywanie tego przepisu potwierdza przyjęcie w DMA założenia o możliwej istotnej roli sądów krajowych przy egzekwowaniu praw przyznawanych użytkownikom przez to rozporządzenie.

Komisja z pewnością będzie wykazywać zainteresowanie i aktywność w sprawach dotyczących stosowania DMA przez sądy krajowe. W tym kontekście art. 39 ust. 2 DMA zobowiązuje państwa członkowskie do przekazywania Komisji kopii wszelkich pisemnych wyroków wydanych przez sądy krajowe, w których stosowane jest to rozporządzenie. Dodatkowo, zgodnie z art. 39 ust. 3 DMA, Komisja może działać jako *amicus curiae*, przedkładając sądom krajowym w toku postępowań uwagi pisemne i ustne dotyczące DMA.

W konsekwencji naruszenie przepisów DMA przez strażnika dostępu może być przedmiotem powództwa wniesionego przez jednostkę, która poniosła szkodę wskutek takiego działania. Ponieważ ani DMA, ani żaden inny akt prawa unijnego nie zawierają obecnie postanowień dotyczących postępowania przed sądami krajowymi w sprawie naruszenia DMA, kwestię tę pozostawiono do uregulowania na poziomie państw członkowskich. Brzmienie tych przepisów może zatem wpływać na zakres możliwych do podniesienia roszczeń (np. roszczenie odszkodowawcze, o zaniechanie czy środki zabezpieczające).

Bezpośredni skutek DMA znajduje także potwierdzenie w treści art. 42 DMA, który potwierdza stosowanie przepisów krajowych implementujących dyrektywę ws. powództw przedstawicielskich[15] w odniesieniu do postępowań dotyczących naruszeń DMA dokonywanych przez strażników dostępu. Jednocześnie art. 43 DMA potwierdza, że postanowienia dyrektywy ws. ochrony sygnalistów[16] stosuje się do zgłoszeń wszelkich naruszeń DMA oraz do ochrony osób dokonujących tych zgłoszeń.

---

[15] Dyrektywa Parlamentu Europejskiego i Rady 2020/1828 z dnia 25 listopada 2020 r. w sprawie powództw przedstawicielskich wytaczanych w celu ochrony zbiorowych interesów konsumentów i uchylająca dyrektywę 2009/22/WE (Dz. Urz. UE L 409, 4.12.2020, s. 1–27).

[16] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz. Urz. L 305, 26.11.2019, s. 17–56).

Bardziej szczegółowe omówienie zasad dotyczących dochodzenia roszczeń z tytułu naruszenia DMA zawarto w rozdziale V dotyczącym egzekwowania DSA i DMA. Jednocześnie nie można wykluczyć, że brak szczególnych przepisów dotyczących bezpośredniego skutku DMA i dochodzenia roszczeń z tytułu jego naruszenia może prowadzić do ograniczenia skuteczności uprawnień użytkowników[17].

4.4. Beneficjenci Aktu o rynkach cyfrowych

4.4.1. Wprowadzenie

Jak wskazano powyżej, „tradycyjnie" w stosunki handlowe wchodzą dwie strony, np. sprzedawca i kupujący. Na rynkach cyfrowych miejsce świadczenia zyskuje większe znaczenie, ponieważ jest organizowane i kontrolowane przez platformy internetowe, które mogą mieć status strażnika dostępu[18]. Z jednej strony, podmioty te są jedynie pośrednikami między sprzedawcami a kupującymi. Z drugiej jednak, biorąc pod uwagę cechy rynków cyfrowych omówione w rozdziale I, strażnicy dostępu zyskują szczególną siłę rynkową oraz zdolność do kształtowania warunków rynkowych i struktury rynku, wpływając na zachowanie użytkowników platform.

W pierwszej serii decyzji wskazujących strażników dostępu z września 2023 r. Komisja ustaliła, że status ten posiada sześć podmiotów[19], do których zaliczają się:

– Alphabet (w odniesieniu do: Google Play, Google Maps, Google Shopping, Google Search, YouTube, Android Mobile, Alphabet's online advertising service i Google Chrome)[20] jako strażnik dostępu podstawowych usług platformowych: wyszukiwarek internetowych, pośrednictwa internetowego, usług reklamowych, platform udostępniania wideo, wyszukiwarek i systemów operacyjnych;

– Amazon (w odniesieniu do Marketplace oraz Amazon Advertising)[21] jako strażnik dostępu usług pośrednictwa i reklam internetowych;

---

[17] R. Podszun, *From Competition Law to Platform Regulation – Regulatory Choices for the Digital Markets Act*, „Economics" 2023, t. 17, nr 1, artykuł 20220037, s. 10.

[18] Zgodnie z definicją przedstawioną w pkt 4.2 niniejszego rozdziału.

[19] Zob. https://digital-markets-act.ec.europa.eu/gatekeepers_en; lista ta może podlegać dalszemu rozszerzeniu. W maju 2024 r. Komisja wskazała jako strażnika dostępu Booking.com oraz zdecydowała o kontynuowaniu postępowania w sprawie wskazania sieci społecznościowej X (dawniej Twitter).

[20] Decyzja Komisji z dnia 5 września 2023 r. wskazująca firmę Alphabet jako strażnika dostępu na podstawie art. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (sprawy DMA.100011 – Alphabet – OIS Verticals; DMA.100002 – Alphabet – OIS App Stores; DMA. 100004 – Alphabet – Online search engines; DMA.100005 – Alphabet – Video sharing; DMA.100006 – Alphabet – Number-independent interpersonal communications services; DMA.100009 – Alphabet – Operating systems; DMA.100008 – Alphabet – Web browsers; DMA.100010 – Alphabet – Online advertising services) (Dz. Urz. UE C, 2023/549, 27.10.2023).

[21] Decyzja Komisji z dnia 5 września 2023 r. wskazująca firmę Amazon jako strażnika dostępu na podstawie art. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 w sprawie kontestowalnych

– Apple (w odniesieniu do AppStore, iOS i Safari[22], a także iPadIOS) jako strażnik dostępu usług pośrednictwa internetowego, wyszukiwarek i systemów operacyjnych;

– ByteDance (w odniesieniu do TikTok)[23] jako strażnik dostępu usługi internetowego serwisu społecznościowego;

– Meta (w odniesieniu do Facebook Marketplace, Facebook, Instagram, WhatsApp, Messenger oraz Meta Ads)[24] jako strażnik dostępu usług internetowych sieci społecznościowych, łączności interpersonalnej niewykorzystujących numerów, pośrednictwa oraz reklam;

– Microsoft (w odniesieniu do LinkedIn oraz Windows PC OS)[25] jako strażnik dostępu usług sieci społecznościowych oraz systemów operacyjnych.

Strażnicy dostępu świadczą usługi platformowe na rzecz dwóch rodzajów użytkowników. Po pierwsze, użytkownicy biznesowi działają na platformie strażnika dostępu w celu oferowania konsumentom swoich usług czy towarów. W tym kontekście są oni klientami platform (odbiorcami usług platformowych) oraz dostawcami usług na rzecz konsumentów. W ramach tej drugiej roli użytkownicy biznesowi konkurują jednak ze strażnikami dostępu, jeśli ci ostatni również prowadzą działalność na rynku niższego rzędu. Przykładowo, Apple zostało wskazane jako strażnik dostępu w odniesieniu do między innymi usługi pośrednictwa, jaką jest AppStore. Jednocześnie Apple jest obecne na platformie AppStore, oferując między innymi aplikację odtwarzania muzyki, Apple Music; na AppStore obecni są również niezależni użytkownicy biznesowi, jak Spotify, którzy konkurują z Apple Music swoją ofertą kierowaną do konsumentów.

---

i uczciwych rynków w sektorze cyfrowym (sprawy DMA.100018 Amazon – online intermediation services – marketplaces; DMA.100016 Amazon – online advertising services) (Dz. Urz. UE C, 2023/905, 15.11.2023).

[22] Decyzja Komisji z dnia 5 września 2023 r. wskazująca firmę Apple jako strażnika dostępu na podstawie art. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (sprawy DMA.100013 Apple – online intermediation services – app stores; DMA.100025 Apple – operating systems i DMA.100027 Apple – web browsers) (Dz. Urz. UE C, 2023/548, 27.10.2023).

[23] Decyzja Komisji z dnia 5 września 2023 r. wskazująca firmę ByteDance jako strażnika dostępu na podstawie art. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (sprawa DMA.100040 ByteDance – Online social networking services) (Dz. Urz. UE C, 2023/552, 27.10.2023).

[24] Decyzja Komisji z dnia 5 września 2023 r. wskazująca firmę Meta jako strażnika dostępu na podstawie art. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (sprawy DMA.100020 Meta – online social networking services; DMA.100024 Meta – number-independent interpersonal communications services; DMA.100035 Meta – online advertising services; DMA.100044 Meta – online intermediation services – marketplace) (Dz. Urz. UE C, 2023/1092, 23.11.2023).

[25] Decyzja Komisji z dnia 5 września 2023 r. wskazująca firmę Microsoft jako strażnika dostępu na podstawie art. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (sprawy DMA.100017 Microsoft – online social networking services; DMA.100023 Microsoft – number-independent interpersonal communications services; DMA.100026 Microsoft – operating systems) (Dz. Urz. UE C, 2023/549, 27.10.2023).

Po drugie, wyróżnić można użytkowników końcowych, którzy są jednocześnie klientami strażników dostępu (od których odbierają takie usługi jak wyszukiwarki czy media społecznościowe) oraz użytkowników biznesowych (odbierających daną usługę czy produkty oferowane przez tych użytkowników).

W takim układzie, gdy działanie strażników dostępu nie jest skutecznie ograniczane przez innych uczestników rynku, okoliczności rynkowe mogą zachęcać strażników do angażowania się w działania na szkodę użytkowników biznesowych (np. przez tzw. self-preferencing, czyli ograniczanie widoczności oferty konkurujących użytkowników biznesowych w celu korzystniejszego przedstawienia własnej oferty w wynikach wyszukiwania).

W konsekwencji cechy i role obydwu rodzajów użytkowników platform wpływają na rozumienie natury i zakresu uprawnień ustanowionych w DMA oraz zakresu, w jakim uprawnienia te mogą być powoływane (egzekwowane) przeciwko strażnikom dostępu w odniesieniu do obszarów działalności zidentyfikowanych w decyzjach wskazujących.

4.4.2. Użytkownicy biznesowi

W art 2 ust. 21 DMA zdefiniowano użytkownika biznesowego jako osobę fizyczną lub prawną działającą w celach handlowych lub zawodowych, która korzysta z podstawowych usług platformowych do celów związanych z dostarczaniem towarów użytkownikom końcowym lub świadczeniem usług na rzecz użytkowników końcowych albo w toku dostarczania towarów takim użytkownikom, albo w toku świadczenia usług na ich rzecz.

Jak wskazano, w ramach swojej działalności użytkownicy biznesowi odgrywają podwójną rolę na platformach cyfrowych. Po pierwsze, oferują oni produkty i usługi swoim klientom jak w każdym innym przedsięwzięciu gospodarczym. Po drugie jednak, czynią to za pośrednictwem platform internetowych, świadczonych przez strażników dostępu. W związku z tym możliwość jakiegokolwiek prezentowania oferty czy zawarcia transakcji z użytkownikiem końcowym jest uwarunkowana staniem się klientem strażnika dostępu.

Biorąc pod uwagę omówione cechy rynków cyfrowych (czy platform internetowych), użytkownicy biznesowi są w istotnej mierze zależni od strażników dostępu przy podejmowaniu działalności online. Warunki umów z platformami oraz ich rzeczywiste wykonanie w dużej mierze wpływają na widoczność danego użytkownika biznesowego na rynku, jego zdolność do dotarcia z ofertą do konsumenta czy w konsekwencji – na opłacalność jego działalności.

Mając na względzie tę asymetrię w sile rynkowej, niezależnie od podejmowanych wysiłków, zazwyczaj użytkownicy biznesowi nie są w stanie skutecznie kwestionować warunków nakładanych na nich przez strażników dostępu. Jeśli strażnik dostępu

wchodzi jednocześnie na rynek niższego rzędu i w konsekwencji konkuruje ze swoimi użytkownikami biznesowymi, zyskuje on istotną przewagę konkurencyjną opartą na szeregu różnych czynników: od dostępu do danych dotyczących zachowania rynkowego czy wyników handlowych osiąganych przez konkurentów na rynku niższego rzędu do zdolności kierunkowania uwagi użytkowników końcowych przez stosowanie odpowiednich algorytmów w odniesieniu do widoczności danej oferty.

Tak nierówne warunki konkurencji, wspólnie z brakiem szczególnych regulacji, mogą zachęcać strażników dostępu do podejmowania nieuczciwych praktyk względem użytkowników biznesowych. W długim okresie takie praktyki mogą prowadzić do zmiany struktury rynku przez wyparcie niektórych dotychczasowych graczy, których miejsce zająć mogą strażnicy dostępu. Strażnicy dostępu są bowiem w stanie przenosić korzyści z siły rynkowej osiągniętej na jednym rynku na inny rynek, na którym dopiero rozwijają swoją obecność. W konsekwencji takie ograniczenie konkurencji skutkować będzie potencjalnym ograniczeniem wyboru konsumentów oraz jakości usług świadczonych przez strażników dostępu na tym nowym rynku.

Sytuację tę można zilustrować przykładem sprawy *Google Shopping*. Google zajmowało bardzo istotną pozycję na rynku ogólnych wyszukiwarek internetowych. Weszło też, pod marką Google Shopping, na nowy rynek usług „porównywarek" zakupów online (ang. *comparison shopping services*, CSS), na którym obecni byli już inni uczestnicy. Jednakże, przyznając w wynikach wyszukiwania preferencje własnej usłudze kosztem innych CSS, Google zdołało wzmocnić pozycję Google Shopping na rynku „porównywarek" i stopniowo (lecz istotnie) ograniczać obecność niezależnych dostawców tego typu usług. W konsekwencji, jeśli współcześnie konsumenci chcą porównać ceny produktów lub usług dostępnych online, zazwyczaj polegają oni na wyszukiwarce Google i nie odwiedzają stron internetowych innych dostawców. Mając ograniczony dostęp do alternatywnych usług tego rodzaju, konsumenci tracą pewność, czy prezentowana jest im rzeczywiście najtańsza oferta, czy też używane są określone algorytmy zwiększające widoczność danej oferty na podstawie innych, nieobiektywnych czynników.

Pojęcie użytkowników biznesowych jest niezależne od jakichkolwiek innych czynników czy progów. Kategoria ta jest zatem bardzo szeroka i może obejmować podmioty od małych i średnich przedsiębiorstw po bardzo duże przedsiębiorstwa międzynarodowe. Również platformy internetowe (jak VLOP w rozumieniu DSA czy strażnicy dostępu w rozumieniu DMA) czy inni pośrednicy mogą być użytkownikami biznesowymi innych podstawowych usług platformowych. Przykładowo, Spotify jest użytkownikiem biznesowym platformy AppStore (świadczonej przez Apple, wskazane w tym zakresie jako strażnik dostępu), a aplikacje Facebook oraz Instagram (świadczone przez Meta, wskazaną jako strażnik dostępu dla sieci społecznościowych) są użytkownikami biznesowymi systemów operacyjnych iOS czy Google Android (dostarczanych odpowiednio przez Apple i Alphabet (Google), wskazane jako strażnicy dostępu dla systemów operacyjnych).

4.4.3. Użytkownicy końcowi

Użytkownika końcowego zdefiniowano w art. 2 ust. 20 DMA jako osobę fizyczną lub prawną, która korzysta z podstawowych usług platformowych w charakterze innym niż użytkownik biznesowy. Użytkownicy końcowi mogą być utożsamieni z konsumentami lub klientami końcowymi, jako że działają oni na platformach w charakterze innym niż komercyjny czy profesjonalny oraz w ramach swojej obecności na platformie są jedynie odbiorcami (a nie dostawcami) usług czy produktów dostarczanych przez inne podmioty.

Podczas gdy wiele przepisów materialnych DMA zdaje się skupiać na poprawieniu pozycji rynkowej użytkowników biznesowych w relacji ze strażnikami dostępu, dobrobyt użytkowników końcowych stanowi równie istotną podstawę DMA. Niektóre obowiązki strażników dostępu są uzasadnione w preambule DMA potrzebą poprawy bądź zapewnienia odpowiedniego wyboru dla użytkowników końcowych. Przykładem jest chociażby uzasadnienie obowiązku zapewnienia dostępu do systemu operacyjnego alternatywnym dostawcom sprzętu (motyw 57 DMA) czy dostępu do danych oraz umożliwienie korzystania z wielu platform (tzw. multi-homing, motyw 59 DMA).

Ochrona wyboru użytkowników końcowych (a przez to ich uprawnień) jest bezpośrednio powiązana z głównymi celami DMA. Między innymi motyw 107 DMA potwierdza, że jednym z celów rozporządzenia jest zapewnienie „kontestowalnego i uczciwego sektora cyfrowego w ogóle, a w szczególności kontestowalnych i uczciwych podstawowych usług platformowych z myślą o promowaniu innowacyjności, wysokiej jakości produktów i usług cyfrowych, uczciwych i konkurencyjnych cen, a także wysokiej jakości i swobody wyboru dla użytkowników końcowych w sektorze cyfrowym".

Użytkownicy końcowi pełnią zatem funkcję podwójnego konsumenta. Nabywają produkty czy usługi od użytkowników biznesowych bądź od platform. Jednocześnie są niekomercyjnymi użytkownikami tych platform, zainteresowanymi dostępem do różnego rodzaju treści (których charakter może być zarówno komercyjny jak i niekomercyjny).

Celem DMA nie jest natomiast ochrona konsumentów (użytkowników końcowych) przed nieuczciwymi praktykami stosowanymi przez ich partnerów handlowych (użytkowników końcowych) – cel ten realizują inne akty prawa konsumenckiego UE. Dlatego potencjalne roszczenia podnoszone przez użytkowników końcowych na podstawie DMA kierowane będą jedynie przeciwko strażnikom dostępu. Jednakże trójstronny charakter rynków cyfrowych (oraz rola użytkowników biznesowych w tym układzie) wpływa na sferę praw konsumentów i potwierdza, że użytkownicy końcowi mogą powoływać się przeciwko strażnikom dostępu na swoje uprawnienia wywodzone z DMA. Przykładowo, art. 5 ust. 3 DMA zakazuje strażnikom dostępu uniemożliwiania użytkownikom biznesowym oferowania tych

samych produktów lub usług użytkownikom końcowym po cenach lub na warunkach innych niż w ramach usług pośrednictwa internetowego świadczonych przez strażników dostępu.

4.5. Uprawnienia zawarte w DMA

4.5.1. Obowiązki strażników dostępu

Jak wskazano w niniejszym rozdziale, art. 5–7 DMA ustanawiają katalog obowiązków i zakazów kierowanych do strażników dostępu. W tym sensie przepisy te stanowią materialną część DMA.

Obowiązki wskazane w art. 5 DMA uważane są za „samowykonalne", natomiast art. 6–7 DMA wprowadzają obowiązki, które mogą podlegać doprecyzowaniu przez Komisję w akcie delegowanym, nakładającym na strażnika dostępu obowiązek wprowadzenia stosownych środków, zapewniających pełną zgodność działania strażnika z obowiązkami, o których mowa w art. 6–7 DMA[26].

Co prawda niektórzy autorzy wyrażają wątpliwości, czy obowiązki te automatycznie przekładają się na uprawnienia użytkowników[27], ale należy przyjąć, że z uwagi na bezpośredni skutek DMA rozporządzenie to może być uznane za źródło praw przyznanych użytkownikom biznesowym i końcowym. Jednak charakter tych obowiązków ma znaczenie w odniesieniu do przynajmniej dwóch wątpliwości.

Po pierwsze: czy rzeczywiście można wywieść prawa z tak określonych obowiązków? W tym kontekście należy zgodzić się z konkluzją, że wszystkie materialne postanowienia DMA spełniają kryteria DMA i mogą być uznane za źródło uprawnień przyznanych użytkownikom biznesowym i końcowym platform[28].

Po drugie: który rodzaj użytkowników (biznesowi, końcowi czy obydwa rodzaje) można uznać za beneficjentów uprawnień, jakie można powołać w postępowaniach przed sądami krajowymi czy innymi organami? Przepisy ustanawiające obowiązki strażników dostępu są długie i mają techniczne brzmienie. W niniejszej sekcji podzielono je na obowiązki związane z prawami przyznanymi (1) obydwu rodzajom użytkowników oraz (2) głównie użytkownikom biznesowym[29].

W ramach tego podziału zidentyfikowano grupy praw i obowiązków, które mają zbliżony przedmiot ochrony lub charakterystykę (np. korzystanie z danych), by

[26] Art. 8 DMA, zob. też: F. Bostoen, op. cit., s. 280–281.

[27] O. Andriychuk, op. cit.

[28] A. Komninos, op. cit., s. 5.

[29] DMA ustanawia szereg praw przyznanych wyłącznie użytkownikom biznesowym, jednak są one związane z podobnymi uprawnieniami przyznanymi użytkownikom biznesowym (zob. na przykład art. 5 ust. 4 oraz ust. 5 DMA omawiane w sekcji dotyczącej postanowień utrudniających przekierowanie użytkownika końcowego). Z uwagi na to bliskie powiązanie funkcjonalne takie uprawnienia zostały zakwalifikowane jako przyznane obydwu rodzajom użytkowników.

omówić je w sposób bardziej tematyczny. Jak wynika z zaproponowanego podziału, należy uznać, że większość uprawnień została przyznana użytkownikom zarówno biznesowym, jak i końcowym. Jednakże w praktyce stosowania DMA może okazać się, że sądy lub organy przyjmą inne podejście w odniesieniu do katalogu beneficjentów konkretnych postanowień.

4.5.2. Prawa przyznane wspólnie użytkownikom biznesowym i końcowym

4.5.2.1. Korzystanie oraz dostęp do danych użytkowników

DMA w dużej mierze skupia się na korzystaniu przez strażników dostępu z danych innych uczestników rynku oraz na dostępie strażników do tych danych. W istocie często spotkać można stwierdzenia, że warunki konkurencji na rynkach cyfrowych bezpośrednio powiązane są z dostępem do danych i że wiele strukturalnych problemów w sektorze cyfrowym wynika z faktu, że strażnicy dostępu mogą dysponować danymi, które nie są dostępne dla jakiegokolwiek innego uczestnika rynku. Praktyki te dotyczą korzystania z danych generowanych zarówno przez użytkowników biznesowych obecnych na danej platformie (np. ich strategie rynkowe), jak i przez użytkowników końcowych (np. wzorce zachowania konsumentów).

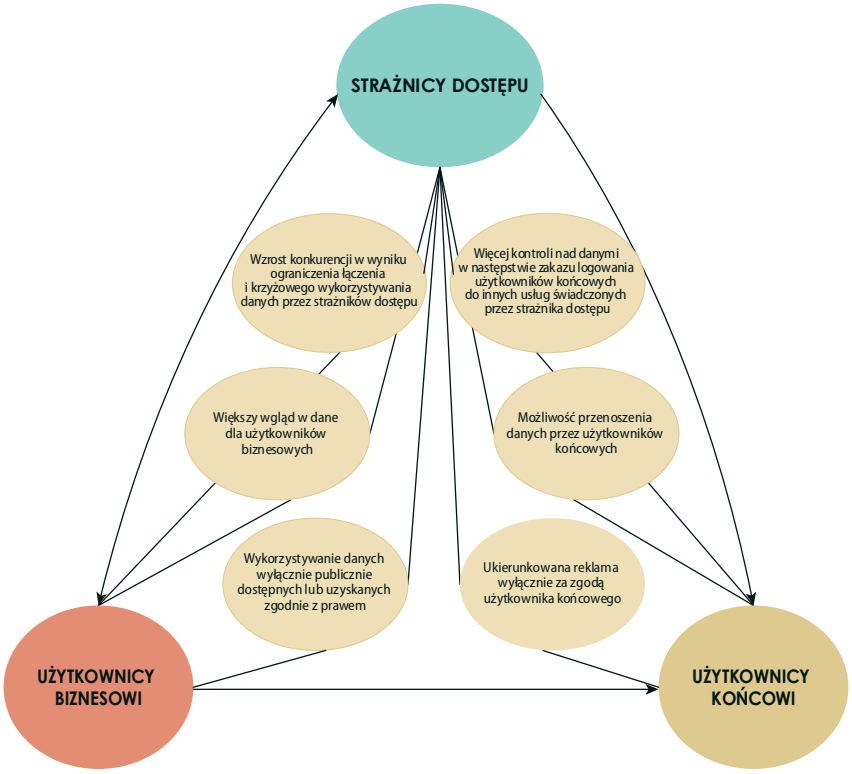
Z pewnością, z uwagi na omawianą wcześniej podwójną rolę strażników dostępu (organizatorzy rynku oraz jednocześnie jego aktywni uczestnicy), otrzymują oni dostęp do danych, które nie są dostępne dla nikogo innego i które stanowią źródło cennych, wrażliwych informacji. Prowadzi to do typowej sytuacji asymetrii informacji, w ramach której strażnicy dostępu otrzymują bezprecedensową przewagę konkurencyjną nad użytkownikami biznesowymi, ponieważ strażnicy dostępu w każdym przypadku będą mieli dostęp do wrażliwych informacji dotyczących skuteczności działań rynkowych ich bezpośrednich konkurentów (np. do portfela klientów, danych sprzedaży czy polityki cenowej). Jednocześnie strażnicy dostępu zyskują przewagę nad użytkownikami końcowymi, dzięki czemu mogą kierować zainteresowanie tych użytkowników na określone oferty, w sposób i w zakresie niemożliwym do wcielenia w normalnych warunkach rynkowych.

W tym kontekście art. 5 ust. 2 lit. a DMA zakazuje przetwarzania, do celów świadczenia internetowych usług reklamowych, danych osobowych użytkowników końcowych, którzy korzystają z usług osób trzecich z wykorzystaniem platform prowadzonych przez strażników dostępu. Z kolei art. 5 ust. 2 lit. b oraz lit. d DMA ustanawiają zakaz łączenia danych osobowych pochodzących z danej podstawowej usługi platformowej świadczonej przez strażnika dostępu (np. z sieci społecznościowej) z danymi osobowymi pochodzącymi z innych usług świadczonych przez tego strażnika (np. ze sklepu internetowego). Natomiast art. 5 ust. 2 lit. c DMA zakazuje strażnikom dostępu wykorzystywania danych osobowych pochodzących z danej

podstawowej usługi platformowej w ramach innych usług świadczonych oddzielnie przez strażnika dostępu (np. dane pozyskane w ramach usługi wyszukiwarki nie mogą być wykorzystywane w innych usługach, jak mapy online czy poczta elektroniczna).

Zakazy związane z korzystaniem z danych zostały rozwinięte w art. 6 DMA. Ustęp 2 zakazuje wykorzystywania danych użytkowników biznesowych w ramach prowadzenia działalności konkurencyjnej z tymi użytkownikami. Zakaz ten stosuje się do danych, które nie są publicznie dostępne i zostały wygenerowane przez użytkowników biznesowych korzystających z danej platformy lub wskutek korzystania przez nich z tej platformy.

Ponadto, art. 6 ust. 9 DMA zapewnia możliwość przenoszenia danych użytkowników końcowych. Oznacza to, że użytkownicy końcowi, na ich wniosek i nieodpłatnie, powinni uzyskać dostęp oraz mieć możliwość przeniesienia na inną platformę (np. do innego systemu operacyjnego czy do innej sieci społecznościowej) swoich danych wygenerowanych w trakcie korzystania z platformy prowadzonej przez strażnika dostępu. Podobnie, zgodnie z art. 6 ust. 10 DMA, użytkownicy biznesowi mają zapewniony dostęp do własnych danych osobowych wygenerowanych w związku z korzystaniem z danej platformy.



Rysunek 5. Kluczowe uprawnienia użytkowników w związku z wykorzystywaniem danych

Dodatkowo, art. 6 ust. 11 DMA wymaga, aby niezależni dostawcy usług wyszukiwarek internetowych mogli żądać i otrzymać dane dotyczące plasowania, zapytań, kliknięć i wyświetleń związanych z nieodpłatnym i płatnym wyszukiwaniem, wygenerowanych przez użytkowników końcowych za pomocą tych wyszukiwarek. Dostęp ten powinien być zapewniony na uczciwych, rozsądnych i niedyskryminacyjnych warunkach.

Kluczowe uprawnienia użytkowników wynikające z obowiązków strażników dostępu związanych z korzystaniem i przetwarzaniem danych podsumowano na rys. 5.

4.5.2.2. Interoperacyjność oraz podobne uprawnienia

Interoperacyjność jest jednym z kluczowych czynników zapobiegających zakłóceniom konkurencji wynikającym z wysokich barier wejścia ustanowionych przez podmioty zasiedziałe na rynku (tu: strażników dostępu) i prowadzących do ograniczenia kontestowalności danego rynku. Zapewnia ona, że jeśli rozwinięte zostanie nowe oprogramowanie czy usługa cyfrowa (np. aplikacja), będą one dostępne dla użytkowników, np. wiodących systemów operacyjnych.

W tym kontekście art. 6 ust. 7 DMA zobowiązuje strażników dostępu do zapewnienia skutecznej interoperacyjności z tymi samymi funkcjami sprzętu i oprogramowania, jakimi dysponują usługi świadczone lub sprzęt dostarczany przez strażnika dostępu. W ten sposób dostawcy usług i sprzętu otrzymują nieodpłatnie dostęp do rynków powstałych wskutek ukształtowania przez strażników dostępu tzw. ekosystemów oprogramowania i sprzętów. Obowiązek zapewnienia interoperacyjności zawarty jest także w art. 6 ust. 6 DMA, który zakazuje strażnikom dostępu ograniczania, technicznie lub pod jakimkolwiek innym względem, możliwości korzystania przez użytkowników końcowych z różnych aplikacji i usług, do których uzyskuje się dostęp za pośrednictwem platform strażników dostępu.

Artykuł 6 ust. 3 oraz ust. 4 DMA dodatkowo zabezpieczają dostęp do rynku dla dostawców usług cyfrowych. Pierwszy ze wskazanych przepisów wymaga umożliwienia użytkownikom końcowym łatwego odinstalowania wszelkich aplikacji w systemie operacyjnym oferowanym przez strażnika dostępu, jeśli tylko nie są one kluczowe dla funkcjonowania danego systemu operacyjnego lub urządzenia, na którym zostały zainstalowane. Przepis ten wymaga także, aby użytkownicy końcowi mogli w łatwy sposób zmienić domyślne ustawienia w systemie operacyjnym, w wirtualnym asystencie i w przeglądarce internetowej strażnika dostępu. Mając możliwości łatwego odinstalowania aplikacji dostarczanych przez strażników dostępu, użytkownicy końcowi zyskują zachętę do używania konkurencyjnych aplikacji dostarczanych przez podmioty trzecie, czyli użytkowników biznesowych.

Swego rodzaju kontynuację tych uprawnień zawiera art. 6 ust. 4 DMA, który stanowi, że strażnik dostępu powinien umożliwiać, również pod względem tech-

nicznym, instalację i skuteczne korzystanie z oferowanych przez podmioty trzecie aplikacji lub sklepów z aplikacjami korzystających (lub współpracujących) z jego systemu operacyjnego oraz zapewniać możliwość uzyskania dostępu do tych aplikacji lub sklepów z aplikacjami w inny sposób niż za pośrednictwem platformy prowadzonej przez strażnika dostępu.

Również art. 5 ust. 7 DMA zapewnia, że użytkownicy zarówno końcowi, jak i biznesowi mają swobodę decyzji co do korzystania i interoperacyjności niektórych usług cyfrowych z platformami strażników dostępu. Wspomniany przepis pozwala użytkownikom na działanie na platformach strażników dostępu niezależnie od takich usług świadczonych przez strażników jak usługi identyfikacyjne, silnik przeglądarki internetowej czy usługi płatnicze.

4.5.2.3. Interoperacyjność usług łączności interpersonalnej niewykorzystujących numerów

Artykuł 7 DMA został w całości poświęcony obowiązkowi strażników dostępu do zapewnienia interoperacyjności usług łączności interpersonalnej niewykorzystujących numerów (ang. *interoperability of number-independent interpersonal communications services*, NI-ICS). NI-ICS należy rozumieć jako usługi łączności interpersonalnej, które nie łączą się z publicznie nadanymi zasobami numeracyjnymi, mianowicie z numerem lub z numerami z krajowych lub międzynarodowych planów numeracji, ani nie umożliwiają połączenia z numerem lub z numerami z krajowych lub międzynarodowych planów numeracji[30]. Do przykładów NI-ICS zaliczyć można takie aplikacje jak Messenger, WhatsApp, Signal czy Telegram.

Jak wyjaśniono w motywie 64 DMA, brak interoperacyjności pozwala strażnikom dostępu, którzy świadczą usługi NI-ICS, wykorzystywać silne efekty sieciowe, co przyczynia się do osłabienia kontestowalności. Co więcej, strażnicy dostępu często oferują NI-ICS jako część stworzonych przez siebie ekosystemów (jak historycznie Messenger na Facebooku czy Direct Messages na Instagramie), co stanowi dodatkową, istotną barierę wejścia na te rynki.

Dlatego art. 7 DMA wymaga, aby strażnicy dostępu świadczący usługi NI-ICS, które zostały ujęte w decyzji wskazującej, zapewniali interoperacyjność podstawowych funkcjonalności swoich usług łączności interpersonalnej niewykorzystujących numerów z tego rodzaju usługami świadczonymi przez innego dostawcę oferującego lub zamierzającego oferować takie usługi w Unii. Strażnicy dostępu powinni zatem zapewnić interoperacyjność przynajmniej następujących podstawowych funkcjonalności, jeśli strażnik dostępu sam dostarcza takie podstawowe funkcjonalności swoim użytkownikom końcowym.

[30] Art. 2 pkt 7 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (Dz. Urz. UE L 321, 17.12.2018, s. 36–214).

Po pierwsze, po wymienieniu tych usług w decyzji wskazującej strażnika dostępu strażnik taki jest zobowiązany do zapewnienia możliwości przesyłania wiadomości tekstowych między dwoma użytkownikami końcowymi, a także udostępniania między takimi użytkownikami obrazów, wiadomości głosowych, wideo i innych załączonych plików w ramach komunikacji metodą „od końca do końca" (ang. *end to end*). Po drugie, po dwóch latach od wskazania jako strażnik dostępu podmioty te zapewniają interoperacyjność tych samych funkcjonalności (tj. przesyłanie metodą „od końca do końca" wiadomości tekstowych oraz udostępniania obrazów, wiadomości głosowych, wideo i innych załączonych plików) w obrębie grup pojedynczych użytkowników końcowych oraz między czatem grupowym a pojedynczym użytkownikiem końcowym. Po trzecie, w ciągu czterech lat od wskazania strażnika dostępu podmioty takie zapewniają interoperacyjność funkcjonalności połączeń głosowych oraz połączeń wideo między dwoma użytkownikami końcowymi oraz między czatem grupowym a użytkownikiem końcowym.

4.5.2.4. Dostęp do treści między platformami, kierowanie użytkowników oraz wiązanie usług

Artykuł 5 ust. 4 oraz ust. 5 DMA zakazują stosowania praktyk zmierzających do kierowania uwagi użytkowników końcowych na ofertę strażników (tzw. anti-steering), a także wszelkich środków wspierających takie praktyki. Po pierwsze, użytkownicy biznesowi mogą nieodpłatnie przedstawiać na platformach strażników swoje oferty użytkownikom końcowym pozyskanym za pośrednictwem tych platform lub innymi kanałami sprzedaży, a także zawierać umowy z tymi użytkownikami końcowymi, niezależnie od tego, czy dla tych celów korzystają z platform dostarczanych przez strażników dostępu. Oferty przedstawiane przez użytkowników biznesowych na platformach strażników dostępu mogą przy tym zawierać warunki inne niż warunki oferowane przez użytkowników biznesowych na platformach strażników.

Podobnie użytkownicy końcowi mają prawo dostępu do treści, subskrypcji, funkcji lub innych elementów przy użyciu aplikacji użytkownika biznesowego oraz prawo korzystania z nich, za pośrednictwem platform strażników dostępu, również w przypadku gdy ci użytkownicy końcowi nabyli wspomniane elementy od użytkownika biznesowego bez korzystania z platformy strażnika dostępu.

Zgodnie z art. 5 ust. 8 DMA, strażnicy dostępu nie mogą uzależniać korzystania, dostępu, rejestracji na platformach przez użytkowników końcowych czy biznesowych od subskrypcji lub zarejestrowania się jako użytkownik innych usług świadczonych przez tych strażników dostępu. Tym samym strażnicy dostępu nie mogą przenosić swojej siły rynkowej z danej platformowy na inną usługę przez sztuczne zwiększanie liczby użytkowników tej usługi (co wzmocniłoby efekty sieciowe oraz mogłoby wyeliminować konkurencję na rynku takich usług).

4.5.2.5. Klauzule najwyższego uprzywilejowania

DMA zawiera także inne postanowienie istotnie inspirowane ogólnym prawem konkurencji oraz nadające istotne uprawnienia użytkownikom biznesowym i końcowym. Artykuł 5 ust. 3 DMA stanowi, że strażnicy dostępu nie mogą uniemożliwiać użytkownikom biznesowym oferowania, przy wykorzystaniu innych platform lub za pomocą własnych kanałów bezpośredniej sprzedaży internetowej, tych samych produktów lub usług użytkownikom końcowym po cenach lub na warunkach innych niż oferowane na platformach strażników dostępu. Rozwiązanie to określane jest jako klauzula najwyższego uprzywilejowania (ang. *most favoured nation*, MFN), co oznacza, że przyznanie korzyści jednemu podmiotowi przekłada się na obowiązek przyznania takich samych korzyści innym podmiotom.

Próby ograniczenia widoczności innych platform czy kanałów sprzedaży mają na celu dalszą koncentrację danego rynku wokół określonego strażnika dostępu oraz ograniczenie konkurencji na tym rynku.

4.5.2.6. Skuteczność i rezygnacja z usługi platformowej

Ogólna skuteczność uprawnień użytkowników jest chroniona przez dwa kolejne postanowienia DMA. O ile mają one nieco odmienny przedmiot ochrony, o tyle zawierają ogólne mechanizmy ochronne użytkowników biznesowych i końcowych.

Artykuł 5 ust. 6 DMA stanowi, że strażnicy dostępu nie mogą, bezpośrednio lub pośrednio, utrudniać użytkownikom dokonywania do właściwych organów (w tym sądów) zgłoszeń dotyczących nieprzestrzegania przez strażnika dostępu jego obowiązków.

Ponadto art. 6 ust. 13 DMA zakazuje strażnikom dostępu wprowadzania nieproporcjonalnych postanowień umownych dotyczących rezygnacji z którejkolwiek z usług platformowych (np. rezygnacja z konta użytkownika w sieci społecznościowej nie może być uzależniona od nadmiernych warunków). W tym kontekście strażnicy dostępu muszą także zapewnić, że warunki rezygnacji są możliwe do wykonania bez zbędnych trudności.

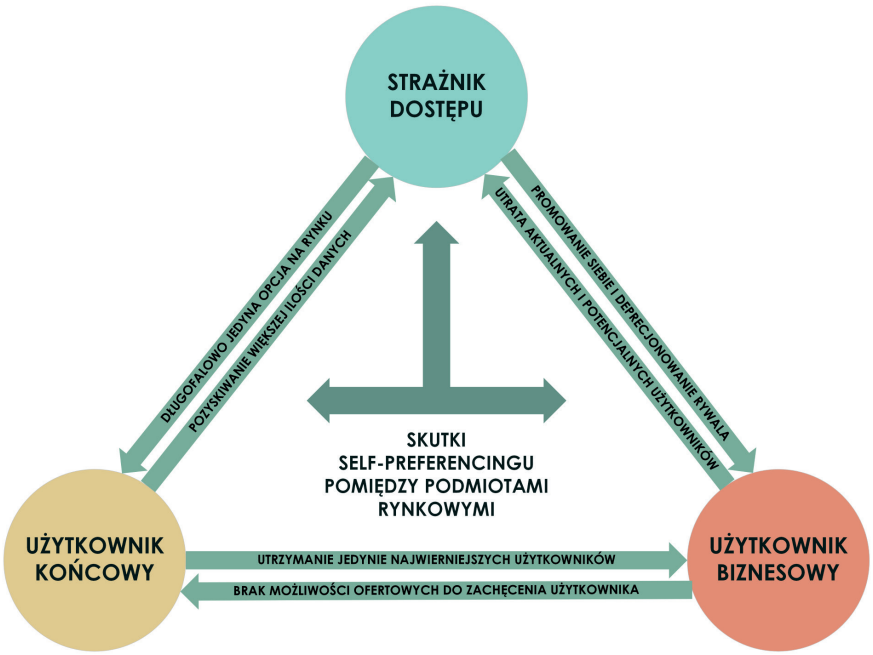
4.5.3. Uprawnienia użytkowników biznesowych

4.5.3.1. Self-preferencing

Artykuł 6 ust. 5 DMA zakazuje stosowania przez strażników dostępu tzw. self-preferencingu, tj. preferowania na platformach własnych usług kosztem podobnych usług świadczonych przez użytkowników biznesowych. Strażnicy dostępu nie mogą zatem, w ramach plasowania oraz związanego z nim indeksowania i badania (craw-

lingu), traktować oferowanych przez siebie usług i produktów na korzystniejszych zasadach niż podobne usługi lub produkty oferowane przez osobę trzecią. Co więcej, strażnik dostępu powinien stosować w ramach plasowania transparentne, uczciwe i niedyskryminujące warunki.

Self-preferencing jest szczególnie szkodliwy w kontekście umacniania negatywnych tendencji na rynkach cyfrowych, jak omówiono w niniejszym rozdziale. Może również prowadzić do dalszej integracji pionowej strażników dostępu, przenoszenia ich siły na kolejne rynki i w konsekwencji do ograniczania konkurencji. Była to też jedna z pierwszych praktyk stwierdzonych i zakazanych przez Komisję przy egzekwowaniu prawa konkurencji w sprawie *Google Shopping*. Istotę omawianej praktyki przedstawiono na rys. 6.



Rysunek 6. Self-preferencing

4.5.3.2. Dostęp do sklepów z aplikacjami na warunkach FRAND

Artykuł 6 ust. 12 DMA wymaga aby każdy strażnik dostępu stosował uczciwe, rozsądne i niedyskryminujące warunki (ang. *fair, reasonable, and non-discriminatory*, FRAND) ogólne dostępu dla użytkowników biznesowych do jego sklepów z aplikacjami, wyszukiwarek internetowych i internetowych serwisów społecznościowych wymienionych w decyzji wskazującej strażnika.

4.5.3.3. Reklamy internetowe

Pozostałe dwa obowiązki związane są z oferowaniem przez strażników dostępu reklam internetowych. W tym kontekście strażnicy dostępu osiągają szczególną przewagę informacyjną nad reklamodawcami oraz wydawcami w zakresie między innymi rzeczywistego zasięgu i skuteczności określonych narzędzi reklamowych. W konsekwencji rynek ten stał się szczególnie nietransparentny dla uczestników innych niż sami strażnicy dostępu. Dlatego art. 5 ust. 9 oraz ust. 10 DMA ustanawiają szczególne obowiązki (oraz odpowiadające im prawa) dotyczące nieodpłatnego dostępu reklamodawców (i odpowiednio wydawców) do informacji dotyczących każdej umieszczanej reklamy.

Artykuł 6 ust. 8 DMA wprowadza dalsze obowiązki informacyjne dla strażników dostępu oferujących usługi reklamowe online. Wymaga on, aby strażnicy dostępu zapewniali reklamodawcom i wydawcom (nieodpłatnie i na ich wniosek) dostęp do stosowanych przez strażnika dostępu narzędzi pomiaru wyników oraz do danych potrzebnych reklamodawcom i wydawcom do przeprowadzenia samodzielnie niezależnej weryfikacji zasobów reklamowych, w tym do danych zagregowanych i niezagregowanych.

4.6. Podsumowanie

Akt o rynkach cyfrowych wpisuje się w szersze podejście regulacyjne Unii Europejskiej do działalności tzw. branży big tech. Celem tego rozporządzenia jest poprawa kontestowalności i uczciwości rynków cyfrowych, a w konsekwencji zapewnienie, że rynki te są dostępne dla podmiotów chcących prowadzić i rozwijać swoją działalność. Chociaż DMA stanowi element ram prawnych rynku wewnętrznego, jest on istotnie inspirowany ustalonym dorobkiem unijnego prawa konkurencji.

Pod względem materialnoprawnym DMA wprowadza szereg precyzyjnych zasad obowiązujących największe podmioty branży big tech, wyznaczone przez Komisję jako strażnicy dostępu. Jak wskazano w niniejszym rozdziale, szczegółowe obowiązki i zakazy wiążące strażników dostępu dotyczą między innymi sposobu wykorzystywania danych czy zapewnienia interoperacyjności między systemami oferowanymi przez różne podmioty.

Z obowiązków tych wynikają uprawnienia (prawa podmiotowe) użytkowników podstawowych usług platformowych świadczonych przez strażników dostępu. Użytkownicy biznesowi korzystają ze swoich uprawnień po to, aby na równych i sprawiedliwych zasadach móc oferować swoje usługi i towary w środowisku cyfrowym, w którym platformy stały się podstawowym miejscem wymiany handlowej. Z kolei uprawnienia przyznane użytkownikom końcowym (konsumentom) zmierzają przede wszystkim do zapewnienia im odpowiedniego wyboru oferowanych usług cyfrowych oraz ich jakości i ceny.

Rozdział V

Dochodzenie praw i sądowa ochrona użytkowników na rynku cyfrowym

5.1. Wprowadzenie

Pełna skuteczność jest jedną z podstawowych zasad unijnego systemu prawnego[1]. Z ugruntowanego orzecznictwa TSUE wynika, że zgodnie z tą zasadą jednostki muszą mieć możliwość powoływania się na prawa wynikające z unijnego ustawodawstwa bądź dochodzenia roszczeń w przypadku ich naruszeń.

W poprzednich rozdziałach omówiono, w jakim zakresie i jakie prawa przyznają użytkownikom platform internetowych zarówno DSA, jak i DMA. Skuteczność ochrony zależy od ram przewidzianych dla wdrożenia i egzekwowania ich postanowień. Innymi słowy, skuteczność ochrony zależy od zakresu i dostępności środków prawnych, regulacji materialnoprawnych oraz proceduralnych pozwalających na egzekwowanie obowiązków od platform i dochodzenie roszczeń przez użytkowników.

Co do zasady egzekwowanie obowiązków z rozporządzeń może się odbywać na dwa sposoby: w drodze nadzoru organów publicznych albo przez jednostki (użytkowników) podnoszących swoje roszczenia przed sądami krajowymi bądź w drodze stosowania innych dopuszczalnych środków prawnych.

Egzekwowanie na drodze publicznoprawnej. Przez środki publicznoprawnego egzekwowania prawa UE należy rozumieć sytuacje, w których wskazanym organom publicznym powierza się kompetencje do nadzorowania wykonywania obowiązków prawnych oraz do stosowania określonych środków nakazujących określone zachowanie, w celu zapewnienia zgodności działań podmiotu, np. platform internetowych, z prawem, np. z DSA i z DMA. W świetle unijnego prawa istnieje w tym zakresie różnorodność rozwiązań: od systemów scentralizowanych (np. wyłączne kompetencje Komisji Europejskiej), przez rozwiązania hybrydowe (egzekwowanie

[1] Zob. wyroki TSUE: z dnia 9 marca 1978 r., sprawa 106/77, *Amministrazione delle Finanze dello Stato przeciwko Simmenthal SpA* (ECLI:EU:C:1978:49), pkt 16; z dnia 19 czerwca 1990 r., sprawa C-213/89, *The Queen przeciwko Secretary of State for Transport, ex parte: Factortame Ltd i inni* (ECLI:EU:C:1990:257), pkt 19; z dnia 20 września 2001 r., sprawa C-453/99, *Courage Ltd przeciwko Bernard Crehan i Bernard Crehan przeciwko Courage Ltd i innym* (ECLI:EU:C:2001:465), pkt 25–26.

przez Komisję oraz organy krajowe), aż do zdecentralizowanych (nadzór powierzony wyłącznie organom krajowym).

Dochodzenie roszczeń z tytułu naruszenia DSA i DMA. Omawiając dochodzenie praw na drodze prywatnoprawnej, skupiono się się na użytkownikach, którzy powołują się na prawa wynikające z aktu prawa UE (DSA czy DMA) i żądają od platformy internetowej dostosowania się do obowiązującej regulacji. Jeśli żądanie takie okaże się nieskuteczne, podmioty prywatne mogą dochodzić swoich praw, wszczynając postępowanie przed sądami krajowymi bądź inną drogą, np. korzystając z alternatywnych metod rozwiązywania sporów. W ramach takich postępowań użytkownicy mogą się potencjalnie domagać określonego zachowania, ale również żądać odszkodowania, jeśli szkoda wynikała z naruszeń DSA czy DMA.

Z systemowej perspektywy należy wskazać, że modele egzekwowania prawa różnią się w zależności od obszaru regulacji. W zakresie egzekwowania na drodze publicznoprawnej można zidentyfikować powierzenie różnych uprawnień Komisji bądź krajowym organom. W takim przypadku zakres kompetencji krajowych organów może być przedmiotem regulacji bezpośrednio w prawie UE bądź być dookreślony w prawie krajowym. Dochodzenie praw na drodze prywatnoprawnej może również być w różnym zakresie uregulowane na poziomie unijnym i krajowym. W tym obszarze zwykle zakres harmonizacji jest nieznaczny, przy pozostawieniu istotnego marginesu swobody państwom członkowskim.

W niniejszym rozdziale przybliżono zatem: egzekwowanie DMA przez organy publiczne, z pierwszoplanową rolą Komisji Europejskiej; egzekwowanie DSA przez organy publiczne przy wyłącznych kompetencjach Komisji w zakresie VLOP i VLOSE oraz z kluczową rolą krajowych koordynatorów ds. usług cyfrowych (DSC) w odniesieniu do innych pośredników. Analizie poddano różne środki ochrony dostępne dla użytkowników i rolę, jaką odgrywają DSC w zakresie zapewnienia zgodności działań platform z obowiązkami w zakresie należytej staranności. Następnie przedstawiono możliwości dochodzenia praw w przypadku naruszeń DSA i DMA na drodze prywatnoprawnej.

5.2. Egzekwowanie DMA przez organy publiczne

5.2.1. Wprowadzenie

Jak wspomniano w rozdziale IV, dotyczącym uprawnień przyznanych użytkownikom przez DMA, wprowadzenie modelu egzekwowania DMA na zasadzie *ex ante* stanowi jedną z kluczowych wartości dodanych tego rozporządzenia w porównaniu do ogólnego prawa konkurencji. Rzeczywiście, egzekwowanie prawa konkurencji odbywa się na zasadzie *ex post*, tj. po wystąpieniu i zidentyfikowaniu potencjalnego naruszenia przez właściwy organ. Podejście to okazało się jednak szczególnie

nieefektywne w odniesieniu do rynków cyfrowych, co wynika z ich dynamiki i struktury[2].

W konsekwencji DMA wprowadza szereg środków zmierzających do zapewnienia bardziej zapobiegawczego podejścia przedstawicieli branży big tech w odniesieniu do raportowania Komisji zgodności ich działań z prawem. Ponadto DMA wyposaża Komisję w szczególne kompetencje dotyczące możliwości prowadzenia określonych postępowań. Komisja otrzymuje dzięki temu kompleksowy i transparentny ogląd rynków cyfrowych w „czasie rzeczywistym" zamiast ustalania pełnego krajobrazu rynkowego dopiero po wystąpieniu konsekwencji danego naruszenia.

Większość środków egzekwowania DMA odpowiada omówionej już części materialnej DMA, tj. art. 5–7 rozporządzenia, które jednocześnie stanowią źródło uprawnień użytkowników biznesowych i końcowych korzystających z platform strażników dostępu. Ze względu na cel niniejszego opracowania, również w ramach tego rozdziału uwaga koncentruje się na tych środkach egzekwowania DMA, które są szczególnie istotne z perspektywy praw użytkowników[3].

Warto zauważyć, że art. 8 DMA ustanawia ogólny obowiązek strażników dostępu do „zapewnienia i wykazania", że wypełniają obowiązki określone w art. 5–7 DMA. Stąd w pierwszej kolejności strażnicy dostępu powinni wprowadzić wszelkie niezbędne środki zapewniające rzeczywistą zgodność ich działań ze szczególnymi obowiązkami, jak również z ogólnymi celami DMA. Po drugie – i w konsekwencji – strażnicy dostępu muszą być w stanie wykazać, że rzeczywiście wprowadzili wszelkie niezbędne środki oraz że są one w pełni skuteczne.

W tym kontekście Komisja może wszcząć postępowanie w celu weryfikacji, czy strażnicy dostępu wypełniają swoje obowiązki. Może też doprecyzować część z tych obowiązków, przyjmując odpowiedni akt wykonawczy.

Jednocześnie, zgodnie z art. 8 ust. 3 DMA, strażnicy dostępu mogą zwrócić się do Komisji z wnioskiem o konsultację i ustalenie, czy środki wprowadzone przez nich w celu wykonania obowiązków rzeczywiście są odpowiednie i skuteczne. Komisja dysponuje uznaniem przy podejmowaniu decyzji o zaangażowaniu się w tego typu dialog, niemniej omawiane rozwiązanie wprowadza ramy dla prowadzonej w dobrej wierze współpracy między strażnikami dostępu a organem odpowiedzialnym za egzekwowanie DMA[4].

---

[2] O. Andriychuk, *The Digital Markets Act: Tailoring the Tailors*, w: K. Tyagi, A.K. Sanders, C. Cauffman (red.), *Digital Platforms, Competition Law and Regulation*, Oxford–New York–Dublin 2024, s. 44 i n.

[3] Szczegółowe omówienie publicznego egzekwowania DMA, zob. ibidem; D. Zimmer, J.F. Göhsl, *Enforcement of the Digital Markets Act*, Verfassungsblog 2024, https://verfassungsblog.de/enforcement-of-the-digital-markets-act/ (dostęp: 3.04.2025).

[4] Jest to również nowe rozwiązanie w porównaniu do ogólnego prawa konkurencji, które w przeważającej mierze oparte jest na samodzielnej ocenie przedsiębiorstw i w przypadku którego nie mogą oni konsultować z Komisją legalności swoich działań.

5.2.2. Szczególne elementy podejścia *ex ante*

W tej części omówione zostaną poszczególne środki wprowadzone przez DMA, które zmierzają do zapewnienia transparentności działań strażników dostępu w relacji z Komisją, użytkownikami platform oraz ze społeczeństwem.

Obowiązki sprawozdawcze. Zgodnie z art. 11 DMA, strażnicy dostępu zobowiązani są składać do Komisji „sprawozdanie opisujące w szczegółowy i przejrzysty sposób środki, które wdrożyli w celu wypełniania obowiązków ustanowionych w art. 5, 6 i 7" DMA. Sprawozdanie powinno zostać złożone w ciągu sześciu miesięcy od dnia wskazania przedsiębiorstwa jako strażnika dostępu oraz być aktualizowane przynajmniej raz w roku.

Celem tego środka jest zapewnienie, że Komisja, jako organ publicznie egzekwujący DMA, dysponuje pełnym i aktualnym oglądem konkretnych działań podejmowanych przez strażników dostępu w odpowiedzi na ich obowiązki ustanowione w omawianym rozporządzeniu. Sprawozdania powinny z jednej strony odnosić się do konkretnych obowiązków, a z drugiej – opisywać poszczególne środki przyjęte w celu zapewnienia zgodności. Pozwala to Komisji na ocenę w czasie rzeczywistym efektywności działań strażników dostępu.

Strażnicy dostępu składają do Komisji również jawną wersję streszczenia sprawozdania, która jest udostępniana publicznie przez Komisję[5]. Podobnie jak w przypadku obowiązków sprawozdawczych w zakresie przejrzystości na podstawie DSA, publiczne wersje sprawozdań zapewniają transparentność działań strażników dostępu przed społeczeństwem. Pozwala to innym organizacjom lub podmiotom prywatnym (w tym użytkownikom biznesowym i końcowym) na lepszy ogląd oraz weryfikację zgodności działań strażników dostępu w konkretnych przypadkach.

Pierwszy zestaw sprawozdań strażników dostępu został przekazany Komisji w marcu 2024 r. Względem niektórych strażników podnoszono głosy krytyczne, że złożone dokumenty są zbyt zdawkowe i ogólne[6]. Z pewnością Komisja powinna wypracować ze strażnikami dostępu odpowiednie podejście do sprawozdań, nawet jeśli stosowne wytyczne zawarto w rozporządzeniu wykonawczym do DMA[7] oraz w opracowanym wzorze sprawozdania[8].

Sprawozdania niezależnych audytorów. Na strażnikach dostępu ciąży także szczególny obowiązek zapewnienia przejrzystości w odniesieniu do stosowanych

[5] Zob. stronę internetową Komisji, na której publikowane są omawiane dokumenty: https://digital-markets-act-cases.ec.europa.eu/reports/compliance-reports (dostęp: 3.04.2025).

[6] Zob. dla przykładu sprawozdanie Apple, które zawiera jedynie 12 stron ogólnych stwierdzeń: https://www.apple.com/legal/dma/dma-ncs.pdf (dostęp: 3.04.2025).

[7] Rozporządzenie wykonawcze Komisji (UE) 2023/814 z dnia 14 kwietnia 2023 r. w sprawie szczegółowych zasad dotyczących prowadzenia przez Komisję niektórych postępowań na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 (Dz. Urz. UE L 102, 17.04.2023, s. 6–19).

[8] Zob. https://digital-markets-act.ec.europa.eu/legislation_en (dostęp: 3.04.2025).

na platformach technik profilowania konsumentów[9]. Jeśli strażnicy stosują tego typu praktykę, powinny złożyć do Komisji oddzielne sprawozdanie przygotowane przez niezależnego audytora.

Podobnie jak w przypadku omówionych powyżej sprawozdań, audyt dotyczący profilowania konsumentów powinien być złożony w ciągu sześciu miesięcy po wskazaniu strażnika dostępu oraz aktualizowany co najmniej raz w roku. Powinno być do niego załączone streszczenie, które nie zawiera danych wrażliwych i może zostać publicznie udostępnione przez Komisję. W konsekwencji użytkownicy platform oraz pozostałe podmioty mogą dowiedzieć się na podstawie raportu, w jaki sposób przetwarzane są ich dane oraz zweryfikować zgodność tych działań z DMA oraz innym prawodawstwem mającym zastosowanie w tym zakresie.

Wewnętrzny nadzór. Strażnicy dostępu mają także obowiązek wprowadzenia do swojej struktury korporacyjnej komórki nadzoru przestrzegania DMA. Jednostka taka powinna cieszyć się wystarczającą niezależnością, kompetencjami, zasobami, odpowiednim statusem w ramach organizacji oraz dostępem do organu zarządzającego w celu monitorowania zachowania przez strażnika dostępu zgodności z DMA. Ponadto, wspomniana komórka współpracuje bezpośrednio z Komisją w celu zapewnienia pełnej zgodności działań strażnika z wymogami DMA.

Postępowania w sprawie badania rynku. Komisja może prowadzić postępowania w sprawie badania rynku w odniesieniu do trzech przypadków: wskazania strażnika dostępu; systematycznego niewypełniania obowiązków przez strażnika; ustalenia występowania nowych usług i nowych praktyk na rynkach cyfrowych. Użytkownicy mogą zajmować stanowisko w tego typu postępowaniach, co może skutkować wzmocnieniem efektywności ich uprawnień.

Postępowania w przedmiocie niewypełniania obowiązków zmierzają do ustalenia, czy strażnik dostępu naruszył któryś z ciążących na nim obowiązków, wynikających z art. 5–7 DMA. Komisja wszczyna postępowanie z urzędu, jednakże może być to inspirowane np. brakiem spójności między sprawozdaniami w przedmiocie zgodności a skargami otrzymywanymi od użytkowników platform czy spostrzeżeniem, że użytkownicy podejmują próby wyegzekwowania swoich praw w postępowaniach przed sądami krajowymi. Artykuł 27 DMA wprost zachęca strony trzecie, w tym użytkowników biznesowych i końcowych, a także konkurentów strażników dostępu, do informowania Komisji o możliwym niewypełnianiu obowiązków przez strażników.

[9] Profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się, zgodnie z art. 4 pkt 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119, 4.05.2016, s. 1–88).

W innego rodzaju postępowaniach w sprawie badania rynku Komisja może zebrać informacje o nowych zjawiskach występujących na rynkach cyfrowych. Ma to pozwolić w ustaleniu nowych rodzajów podstawowych usług platformowych (świadczenie których warunkuje wskazanie danego przedsiębiorstwa jako strażnika dostępu) albo nowego rodzaju praktyk ograniczających konkurencję i stosowanych przez strażników dostępu.

5.2.3. Niewypełnianie obowiązków

Jeśli omówione wyżej środki okażą się niewystarczające, Komisja może wszcząć postępowanie zmierzające do wydania decyzji stwierdzającej niewypełnienie obowiązków. Sprawy takie są pod kątem proceduralnym podobne do postępowań z zakresu prawa konkurencji. W toku postępowania Komisja dysponuje zatem typowymi kompetencjami pozwalającymi na zebranie odpowiednych dowodów, włączając w to kompetencję do żądania udzielenia informacji i wyjaśnień, przeprowadzania rozmów z pracownikami czy przeprowadzenia kontroli z przeszukaniem w siedzibie przedsiębiorcy.

W pilnych przypadkach Komisja może także przyjąć środki tymczasowe, o ile stwierdzi ryzyko wystąpienia poważnej i nieodwracalnej szkody dla użytkowników biznesowych bądź końcowych. W ramach środków tymczasowych Komisja może nakazać strażnikowi dostępu podjęcie jakiegokolwiek działania niezbędnego do ochrony interesów innych stron, do momentu wydania decyzji kończącej postępowanie w sprawie naruszenia.

Postępowanie w sprawie systematycznego niewypełniania obowiązków może zostać zakończone decyzją, zgodnie z którą – wbrew pierwotnym zastrzeżeniom – strażnik dostępu jednak wypełniał swoje obowiązki wynikające z DMA. Alternatywnie Komisja może przyjąć akty wykonawcze (decyzje), które (1) nakładają środki zaradcze, (2) przyjmują odpowiednie zobowiązania strażnika dostępu czy (3) stwierdzają niewykonanie przez strażnika dostępu określonego obowiązku.

Środki zaradcze mogą zostać nałożone, jeśli z powodu niewykonania obowiązków strażnik dostępu umocnił lub rozszerzył swoją pozycję w odniesieniu do któregokolwiek z warunków wskazania strażnika dostępu. Środki zaradcze mogą mieć charakter behawioralny (np. nakazanie określonego działania, jak przyznanie dostępu do sklepu z aplikacjami twórcom aplikacji) czy strukturalny (np. wyzbycie się kontroli nad zorganizowaną częścią działalności)[10].

[10] Przykładowo, można się spodziewać, że Komisja przyjmie środek strukturalny względem Google w postępowaniu dotyczącym reklam internetowych i tym samym nakaże tej spółce wyzbyć się kontroli nad jedną z działalności związanych z działalnością Google na rynku reklam online, zob. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3207 (dostęp: 3.04.2025). Sprawa prowadzona jest na podstawie art. 102 TFUE, a nie na podstawie DMA. Niemniej, istota strukturalnych środków zaradczych pozostaje ta sama w obydwu rodzajach postępowań.

Zobowiązania mogą zostać zaproponowane przez strażnika dostępu w toku postępowania przed Komisją. W istocie muszą one odpowiadać na wstępne zastrzeżenia podniesione przez Komisję oraz zapewnić, że zarzucane naruszenie zostanie zakończone. Komisja może zaakceptować zaproponowane zobowiązania (albo ustalać ich dokładny zakres ze strażnikiem dostępu) i przyjąć je w formie decyzji wiążącej strażnika dostępu.

Decyzje stwierdzające niewypełnienie obowiązków są przyjmowane, gdy strażnik dostępu narusza (1) obowiązki określone w art. 5–7 DMA, (2) szczególne środki nałożone na strażnika dostępu, (3) środki zaradcze, (4) środki tymczasowe, (5) zobowiązania wiążące strażnika na podstawie decyzji Komisji.

Grzywny. Decyzja stwierdzająca niewykonanie obowiązków może także nakładać grzywnę w wysokości do 10% łącznego światowego obrotu uzyskanego przez strażnika dostępu w roku obrotowym poprzedzającym wydanie decyzji. Proporcja 10% jest stosowana także w prawie konkurencji i jest uważana za bardzo wysoką w kontekście pełnionej funkcji odstraszającej. Jednakże w przypadku powtarzających się naruszeń DMA wysokość grzywny może wzrosnąć do maksymalnie 20% obrotu osiąganego przez strażnika dostępu[11].

5.3. Egzekwowanie DSA na drodze publicznoprawnej

5.3.1. Właściwe organy krajowe i koordynatorzy do spraw usług cyfrowych

DSA nakłada na pośredników liczne obowiązki w zakresie należytej staranności, zmierzające do ochrony użytkowników w relacji z pośrednikami internetowymi. Obowiązki te były przedmiotem dyskusji w rozdziałach II i III, ze szczególnym naciskiem na sferę moderowania treści i ochronę konsumentów. W porównaniu z dyrektywą 2000/31, której rozdział 3 (art. 16–20) poświęcony jest narzędziom skutecznej implementacji, DSA reguluje znacznie szerszy zakres instrumentów, w przeważającej mierze w zakresie publicznoprawnego egzekwowania przepisów rozporządzenia (art. 49–88 DSA). Odpowiedzialność za ich stosowanie należy do państw członkowskich i Komisji, które – zgodnie z art. 56 ust. 5 DSA – egzekwują stosowanie rozporządzenia w ścisłej współpracy. Współpracy tej służy w szczególności ustanowienie Europejskiej Rady ds. Usług Cyfrowych (European Board for Digital Services, EBDS).

[11] Rozwiązanie to uwzględnia niedawne obserwacje, że dla niektórych strażników dostępu dotychczasowe wysokości kar pieniężnych nie były dostatecznie odstraszające i nie przewyższały korzyści uzyskiwanych wskutek naruszeń. Zob. dla przykładu https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1161 (dostęp: 3.04.2025).

Państwo członkowskie może wyznaczyć jeden lub więcej właściwych organów krajowych, ale tylko jednemu z nich należy powierzyć rolę koordynatora (DSC)[12]. Zakres swobody państwa członkowskiego obejmuje zatem utworzenie nowych organów bądź dodanie nowych kompetencji istniejącym podmiotom. Podejście takie było już wcześniej przyjęte w Unii, na przykład w RODO czy w dyrektywie AVMSD[13]. W Irlandii czy we Włoszech wskazano jako DSC istniejące krajowe organy w zakresie mediów, w innych państwach rolę DSC powierzono nowym organom regulacyjnym[14]. We Francji połączenie CSA (Conseil Supérierur de l'Audiovisuel) – organu odpowiedzialnego za media audiowizualne, i l'Hadopi (Haute Autorité pour la Diffusion des Ouevres et la Protection de Droit sur l'Internet) skutkowało utworzeniem Arcom: Autorité de la communication audiovisuelle et numérique[15]. Niektóre państwa przyznały wiodącą rolę regulatorom rynku telekomunikacyjnego, tak jak jest to planowane w Polsce[16]. Do obowiązków państwa należy zapewnienie, że DSC ma wystarczające zasoby finansowe i ludzkie, zagwarantowaną autonomię w zarządzaniu budżetem oraz że działa transparentnie i bez zbędnej zwłoki. Koordynatorzy są zobowiązani do działania w sposób niezależny, bez przyjmowania jakichkolwiek instrukcji i nie podlegając zewnętrznym wpływom[17].

Koordynatorzy tworzą EBDS, o charakterze doradczym, w celu wspierania spójnego stosowania i skutecznego stosowania DSA[18]. Z uwagi na transgraniczną naturę usług pośrednich, w DSA wprowadzono szereg rozwiązań ułatwiających współpracę pomiędzy DSC państwa siedziby ISP a DSC państwa przeznaczenia usługi[19], w ramach ogólnego obowiązku współpracy[20]. DSC państwa siedziby, może zwrócić się do innych DSC o przekazanie niezbędnych informacji, w ramach wzajemnej pomocy[21], może również inicjować i prowadzić wspólne czynności sprawdzające[22].

---

[12] Art. 49 ust. 1 i ust. 2 DSA.

[13] Art. 30 dyrektywy AVMSD wymaga, by państwo członkowskie utworzyło jeden lub więcej organów czy ciał krajowych, które spełniają warunki niezależności lub bezstronności. Art. 51 ust. 1 RODO również wymaga ustanowienia jednego lub więcej niezależnych organów nadzorczych.

[14] Lista koordynatorów według państw członkowskich dostępna na stronie: https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs (dostęp: 3.04.2025).

[15] Arcom, https://www.arcom.fr/nous-connaitre/decouvrir-linstitution (dostęp: 3.04.2025).

[16] W Polsce proponuje się przyznać kompetencje Koordynatora ds. Usług Cyfrowych Prezesowi Urzędu Komunikacji Elektronicznej (UKE), projekt ustawy o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw (UC21), aktualny stan prac: https://legislacja.rcl.gov.pl/projekt/12383101/ (dostęp: 3.04.2025).

[17] Art. 50 DSA; J. Jaursch, *Platform Oversight: Here Is What Strong Digital Coordinator Should Look Like*, w: J. van Hoboken et al. (red.), *Putting the DSA into Practice: Enforcement, Access to Justice and Global Implications*, Berlin 2023, s. 98, https://verfassungsblog.de/wp-content/uploads/2023/02/vHoboken-et-al_Putting-the-DSA-into-Practice.pdf (dostęp: 3.04.2025).

[18] Art. 61–62 DSA.

[19] Motywy 126–131 DSA.

[20] Art. 58 DSA.

[21] Art. 57 DSA.

[22] Art. 60 DSA.

DSC państwa przeznaczenia, podejrzewając że ISP narusza obowiązki z rozporządzenia w sposób, który może negatywnie wpływać na odbiorców usługi, może zwrócić się do DSC państwa siedziby z wnioskiem o dokonanie oceny sprawy oraz przyjęcie niezbędnych środków i egzekwowanie przestrzegania rozporządzenia[23]. W przypadku, kiedy problem dotyczy co najmniej trzech krajów, podobny wniosek może skierować EBDS.

W przypadku naruszeń o charakterze transgranicznym, podobnie jak w kwestii nadzoru nad VLOP i VLOSE, DSA przypisuje podstawową rolę Komisji Europejskiej[24]. Ostateczna kontrola nad tym, czy DSC wykonują zobowiązania do odpowiedzi na kierowane wnioski, należy do Komisji. Na podstawie wniosku skierowanego przez EBDS Komisja może zwrócić się do DSC o ponowną ocenę danej sprawy, niezależnie od ogólnych kompetencji do skierowania skargi do TSUE na niestosowanie się do przepisów rozporządzenia przez dane państwo członkowskie[25].

5.3.2. Uprawnienia w zakresie egzekwowania. Sankcje

Aby zapewnić skuteczne przestrzeganie zasad świadczenia usług cyfrowych poddanych harmonizacji w DSA (nadzór nad nimi) oraz umożliwić reagowanie na przypadki ich nieprzestrzegania (egzekwowanie), DSC przyznano kompetencje określone w art. 51–52 DSA[26]. Pierwszy z tych przepisów rozróżnia trzy typy uprawnień DSC, w zakresie: czynności dochodzeniowych, egzekwowania oraz stosowania środków dodatkowych.

Dochodzenie i egzekwowanie. Uprawnienia w zakresie czynności dochodzeniowych mają służyć uzyskiwaniu informacji związanych z podejrzeniem naruszenia DSA. W tym celu na podstawie art. 51 ust. 1 DSA DSC mogą sięgać zarówno po źródła osobowe (wezwania do udzielenia stosownych informacji lub złożenia wyjaśnień), jak i źródła rzeczowe, w tym szczególnie nośniki informacji, co wymagać może dostępu do pomieszczeń określonych podmiotów. W zakresie egzekwowania przepisów DSA katalog uprawnień DSC, wskazanych w art. 51 ust. 2 DSA, obejmuje narzędzia administracyjne w postaci zatwierdzania zobowiązań proponowanych przez dostawców, nakazów zaprzestania naruszeń, nakładania grzywien lub kar pieniężnych oraz przyjmowania środków tymczasowych .

Uprawnieniami szczególnego typu są z kolei środki dodatkowe mające charakter narzędzi *ultima ratio*. Przewidziane zostały w przypadku, kiedy mimo wyczerpania

[23] Art. 58 DSA.

[24] Art. 58 ust. 1 DSA; zob. pkt 3.3.3 omawiający szczególne kompetencje Komisji w zakresie VLOP i VLOSE.

[25] Art. 59 i motyw 129 DSA.

[26] Na mocy art. 49 ust. 4 DSA uprawnienia te przysługują również wszelkim innym właściwym organom wyznaczonym przez państwa członkowskie do wykonywania przepisów DSA.

uprawnień wskazanych powyżej „naruszenie nie zostało usunięte lub nadal trwa i wyrządza poważne szkody" (art. 51 ust. 3 DSA). Wówczas DSC może żądać od dostawcy przyjęcia i przedłożenia planu działań naprawczych lub skorzystać nawet z uprawnienia do nakazania tymczasowego ograniczenia dostępu odbiorców do usługi (interfejsu internetowego), której dotyczy naruszenie.

Procedura. Wykonywanie przez DSC powyższych uprawnień na podstawie DSA w kontekście proceduralnym, w tym z uwagi na podstawowe gwarancje towarzyszące relacji państwo–obywatel, będzie wymagało sięgnięcia do właściwych przepisów prawa krajowego dla danego DSC (zob. przykład Polski poniżej). Stąd w art. 52 ust. 5–6 DSA umieszczono jedynie odesłanie do ogólnych zasad, wśród nich akcentując prawo do poszanowania życia prywatnego, prawo do obrony, w tym prawa do bycia wysłuchanym oraz dostępu do akt, z zastrzeżeniem prawa do skutecznego środka prawnego.

Sankcje. Uzupełnieniem uprawnień DSC, tak w zakresie egzekwowania, jak również w zakresie czynności dochodzeniowych, jest przewidziana w art. 52 DSA kompetencja do wymierzania sankcji. Przybierają one dwojaką postać: grzywien oraz okresowych kar pieniężnych przewidzianych za określone naruszenia w maksymalnej wysokości odnoszonej do rocznego światowego obrotu lub dochodu danego dostawcy usług pośrednich. Podobnie jak w przypadku środków przyjmowanych DSC również sankcje muszą spełniać ogólny wymóg skuteczności, odstraszania i proporcjonalności, doprecyzowany na gruncie stosownych przepisów krajowych.

Przykład Polski. Wedle projektu ustawy będącej przedmiotem prac legislacyjnych w Polsce funkcję DSC pełnić ma Prezes Urzędu Komunikacji Elektronicznej. Jednocześnie planowane jest wyznaczenie Prezesa Urzędu Ochrony Konkurencji i Konsumentów[27] jako organu właściwego. Temu ostatniemu, w ślad za art. 49 ust. 2 DSA, mają zostać powierzone uprawnienia w zakresie spraw dotyczących nadzoru nad wykonywaniem obowiązków dostawców platform internetowych B2C z art. 29–32 DSA (zob. rozdział III pkt 3.3). Przewidywane jest również wprowadzenie jednolitej procedury realizującej art. 51–52 DSA dla obu właściwych organów, w wielu elementach[28] wzorowanej na rozbudowanych regułach proceduralnych towarzyszących aktywności administracyjnej Prezesa Urzędu Ochrony Konkurencji i Konsumentów.

---

[27] Już teraz organ ten w zakresie swoich kompetencji łączy sprawy antymonopolowe (antykonkurencyjne porozumienia oraz kontrola koncentracji) ze sprawami z zakresu ochrony zbiorowych interesów konsumentów (naruszenia zbiorowych interesów konsumentów oraz stosowanie niedozwolonych postanowień wzorców umów).

[28] Warto tutaj zwrócić uwagę na przewidzianą w planowanych przepisach (por. przyp. 17 powyżej) kompetencję sądu powszechnego wyspecjalizowanego w sprawach z zakresu ochrony konkurencji i konsumentów (Sąd Ochrony Konkurencji i Konsumentów z siedzibą w Warszawie) do rozpatrywania odwołań od decyzji administracyjnych obu organów właściwych w sprawach stosowania DSA.

5.3.3. Egzekwowanie w odniesieniu do VLOP/VLOSE

Konsekwencją ukształtowania na gruncie DSA odrębnych reguł należytej staranności dla VLOP oraz VLOSE są przeznaczone dla tej grupy dostawców usług pośrednich narzędzia kontroli, nadzorowania, monitorowania oraz egzekwowania (art. 64–83 DSA). Potwierdzają one podział kompetencji między Komisją a państwami członkowskimi przyjęty na gruncie art. 56 DSA. Wedle tego modelu Komisja[29] zajmuje centralną pozycję w zakresie nadzorowania i egzekwowania obowiązków nałożonych na VLOP oraz VLOSE. Model ten charakteryzuje się jednocześnie ścisłą współpracą zaangażowanych podmiotów.

Znaczenie współpracy zaangażowanych instytucji jest widoczne już w kontekście rozwoju wiedzy eksperckiej i zdolności służących skutecznemu egzekwowaniu DSA. Artykuł 64 DSA przewiduje w tym zakresie różne formy współdziałania instytucjonalnego między Komisją, EBDS, DSC, a także z udziałem potencjalnie innych właściwych organów. Z uwagi na przewidziane również w obrębie DSA inne formy działań eksperckich, towarzyszące choćby konkretnym obowiązkom w zakresie należytej staranności[30], ale także stosowane przez Komisję narzędzia egzekwowania DSA[31], należy oczekiwać, że w praktyce zasób tej wiedzy będzie stanowił szczególną wartość przy ocenie praktyk przede wszystkim platform, ale także ich użytkowników.

Korzystanie z uprawnień przyznanych Komisji w zakresie czynności dochodzeniowych (sprawdzających) może zostać zainicjowane z własnej inicjatywy Komisji lub na wniosek DSC. Przy czym w tym drugim przypadku DSA określa szczególne wymagania formalne oraz materialne dla wniosków kierowanych przez DSC do Komisji o ocenę przypadków podejrzenia naruszenia przepisów przez VLOP oraz VLOSE (art. 65 DSA). Z kolei w przypadku decyzji Komisji o wszczęciu postępowania[32] przewidziano wielostronny obieg informacji uwzględniający obok Komisji VLOP

[29] Por. dyskusję na temat efektywności tego modelu, w tym rozwiązań przyjmowanych na gruncie innych regulacji w obszarze cyfrowej transformacji w UE: A. Zhelyazkova, *Challenges in EU Law Enforcement and the Digital Age*, w: M. Scholten (red.), *Research Handbook on the Enforcement of EU Law*, Cheltenham–Northampton 2023, s. 100; K. Söderlund, S. Larsson, *Enforcement Design Patterns in EU Law: An Analysis of the AI Act*, „Digital Society" 2024, t. 3, artykuł 41, s. 7.

[30] Wymóg wiedzy eksperckiej towarzyszy zresztą poszczególnym instrumentom DSA, zarówno w przypadku organów pozasądowego rozstrzygania sporów (art. 21 ust. 3 lit. b), zaufanych podmiotów sygnalizujących (art. 22 ust. 2), organizacji prowadzących audyty (art. 37 ust. 3) czy zweryfikowanych badaczy (art. 40 ust. 8).

[31] Obok podmiotów wskazanych bezpośrednio w przepisach DSA należy mieć na uwadze funkcjonujące od 2018 r. Obserwatorium Gospodarki Platform Internetowych (decyzja Komisji z dnia 26 kwietnia 2018 r., C(2018) 2393 final), o którym wspomniano w motywie 137 DSA, oraz Europejskie Centrum Przejrzystości Algorytmicznej.

[32] Pierwsze takie postępowania Komisja wszczęła jeszcze w grudniu 2023 r. wobec dostawcy platformy X (poprzednio Twitter), a w 2024 r. kolejno wobec dostawców takich usług jak TikTok, AliExpress, Facebook, Instagram oraz Temu – zob. stosowne odniesienia do decyzji Komisji oraz komunikaty prasowe na poświęconej temu stronie: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (dostęp: 3.04.2025).

oraz VLOSE, krajowych koordynatorów, EBDS, a także inne właściwe organy zaangażowane do sprawy (motyw 148 preambuły, art. 66 DSA). Wspierać go ma działanie systemu wymiany informacji („AGORA") utworzonego na podstawie art. 85 DSA[33].

Instrumenty egzekwowania. Podstawowe instrumenty, w jakie DSA wyposaża Komisję w celu egzekwowania obowiązków VLOP i VLOSE, są zasadniczo podobne do narzędzi, które znane są choćby z unijnego prawa konkurencji (por. art. 18–21 oraz 23–26 rozporządzenia Rady (WE) Nr 1/2003[34]) czy przepisów dotyczących rynków cyfrowych (por. art. 20–34 DMA)[35], które wraz z DSA stanowiły jeden pakiet regulacyjny jako tzw. Digital Services Package. Unijny ustawodawca dopasowuje ten model scentralizowanego egzekwowania unijnych przepisów do architektury DSA (por. rozdział III pkt 3.2), w tym w szczególności ryzyk systemowych wynikających z zaprojektowania, funkcjonowania i korzystania z usług VLOP lub VLOSE.

Komisja może zatem żądać udzielenia informacji związanych z podejrzeniem naruszenia prawa stosownie do art. 67 DSA. Przepis ten określa między innymi krąg podmiotów, do których Komisja może kierować takie żądania[36], czyniąc to w drodze zwykłego wniosku czy decyzji. Z kolei art. 68 DSA ustanawia uprawnienie Komisji do odbierania wyjaśnień i otrzymywania oświadczeń, co sprzyja prowadzeniu czynności sprawdzających związanych z podejrzeniem naruszenia. Istotne znaczenie ma również doprecyzowane w akcie wykonawczym Komisji[37] uprawnienie z art. 69 DSA do przeprowadzenia kontroli w pomieszczeniach danej VLOP lub VLOSE, a także innych osób wskazanych w art. 67 ust. 1 DSA.

Wachlarz decyzji, które Komisja może podejmować w ramach egzekwowania przepisów DSA wobec VLOP i VLOSE, obejmuje narzędzia typowe w postaci środków tymczasowych (art. 70) czy zobowiązań[38] (art. 71). Komisja może z nich korzystać jeszcze w toku prowadzonych postępowań. Przesłanki decyzji stwierdzającej nieprzestrzeganie przepisów określa z kolei art. 73 DSA. Charakter narzędzi sankcjonujących mają z kolei decyzje nakładające grzywny (art. 74) lub okresowe

[33] Zob. rozporządzenie wykonawcze Komisji (UE) 2024/607 z dnia 15 lutego 2024 r. w sprawie ustaleń praktycznych i operacyjnych na potrzeby funkcjonowania systemu wymiany informacji na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 (akt o usługach cyfrowych) (Dz. Urz. UE L, 2024/607, 16.02.2024).

[34] Rozporządzenie Rady (WE) nr 1/2003 z dnia 16 grudnia 2002 r. w sprawie wprowadzenia w życie reguł konkurencji ustanowionych w art. 81 i 82 Traktatu (Dz. Urz. UE L 1, 4.01.2003, s. 1–25).

[35] Por. rozdział IV poświęcony DMA.

[36] Por. informacje na stronie przywołanej w przypisie 32 wskazujące na konkretne przypadki postępowań wszczynanych przez Komisję.

[37] Zob. rozporządzenie wykonawcze Komisji (UE) 2023/1201 z dnia 21 czerwca 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, 22.06.2023, s. 51–59).

[38] Po raz pierwszy taką decyzję Komisja wydała wobec usługi TikTok – zob. komunikat prasowy Komisji (UE) z dnia 5 sierpnia 2024 r., TikTok Commits to Permanently Withdraw TikTok Lite Rewards Programme from the EU to Comply with the Digital Services Act, https://ec.europa.eu/commission/presscorner/detail/en/IP_24_4161 (dostęp: 3.04.2025).

kary pieniężne (art. 76) wydawane z uwzględnieniem charakteru naruszenia przepisów oraz przy zachowaniu sądowej kontroli ze strony TSUE (art. 81).

Rozwiązaniem specyficznym dla DSA jest system wzmożonego nadzoru ustanowiony na mocy art. 75, a służący eliminowaniu naruszeń dodatkowych obowiązków w zakresie zarządzania ryzykiem systemowym nałożonych na VLOP oraz VLOSE w art. 33–43 DSA. Wzmożony nadzór ma charakter obligatoryjny i jest powiązany z decyzją wydaną na podstawie art. 73 DSA. W jego ramach przewidziano między innymi obowiązek sporządzenia i przekazania DSC, Komisji oraz EBDS planu działania określającego środki wystarczające do zaprzestania lub usunięcia naruszenia przez dostawcę.

Instrumenty monitorowania. Obok nadzoru, kontroli oraz egzekwowania w DSA szczególną wagę przywiązuje się do monitorowania skutecznego wdrożenia i przestrzegania jego przepisów. W tym celu art. 72 DSA przyznaje Komisji uprawnienie[39] do występowania z nakazem udzielenia dostępu do baz danych i algorytmów danej VLOP lub VLOSE lub nakładania na te podmioty obowiązku przechowywania określonych dokumentów. Przy działaniach z zakresu monitorowania uwzględniona jest możliwość korzystania z wiedzy eksperckiej i specjalistycznej, co współgra z założeniem współpracy instytucjonalnej wynikającym z art. 64 DSA.

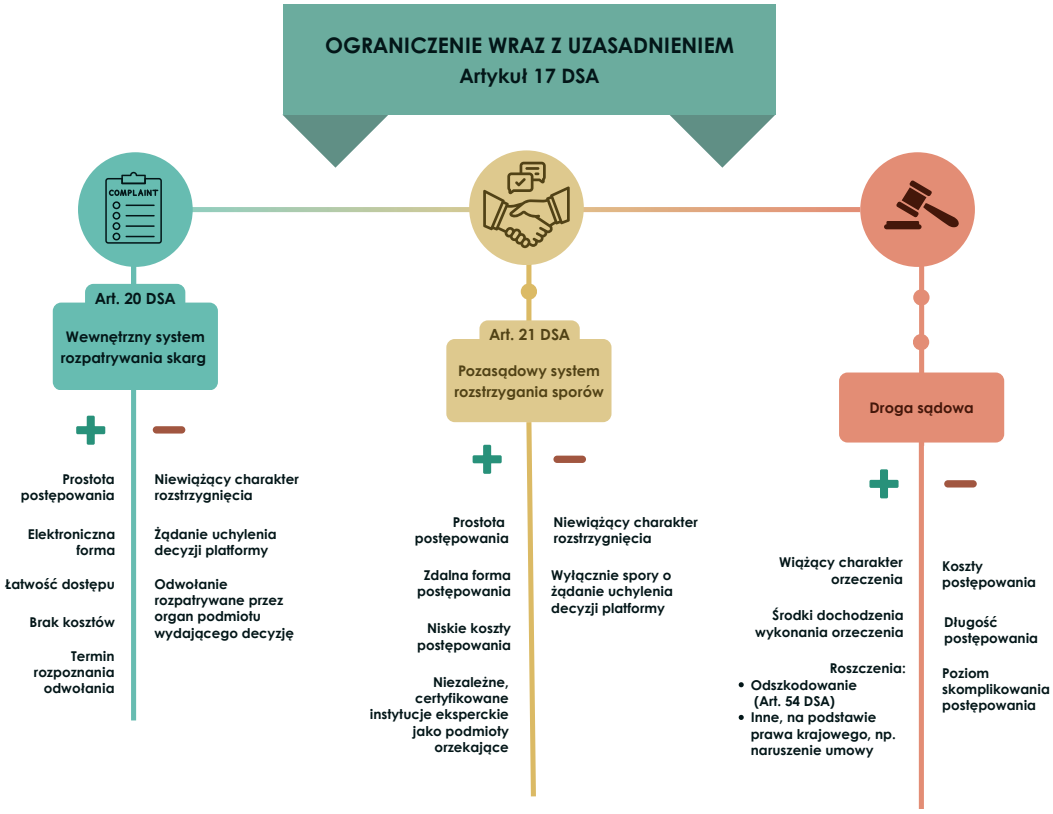
Wątek współpracy pojawia się również w postaci odrębnego uprawnienia Komisji do kierowania do DSC lub sądów krajowych wniosków o podjęcie działań na podstawie art. 51 ust. 3 DSA. Ten ostatni przepis – przywołany wcześniej przy okazji omawiania uprawnień DSC – ustanawia narzędzie typu *ultima ratio*. Sięganie po nie przez Komisję odbywa się na zasadach określonych w art. 82 DSA. Jego stosowanie, szczególnie z udziałem sądów krajowych, może być przyczynkiem do korzystania z trybu prejudycjalnego (zob. art. 82 ust. 3 DSA, który odsyła do art. 267 TFUE). Poza tym przepis ten uwzględnia wątek spójności rozstrzygnięć sądów krajowych z decyzjami Komisji, szczególnie rozważanymi przez Komisję w trakcie postępowania wszczętego na gruncie przepisów DSA. Wzorem dla tego mechanizmu współpracy z sądami krajowymi był zapewne art. 16 ust. 2 przywołanego już rozporządzenia Rady (WE) nr 1/2003. Został on również wykorzystany w art. 39 ust. 5 DMA. We wszystkich tych przypadkach służyć ma jednolitemu stosowaniu oraz egzekwowaniu prawa UE.

5.3.4. Spory użytkowników z platformami – rola DSC

DSC odgrywają istotną rolę w **strukturze uregulowań dotyczących środków ochrony** dostępnych użytkownikom i w zakresie wzmacniania ich pozycji środowisku platform. Kompetencje DSC można rozpatrywać z kilku perspektyw: (1) użytkownika

[39] Doprecyzowane w przepisach rozporządzenia wykonawczego Komisji (UE) 2023/1201.

uprawnionego do zgłoszenia nielegalnych treści zgodnie z art. 16 DSA, (2) odbiorcy usługi, którego treści zostały ograniczone decyzją platformy, i (3) konsumenta, którego prawo do bezpieczeństwa i informacji zostały naruszone. W świetle DSA sposoby dochodzenia ochrony obejmują: **wewnętrzny system rozpatrywania skarg, możliwość inicjowania postępowań przed pozasądowymi organami rozstrzygania sporów bądź dochodzenia odszkodowania przed sądami krajowymi** (rys. 7). DSA zapewnia **również prawo do wniesienia skargi bezpośrednio do DSC** miejsca zamieszkania odbiorcy usługi.



Rysunek 7. Środki ochrony użytkowników

W kontekście środków ochrony postanowienia DSA odnoszą się do: (1) odbiorcy usługi, w art. 20 i 21, włączając w to użytkowników, którzy zgłosili nielegalne treści zgodnie z art. 16[40], (2) odbiorcy usługi, a także do wszelkich podmiotów, organizacji i zrzeszeń upoważnionych do wykonywania w ich imieniu praw przyznanych

[40] D. Lubasz podkreśla, że uprawnienie do zgłaszania nie jest i nie może być ograniczone wyłącznie do odbiorców usługi hostingu, D. Lubasz, M. Namysłowska (red.), *Akt o usługach cyfrowych. Komentarz*, Warszawa 2024, s. 400.

niniejszym rozporządzeniem[41] w kontekście prawa do wnoszenia skargi z art. 53, oraz (3) jedynie do „odbiorcy usługi" w art. 54 odnoszącym się do roszczeń odszkodowawczych. Wynika stąd, że **każdy użytkownik, który zgłosił nielegalne treści**, może wnieść skargę do platformy na tych samych zasadach jak odbiorcy usługi, a jeżeli takiego użytkownika dotyczy decyzja wymieniona w art. 20 ust. 1 DSA może zadecydować o skierowaniu sprawy do organu pozasądowego rozstrzygania sporów.

W świetle DSA jedynie platformy internetowe, a nie wszyscy dostawcy usługi hostingu, są zobowiązani do ustanowienia wewnętrznych mechanizmów rozpatrywania skarg i tylko ich decyzje mogą być kwestionowane w postępowaniach przed pozasądowymi organami rozpatrywania sporów. W zakresie swoich uprawnień jako organów nadzorujących platformy DSC powinni reagować, **jeśli nie ustanowiono odpowiednich mechanizmów zgłaszania bądź wewnętrznego systemu rozpatrywania skarg**. W art. 16 i 20 DSA wskazano wyraźnie warunki, jakie te mechanizmy powinny spełniać. Ocena, czy są one łatwo dostępne, przyjazne dla użytkownika, w pełni dostępne online i pozwalają na składanie odpowiednio uzasadnionych zgłoszeń, należy do DSC[42]. Podobne wymogi ustanowiono dla wewnętrznych systemów zgłaszania skarg[43]. W zakresie zapewniania bezpieczniejszej przestrzeni i ochrony przed nielegalnymi treściami DSC mają za zadanie przyznawać status **„zaufanego podmiotu sygnalizującego"** eksperckim jednostkom, których zgłoszenia korzystają z priorytetowego traktowania i są rozpatrywane bez zbędnej zwłoki[44]. W zakresie ochrony użytkowników przed dyskrecjonalnymi decyzjami platform rolę DSC można postrzegać w **zakresie certyfikowania pozasądowych organów rozpatrywania sporów** (ODS).

W postępowaniu certyfikacyjnym DSC ocenia, czy wnioskodawca spełnia wymagania niezależności i bezstronności, włączając w to niezależność finansową organu i jego członków[45], czy jest zdolny rozwiązywać spory szybko, skutecznie i oszczędnie, na podstawie jasnych, dostępnych publicznie zasad dotyczących procedur, zgodnych z prawem krajowym[46]. Proces certyfikacji zmierza do zapewnienia organów godnych zaufania, eksperckich, niezależnych od platform i szeroko dostępnych. DSC ocenia, czy wnioskodawca posiada wymagany zakres wiedzy i doświadczenia w odniesieniu do rodzaju nielegalnych treści, np. stanowiących naruszenie własności intelektualnej, czy treści stanowiących „mowę nienawiści" bądź w odniesieniu do oceny warunków świadczenia usługi jednego lub więcej typów platform[47].

[41] Art. 86 DSA.

[42] Art. 16 ust. 1 DSA; zgodnie z art. 56 ust. 3 DSA Komisja ma również uprawnienia w zakresie nadzorowania i egzekwowania niniejszego rozporządzenia wobec VLOP i VLOSE, w zakresie innym niż określony w rozdziale 3 sekcja 5.

[43] Art. 20 ust. 1 DSA.

[44] Art 22 ust. 1 DSA.

[45] Wynagrodzenie przyznawane jest na poziomie niezwiązanym z wynikiem postępowania.

[46] Lista wszystkich warunków jest wskazana w art. 21 ust. 3 DSA.

[47] Art. 20 ust. 3 lit. b DSA.

DSC, w świetle powyższego, biorą aktywny udział w kształtowaniu alternatywnego systemu rozstrzygania sporów z platformami. Kwestia zapewnienia ochrony praw podstawowych użytkowników, w działaniach ODS jest uważana za z jednej strony pożądaną, z drugiej – niejasną w świetle DSA[48]. Teoretycznie ich rola mogłaby być kluczowa, jako że są to organy niezależne od platform, łatwo dostępne i eksperckie. Certyfikowane organy mają obowiązek składania sprawozdań DSC, a DSC z kolei, w swoich raportach powinni identyfikować systemowe niedociągnięcia, braki czy trudności i mogą zalecać i promować dobre praktyki poprawiające funkcjonowanie alternatywnych systemów rozstrzygania sporów. Dla użytkownika oznacza to, że organy publiczne monitorują odpowiednie funkcjonowanie alternatywnych systemów rozstrzygania sporów, co stanowi ich zaletę. Z drugiej strony jednak, korzystanie z takich systemów nie zapewnia uzyskania rozstrzygnięcia wiążącego dla stron[49].

Nadzór nad **dopełnieniem obowiązków sprawozdawczych przez pośredników** należy co do zasady do DSC[50]. Nieopublikowanie raportów bądź nieprzedstawianie wymaganych danych co do np. liczby zgłoszeń w ramach mechanizmu z art. 16 stanowi naruszenie DSA. Również do DSC powinna należeć ocena, czy informacje przedstawione w sprawozdaniach, np. w odniesieniu do wykorzystywania automatycznych narzędzi moderowania treści[51], są zgodne z wymogami określonymi w DSA. Systematyczna analiza przedkładanych raportów i dostępnych danych, jak np. publicznie dostępnych uzasadnień decyzji o moderowaniu treści, nie jest wyraźnie wskazanym obowiązkiem DSC, jednakże jest pożądana. Inne podmioty, takie jak badacze, zaufane podmioty sygnalizujące czy NGO, mogą przyczyniać się do tych analiz. DSC mają kompetencje w zakresie **przyznawania statusu „zweryfikowanego badacza"** i w zakresie wniosków kierowanych do VLOP i VLOSE o udostępnienie danych, dla celów badań i analizy systemowego ryzyka w Unii, wynikającego z działań platform[52].

Każdy usługobiorca **ma prawo wnieść skargę do DSC, zgodnie z art. 53 DSA**. Podmioty zgłaszające treści na podstawie art. 16 DSA nie zostały wskazane w treści przepisu. Pozostaje zatem niejasne, czy złożenie zgłoszenia zgodnie z art. 16 skutkuje uzyskaniem statusu „odbiorcy usługi"[53]. Konsumenci należą do

[48] Zob. J.P. Quintais et al., *Discussion Report. The Role of Fundamental Rights in Out-of-Court Dispute Settlement under art. 21 DSA*, November 2024, s. 2–6, https://www.user-rights.org/media/50/download/Discussion%20Report%20No.%202%20-%20Article%2021%20-%20Academic%20Advisory%20Board.pdf?v=1&inline=1 (dostęp: 3.04.2025).

[49] Art. 21 ust. 2 DSA.

[50] Podstawowe obowiązki w zakresie raportowania wynikają z art. 15 DSA, a dodatkowe obowiązki przewidują dalsze postanowienia dotyczące platform internetowych oraz tzw. VLOP i VLOSE. Zgodnie z art. 56 ust. 3, w odniesieniu do VLOP i VLOSE Komisja ma uprawnienia w zakresie nadzorowania i egzekwowania również innych obowiązków, niż te wskazane w rozdziale 3 sekcja 5 DSA.

[51] Art. 15 ust. 1 lit. e DSA.

[52] Art. 40 ust. 4 i 8 oraz art. 34 DSA.

[53] Za takim stanowiskiem przemawia argument, że użytkownik korzysta z funkcjonalności usługi, tak więc korzysta z samej usługi w odniesieniu do informacji, którą uważa za nielegalną. W przypadku, w którym dostawca usługi hostingu naruszył art. 16 ust. 4 i, uchybiając obowiązkowi potwierdzenia otrzymania

kategorii „odbiorców usługi" i mogą wnosić skargi na naruszenia DSA, włączając w to naruszenia sekcji 4, w której nałożono szczególne obowiązki na platformy umożliwiające transakcje B2C.

DSA w zakresie skarg użytkowników wskazuje tylko na podstawowe wymogi, zgodnie z którymi DSC ma ocenić skargę i może przekazać ją odpowiednim organom (takim jak organy ochrony konsumenta)[54] bądź do DSC miejsca zamieszkania. Każda ze stron ma prawo bycia wysłuchanym i uzyskiwania odpowiednich informacji w toku postępowania zainicjowanego skargą. Szczegóły procedur powinny być jednak regulowane przez prawo krajowe. DSA milczy na temat rodzaju działania czy odpowiedzi, jakie powinni podjąć DSC. Ponieważ DSC jest organem właściwym w zakresie wszystkich spraw związanych z nadzorem i egzekwowaniem obowiązków wynikających z DSA, z całą pewnością może skorzystać z przysługujących mu kompetencji co do ustalania, czy doszło do naruszenia DSA, przy zachowaniu wymogu proporcjonalności działań, uwzględniając naturę, ciężar, powtarzalność naruszeń i okres ich trwania. Wynika to pośrednio z obowiązku raportowania o liczbie otrzymanych skarg i przekazywania informacji o podjętych działaniach[55].

Skargi z art. 53 mogą dotyczyć oczywistych naruszeń DSA, takich jak brak wewnętrznego mechanizmu zgłaszania skarg, ale również spraw indywidualnych, takich jak skarga na to, że działania dostawcy usług nie były terminowe, przeprowadzane z należytą starannością i prowadziły do arbitralnych rozwiązań, a więc naruszały warunki wskazane w art. 14 ust. 4 bądź w art. 20 ust. 4. Takie skargi stanowią wyzwanie dla organów administracyjnych. Jak słusznie wyjaśnia irlandzki DSC, Comisiún na Meán, rolą DSC nie jest bycie sądem[56]. Do zadań DSC należy jednak ocena, czy pośrednicy działają z należytą starannością, a prawo do składania skargi przez jednostki, a więc ewidentnie w sprawach indywidualnych, jest prawem bezpośrednio wynikającym z rozporządzenia.

5.4. Egzekwowanie DSA na drodze prywatnoprawnej

Skuteczność praw odbiorców usług, które można zidentyfikować na gruncie DSA na podstawie ustanowionego w tym rozporządzeniu zestawu zharmonizowanych obowiązków dostawców usług pośrednich w zakresie należytej staranności, zależy

zgłoszenia, nie zareagował, a użytkownik uznaje, że dostawca usługi nie działał z należytą starannością, niearbitralnie i obiektywnie (art. 16 ust. 6), art. 20 i 21 nie znalazłyby zastosowania, użytkownik powinien być uprawniony do złożenia skargi do DSC zgodnie z art. 53, jako odbiorca usługi.

[54] W Polsce mógłby to być przypadek przekazania sprawy Prezesowi Urzędu Ochrony Konkurencji i Konsumentów (UOKiK).

[55] Art. 55 ust. 1 DSA.

[56] Comisiún na Meán, Complaints guide, https://www.cnam.ie/general-public/report-complain/something-i-saw-or-experienced-online/what-can-i-report/#whatyoucantreport (dostęp: 3.04.2025).

od poprawnego doboru narzędzi prawnych służących egzekwowaniu wspomnianych obowiązków. W unijnej polityce konsumenckiej (por. rozdział I) w tym kontekście można przywołać ogólne prawo do odszkodowania (ang. *the right of redress*) oraz prawo do bycia wysłuchanym (ang. *the right to be heard*), które będą miały pełne zastosowanie w środowisku cyfrowym. Dla ogółu odbiorców usług podobne znaczenie będzie miało prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu (art. 47 KPP UE) oraz analogiczne konstrukcje praw podstawowych wynikających z porządków krajowych, a precyzowane w postaci skonkretyzowanych uprawnień i roszczeń w ustawodawstwie krajowym.

Z przepisów rozdziału 4 DSA wyłania się model egzekwowania oparty w głównej mierze na instrumentach prawa publicznego (ang. *public enforcement*). Niemniej, *private enforcement* należy traktować w sposób komplementarny jako potencjalnie źródło instrumentarium prawnego służącego przestrzeganiu zasad świadczenia usług cyfrowych. Nie ulega przy tym wątpliwości, że realizacja szeregu obowiązków przewidzianych w DSA będzie miała szczególne znaczenie dla praktycznego wykonywania praw użytkowników dochodzonych w trybie *private enforcement*. W tym kontekście wskazać można na obowiązek wyznaczenia przez dostawcę usług pośrednich pojedynczego punktu kontaktowego dla odbiorców usług (art. 12 DSA), mechanizmy zgłaszania i działania dotyczące dostawców usług hostingu, w tym platform internetowych (art. 16 DSA), oraz mający zastosowanie do platform internetowych obowiązek zapewnienia odbiorcom usługi dostępu do wewnętrznego systemu rozpatrywania skarg w połączeniu z mechanizmem pozasądowego rozstrzygania sporów (art. 20–21 DSA).

Roszczenia odszkodowawcze. Wśród narzędzi służących egzekwowaniu DSA w kontekście *private enforcement* centralne znaczenie ma jednak art. 54. Stanowi on podstawę do dochodzenia roszczeń odszkodowawczych z tytułu naruszenia przez dostawców ich obowiązków wynikających z rozporządzenia. W porównaniu z podobnym przepisem z regulacji służącej ochronie danych osobowych (art. 82 rozporządzenia UE 2016/679[57]) art. 54 DSA jest konstrukcją normatywną znacznie mniej rozbudowaną. Prawo do żądania odszkodowania przyznaje odbiorcom usługi (użytkownikom)[58] wobec dostawców usług pośrednich, jednocześnie posługując się pojęciem szkody i straty[59]. W zakresie dochodzenia tych roszczeń DSA odsyła

[57] Dopiero od niedawna na gruncie tego rozporządzenia zasady ustalania odszkodowania przez sądy krajowe są przedmiotem wyjaśnień w ramach *case law* TSUE, zob. wyrok TSUE z dnia 4 maja 2023 r. w sprawie C-300/21, *UI przeciwko* Österreichische *Post AG* (ECLI:EU:C:2023:370). Wydaje się art. 54 DSA tym bardziej będzie wymagał aktywności orzeczniczej TSUE.

[58] Nie posłużono się tutaj rozróżnieniem na użytkowników będących konsumentami lub przedsiębiorcami, chociaż propozycji tego przepisu towarzyszyła argumentacja zorientowana na ochronę konsumentów, na co wskazuje opinia Europejskiego Komitetu Ekonomiczno-Społecznego (EKES) w sprawie rozporządzenia Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (Akt o usługach cyfrowych) i zmieniającego dyrektywę 2000/31/WE (INT/929-EESC-2021, 27.04.2021), pkt 4.2.

[59] Z uwagi na potrzebę jednolitej interpretacji tych pojęć na gruncie prawa unijnego, ale także praktykę sięgania przez unijnego ustawodawcę po odmienną terminologię, co pokazuje choćby przykład art. 82 rozporządzenia UE 2016/679, warto mieć na uwadze dyskusję na temat roszczeń odszkodowawczych na grun-

w sposób ogólny do przepisów prawa UE oraz do prawa krajowego w preambule (motyw 121), wyjaśniając jedynie, że takie odszkodowanie powinno pozostawać bez uszczerbku dla innych możliwości odwołania się dostępnych na mocy przepisów o ochronie konsumentów. Wprowadzenie tego przepisu jako samodzielnej podstawy dochodzenia roszczeń odszkodowawczych stanowi niewątpliwie istotny element wzmocnienia praw użytkowników cyfrowych usług rozumianego jako jeden z celów unijnej polityki cyfrowej. Należy jednak podkreślić, że skuteczność roszczeń z art. 54 DSA każdorazowo będzie wymagała sięgnięcia po instrumentarium dostępne na gruncie porządków krajowych (np. odrębne podstawy dla kontraktowego i deliktowego reżimu odpowiedzialności odszkodowawczej, przepisy procedury cywilnej) z zachowaniem zasad bezpośredniego stosowania i bezpośredniego skutku.

Egzekwowanie praw konsumentów. Rola prawa krajowego i unijnego w ramach *private enforcement* obowiązków dostawców usług na gruncie DSA jest szczególnie widoczna w zakresie ochrony praw konsumentów. W tym obszarze istotną rolę będą odgrywały dotychczasowe przepisy prawa konsumenckiego przyjęte w porządkach prawnych państw członkowskich UE w ślad za ustawodawstwem unijnym (por. uwagi w rozdziale III). Mogą być to choćby instrumenty ochronne wynikające z dyrektywy 2005/29/WE, ostatnio znowelizowanej przez tzw. dyrektywę Omnibus[60] głównie w odpowiedzi na rozwój narzędzi cyfrowych. Przykładem ich powiązania z przepisami statuującymi określone obowiązki dostawców usług w DSA jest sprawa zainicjowana w Niemczech przez tamtejszą organizację pozarządową przeciwko dostawcy platformy cyfrowej (Etsy) na tle art. 30 DSA[61].

Wskazać przy tym należy, że aktywność indywidualnych odbiorców usług, ale także organizacji reprezentujących ich interesy (np. jako konsumentów lub przedsiębiorców), w egzekwowaniu poszczególnych przepisów DSA będzie rozstrzygająca z perspektywy *private enforcement*. Pomocne przy tym okażą się również działania szczególnej kategorii podmiotów w postaci tzw. zaufanych podmiotów sygnalizujących, zarówno w związku z ich legitymacją do dokonywania zgłoszeń zgodnie z art. 16 DSA, jak i z powiązaną z tym sprawozdawczością (art. 22 ust. 3 DSA).

Powództwa przedstawicielskie. W omawianym tutaj obszarze istotną rolę odgrywają instrumenty istniejące w formie powództw przedstawicielskich. W odpowiedzi na transformację cyfrową Unia Europejska przyjęła w tym zakresie

cie prawa prywatnego w UE: Ch. von Bar, The Notion of Damage, w: A. Hartkamp et al. (red.), *Towards a European Civil Code*, 4 wyd., Alphen aan den Rijn–Nijmegen 2011, s. 387; M. Bussani, V. Palmer, *The Frontier between Contractual and Tortious Liability in Europe: Insights from the Case of Compensation for Pure Economic Loss*, w: A. Hartkamp et al. (red.), *Towards a European Civil Code*, op. cit., s. 946.

[60] W interesującym tutaj zakresie dochodzenia roszczeń nałożyła ona na państwa członkowskie obowiązek wprowadzenia w krajowych porządkach prawnych proporcjonalnych i skutecznych środków prawnych dostępnych dla konsumentów, którzy ucierpieli na skutek nieuczciwych praktyk handlowych. Środki te mogą obejmować prawo do żądania odszkodowania za szkodę poniesioną przez konsumenta oraz, w stosownych przypadkach, prawo do żądania obniżenia ceny lub rozwiązania umowy (por. motyw 16 dyrektywy Omnibus).

[61] Zentrale zur Bekämpfung unlauteren Wettbewerbs, Wettbewerbszentrale klagt gegen Etsy, 8.04.2024, https://www.wettbewerbszentrale.de/wettbewerbszentrale-klagt-gegen-etsy/ (dostęp: 3.04.2025).

nowe przepisy zorientowane na ochronę konsumentów w postaci dyrektywy (UE) 2020/1828[62] oparte na zasadzie minimalnej harmonizacji. W porządkach krajowych, czego przykładem jest Polska[63], wprowadzono przepisy umożliwiające dochodzenie różnorodnych roszczeń w postępowaniu grupowym, przyznając je zarówno konsumentom, jak i przedsiębiorcom. W kontekście usług cyfrowych, w których źródło równoczesnych naruszeń interesów wielu użytkowników może być skonkretyzowane, jednolita praktyka dostawcy usługi, krajowe narzędzia typu *class actions* stosowane w drodze *private enforcement*, szczególnie w przypadku występowania niewielkich szkód, których dochodzenie może okazać się dla pojedynczego użytkownika nieefektywne, mogą być wykorzystywane w powiązaniu z przepisami DSA.

Co więcej, DSA wydaje się wyraźnie zachęcać do takiego rozwiązania, wprost wskazując w art. 86, że „odbiorcy usług pośrednich mają co najmniej prawo umocować podmiot, organizację lub zrzeszenie do wykonania w ich imieniu praw przyznanych niniejszym rozporządzeniem". Dzięki temu poszczególne prawa użytkowników, w szczególności związane z dokonywaniem zgłoszeń, zaskarżaniem decyzji podjętych przez dostawców usług pośrednich oraz wnoszeniem skarg przeciwko dostawcom w związku z naruszeniami DSA, realizowane przez wyspecjalizowane organizacje działające w imieniu odbiorców (por. motyw 149 DSA), zostają dodatkowo wzmocnione, tym samym wspierając egzekwowanie DSA.

Środki ochrony praw dostępne dla użytkowników. Z perspektywy prawa Unii Europejskiej konsumenci, również na rynku usług cyfrowych, w egzekwowaniu swoich praw na tle DSA mogą sięgnąć po znacznie bardziej rozbudowane narzędzia niż inne kategorie odbiorców usług, w tym użytkownicy profesjonalni oraz ich kontrahenci (B2B). Ci ostatni będą w znacznej mierze zdani na wykorzystanie instrumentarium dostępnego na gruncie prawa krajowego w formie kontraktowych lub deliktowych reżimów odpowiedzialności. Na tym tle w prawie krajowym daje się zaobserwować tendencja do poszerzania pola zastosowania reżimu konsumenckiego szczególnie w stosunku do małych przedsiębiorców[64]. Przepisy DSA mogą zatem okazać się katalizatorem głębszych zmian regulacyjnych służących efektywnej ochronie praw wszystkich kategorii odbiorców usług. W połączeniu z potencjalnym „efektem brukselskim" DSA może w ten sposób przyczynić się do promowania wysokich standardów ochrony użytkowników cyfrowych usług w wymiarze globalnym.

---

[62] Dz. Urz. UE L 409, 4.12.2020, s. 1–27.

[63] J. Mucha, *From Recipe to Reality: The Polish Way of Collective Redress*, „ERA Forum" 2024, t. 25, s. 97.

[64] Jej przykładem na gruncie prawa polskiego jest stosowanie części przepisów ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz.U. 2024 poz. 1061) dotyczących ochrony konsumentów (między innymi w zakresie abuzywnych wzorców umów) do osób fizycznych prowadzących działalność gospodarczą w efekcie zmian regulacyjnych przyjętych w 2019 r. Z kolei w prawie niemieckim wskazać można na Verbandsklagenrichtlinienumsetzungsgesetz z 2023 r. (BGBl. I Nr. 272 S. 1), która w zakresie powództw grupowych tzw. małych przedsiębiorców (niem. *kleine Unternehmen*) każe traktować jako konsumentów.

5.5. Egzekwowanie przez podmioty prywatne uprawnień wynikających z DMA

5.5.1. Kontekst systemowy

DMA oraz ochrona praw użytkowników. Kwestia dochodzenia roszczeń z tytułu naruszenia uprawnień ustanowionych w DMA nie została uregulowana w tym rozporządzeniu. Dlatego można wyrazić wątpliwość, czy podmioty prywatne, w szczególności użytkownicy biznesowi i końcowi, mogą w ogóle powoływać się na art. 5–7 DMA w postępowaniach przeciwko strażnikom dostępu przed sądami krajowymi.

Wyróżnić można poglądy sceptyczne wobec tezy, że naruszenie DMA może stanowić podstawę dochodzenia roszczeń. Jednakże zgodnie z dominującym stanowiskiem DMA stanowi źródło uprawnień przyznanych jednostkom i może być egzekwowany prywatnoprawnie. Część argumentów na rzecz tej tezy została przytoczona w rozdziale IV.

Skuteczna ochrona sądowa użytkowników biznesowych i końcowych stanowi jeden z kluczowych celów DMA, wspomnianych w preambule do tego aktu. W motywie 42 stwierdzono, że „ważne jest, aby zabezpieczyć prawo użytkowników biznesowych i użytkowników końcowych […] do zgłaszania obaw dotyczących nieuczciwych praktyk strażników dostępu poprzez zwracanie uwagi odpowiednich organów administracyjnych lub innych organów publicznych, w tym sądów krajowych".

Najistotniejszym przepisem w tym kontekście jest art. 39 DMA, który określa zasady współpracy między Komisją a sądami krajowymi stosującymi materialne postanowienia DMA. Po pierwsze, przepis ten ustanawia ramy prawne dla wymiany informacji między Komisją a sądami krajowymi. Pozwala to sądom na wykorzystanie wartościowego materiału dowodowego zebranego przez Komisję (np. w toku postępowania w sprawie badania rynku) dla celów postępowań dotyczących roszczeń z tytułu naruszenia DMA.

Powołany przepis pozwala także działać Komisji jako *amicus curiae* w postępowaniach krajowych dotyczących stosowania DMA. Komisja może zatem przedkładać sądom krajowym swoje uwagi na piśmie oraz – jeżeli zezwala na to procedura krajowa oraz sąd prowadzący postępowanie – ustnie.

Przepis ten zawiera także istotną regułę spójności, zgodnie z którą sądy krajowe nie powinny wydawać wyroków sprzecznych z decyzją przyjętą przez Komisję na podstawie DMA. Powinny także unikać wydawania wyroków pozostających w sprzeczności z decyzją rozważaną przez Komisję w trakcie postępowania wszczętego na podstawie DMA. Zasady te pozostają bez uszczerbku dla kompetencji sądów krajowych do zadawania pytań prejudycjalnych zgodnie z art. 267 TFUE[65].

[65] W praktyce ciekawe może okazać się obserwowanie, na ile sądy krajowe będą skore do sprawdzania granic wspomnianych zasad i kierować pytania prejudycjalne do TSUE w przedmiocie możliwych odchyleń

Możliwość dochodzenia roszczeń z tytułu naruszenia DMA znajduje także potwierdzenie w art. 42 tego rozporządzenia. Przepis ten odnosi się do powództw przedstawicielskich i potwierdza stosowanie przepisów dyrektywy 2020/1828 do powództw przedstawicielskich wytaczanych w związku z naruszeniem DMA przez strażników dostępu. Powództwa przedstawicielskie zostały szerzej opisane w pkt 5.4 niniejszego rozdziału.

Powiązania z dochodzeniem roszczeń z tytułu naruszenia prawa konkurencji. Dyskusja dotycząca możliwości i zakresu dochodzenia roszczeń z tytułu naruszenia DMA może przypominać podobne debaty z przeszłości odnoszące się do dochodzenia roszczeń z tytułu naruszenia prawa konkurencji. Jak wynika z ustalonego orzecznictwa TSUE, skoro celem prawa konkurencji jest przyznanie uprawnień podmiotom prywatnym, podmioty te mają prawo dochodzenia odszkodowania z tytułu szkody powstałej wskutek naruszenia prawa konkurencji[66]. Wnioski te znajdują także potwierdzenie w odniesieniu do stosowania prawa konkurencji na rynkach cyfrowych[67].

Wspomniana linia orzecznicza stanowiła jeden z czynników prowadzących do przyjęcia dyrektywy odszkodowawczej[68]. Harmonizuje ona niektóre aspekty prawa krajowego w odniesieniu do kierowania powództw z tytułu szkody powstałej w wyniku naruszenia prawa konkurencji. Dyrektywa odszkodowawcza między innymi harmonizuje przepisy dotyczące wykorzystania dowodów zebranych przez organy ochrony konkurencji, ustalania wysokości szkody czy ustalania domniemania naruszenia, jeśli zostało ono stwierdzone w decyzji organu ochrony konkurencji.

Jednakże zakres zastosowania dyrektywy odszkodowawczej nie został poszerzony na poziomie unijnym o naruszenia DMA. W związku z tym to do decyzji państw członkowskich należy ewentualne uwzględnienie naruszenia DMA w ustawach krajowych dokonujących wdrożenia dyrektywy odszkodowawczej. Przykładowo rozwiązanie takie zostało zastosowane w Niemczech w Gesetz gegen Wettbewerbsbeschränkungen (pol. Ustawa o przeciwdziałaniu ograniczeniom konkurencji)[69].

---

od praktyki decyzyjnej Komisji na potrzeby postępowań dotyczących roszczeń z tytułu naruszenia DMA i tym samym balansowania wyraźnie sformułowanych postanowień DMA z kompetencją sądów krajowych do bezpośredniego stosowania prawa unijnego.

[66] Z zasady pełnej skuteczności prawa konkurencji wynika, że „sądy krajowe, które w ramach swojej właściwości muszą zastosować przepisy prawa wspólnotowego, zobowiązane są do zagwarantowania pełnej skuteczności tych norm i do ochrony praw, które przyznają one jednostkom"; zob. sprawa C-453/99, *Courage przeciwko Crehan*, pkt 19, 25–26.

[67] Zob. wyrok TSUE z dnia 18 kwietnia 2024 r., C-605/21, *Heureka Group a.s. przeciwko Google LLC*, (ECLI:EU:C:2024:324), pkt 61.

[68] Dyrektywa Parlamentu Europejskiego i Rady 2014/104/UE z dnia 26 listopada 2014 r. w sprawie niektórych przepisów regulujących dochodzenie roszczeń odszkodowawczych z tytułu naruszenia prawa konkurencji państw członkowskich i Unii Europejskiej, objęte przepisami prawa krajowego (Dz. Urz. UE L 349, 5.12.2014, s. 1–19).

[69] Artykuł 33 ust. 1 ustawy wprost stanowi, że „ktokolwiek narusza […] art. 101 lub art. 102 [TFUE] lub art. 5, 6 albo 7 [DMA] […] jest zobowiązany wobec osoby dotkniętej tym naruszeniem do naprawy szkody wynikłej z tego naruszenia".

5.5.2. Uprawnienia podlegające egzekwowaniu przez podmioty prywatne

Jak wskazano w rozdziale IV, materialnoprawne obowiązki nałożone na strażników dostępu zostały ustanowione w art. 5–7 DMA i przekładają się one na uprawnienia podmiotów prywatnych, w szczególności użytkowników biznesowych i końcowych. Stąd wskazane przepisy mogą stanowić podstawę dochodzenia roszczeń w postępowaniach przed sądami krajowymi.

Przykładowo, użytkownik biznesowy może dochodzić odszkodowania, jeśli strażnik dostępu nie odblokuje swojego ekosystemu dystrybucji aplikacji albo wykorzystuje publicznie niedostępne dane wygenerowane na platformie przez klientów owego użytkownika biznesowego. Z kolei użytkownicy końcowi mogliby między innymi wnosić roszczenia przeciwko strażnikom dostępu, jeśli nie umożliwiono by im łatwego odinstalowania określonego oprogramowania z systemu operacyjnego albo gdyby strażnik dostępu nie zapewnił możliwości przenoszenia danych poza świadczoną przez niego usługę platformową.

Biorąc pod uwagę, że ani DMA, ani dyrektywa odszkodowawcza nie zawierają szczególnych przepisów dotyczących dochodzenia roszczeń z tytułu naruszenia art. 5–7 DMA, kwestia ta pozostaje przedmiotem ewentualnych regulacji krajowych. Państwa członkowskie dysponują zatem uznaniem w zakresie wprowadzenia konkretnych rozwiązań materialnoprawnych i proceduralnych związanych z dochodzeniem tego typu roszczeń (autonomia regulacyjna), pod warunkiem że zachowane są zasady ogólne: skuteczności i równoważności.

Brak unijnych regulacji dotyczących dochodzenia roszczeń z tytułu naruszenia DMA może stanowić istotne wyzwanie zarówno dla strażników dostępu, jak i dla użytkowników dochodzących swoich praw. Dla użytkowników biznesowych i końcowych brak jasnych reguł w określonej jurysdykcji może zniechęcać do wniesienia powództwa. Różnice między państwami członkowskimi mogą doprowadzić do zjawiska *forum shopping*, tj. poszukiwania najbardziej dogodnej jurysdykcji. Pomimo rozwiązań zawartych w art. 39 DMA występowanie tego zjawiska może stanowić zagrożenie dla spójności i jednolitego stosowania DMA.

Jednocześnie niedawne przykłady dowodzą, że naruszenie prawa konkurencji w sektorze cyfrowym może stanowić podstawę do wnoszenia przez podmioty prywatne wysokich roszczeń. Przykładowo, w lutym 2024 r. ponad 30 wydawców mediów z Unii Europejskiej wniosło powództwo przeciwko Google, w którym dochodzą odszkodowania w wysokości ponad 2 mld euro za zarzucane naruszenia w ramach działalności reklamowej w Internecie[70].

[70] Więcej informacji na stronie: https://adtechclaim.eu/ (dostęp: 3.04.2025). Sprawa podąża za decyzją francuskiego urzędu ochrony konkurencji, ale odzwierciedla też postępowanie prowadzone w podobnej sprawie przez Komisję.

5.6. Podsumowanie

Jak wynika z analizy przeprowadzonej w niniejszym rozdziale, DSA i DMA wprowadzają pewne nowatorskie rozwiązania odnośnie do nadzoru nad wypełnianiem obowiązków wynikających z tych rozporządzeń. W przypadku DMA kluczowa zmiana w porównaniu z ogólnymi regułami prawa konkurencji polega na uzupełnieniu podejścia *ex post*, opartego na własnej ocenie przedsiębiorstwa, o podejście *ex ante*. W zakresie DSA nowością są obowiązki związane z należytą starannością, mające służyć zapewnieniu transparentnego i bezpiecznego środowiska internetowego. Konstrukcja obowiązków w zakresie należytej staranności obejmuje również perspektywę konsumencką, co wymaga przyznania nowych kompetencji krajowym organom ochrony konsumenta.

Model egzekwowania przepisów DSA i DMA wykazuje pewne podobieństwa, ale również istotne różnice. Zrozumienie cech omawianych modeli jest kluczowe dla użytkowników w kontekście dochodzenia swoich praw w relacji z platformami internetowymi.

Wspólne podejście w zakresie publicznoprawnego egzekwowania prawa jest widoczne przede wszystkim odnośnie do największych cyfrowych spółek, tzn. VLOP/VLOSE w świetle DSA i do „strażników dostępu" na podstawie DMA. W tym kontekście szczegółowa lista obowiązków zawartych w obu aktach jest powiązana z dalszymi obowiązkami w zakresie „wykazania zgodności" z rozporządzeniami (tzw. *compliance*) i obowiązków w zakresie przejrzystości. W ten sposób Komisja Europejska uzyskuje lepszy i stały wgląd w postępowanie dużych platform internetowych. Jeśli platformy te nie dostosują się do wymogów DSA bądź DMA, Komisja może wszcząć postępowania zmierzające do zapewnienia pełnej zgodności działań platformy z obowiązującymi wymogami. Komisja może również nałożyć kary finansowe lub zastosować inne środki wobec pośredników naruszających rozporządzenie.

Jakkolwiek Komisja posiada wyłączne kompetencje do nadzorowania największych platform, może nadal współpracować z właściwymi organami krajowymi. DSA wymaga oferowania wzajemnego wsparcia i ścisłej współpracy między Komisją a koordynatorami ds. usług cyfrowych (DSC), tak aby zapewnić jednolite stosowanie rozporządzenia. W świetle DMA Komisja może poprosić krajowe organy ochrony konkurencji o wsparcie w zakresie badania rynku, jak również o wymianę istotnych informacji odnoszących się do działań strażników dostępu w danym państwie członkowskim.

Taki scentralizowany system egzekwowania obowiązków służy wzmocnieniu praw użytkowników. Istotnie art. 53 DSA przyznaje użytkownikom prawo do wniesienia skargi na działanie platform do DSC, jeśli uznają, że doszło do naruszenia DSA. W DMA nie przewidziano rozwiązań podobnych do tych w DSA, należy jednak zauważyć, że składanie skarg do Komisji jest możliwe w świetle reguł ogólnych, z kolei skargi do organów krajowych są uregulowane na poziomie krajowym.

Różnice między DSA a DMA są najbardziej wyraźne w kontekście ich stosowania względem mniejszych platform internetowych. DMA znajduje zastosowanie wyłącznie do największych usługodawców, strażników dostępu, z kolei DSA nakłada obowiązki na wszystkie platformy i szerzej: ogólnie na dostawców usług pośrednich. W tym zakresie system egzekwowania obowiązków jest zdecentralizowany, a krajowym DSC przyznaje się w rozporządzeniu odpowiednie kompetencje. Należy przy tym zauważyć, że stosowanie DMA może się wiązać z równoległymi działaniami krajowych organów ochrony konkurencji bądź Komisji względem podmiotów, które nie spełniają warunków wskazania jako strażnika dostępu.

Dochodzenie roszczeń przez użytkowników. Rozwiązania dotyczące roszczeń użytkowników zostały wyraźnie przewidziane wyłącznie w DSA (art. 54), ale z ogólnych reguł prawa UE, w tym z zasady skutku bezpośredniego i z zasady skuteczności wynika, że użytkownicy i inne kategorie podmiotów indywidualnych mogą powoływać się bezpośrednio na postanowienia DSA i DMA przed sądami krajowymi, dochodząc praw przyznanych im w tych rozporządzeniach. Mogą również dochodzić odszkodowania za szkody wynikające z naruszeń DSA czy DMA.

Konkluzje

Niniejszą publikację poświęcono analizie praw użytkowników w ramach tzw. pakietu usług cyfrowych, obejmującego DSA oraz DMA. Cele obu rozporządzeń powinny pozostawać zbieżne z koncepcją jednolitego rynku cyfrowego. Uwzględniając sposób, w jaki ta idea nakreślona została w dokumentach unijnych, zarówno w postaci *soft law*, jak i w aktach prawa pochodnego, dotyczących poprawy funkcjonowania rynku wewnętrznego[1], szczegółowe rozważania skoncentrowano na trzech głównych obszarach: (1) ułatwianiu **działalności gospodarczej w środowisku online**, w tym zapewnieniu **uczciwości i konkurencyjności** (kontestowalności) **na rynkach cyfrowych**, (2) przepływach i dostępie do **kluczowych zasobów, jakimi są informacje oraz dane**, oraz (3) ochronie **podstawowych wartości i praw**, jak np. prawo do otrzymywania i przekazywania informacji czy ochrona konsumentów.

W sformułowaniach odnoszących się do **nadrzędnych celów DSA** wskazuje się na poprawę funkcjonowania rynku wewnętrznego, której służy ustanowienie zharmonizowanych ram prawnych dla wyłączeń odpowiedzialności dostawców usług pośrednich w powiązaniu z dodatkowymi obowiązkami należytej staranności. W rezultacie bezpieczne, przewidywalne i budzące zaufanie środowisko internetowe ma stanowić przestrzeń komunikacji między użytkownikami, w ramach działalności o charakterze gospodarczym lub innym. W centrum uwagi pozostają praktyki platform, które dostarczają cyfrową infrastrukturę służącą naszej codziennej aktywności. Cechą, która odróżnia platformy cyfrowe od innych pośredników, jest ich zaangażowanie w **rozpowszechnianie informacji**. Ich znacząca rola w ułatwianiu dostępu do informacji skutkuje licznymi obowiązkami w zakresie należytej staranności. Obejmują one obowiązki w zakresie wyjaśnień, warunków świadczenia usług, udostępniania użytkownikom określonych funkcji interfejsu platformy czy w zakresie sprawozdawczości. Takie dodatkowe obowiązki nie „ułatwiają" zapewne **platformom, traktowanym jako podmioty gospodarcze**, świadczenia usług. Jednakże jednolity zestaw reguł, jaki wyłania się z przepisów DSA, ma przewagę nad mozaiką krajowych porządków prawnych, uznawanych zazwyczaj za bariery dla transgranicznej działalności gospodarczej. Z kolei z perspektywy użytkowników przepisy DSA ewidentnie wzmacniają prawo do informacji, w tym informacji przeznaczonych dla konsumentów, określając jednocześnie zarówno sam rodzaj wymaganych informacji, jak i sposób ich dostarczenia użytkownikom.

[1] Art. 114 TFUE stanowi traktatowe oparcie zarówno dla DSA, jak i dla DMA.

Celem DSA jest zmniejszenie ryzyka związanego z aktywnością użytkowników w mediach społecznościowych, platformach umożliwiających udostępnianie treści (czyli dzielenie się nimi) czy internetowych platformach handlowych. Głównym przedmiotem regulacji jest zapobieganie rozpowszechnianiu **treści niezgodnych z prawem oraz szkodliwych w inny sposób**, godzących w interesy użytkowników. W zakresie moderowania treści udostępnienie użytkownikom funkcji umożliwiających zgłaszanie bezprawnych treści stanowi jasno sformułowany obowiązek dostawców platform, co implikuje **prawo do zgłaszania** przez każdą osobę mającą wiedzę o takich treściach przechowywanych przez dostawcę usługi. Warto zauważyć, że pojęcie „nielegalnych treści" zostało zdefiniowane w DSA w sposób szeroki, obejmujący zarówno kwalifikację uwzględniającą odpowiedzialność karnoprawną, jak też treści niezgodne z przepisami unijnymi lub krajowymi, niezależnie od przedmiotu i charakteru danej regulacji.

W rozdziale II badano, co przynosi DSA w kontekście **ryzyka**, jakie moderowanie treści przez platformy internetowe rodzi dla praw podstawowych, szczególnie w zakresie delegowania platformom funkcji sądowniczych, braku przejrzystości oraz skutecznych środków ochrony prawnej. DSA wprowadza konkretne **obowiązki służące transparentności** dotyczące zarówno wyjaśniania własnej polityki, uzasadniania decyzji użytkownikom, jak i raportowania czynności w zakresie moderowania treści oraz wykorzystywania narzędzi opartych na systemach algorytmicznych. Nowe informacje ujawniane przez platformy internetowe lub udostępniane zweryfikowanym badaczom powinny służyć skutecznemu egzekwowaniu przepisów rozporządzenia. W celu zapewnienia skutecznej ochrony praw podstawowych informacje przekazywane użytkownikom muszą obejmować również dane na temat dostępnych środków ochrony prawnej. W kontekście egzekwowania omawianych przepisów uzasadnione jest pytanie nie tylko o to, jak zapewnić, aby faktycznie przekazywano sprawozdania lub uzasadnienia użytkownikom, lecz również co zrobić, by spełniały one wymogi „istotn[ych] i zrozumiał[ych]" informacji (art. 15 ust. 4 pkt c DSA) czy informacji „jasn[ych] i łatwo zrozumiał[ych] oraz na tyle dokładn[ych] i szczegółow[ych], na ile można tego zasadnie oczekiwać w danych okolicznościach" (art. 17 ust. 4 DSA).

Wyraźny cel DSA, jakim jest wzmocnienie skuteczności ochrony praw podstawowych, jasno wyraża nałożony na pośredników obowiązek działania „z należytą starannością, w sposób obiektywny i proporcjonalny" przy stosowaniu i egzekwowaniu ograniczeń w zakresie moderowania treści, z jednoczesnym „należytym uwzględnieniem […] praw podstawowych odbiorców usługi, takich jak wolność wypowiedzi, wolność i pluralizm mediów" (art. 14 ust. 4 DSA).

Ponieważ uwaga nasza koncentruje się na relacji platforma–użytkownik, należy zauważyć, że **koncepcja użytkownika na gruncie przepisów DSA** bazuje na dwóch podstawowych, wyraźnie zdefiniowanych pojęciach: odbiorcy usługi oraz konsumenta. Tym samym ochronne podejście, towarzyszące relacjom rynkowym

konsumentów, jest obecne również w odniesieniu do każdej osoby fizycznej lub prawnej, która korzysta z usług pośrednich w celu poszukiwania informacji lub ich udostępniania. Pewne „prawa", jak choćby prawo do zgłaszania nielegalnych treści, powinny być zagwarantowane w możliwie najszerszy sposób każdej osobie. **Wzmocnieniu ochrony użytkowników** służy możliwość składania skarg do DSC. Przysługuje ona każdemu: odbiorcom usługi, a także (w ich imieniu) wszelkim podmiotom, organizacjom i zrzeszeniom upoważnionym do wykonywania praw przyznanych w DSA. **Pozycja konsumentów** została uwzględniona w sposób szczególny w kontekście przepisów dotyczących **platform typu B2C**.

Godne zaufania środowisko platform cyfrowych powinno uwzględniać wysoki poziom ochrony konsumentów jako jedną z podstawowych zasad UE. Już w rozdziale I wyjaśniono, że przez odwołanie do dotychczasowego dorobku *acquis consommateur*, a także uznanie unijnych standardów ochrony praw konsumentów wypracowanych jeszcze w odniesieniu do rzeczywistości rynkowej sprzed ery cyfrowej, DSA w głównej mierze służy ochronie interesów użytkowników również w środowisku online, realizując w ten sposób najnowsze wytyczne polityki unijnej w tym obszarze.

Także wymogi należytej staranności w zakresie identyfikowalności przedsiębiorców, zgodności w fazie projektowania czy prawa do informacji (art. 28–32 DSA) uwzględniające interesy konsumentów na platformach B2C realizują w zasadzie klasyczny paradygmat informacyjny stanowiący fundament polityki konsumenckiej. Niewątpliwie wzmacniają one pozycję konsumentów, ale – co podkreślono w rozdziale III – przepisy te są próbą odzwierciedlenia specyfiki złożonych relacji transakcyjnych środowiska cyfrowego platform internetowych.

Z kolei wątki konsumenckie obecne w pozostałych przepisach DSA, jak choćby te dotyczące warunków korzystania z usług, reklamy internetowej czy ochrony małoletnich, aczkolwiek bardzo widoczne, można traktować jako zalążki nowego podejścia do ochrony użytkowników w kontekście wyzwań, jakie przed prawodawcą unijnym stawia środowisko online.

Urzeczywistnienie koncepcji jednolitego rynku cyfrowego nie będzie możliwe bez ugruntowania praw użytkowników oraz stanowiących ich odpowiedniki obowiązków dostawców usług pośrednich. Służyć ma temu harmonizacja rozbudowanego instrumentarium nadzorowania, egzekwowania oraz monitorowania przestrzegania przepisów DSA. Prezentując ten rozbudowany zestaw narzędzi, w znacznej mierze mający postać *public enforcement*, ale z komponentami w postaci *private enforcement*, podkreślono znaczenie współpracy instytucji odpowiedzialnych za wdrażanie DSA na poziomie unijnym oraz krajowym.

W tym kontekście cele DMA mogą wydawać się bardziej szczegółowe i zorientowane rynkowo. Jak wcześniej wskazano, DMA zmierza przede wszystkim do usunięcia strukturalnych problemów występujących na rynkach cyfrowych oraz do przywrócenia równowagi w sile rynkowej między strażnikami dostępu (którzy często mają jednocześnie status bardzo dużych platform w rozumieniu DSA) oraz

użytkowników platform, które są prowadzone przez tych największych uczestników rynku. Stąd **zasadniczym celem DMA jest zapewnienie kontestowalności i uczciwości na rynkach cyfrowych**. O ile DMA stanowi element prawa rynku wewnętrznego i wprost dotyczy aspektów ekonomicznych, o tyle coraz częściej spotkać można twierdzenia, że rozporządzenie to może także chronić inne wartości, o mniej ekonomicznym charakterze (jak pluralizm w społeczeństwie demokratycznym).

W odniesieniu do kontestowalności, DMA wprowadza szereg obowiązków strażników dostępu w celu ułatwienia nowych wejść na rynki cyfrowe oraz wzmocnienia presji konkurencyjnej wywieranej na strażników przez przynajmniej potencjalnych konkurentów. Na podstawie preambuły DMA można stwierdzić, że z kolei **uczciwość rynków cyfrowych jest rozumiana jako równowaga między prawami i obowiązkami użytkowników biznesowych, gdy strażnik dostępu nie korzysta z nieproporcjonalnej przewagi**. Dlatego, nawet jeśli pod względem legislacyjnym prawodawca unijny skupia się przede wszystkim na wprowadzeniu publicznie egzekwowanych obowiązków strażników dostępu, to z podstawowego celu DMA wynika, że równie istotne jest wzmocnienie praw i siły rynkowej użytkowników biznesowych i końcowych, będących kontrahentami strażników dostępu.

Również z przepisów szczególnych DMA, omówionych w tej publikacji, wynika, że **przyznanie i egzekwowanie uprawnień użytkowników platform stanowi istotę tego rozporządzenia**. Uprawnienia te są odzwierciedlone w obowiązkach strażników dostępu, a w większości przypadków ich beneficjentami są obydwa rodzaje użytkowników: biznesowi i końcowi. Obowiązki te obejmują kilka obszarów działalności, tj. interoperacyjność między platformami strażników dostępu a innymi usługami cyfrowymi, przetwarzanie i korzystanie z danych użytkowników przez strażników dostępu, nieuczciwe praktyki oraz wymogi przejrzystości w przypadku reklam internetowych.

Powszechnie twierdzi się, że użytkownicy biznesowi są głównymi beneficjentami DMA. Przedsiębiorcy ci korzystają z platform jako rynku, na którym możliwe jest prowadzenie ich działalności: prezentowanie oferty klientom oraz zawieranie transakcji. DMA ma na celu zapewnienie, że użytkownicy ci pozostają niezależni od strażników dostępu i że nie zostaną wyparci z rynku przez strażników, którzy w nieuczciwy sposób rozciągają swoją siłę rynkową z platform na poszczególne rynki produktów czy usług.

Jednakże DMA wpływa także na pozycję użytkowników końcowych. Są to podmioty, które korzystają z platform w celach niekomercyjnych, przede wszystkim jako konsumenci. Po pierwsze, DMA przyznaje im konkretne uprawnienia (takie jak prawo do łatwego odinstalowania aplikacji z systemu operacyjnego czy do przeniesienia danych osobowych z jednej platformy na inną). Po drugie, podobnie jak w przypadku prawa konkurencji, ogólnym celem DMA jest ochrona dobrobytu konsumenta i zapewnienie mu odpowiedniego wyboru, nawet jeśli odbywa się to pośrednio przez nałożenie obowiązków na strażników dostępu lub przyznanie innych uprawnień użytkownikom biznesowym.

Wprowadzenie ram prawnych poświęconych jednolitemu rynkowi cyfrowemu stanowi nowy etap w rozwoju prawa rynku wewnętrznego. Realia rynkowe są dynamiczne i oparte na rozwoju raczej technologicznym niż prawnym. W momencie ukazania się niniejszej publikacji minął już termin na wdrożenie DSA oraz DMA w porządkach krajowych, uzupełniające ramy dla egzekwowania tych aktów. Spośród wszystkich państw członkowskich jeszcze tylko Polska nie wyznaczyła koordynatora ds. usług cyfrowych. Z kolei niektórzy koordynatorzy już wskazują na doniosłość praw użytkowników czy konsumentów[2]. Kluczowe znaczenie ma kwestia, czego użytkownicy mogą oczekiwać od organów monitorujących stosowanie omawianych aktów oraz w jakich okolicznościach roszczenia i skargi indywidualne mogą stanowić odpowiednie rozwiązanie dla użytkowników. Pierwsze doświadczenia wskazują na większą transparentność w sektorze cyfrowym, czego dowodzą przykłady EU Transparency Database[3] czy sprawozdania w zakresie przejrzystości, składane przez dostawców bardzo dużych platform internetowych (VLOP) i bardzo dużych wyszukiwarek internetowych (VLOSE)[4].

Z końcem 2025 r. powinno ukazać się pierwsze sprawozdanie na temat stosowania art. 33 DSA oraz informujące o tym, jak DSA wzajemnie oddziałuje z innymi aktami prawa unijnego dotyczącymi jednolitego rynku cyfrowego, w szczególności z aktami poprzedzającymi wprowadzenie DSA[5]. Następnie wydane zostaną bardziej wyczerpujące sprawozdania oceniające efektywność DMA (w 2026 r.)[6] oraz DSA (w 2027 r.)[7].

Dalsze działania mające na celu obserwowanie, komentowanie i rekomendowanie odpowiedniego podejścia są podejmowane w świecie akademickim[8]. Odpowiedzi na pytania przedstawione w przedmiotowej publikacji uwarunkowane są nie tylko jakością sprawozdań instytucjonalnych. Istnieje tu bowiem istotne powiązanie między poziomem zaangażowania krajowych koordynatorów ds. usług cyfrowych oraz Komisji Europejskiej w analizę dostępnych danych, badaczami przedstawiającymi analizy publicznie dostępnych danych, dostępem do danych w ramach ustalonych w DSA oraz aktywnością użytkowników i ich przedstawicieli. Z tej perspektywy niniejszy Handbook stanowi zaproszenie do dalszej pracy i badań w omówionych obszarach problemowych.

---

[2] Irlandzki koordynator opublikował przewodnik w sprawie składania skarg: Digital Services Act – Your right to complain, https://www.cnam.ie/onlinecomplaints/; niemiecki koordynator wymienił uprawnienia użytkowników na swojej stronie internetowej: Rechte von Nutzern https://www.dsc.bund.de/DSC/DE/3Verbraucher/1VB/start.html; koordynator francuski, ARCOM, udziela odpowiedzi na pytanie, co DSA wnosi z perspektywy użytkownika, Qu'est-ce que ce règlement va changer pour moi?, https://www.arcom.fr/actualites/5-informations-retenir-sur-le-reglement-sur-les-services-numeriques-rsn-ou-digital-services-act-dsa (dostęp: 3.04.2025).

[3] https://transparency.dsa.ec.europa.eu/ (dostęp: 3.04.2025).

[4] https://digital-strategy.ec.europa.eu/en/policies/dsa-brings-transparency (dostęp: 3.04.2025).

[5] Art. 91 ust. 1 DSA.

[6] Art. 53 ust. 1 DMA.

[7] Art. 91 ust. 1 DSA.

[8] Jak na przykład DSA Observatory, https://dsa-observatory.eu/ (dostęp: 3.04.2025).

RIGHTS OF USERS IN THE DIGITAL SINGLE MARKET

Handbook

Introduction

The purpose of this handbook is to explain and critically analyse the position of users and rights of users in the digital single market.

In the last four years, the body of EU regulations and directives, and also soft law documents, addressing the digital single market has grown substantially. Users' rights are specifically addressed in the Data Act, for example, and the logic of identifying and sustaining users' rights is already present in the General Data Protection Regulation (GDPR). Out of this complex body of the regulatory instruments we focus on the Digital Services Act (DSA) and Digital Markets Act (DMA).

These two recent and comprehensive EU Regulations, proposed as the Digital Services Package, impose direct obligations on intermediary service providers (ISP), based on the concept of augmenting their responsibility and due diligence, and ensuring fairness and contestability of digital markets. The DSA expressly refers to the need to establish "safe, predictable and trusted online environment" with effective protection of fundamental rights, while the DMA advances the regulatory framework for "contestable and fair markets in the digital sector," which benefits business and end-users.

Users, understood as service recipients, consumers, business and end users, are thus central to the regulatory framework for Digital Single Market. In this book, we first discuss the concept and evolution of the regulatory framework for the Digital Single Market (Chapter I) before moving on to analyse three key problems: (1) enhancing the protection of fundamental rights of users in the area of content moderation under the DSA (Chapter II); (2) mapping consumer benefits under the DSA (Chapter III); and (3) the scope of rights granted upon digital markets participants by the DMA (Chapter IV).

The analysis poses questions related to whether any new rights are granted by the DSA and the DMA and how the users' position with respect to existing rights is reinforced with the new tools. We indicate the high expectations towards that regulatory package, given the explicit objective of "effective protection" or "benefits" to users. Whether this will merely be an empty promise depends on a number of factors: Are the DSA and the DMA fit for the evolving technologies? Are their relations with pre-existing EU law clear and coherent? What is the framework for the enforcement of obligations imposed on intermediaries?

The last chapter is therefore dedicated to the issue of public and private enforcement of the DSA and the DMA. Here, we observe how the enforcement framework is still in the development phase, and we underline key synergies and differences in the approach taken in both Regulations. The ultimate question is whether it is clear what the user may expect from the public enforcement, and when should the individual claims and complaints be the viable option.

This handbook is the result of the work of the team in the Jean Monnet Chair Digital Single Market and the Free Flow of Information (2022–2025). In the course of the project, we cooperated with PhD candidates and doctoral students. The figures accompanying the chapters are the result of this cooperation. We would therefore like to thank: Jakub Bąchor, Jakub Drąg, Krzysztof Jeromin, Wiktor Kępiński, Weronika Łomako, Daria Słomowicz, Marianna Zawal.

Chapter I

Digital Single Market and the regulatory framework for rights of users

1.1. The concept of the Digital Single Market – Introduction

The concepts of "information society" or "knowledge-based economy" have been discussed as strategic objectives in the EU since the late 1990s, along with the advent of internet and new communication opportunities. The term "digital single market" (DSM) was explained in the 2015 communication on the DSM strategy.[1] As proposed by the Commission, DSM is an area where free movement of goods, services, people and capital is ensured, and which allows "individuals and businesses to seamlessly access and exercise online activities." To achieve that, the Commission proposed a package of EU reforms, continued and developed under the strategical priority of "Digital Europe."[2]

In 2015 the Digital Evolution Index (DEI)[3] indicated that 8 EU countries have so far developed well, but are "losing a momentum"; another 7 EU countries, including Poland, should "watch out," as they may miss important opportunities, and only 2 were in the "stand-out" category of digital development. This indicated the differences between EU countries hampering the achievement of truly digital, single market.[4]

At the time, the objective of harmonization has been laws aimed at improving digital infrastructure and ensuring better access for consumers and businesses, while gradually building safety from illegal content. This has resulted in regulations addressing geo-blocking, free movement of non-personal data, or portability of content services, and directives amending existing EU copyright or media law. The landmark

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *A Digital Single Market Strategy for Europe*, COM/2015/0192 final.

[2] European Commission, *Shaping Europe's Digital Future*, https://eufordigital.eu/wp-content/uploads/2020/04/communication-shaping-europes-digital-future-feb2020_en_4.pdf (accessed: 3.4.2025).

[3] Digital Evolution Index developed at the Fletchers School at Tufts University; B. Chakravorti, Ch. Tunnard, R.S. Chaturvedi, *Where the Digital Economy is Moving Fastest*, Harvard Business Review, Analytic Services, 9.2.2015, https://hbr.org/2015/02/where-the-digital-economy-is-moving-the-fastest (accessed: 3.4.2025).

[4] The achievement of digital transfomation priority targets is measured in the EU by the DESI (Digital Economy and Society Index), https://ec.europa.eu/newsroom/dae/redirection/document/106717 (accessed: 3.4.2025).

General Data Protection Regulation[5] introduced two goals: fostering free movement of services, and protection of personal data in the context of fundamental rights. This highlights an important feature of the DSM law: it advances market freedoms and aims to ensure the protection of fundamental rights. It is not only the case of GDPR, with Art. 16 Treaty on the Functioning of the European Union (TFEU)[6] as its legal basis, but also of the Digital Services Act based on Art. 114 TFEU.

The analysis of what has been achieved so far leads to the conclusion that we should analyse digital single market law through the lens of: (1) facilitating online business activities, as part of freedom to provide services, while ensuring fairness in competition; (2) addressing core resources of information and data; and (3) protecting the values enshrined in the Charter of Fundamental Rights (CFREU).[7] Freedom to provide services, and especially freedom to provide information society services, remains the core of the DSM.

1.2. Digital Services Package as part of shaping Digital Europe legislative initiatives

The strategies and initiatives mentioned above have resulted in a number of regulatory steps regarding the digital sector. In 2019, the European Parliament and the Council adopted the 'Platform-to-Business Regulation' (P2B).[8] This regulation was the first ever step in EU law to regulate online platforms' (intermediaries') practices *vis-à-vis* their business users. Indeed, the user perspective seems to predominate the preamble, which acknowledges that many consumers (end users) use online platforms in the EU and thus platforms "are key enablers of entrepreneurship and new business models, trade and innovation, which can also improve consumer welfare" as well as being "crucial for the commercial success of undertakings who use such services to reach consumers" (Rec. 1 and 2 of P2B Regulation).

The 2020 Communication from the Commission[9] sought to further respond to challenges and opportunities related to the observed digital transformation. In this context, the Communication stresses that citizens (or simply "people") remain

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, pp. 1–88).

[6] Treaty on the Functioning of the European Union of 13.12.2007 – consolidated version (OJ C 202, 7.6.2016, pp. 47–360).

[7] OJ C 326, 26.10.2012, pp. 391–407.

[8] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019, pp. 57–79).

[9] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's digital future, COM(2020) 67 final (section B), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52020DC0067 (accessed: 3.4.2025).

the central and core element of these considerations. The Commission intended to regulate "technology that works for people," a "fair and competitive economy" in which a level playing field for businesses would be ensured, the most vulnerable consumers protected, and "private gatekeepers to markets, customers and information" adequately regulated. The other key objectives identified in the Communication were to ensure and safeguard "an open, democratic and sustainable society" and to "build a genuine European single market for data."

The Commission's Communication from 2020 was followed by a series of public consultations in which the Commission sought to verify the need for introduction of a new, general digital services regulation, which would relate to the fundamentals of the e-commerce directive. The initiative was not only intended to address freedom to provide digital services, but also to protect users' safety and to ensure the respect of their fundamental rights. This is also confirmed by the need to introduce a separate "New Competition Tool," dedicated precisely to the largest platforms acting as gatekeepers in digital markets and seeking to restore the balance between the largest online platforms and their business users, with the view of ensuring consumers' widest choice.[10]

These actions resulted in proposals of the DSA[11] and DMA.[12] However, from the very outset, these have been deemed a "single set of rules" with two objectives: firstly, to create a safer digital space, allowing European Union citizens and other persons to exercise their fundamental rights including a high level of consumer protection[13]; secondly, to establish a level playing field in the digital sector, and thus restore market balance between its entities, including business users.[14]

1.3. From e-commerce to the DSA

1.3.1. Freedom to provide information society services

The E-commerce directive of 2000 (ECD)[15] was the first step towards ensuring the freedom to provide information society services (ISS). Regulatory interventions in

[10] European Commission: Directorate-General for Competition and H. Schweitzer, *The New Competition Tool: Its Institutional Set up and Procedural Design: Expert study*, Brussels 2020, https://data.europa.eu/doi/10.2763/060011 (accessed: 3.4.2025).

[11] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, pp. 1–102).

[12] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, pp. 1–66).

[13] Rec. 3 and Art. 1(1) DSA.

[14] See: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (accessed: 3.4.2025).

[15] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce) (OJ L 178, 17.7.2000, pp. 1–16).

this area were approached carefully, as it was recognized that ISS can be a reflection of "a more general principle" of "freedom of expression."[16] The concept of ISS, as defined in the directive 2015/1535[17] remains the key building block for legal definitions of services in the DSM area, such as "intermediary services" in the DSA, or "video-sharing platform services" in the AVMSD.[18] The term ISS covers a broad range of online activities, such as selling goods, offering information or commercial communications, or providing for search tools.[19] It includes any service normally provided by remuneration, at a distance, through electronic means and at the individual request of the recipient of a service. Such services are often free for users, but remunerated through advertising.

Fostering the freedom to provide services demanded the abolition of obstacles resulting from a lack of legal certainty, and differences in national laws. Therefore, ECD (Art. 1(2)) aimed at harmonizing selected areas.[20] Particular attention should be given to **three pillars of freedom to provide ISS**: the internal market clause and principle excluding prior authorization (Art. 3–4) liability exemptions (Art. 12–14) and prohibition on imposition of any general monitoring obligation (Art. 15). According to the "internal market clause" or "the country-of-origin principle," information society service providers are obliged to comply with the law of a Member State of establishment, unless derogation from this principle is allowed under Art. 3(4). This rule applies only in the areas harmonized by ECD,[21] and many fields, including copyright or media law, remain outside the scope of directive. Member States are not allowed to establish any authorization procedure for any activity falling in the scope of ISS. Member States may not impose any provisions that would impose an obligation to monitor, or filter all content available on ISS. This applies to intermediary services, providing a mere conduit, caching or hosting, and is subject to extensive debate reflected in case law[22] and academic literature.

---

[16] Rec. 9 ECD.

[17] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 Laying down a Procedure for the Provision of Information in the Field of Technical Regulations and of Rules on Information Society Services (OJ L 241, 17.9.2015, pp. 1–15, n.d.).

[18] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (OJ L 95, 15.4.2010, pp. 1–24).

[19] Rec. 18 ECD.

[20] Art. 1(2) lists internal market and establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and cooperation between Member States.

[21] Art. 2(h) ECD.

[22] Cases: C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* (ECLI:EU:C:2012:85); C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited* (ECLI:EU:C:2019:821).

1.3.2. Liability exemptions in the ECD

The so-called **"safe harbours"** (horizontal liability exemptions) were established to ensure smooth development of digital infrastructure for communications. As was briefly explained, ECD created immunity for those ISPs "(1) who are mere neutral and transient conduits for tortious or unlawful material authored and initiated by others (Art. 12); (2) for caching local copies of third parties' tortious or unlawful data (Art. 13)" and for those "(3) who store third parties' tortious or unlawful material while having neither actual knowledge of the "unlawful activity or information" nor an awareness of facts or circumstances from which that "would have been apparent" (Art. 14).[23] This regime created a technology-neutral environment at the time when online platforms did not have the characteristics they have today, and facilitated their scaling up.[24] The rise of online platforms provoked many questions as to the application of the E-commerce Directive, reflected in the case law of the Court of Justice of the European Union (CJEU).

AG Szpunar in the *Uber* case objected to the ECD being interpreted "as meaning that any trade-related online activity, be it merely incidental, secondary or preparatory in nature, which is not economically independent is, per se, an information society service."[25] The CJEU found intermediations services such as those provided by Uber inherently linked to offline activity and therefore falling into the category of transport services, and not ISS.[26] In contrast, in the *Airbnb* case, the court found that such an intermediation service, connecting future guests with hosts in the short-term house rental and providing a number of ancillary services, constitutes an ISS.[27] Star Taxi App, an intermediary service connecting passengers with taxi drivers, was also found to fulfil the criteria for ISS.[28] Offering access to a local free wi-fi network was considered as ISS access service, as it is provided for the purpose of advertising the goods sold or services supplied by the provider.[29]

---

[23] G.B. Dinwoodie, *A Comparative Analysis of the Secondary Liability of Online Service Providers*, in: G.B. Dinwoodie (ed.), *Secondary Liability of Internet Service Providers*, Cham 2017, p. 34.

[24] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe (COM (2016) 288 final, n.d.), p. 8.

[25] Opinion of Advocate General Szpunar of 11 May 2017, Case C-434/15, *Asociación Profesional Elite Taxi v Uber Systems Spain, SL,* (ECLI:EU:C:2017:364), para. 37.

[26] Judgment of CJEU of 20 December 2017, Case C-434/15, *Asociación Profesional Élite Taxi v Uber Systems Spain, SL* (ECLI:EU:C:2017:981).

[27] Judgment of CJEU of 19 December 2019, Case C-390/18, *Criminal proceedings against X* (ECLI:EU:C:2019:1112).

[28] Judgment of CJEU of 3 December 2020, Case C-62/19, *Star Taxi App SRL v Unitatea Administrativ Teritorială Municipiul Bucureşti prin Primar General and Consiliul General al Municipiului Bucureştisrl* (ECLI:EU:C:2020:980).

[29] Judgment of CJEU of 15 September 2016, Case C-484/14, *Tobias Mc Fadden v Sony Music Entertainment Germany GmbHMcFadden* (ECLI:EU:C:2016:689).

The area of IP law infringements challenged the framework for liability exemptions, especially for hosting. In the leading cases, *Google France* and *L'Oréal*, the CJEU indicated that ISP is eligible for a liability exemption under Art. 14 if it does not play an active role that would give it knowledge of, or control over, data stored.[30] In the *L'Oréal* case, CJEU added that such a selling platform cannot shield itself from liability "if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realized that the offers for sale in question were unlawful" and did not react expeditiously.[31] The aspect of the diligent behaviour of a hosting service provider was further elaborated on in the *YouTube* case. The CJEU indicated that if a hosting service provider generally knows that the service in question may be used for infringing copyright, as a reasonably diligent economic operator it is expected to put in place appropriate technological measures.[32] This ruling precedes the DSA, where some of the due diligence obligations are imposed directly on ISPs. In the light of this case law, many questions remained open regarding the scope of ISS and intermediary services, the standard of conduct expected from intermediary service providers,[33] and on their accountability[34] or "obligations without liability."[35]

1.3.3. Regulating online platforms – the road to the DSA

The essential question in the area of online platforms regulation was how to ensure that ISPs engage "responsibly" in fighting illegal content, do not distort fair competition, nor create risks for consumers. These deliberations were framed in the Communication on online platforms,[36] and were followed by the legislative proposals to amend copyright law, the Audiovisual Media Services Directive, in the regulations on fighting terrorist content and ensure fairness and transparency for business users. The 2018 Recommendation on tackling illegal content[37] offered

[30] Judgment of CJEU of 23 March 2010, joined Cases C-236/08–C-238/08, *Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA i Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others* (C-238/08) (ECLI:EU:C:2010:159), para. 120.

[31] Judgment of CJEU of 12 July 2011, Case C-324/09, *L'Oréal SA and Others v eBay International AG and Others* (ECLI:EU:C:2011:474), paras. 122–124.

[32] Judgment of CJEU of 22 June 2021, joined Cases C-682/18 and C-683/18, *Frank Peterson v Google LLC and Others and Elsevier Inc. v Cyando AG* (EU:C:2021:503), para. 83.

[33] Ch. Angelopoulos, *European Intermediary Liability in Copyright: A Tort Based Analysis*, PhD thesis, Universiteit van Amsterdam 2016, https://hdl.handle.net/11245/1.527223, p. 251 et seq.

[34] M. Husovec, *Accountable, Not Liable: Injunctions Against Intermediaries*, "TILEC Discussion Paper" 2016, no. 2016-012, http://dx.doi.org/10.2139/ssrn.2773768.

[35] G. Dinwoodie, op. cit., p. 38.

[36] COM (2016) 288 final.

[37] Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, C/2018/1177 (OJ L 63, 6.3.2018, pp. 50–61).

non-binding and horizontal guidance addressing platforms' liability and encouraged proactive measures towards illegal content, including the use of automated means for detection of illegal content. However, the latter has been restricted to actions that are specific, proportionate and appropriate, subject to adequate safeguards (Rec. 3). The copyright expressed in the Digital Single Market Directive (CDSM) of 2019[38] and amendment to the AVMSD of 2018[39] illustrate different attempts to ensure platforms' responsibility. The CDSM introduced specific liability exemptions for online content sharing platforms (Art. 17), raising the expectations of online platforms. AVMSD, on the other hand, introduced additional obligations for video sharing platforms, supplementing Art. 14 of E-commerce Directive, and subject to control by national regulatory authorities in the area of media (Art. 28b). The aim of these revisions of existing harmonized legal framework was to bring about the right regulatory framework for the digital economy, and sustainable development of platform business model.[40] Enactment of Digital Services Act as a horizontal regulation for intermediary services was initiated in 2020 Communication on shaping Europe's digital future.[41] In this context, the DSA appears less market-oriented, targeting citizens' empowerment and building a trustworthy digital environment.

The proposal for the DSA highlighted that not all of the ECD objectives were achieved.[42] The DSA aims at complementing the objectives of freedom to provide intermediary services (ISP),[43] building on the principles of the ECD, and clarifying the responsibilities and obligations of ISPs.[44] Liability exemptions and a ban on general monitoring obligations are now uniformly regulated in the DSA (Chapter 2), and accompanied with a separate chapter on due diligence obligations (Chapter 3).

[38] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, pp. 92–125).

[39] Directive (EU) 2018/1808 of 14 November 2018 Amending Directive 2010/13/EU on the Coordination of Certain Provisions Laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) in View of Changing Market Realities (OJ L 303, 28.11.2018, pp. 69–92).

[40] COM (2016) 88 final.

[41] COM (2020) 67 final, p. 12.

[42] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM/2020/825 final, Brussels, 15.12.2020), p. 7.

[43] Defined in Art. 3(g) DSA.

[44] F. Wilman, *The Digital Services Act (DSA) – An Overview*, 16.12.2022, http://dx.doi.org/10.2139/ssrn.4304586.

1.4. EU Consumer Protection Policy towards Digital Transformation

The starting point for determining the extent to which EU consumer protection law affects the legal position of consumers should be an explanation of whether and how the policy on consumer protection, which has been conducted on the level of European Communities for nearly half a century, addresses the development of digital technologies, or more broadly, the shaping of the information society. At the outset, the situation that emerges from the review of selected sources below can be summarized by the slogan "what is illegal offline should be illegal online" (Fig. 1).

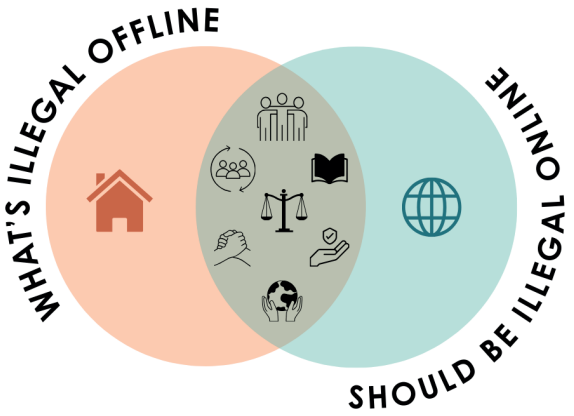


Figure 1: Consumer protection policy in the digital environment

In the Figure 1 both spheres (online and offline) are treated equivalently and are in a relationship of (partial) mutual overlap. The icons placed in the shared area are intended to symbolize the catalogue of fundamental consumer rights. Beyond shared area, distinct areas are left, highlighting the specific characteristics and unique differences of each of these spheres.

A key element in understanding this slogan is the concept of the "consumer" adopted in one of the first *soft law* documents[45] outlining non-binding regulatory principles in the area of consumer protection policy. In the 'First programme' of 1975, the EEC Council recognized that the "consumer is no longer seen merely as a purchaser and user of goods and services for personal, family or group purposes but also as a person concerned with the various facets of society which may affect

[45] EU *soft law* represents a specific issue considered in the discussion on the sources of EU law – cf. J. Köndgen, *Die Rechtsquellen des Europäischen Privatrechts*, in: K. Riesenhuber (ed.), *Europäische Methodenlehre: Handbuch für Ausbildung und Praxis*, Berlin 2006, p. 155.

him either directly or indirectly as a consumer."[46] This concept is a combination both economic and social dimensions. The former, which reduces the consumer to the role of a passive participant in market transactions, was already deemed insufficient at the time. It required supplementation with a social dimension, which was understood in very broad terms, linking the concept of the consumer with that of the citizen. Considering the course of integration processes that have shaped the EU, this, in turn, may justify reference to the idea of the *market citizen* (Ger. *Marktbürger*).[47]

Only after defining the concept of the consumer in this way did the EC Council establish the main elements of its policy. These were expressed in the form of a catalogue of five "basic rights" covering protection of health and safety, protection of economic interests, redress, information and education, and the right of representation (the right to be heard).[48] This catalogue remains relevant today in almost unchanged form, although over the following decades of consumer policy development, one can observe its transformation and the shifting of emphasis within its components, taking into account changes occurring in the socio-economic environment.

Following the widespread adoption of information technologies in the mid-1990s, the priorities of Community consumer policy began to include measures enabling consumers to benefit from the opportunities presented by the information society. At that time, the policy was markedly oriented towards ensuring consumers' access to the emerging information system (accessibility), combined with the recognition of the need to develop new user skills, including through education.[49] However, references to consumer rights in the documents outlining plans to respond to the digital revolution at the Community level remained very scarce.[50]

In the context of fundamental individual rights, these policy documents recognize the need for privacy protection, although it is not directly linked to the traditional catalogue of consumer rights. It was not until the adoption of the 1999 Council Resolution on the Consumer Dimension of the Information Society[51]

[46] Council Resolution of 14 April 1975 on a preliminary programme of the European Economic Community for a consumer protection and information policy (OJ C 92, 25.4.1975, pp. 1–16), annex, Rec. 3.

[47] Cf. J. Köndgen, op. cit., p. 138; S. Weatherill, *Law and Values in the European Union*, Oxford 2016, pp. 390–391. Such a terminological hybrid can be criticized as an attempt to transform interpersonal relationships into forms of market exchange (A. Aldridge, *Konsumpcja*, trans. M. Żakowski, Warsaw 2006, p. 114).

[48] EC Council, Resolution of 14 April 1975, annex, Rec. 3.

[49] Commission of the EC, Communication from the Commission. Priorities for Consumer Policy 1996–1998, COM(95) 519 final, Brussels, 31.10.1995, p. 8.

[50] Cf. Commission of the EC, Europe's Way to the Information Society. An Action Plan. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, COM(94) 347 final, Brussels, 19.7.1994, pp. 3–4; Commission of the EC, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions. Europe at the Forefront of the Global Information Society: Rolling Action Plan, COM(96) 607 final, Brussels, 27.11.1996, p. 6.

[51] Council Resolution of 19 January 1999 on the Consumer Dimension of the Information Society (OJ 1999/C 23/01).

that a reorientation in the existing Community policies was clearly signalled. The concept of the "information society" itself is not defined in this Resolution. Instead, it includes the phrase "new technologies for the transmission and storage of information […] that are having a profound impact on society in general."[52] The Council lists as many as 11 issues of particular importance from the consumer perspective, including transparency regarding the quantity and quality of information, the protection of children, and as privacy and personal data protection (Rec. 4), while emphasizing that confidence and trust[53] are prerequisites for consumers to accept and participate in the information society (Rec. 5).

In turn, building this trust and confidence, according to the Resolution (Rec. 6), requires providing consumers with protection regarding new technologies: "an equivalent level of protection regarding the new technologies as is available in traditional consumer transactions by the application of existing principles of consumer policy to the new products and services available in the information society." This statement appears to be crucial for understanding the direction that the Council Resolution of 1999 set for consumer policy in the emerging digital environment.[54]

Despite 25 years having passed since the adoption of the above resolution, it remains relevant today. This is confirmed by examples from the latest EU documents, both in the area of consumer *soft law* and, more broadly, in the legal framework of the digital environment. Below, in chronological order, three sources are indicated that have a clear connection with the EU regulatory framework for the information society, where the legal instrument of the DSA plays a central role.

Even during the legislative work on the DSA proposal, at the stage of the preliminary political agreement between the Council and the European Parliament, one of the press releases reporting the Council's general approach refers to this formula, emphasizing that "the proposal follows the principle that what is illegal offline should also be illegal online."[55]

Another example is provided by the New Consumer Agenda,[56] which outlines the main directions of consumer policy to be implemented between 2020 and 2025.

---

[52] Ibidem, Rec. 1.

[53] The role of trust in the digital environment can be assessed differently depending on whether it is approached in a communicative context or a commercial one (cf. R. Hardin, *Trust*, Cambridge 2006, p. 100 et seq.).

[54] In the comments accompanying this document, the need for caution in simply implementing previously known principles into the online environment was also highlighted: M. de Cock Buning et al., *Consumer@Protection.EU: An Analysis of European Consumer Legislation in the Information Society*, "Journal of Consumer Policy" 2001, vol. 24, p. 329. In this sense, it was observed in the first decade of the 21st century that, "so far, the internet, the biggest network of all history, may have relatively little of the often rich and manifold value of usual networks" – R. Hardin, op. cit., p. 116.

[55] Council of the EU, Press release of 25 November 2021, https://www.consilium.europa.eu/pl/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act/ (accessed: 3.4.2025).

[56] European Commission, Communication from the Commission to the European Parliament and the Council. New Consumer Agenda. Strengthening consumer resilience for sustainable recovery, COM(2020) 696 final, Brussels, 13.11.2020.

The Commission designed it around five key priority areas. After the green transition, the second place on this list is occupied by the digital transformation.[57] In the elaboration of this element of the Agenda, we find several references to individual actions of the Commission, including one concerning a proposal for the DSA, which had been already submitted by the Commission at that time. In the particular paragraph, the Commission explicitly states that the DSA "will ensure that consumers are protected effectively against illegal products, content and activities on online platforms as they are offline."[58] A similar statement appears in several other parts of the current consumer policy programme.[59]

Finally, in the European Declaration on Digital Rights and Principles for the Digital Decade of 2022,[60] Chapter 1 (Putting people at the centre of the digital transformation), a commitment is expressed to "take the necessary measures to ensure that the values of the Union and the rights of individuals recognized in Union law are respected both online and offline."[61] Although the similarity of this phrase to the one from the 1999 Council Resolution is not as apparent as in the case of the two previous sources, the very juxtaposition of the two spheres (offline and online) seems significant. Even if the Declaration does not specifically mention consumers (referring to the broader term 'users'), it includes clear references to classic consumer rights (e.g. safety, freedom of choice, participation). This allows the Declaration to be interpreted in the context of modern consumer policy.

In light of the ongoing push to regulate digital markets and services, EU consumer policy consistently incorporates issues specific to the information society into the traditional catalogue of consumer rights. This was already evident in the early actions taken at the community level in response to the development of information technologies. This trend[62] is equally apparent in recent legislative initiatives affecting the digital environment, including the DSA and DMA. Figure 2 provides a summary comparison of the central issues expressed in the aforementioned documents from 1975, 1999, and 2022.

---

[57] Ibidem, p. 2.

[58] Ibidem, p. 11.

[59] This is also mentioned at the very beginning of section 3.2, which is dedicated to the key priority area of digital transformation: ibidem, p. 10.

[60] European Declaration on Digital Rights and Principles for the Digital Decade (OJ C 23, 23.1.2023, pp. 1–7).

[61] Ibidem, p. 2.

[62] Even if it can be associated with the risk of fragmentation of consumer law – see: F. de Elizalde, *Fragmenting Consumer Law Through Data Protection and Digital Market Regulations: The DMA, the DSA, the GDPR, and EU Consumer Law*, "Journal of Consumer Policy" 2025, https://doi.org/10.1007/s10603-025-09584-3.

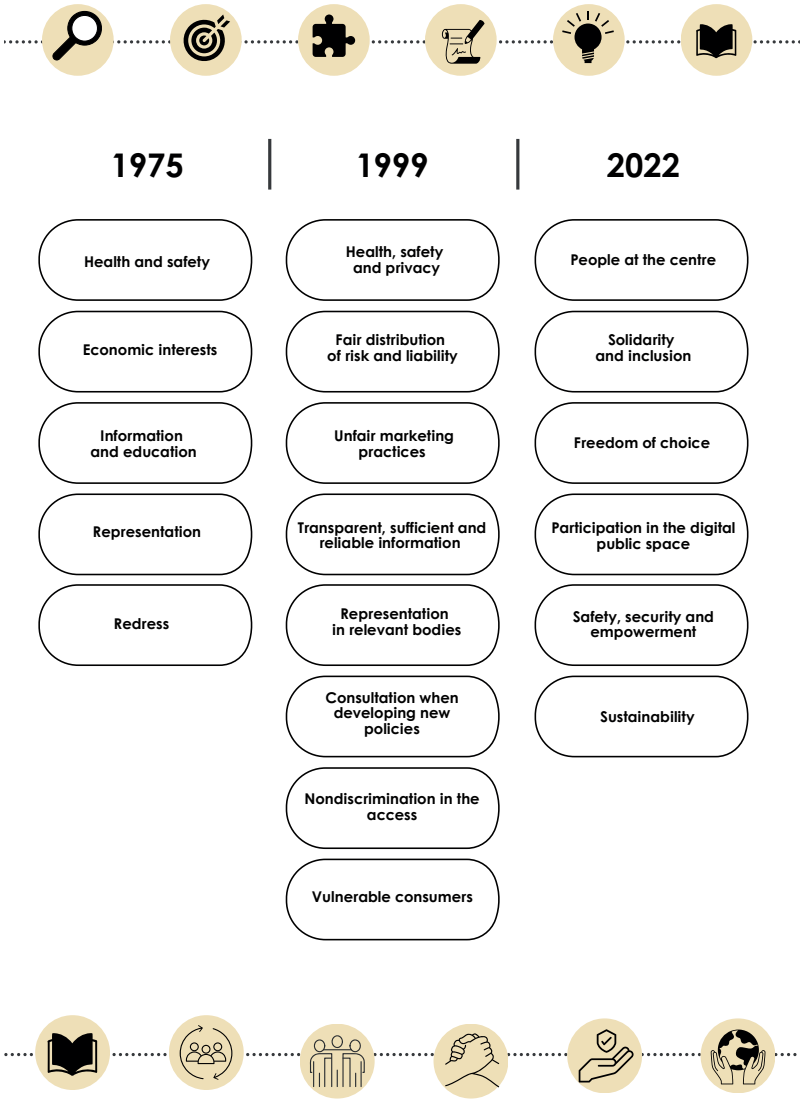


Figure 2: Development of consumer protection policy in the digital environment

In the Chapter III below dedicated to the former regulation, focusing on mapping consumer rights, several specific references are made to the overarching motto of EU consumer policy in the digital environment identified above.

1.5. From Competition Law to the Digital Markets Act

1.5.1. Interplay between EU competition law and the Digital Markets Act

Competition law establishes regulatory tools allowing for response to undertakings' conduct that undermines the internal market and distorts competition. The European Commission's enforcement practice proves that in recent years, most of the big tech companies were found to infringe the prohibition to abuse a dominant position, as stipulated by Art. 102 TFEU. Indeed, this provision has been consequently applied to address anti-competitive behaviours adopted by Google,[63] Amazon,[64] Facebook (now Meta)[65] or Apple.[66]

However, there are features of EU competition law that make it less appropriate or effective in responding to challenges specific for digital markets. These regard the substance, enforcement and overall nature of competition law.[67]

First, competition law is in essence substantively limited to instances of anti-competitive agreements (Art. 101 TFEU), abuse of dominant position (Art. 102 TFEU), and control of concentrations (EU Merger Regulation). Consequently, a given market conduct needs to fall into either of these specific categories to possibly be found to infringe competition law. Within the scope discussed here, the prohibition to abuse a dominant position most often applies. However, it requires demonstrating that, firstly, a given company does indeed hold a dominant position on a given market and, secondly, that its specific behaviour amounted to specific abuse of that dominance. Therefore, there is a risk that some unfair or harmful practices would not have been caught by competition law if not performed by dominant undertakings within the meaning of Art. 102 TFEU.

Secondly, most competition law enforcement is preceded by self-assessment, occurs *ex post*, and requires extensive investigation of what are often very complex matters. These are market actors that shall assess themselves whether their behaviour complies with EU competition rules. In the event of non-compliance, it needs to be identified by the European Commission (or a national competition authority). In such cases, the Commission may initiate proceedings in which it examines in detail a given market conduct and engages in an in-depth market investigation. All factors combined mean that it can take several years between the initiation of anti-compet-

[63] See cases from the Commission of: 2 June 2017, Google Search (Shopping) (Case AT.39740); of 18 July 2018, Google Android (Case AT.40099); of 14 July 2016, Google Search (AdSense) (Case AT.40411).

[64] See cases from the Commission: of 4 May 2017, E-books (Amazon) (Case AT.40153); of 2 March 2023, Amazon Marketplace (Case AT.40462); of 2 March 2023, Amazon – Buy Box (Case AT.40703).

[65] See case from the Commission of 14 November 2024, Facebook Marketplace (Case AT.40684).

[66] See following cases from the Commission: of 4 March 2024, Apple – App Store Practices (music streaming) (Case AT.40437); of 22 November 2024, Apple – App Store Practices (e-books/audiobooks) (Case AT.40652) and of 24 June 2024, Apple – App Store Practices (other applications) (Case AT.40716).

[67] Rec. 5 DMA.

itive conduct and the Commission's decision requiring to bring that behaviour to an end. Such a long duration may be particularly unfortunate with regard to digital markets due to the intense dynamics of the competitive landscape in these markets.

Thirdly, and more systematically, traditional EU competition law will not deal conceptually with systemic market failures resulting from gatekeepers' behaviours.[68] This results from the above-mentioned limited toolbox and characteristics of enforcement mechanisms, but also from the nature and goals of competition law. These are to respond to specific anti-competitive conduct and not to restructure the market or heal its overall, systemic failures.

Therefore, the EU legislator identified the need to introduce specific tools enabling effective responses to gatekeepers' practices, as well as ensuring contestability and fairness on digital markets.[69] These are now included in the Digital Markets Act.

Although the DMA forms part of internal market legislation, it is very much inspired by competition law, including its goals, structure and enforcement practice regarding large tech companies. It is also designed to remedy the limits identified in the enforcement of Art. 102 TFEU in digital markets.[70]

The DMA's entry into force and full application are without prejudice to the application of competition law to gatekeepers' practices if they prove to be anticompetitive under Art. 101–102 TFEU.[71] As confirmed in the DMA's preamble, this regulation is complementary with competition law and does not seek any collision with that framework. The lack of collision seems to be supported by the fact that competition law and the DMA pursue slightly different objectives. While the former focuses on protecting undistorted competition on any given market, the latter seeks to ensure that the markets experiencing gatekeepers' presence remain or become fair and contestable.[72]

At the same time, in terms of enforcement, the Commission and national authorities need to respect the principle of *ne bis in idem* and therefore shall coordinate their proceedings in order to avoid parallel reactions to the same conduct under competition law and the DMA.[73]

1.5.2. Overall characteristics of digital markets and DMA's goals

The DMA's actual title is the 'Regulation on contestable and fair markets in the digital sector'. Indeed, the Regulation primarily seeks to ensure digital markets'

[68] Commission Staff Working Document – Impact Assessment accompanying the proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Act), SWD(2020) 363 final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020SC0363, paras. 68 et seq., 119.

[69] As discussed in Section regarding the Digital Services Package as part of shaping Digital Europe legislative initiatives, primarily this set of rules was called generally as "the New Competition Tool."

[70] F. Bostoen, *Understanding the Digital Markets Act*, "Antitrust Bulletin" 2023, vol. 68, no. 2, p. 265.

[71] Art. 1(6) DMA.

[72] Rec. 11 DMA.

[73] Rec. 86 DMA.

contestability and fairness. In general, markets are contestable when they will still be unable to restrict competition, e.g. by artificially raising prices, even if there are only few market actors, or just one exists. This can be true in a scenario in which there are low or no barriers to entry to a given market and therefore the incumbents' conduct will be constrained by potential entries to that market. Therefore, contrary to the basic monopoly models, undertakings active in contestable markets will not be able to act independently from their customers or suppliers, and thus not engage in anti-competitive conduct.

Indeed, current characteristics of the digital sector imply that these markets are far from being contestable or fair. These characteristics include the following: increasing concentration (translating into a lower number of platform services providers); vertical and online integration of online platforms; extreme scale economies (meaning that additional business or end users are gathered at nearly zero marginal costs); very strong network effects (the more users of a given platform, the greater its ability to attract remaining part of the demand); an ability to connect many business users with many end users through the multi-faceted nature of these services; lock-in effects (i.e. users need to put much effort or costs to switch from current service provider to their competitor); and a lack of multi-homing (i.e. both business and end users' propensity to use parallelly several competing platform services).[74]

In such a market environment, it is difficult to legitimately expect new entries into platform markets. Hypothetically, even if Google lowered the quality of its online search services (e.g. by using algorithms effectively preferring a given type of content or websites), or Meta started charging certain fees from its Facebook and Instagram users, it would be difficult for new entrants to successfully gain significant share in the search services or social media markets.

As a result, the largest core platform service providers came to be regarded as the 'gatekeepers'. Recital 6 DMA reads that such gatekeepers have a significant impact on the internal market, providing gateways for many business users to reach end users everywhere on different digital markets. Traditionally, trade would take place in a number of various, mutually independent areas. However, the increasing tendency of transforming it into e-commerce on online platforms means that these platforms became marketplaces and gained powers to shape market conditions and market structure.

This is particularly challenging when a given platform is vertically integrated and therefore present at the same time in the upstream market (online platform service, the marketplace) and the downstream market (acting as other business users' competitor, e.g. Amazon's shop competing with other sellers active on that platform when selling books). In such a scenario, the gatekeeper has an additional incentive to treat their business users (at the same time, competitors in downstream markets) unfairly, for the benefit of gatekeeper's own downstream services.

[74] Rec. 2 DMA.

Therefore, the DMA's goal is to restore the proper balance between digital markets participants: the largest platforms (or, gatekeepers) and their users, both business and end users. More specifically, the DMA seeks to provide business and end users with appropriate regulatory safeguards against unfair practices adopted by gatekeepers. In a broader sense, the introduction of the DMA followed on from noticing certain systemic market failures and it now aims at improving the proper functioning of the internal market and eliminating its fragmentation occurring in specific digital market areas.[75]

1.6. Conclusions

In the sections above, we presented the legal context in which the Digital Services Package was adopted. In particular, we discussed those areas that are further explored in subsequent chapters: the introduction of due diligence obligations as a response to the deficiencies of the ECD, ensuring the effective protection of consumers, and introducing the *ex-ante* approach to the market practices of gatekeepers, to complement existing competition rules. The main thrust of our analysis concerns the activities of online platforms and the need for enhanced protection of platform users.

From the regulatory perspective, the role of online platforms is not only to store information, as in the case of simple hosting services, but also to disseminate various categories of information. The DSA and the DMA recognize that the functioning of platforms includes different relations with users or businesses, briefly referred to as C2C (consumer-to-consumer), B2C (business-to-consumer), B2B (business-to-business), P2C (platform-to-consumer) or P2B (platform-to-business). Therefore, the Regulations discussed address several aspects of platform relations with business users, practices concerning consumers, and end users or the activities of different service recipients. Platform users employ these services for sharing and seeking information, buying and selling, entertainment, education or brand marketing. The possibilities for users seem infinite.

The concept of "a user," as framed by the European Declaration on Digital Rights and Principles for the Digital Decade, reflects the current stance that we need to look at online activities beyond market-related concepts. This is best expressed with the commitment of the EU Institutions that "technology should serve and benefit all people living in the EU and empower them to pursue their aspirations, in full security and respect for their fundamental rights." The objectives of the DSA and the DMA forward this vision of a "fair digital environment,"[76] which is subject to critical analysis in this handbook.

[75] Rec. 7 DMA.

[76] Art. 1.1, 10 and 11 of the European Declaration on Digital Rights and Principles for the Digital Decade.

Chapter II

Content moderation and rights of users in the Digital Services Act – protected or neglected?

2.1. Introduction

The DSA offers the regulatory answer to a long discussion on intermediary service providers' (ISP) liability and infringements, threats or harms occurring due to the ease of communication offered by online platforms. New "due diligence" obligations introduced in Chapter 3 of the DSA focus on content moderation mechanisms, as well as enhancing consumer protection.[1] Due diligence obligations differ depending on the type of the service provider. Sections 1–5 of Chapter 3 reflect the graduated approach: from basic obligations applicable to all ISPs, to obligations imposed solely on very large online platforms (VLOPs) and very large online search engines (VLOSEs). Three categories of ISPs fall within the scope of the DSA: mere conduit, caching and hosting service providers.[2] The more the service providers are involved in the process of disseminating the information online, the more obligations are imposed. This involvement includes storing (hosting service providers) storing and disseminating information to the public (online platforms) or storing and disseminating information with a potential impact on a substantial number of active recipients (VLOPs and VLOSEs).[3] When not specified otherwise in this chapter, the focus lies on online platforms as services offering the possibility to make information available to the public, and thus, most relevant from the perspective of freedom of expression.

Harmonized due diligence obligations are imposed to achieve certain public policy objectives, such as building safety and trust for recipients of the service, protecting fundamental rights, ensuring accountability of service providers and empowerment of service recipients.[4] The due diligence chapter includes the obligation to implement content moderation mechanisms, obligations in the area of

[1] With the provisions addressing online interfaces, advertising or information about products and services accessible on platforms.

[2] Art. 3(g) of Digital Services Act (DSA) (OJ L 277, 27.10.2022, pp. 1–102).

[3] Definitions provided in art. 3(e) and 33(1) DSA, where the threshold for 45 mln active users per month.

[4] Rec. 40 DSA.

informing users, or reporting and making data concerning the service accessible. Clearly, a service recipient, defined as a legal or natural person using a service to seek information or make it accessible,[5] is at the heart of this regulation, as the one to protect, the one to empower, and the one whose fundamental rights require enhanced protection. The user, as a recipient of information, should be protected from being harmed, bullied, disturbed or offended. Under the DSA, content moderation, as a tool for such protection, encompasses any activity aiming at detecting, identifying and addressing illegal content or information incompatible with the terms of service, with an array of measures restricting its accessibility or visibility.[6] However, content moderation mechanisms may also limit one's freedom to impart information. The risks of content moderation for fundamental rights have been studied at international and regional levels, and have already led to some recommendations being formulated. Three major risks were identified in the area of fundamental rights: (1) the risk of delegating the judicial function to assess the legality of content to platforms; (2) the lack of transparency, particularly of the decision-making process on platforms, of the use of automated tools, and the grounds for content moderation decisions and; (3) the lack of effective, or inadequate, legal remedies.[7]

In Europe, the DSA is the key act addressing how intermediaries build and operate the digital infrastructure for communication and information flows. There is a clear demand that platforms should be 'responsible' for the safe digital space, and an implied imperative that, as business operators, they ensure respect for fundamental rights.[8] In this light, this chapter undertakes to discuss any potential 'users' rights' that can be derived from platforms by means of diligence obligations in the area of content moderation. Starting with the risks that content moderation may pose to users, it presents regulatory answers offered by the DSA and discusses if, and how, users are empowered to protect their freedom of expression.

[5] Art. 3(b) DSA.

[6] Definition of content moderation in art. 3(t) DSA.

[7] Based on the assessment of risks and concerns in: D. Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Geneva 2018, pp. 10–14; *Side-stepping Rights: Regulating Speech by Contract: Policy Brief*, London 2018, pp. 14–18, https://www.article19.org/wp-content/uploads/2018/06/Regulating-speech-by-contract-WEB.pdf (accessed: 3.4.2025); E. Pírková, J. Pallero, *26 Recommendation on Content Governance: A Guide for Lawmakers, Regulators and Company Policy Makers*, Access Now, 2020, pp. 14–18, https://www.accessnow.org/guide/guide-how-to-protect-human-rights-in-content-governance/ (accessed: 3.4.2025).

[8] According to the rules on business and human rights, *Guiding Principles on Business and Human Rights, Implementing the UN Protect-Respect-Remedy Framework*, New York and Geneva 2011, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf (accessed: 3.4.2025).

2.2. User empowerment in content moderation

Civil rights organizations recommend minimum content moderation. From the perspective of the freedom to impart and receive information, it seems that the less content moderation, the better. If incentives for more content moderation exist, they may easily result in problems of over-moderation and over-blocking of users' content,[9] and engaging platforms in the role that should be attributed only to judges.

An interesting example of the idea of drastically limiting content moderation being put into practice came from Twitter. The platform, rebranded as X, was steered towards a new direction of 'an all-in-one' platform. The press extensively discussed how its owner, Elon Musk, wants a "free speech utopia" with his vision of the online app as a "public town square."[10] It was proposed in the discussion that to truly have free speech, we need content moderation.[11] The X platform chose a different direction, restricting the number of content moderators, thus raising questions about how is it going to deal with influx of hate speech and disinformation.[12] This approach was tested in October 2023 with the Hamas attack in Israel. As the DSA was already in force,[13] and X is one of the VLOPs, the European Commission requested information to investigate how the platform fights illegal content, particularly terrorist content, violent content and hate speech, and mitigates the risks stemming from the massive spread of such content.[14] X published a transparency report, underlining the value of free expression in an attempt to ensure both freedom of expression and safety, in line with the objectives of the DSA.[15] The Commission, nevertheless,

---

[9] N. Elkin-Koren, M. Peerel, G.de Gregorio, "Iowa Law Review" 2022, vol. 107, pp. 989–994, https://ilr.law.uiowa.edu/sites/ilr.law.uiowa.edu/files/2023-02/A2_ElkinKoren_DeGregio_Perel.pdf; O.L. Haimson et al., *Disproportionate Removals and Differing Content Moderation Experiences for Conservative, Transgender, and Black Social Media Users: Marginalization and Moderation Gray Areas*, "Proceedings of the ACM on Human-Computer Interaction" 2021, vol. 5, no. CSCW2, article 466, https://doi.org/10.1145/3479610.

[10] Elon Musk talks about his plans for Twitter at TED, YouTube, 14.4.2022, https://www.youtube.com/watch?v=WrH-CTRrj_I (accessed: 3.4.2025).

[11] E. Dworkin, *Elon Musk Wants a Free Speech Utopia: Technologists Clap Back*, The Washington Post, 18.4.2022, https://www.washingtonpost.com/technology/2022/04/18/musk-twitter-free-speech/ (accessed: 3.4.2025).

[12] B. Ortutay, M. O'Brien, The Associated Press, *Elon Musk Fires Outsourced Content Moderators Who Track Hate and Harmful Posts on Twitter*, Fortune, 14.11.2022, https://fortune.com/2022/11/13/twitter-elon-musk-fires-outsourced-content-moderators-track-hate-harmful/ (accessed: 3.4.2025); X Safety, *Freedom of Speech, Not Reach: An Update on our Enforcement Philosophy*, Blog X, 17.4.2023, https://blog.twitter.com/en_us/topics/product/2023/freedom-of-speech-not-reach-an-update-on-our-enforcement-philosophy (accessed: 3.4.2025).

[13] Regulation is applicable since February 2024, but some provisions addressing VLOPs are applied since November 2022, Art. 93 DSA.

[14] The Commission send request for information to X, European Union, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4953 (accessed: 3.4.2025).

[15] X transparency report, https://transparency.twitter.com/dsa-transparency-report.html (accessed: 3.4.2025).

opened formal proceedings against X in December 2023,[16] and X decided to invest more in content moderation.[17] The Commission requested more information on recommender systems, and content moderation from X, and continues the investigation[18]. Based on this example, it is clear that we can hardly imagine an online platform without content moderation.

2.2.1. Incentives for moderation

It was indicated early in the discussion on platforms' responsibility that content moderation is an inherent feature of online platforms, an essential component that defines an online platform.[19] When the DSA was drafted, voluntary content moderation was a well-established practice of online platforms with global reach. The DSA remains subject to criticism as to how it may lead to more content moderation. The criticism include fostering algorithmic enforcement to fight illegal and harmful content.[20]

Firstly, the criticism may be linked to the DSA's primary objective of "setting out harmonized rules for a safe, predictable and trusted online environment", which includes effective protection of fundamental rights. The wording of Art. 1 DSA indicates that "safety" takes precedence. This is in line with the broader context of making platforms responsible and engaging them in the protection of EU values. The objective here is to engage online platforms without crossing the red line of making them the ultimate regulator of content availability.

Secondly, online platforms' engagement in voluntary content moderation may be encouraged with provisions clarifying the scope of liability exemptions. Art. 7 DSA ensures that intermediary service providers are not excluded from the scope of liability exemptions provided for in Art. 4–6 if they engaged "in good faith and in a diligent

[16] Commission investigates potential violation of 34(1), 34(2) and 35(1), 16(5) and 16(6), 25(1), 39 and 40(12) of the DSA – *Commission opens formal proceedings against X under the Digital Services Act*, European Union, 18.12.2023, https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6709 (accessed: 3.4.2025).

[17] The reports submitted to the European Commission indicated that the number of content moderators on X is noticeably lower than on other platforms. S. Dang, *Musk's X Aims to Hire 100 Content Moderators in Austin by End of Year*, Reuters, 27.1.2024, https://www.reuters.com/technology/musks-x-aims-hire-100-content-moderators-austin-by-end-year-2024-01-27/ (accessed: 3.4.2025).

[18] Press release, 17 January 2025, *Commission addresses additional investigatory measures to X in the ongoing proceedings under the Digital Services Act*, https://digital-strategy.ec.europa.eu/en/news/commission-addresses-additional-investigatory-measures-x-ongoing-proceedings-under-digital-services (accessed: 3.4.2025).

[19] T. Gillespie, *Custodians of the Internet. Platforms, Content Moderation and the Hidden Decisions That Shape Social Media*, New Haven and London 2018, p. 21.

[20] M.L. Montagnani, Virtues and Perils of Algorithmic Enforcement and Content Regulation in the EU-A Toolkit for A Balanced Algorithmic Copyright Enforcement, "Case Western Reserve Journal of Law, Technology and Internet" 2019–2020, vol. 11, no. 1, p. 11, https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=3767008 (accessed: 3.4.2025).

manner," voluntarily and on their own initiative in investigations or took other measures aiming at "detecting, identifying and removing, or disabling access to, illegal content." This provision is compared to the so-called "good Samaritan"[21] clause resulting from section 230 CDA[22] in the US law. The E-commerce Directive did not contain a similar provision, and only "passive" intermediaries, for example, hosting service providers, could shield themselves from liability.[23] The DSA forwards the concept of providing the service "neutrally" rather than "passively." The preamble guides on understanding when the provider is neutral: when it confines the service to "merely technical and automatic processing of the information provided by the recipient of the service"; facilitating illegal activities is not the main purpose of the service; and a service provider is in no way involved with the information transmitted or accessed.[24] Furthermore, service providers remain "neutral" when they implement different content moderation tools to remove illegal content, which is one of their "due diligence" obligations. Platforms' "voluntary initiatives" may take place based on platforms' terms and conditions (T&C), and, in practice, include fighting lawful but unwanted content and illegal content. The understanding of "neutrality" as a feature describing activities of online platform is dubious. According to the statistics,[25] the majority of content moderation decisions are taken based on platforms' own policy. It is therefore questionable whether they are still "neutral" when moderating digital communication.

Thirdly, the DSA is without prejudice, and does not limit, the incentives for content moderation that result from previous harmonization. Art. 17 of the Copyright in the Digital Single Market Directive introduced a special regime for liability of online content sharing service providers (OCSSPs). The prevailing opinion is that OCSSPs are strongly incentivized to moderate content, as Art. 17 provides that when no authorization for content available on a platform was granted, despite platforms' "best efforts," a service provider must make best efforts "in accordance with high industry standards of professional diligence (…) to ensure the unavailability of specific works and other subject matter for which the rightsholders have provided the service providers with the relevant and necessary information", to shield itself from liability. Article 17 of the CDSM directive remains a *lex specialis* to the DSA. It definitely excludes the application of Art. 6 DSA, and instead the special regime

[21] F. Wilman, *Between Preservation and Qualification: The Evolution of the DSA's Liability Rules in Light of the CJEU's Case Law*, in: J. van Hoboken et al. (eds.), *Putting the DSA into Practice: Enforcement, Access to Justice and Global Implications*, Berlin 2023, p. 37, https://www.ivir.nl/publicaties/download/vHoboken-et-al_Putting-the-DSA-into-Practice.pdf (accessed: 3.4.2025).

[22] Communications Decency Act of 1995, Congress.gov, https://www.congress.gov/bill/104th-congress/senate-bill/314 (accessed: 3.4.2025).

[23] M. Piech, *Pośrednicy internetowi w prawie Unii Europejskiej. Rola i obowiązki wobec treści użytkowników*, Warsaw 2019.

[24] Rec. 18–21 DSA.

[25] *DSA Transparency Database*, European Union, https://transparency.dsa.ec.europa.eu/ (accessed: 3.4.2025).

for host providers' liability exemption from Art. 17(4) CDSM is applicable.[26] It has not been clarified, however, whether the application of Art. 7 is also not applicable to OCSSPs. It appears that under Art. 17(4) all activities undertaken by OCSSPs to ensure the unavailability of copyright infringing content, as well as preventing their future uploads, are formally "voluntary". This is a legal condition to be exempted from liability, therefore some argue that Art. 17(4) leaves very little scope for voluntary actions. Therefore, the possibility of invoking Art. 7 should not be excluded, although it may not be relevant in practice. Copyright liability is an example of a strong incentive for content moderation.

The DSA does not include an express obligation to moderate content, and it precludes any general monitoring obligation (Art. 8). Clearly, however, there are obligations to take actions based on orders from public authorities (Art. 9 and 10) and to take actions based on submitted notices (Art. 16). Article 7, on the other hand, confirms the DSA's favourable position as to the platforms' own, voluntary moderation initiatives.

The DSA imposes a clear obligation to put content moderation mechanisms in place. Taking into account the obligation to respond to notices, no doubts exist as to the necessity of moderating illegal content, if justified notices are submitted. The notices satisfying the conditions set in Art. 16(2) are considered as giving rise to the knowledge or awareness in the context of liability exemption: if the service provider does not react expeditiously to remove or disable access to such illegal content, it cannot shield itself from liability for its dissemination, notwithstanding the grounds of such liability (whether civil, criminal or administrative). As the DSA ensures that no general monitoring obligation, nor obligation to actively seek facts or circumstances indicating illegal activity may be imposed on hosting service providers, it confirms that online platforms are obliged to be reactive in the area of illegal content. Their active approach seems to be welcome under Art. 7 DSA, as discussed above, as long as the red line of "no prior censorship" or stepping into the judicial role is crossed.

5.2.2. "Right" to report

In an attempt to translate the DSA provisions into users' rights, to raise awareness of the new environment, Bits of Freedom explains that in the context of fairer content

[26] J.P. Quintais, S. Schwemer, *The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?*, "European Journal of Risk Regulation" 2022, vol. 13, no. 2, p. 207, https://doi.org/10.1017/err.2022.1; E. Rosati, *The Digital Services Act and Copyright Enforcement: The Case of Article 17 of the DSM Directive*, in: M. Cappello (ed.), *Unravelling the Digital Services Actpackage*, Strasbourg 2021, p. 76, https://rm.coe.int/iris-special-2021-01en-dsa-package/1680a43e45. Art. 17(3) of the CDSM states that Art. 14(1) of the ECD that was repealed by the DSA is not applicable when an OCSSP performs an act of communication to the public or an act of making available of a work to the public under the conditions set out in Art. 17(1) CDSM.

moderation, platforms are required to make it easy to report illegal content.[27] This could be termed the "right to report." The user, who in this context is any individual or entity, is empowered by the existence of a certain functionality, 'a button'. Users may reasonably expect a clear indication how to access electronic form they can easily complete in order to submit a notification. If this is not the case, 'recipients of the service', or any organization or body mandated to exercise the rights conferred by this Regulation, have the right to lodge a complaint to a digital services coordinator (DSC) in the country where the complainant is established.[28] It should be pointed out that the functionality to submit a report needs to be offered to anyone, while the complaint may be lodged by the service recipient or mandated entity. It should be noted that submitting a notice should be available to anyone, but only the service recipient, or the entity indicated in Art. 53 DSA, is entitled to file a complaint.

The "right to report" illegal content should be framed in the broader context of the European Declaration on Digital Rights and Principles for the Digital Decade. Under the principle of 'a protected, safe and secure environment', it underlines that "everyone should have access to digital technologies, products and services that are by design safe, secure." Therefore the EU institutions commit to countering and holding accountable those that promote violence and hatred through digital means.[29] There is no full synergy between this soft law provision and the DSA. The latter is, at the same time, narrower, addressing a functionality that serves the general purpose of safety, and in a broader scope, as it aims to fight all illegal content, and does not target only violence or hatred. The findings of the EU-commissioned survey indicate that in 2018, 65% of respondents did not regard the Internet as safe: of the 61% of respondents who conducted any internet activity, only one in five informed the service provider about illegal content they encountered.[30] The DSA definitely aims at improving both safety, user empowerment and, potentially, the user's active participation and contribution to a safe place. As indicated in the DSA recitals, obligations and conditions imposed in Art. 16 should "ensure timely, diligent and non-arbitrary processing of notices" and provides for "robust safeguards," particularly for the protection of fundamental rights such as freedom of expression of service recipients.[31] Countering over-blocking can be exemplified with the provision that an ISP is only considered to gain specific knowledge or awareness, in the meaning of Art. 6 DSA, if notices allow the diligent service provider "to identify the illegality of the relevant activity or information without a detailed legal

[27] *Stay Loud. Know Your Rights*, Bits of Freedom, 17.4.2024, https://www.jouwplatformrechten.nl/en/rights/moderation (accessed: 3.4.2025).

[28] Art. 53 DSA.

[29] Art. 16(b) of the European Declaration on Digital Rights and Principles for the Digital Decade.

[30] *Flash Eurobarometer 469. Report. Illegal Content Online*, European Union, 4.6.2018, https://europa.eu/eurobarometer/surveys/detail/2201 (accessed: 3.4.2025).

[31] Rec. 52 DSA.

examination."[32] Therefore, if the service provider decides to allow for reporting of content violating terms of services, it is desirable to apply the same structure as for illegal content,[33] especially if the terms of service refer both to illegal content and content non-compliant with platform policy.

By expressly obliging intermediaries to ensure an easy possibility to report illegal content, the DSA goes a step further than existing content regulation at the EU level. In the AVMSD, ensuring transparent and user-friendly mechanisms for users to report or flag videos constituting incitement to violence or hatred or a criminal offence under EU law is listed as one of the measures that a video-sharing platform (VSP) **may** apply to counter illegal content. National Regulatory Authorities should find such tools to be necessary, however, otherwise this could lead to internal conflict with provisions prohibiting the application of any *ex-ante* measures or upload filters.[34] As stressed in the Impact Assessment, the DSA complements the AVMSD with more detailed requirements with regard to transparency and user complaints.[35] Under the DSA, users always need to be able to easily report illegal content.

The applicability of Art. 16 DSA in the area of copyright prompted numerous doubts, as the CDSM Directive establishes the specific regime of liability.[36] Rights holders are the best placed to notify service providers about copyright-infringing content, and thus they constitute a sub-category of 'platform users'. Service providers should prevent the availability of copyright-infringing content.[37] This is regulated by the provisions of the CDSM Directive, as *lex specialis* to the DSA. The concern for freedom of expression is that OCSSPs voluntarily implement general monitoring filtering.[38] However, such mechanisms are subject to limits set by the CJEU's case law and have to distinguish between lawful and unlawful content, otherwise their application would be incompatible with the freedom of expression.[39] Notices may be submitted in cases when despite the cooperation with the rights holders, or in the absence of such a cooperation, infringing content appears online. Application of Art. 16(1)–(2) would ensure that establishing reporting tools is the service provider's obligation. As noted prior to DSA enactment, harmonized notice and action procedure should be complementary to copyright enforcement rules.[40] Furthermore, application of Art. 16(2) would uniformly clarify when notices are sufficiently substantiated, adding the detailed requirement to provide the URL. Eventually,

[32] Art. 16(3) DSA.

[33] Art. 16(3) DSA could not be applied directly, but perhaps *per analogiam*.

[34] Art 28(b) AVMSD.

[35] European Commission, Impact Assessment of the Digital Services Act (SWD (2020) 348 final, n.d.), para. 290.

[36] E. Rosati, op. cit.; J.P. Quintais, S.F. Schwemer, op. cit.

[37] Art. 17(4) (a) and (b) CDSM.

[38] E. Rosati, op. cit., p. 75.

[39] Judgment of CJEU of 26 April 2022, Case C-401/09, *Poland v Parliament and the Council of the European Union* (ECLI:EU:C:2022:297), para. 90.

[40] European Commission, Impact Assessment of the Digital Services Act, para. 291.

application of Art. 16(3), even if formally linked to Art. 6 DSA, is in line with CJEU interpretation of liability exemption provisions. Information provided by users only gives rise to 'actual knowledge'[41] when content is manifestly illegal, meaning the service provider can identify illegal activity without detailed legal examination.[42] Apart from empowering users, Art. 16 DSA imposes conditions for notices that serve protection against over moderation. Protection of users' fundamental rights is also essential in the area of IP protection. Furthermore, the DSA establishes the specific enforcement framework, which would allow a complaint if no reporting mechanism is established, or in case of other infringement of Art. 16.[43]

2.3. Transparency of content moderation for users: right to be informed

The discussion on platform transparency has been a key aspect of the debate on platform governance. It centres around two issues: transparency for individual users, and transparency linked to public accountability. The latter includes information provided to public authorities, published online for the general public, and provided to selected users acting in the interests of society, such as vetted researchers. Civil society organisations recommended high standards for transparency,[44] especially in the areas of automated content moderation based on a platform's terms of service, to limit the unpredictability of content restrictions.[45] Transparency reports have been published since 2013.[46] These practices were analysed in research to offer some insight into what do we learn from the numbers published by platforms,[47] or how it impacts user behaviour.[48] A substantial study on platform transparency comes

[41] In the event of the service provider having actual knowledge of illegal content, it may not rely on liability exemption (Art. 6 DSA). In the light of special regime of Art. 17 (4), if OCCSP did not act expeditiously based on sufficiently substantiated notice, it shall be liable for communicating to the public of this content.

[42] Case C-401/09, *Poland v Parliament and the Council of the European Union*, para. 91.

[43] Art. 53 DSA.

[44] E. Pírková, J. Pallero, op. cit., p. 33; Santa Clara Principles on content moderation 2.0, https://santaclaraprinciples.org/ (accessed: 3.4.2025).

[45] Council of Europe, *Content Moderation: Best Practices Towards Effective Legal and Procedural. Frameworks for Self-Regulatory and Co-regulatory Mechanisms of Content Moderation, Guidance Note Adopted by the Steering Committee for Media and Information Society (CDMSI) at Its 19th Plenary Meeting, 19–21 May 2021*, 2021, p. 42, https://edoc.coe.int/en/internet/10198-content-moderation-guidance-note.html (accessed: 3.4.2025); D. Kaye, op. cit., Recommendations 69 and 71, p. 20.

[46] See https://www.tspa.org/curriculum/ts-fundamentals/transparency-report/history-transparency-reports/ (accessed: 3.4.2025).

[47] E. Goldman, *Content Moderation and Remedies*, "Michigan Technology Law Review" 2021, vol. 28, no. 1, article 2, p. 57, https://doi.org/10.36645/mtlr.28.1.content.

[48] S. Jhaver, A. Bruckman, E. Gilbert, *Does Transparency in Moderation Really Matter?: User Behavior After Content Removal Explanations on Reddit*, "Proceedings of the ACM on Human-Computer Interaction" 2019, vol. 3, no. CSCW, article 150, p. 152, https://doi.org/10.1145/3359252.

from the US, with questions how to evaluate the regulatory approach for meaningful transparency,[49] which can be summarized as follows: what is the information we demand and what decisions will be made based on it?[50] What can we learn from information provided and shall it serve improvements in the platform environment?

In Europe, the DSA enhances the regulatory framework, where transparency is meant to be the key to establishing an environment in which fundamental rights receive effective protection. Transparency, as the cornerstone of due diligence obligations, is what should ensure predictability, and predictability should effectively counter the risks of vague rules, the broad margin of discretion, and limit unclear moderation outcomes. To highlight users' rights in the area of content moderation, transparency obligations can be can be discussed from the perspective of:

a) Users' right to be informed as a service recipient, about content moderation rules (Art. 14 DSA).

b) Users' right to be informed when freedom of expression is affected (Art. 17 DSA).

c) General access to reports on content moderation prepared by online platforms (Art. 15, 22, 42 DSA).

Ad a) Terms and conditions

In the AVMSD, the first attempt to harmonize fighting illegal and harmful content with moderation tools, the emphasis was placed on informing users about illegal and harmful content[51] that would be restricted on platforms.[52] This approach evolved[53] and the DSA now demands that any hosting service provider, firstly, informs about any restrictions on the use of a service with respect to information provided by the user, and secondly, about ***any policies, procedures, measures and tools used for the purpose of content moderation*** in the T&C. The latter includes information about algorithmic decision-making and human review, and procedural rules of the internal complaint-handling system. The first set of information on 'any restrictions' could refer to the general profile of the service, highlighting the type of content that the service is designed for. This set of information may also include explanations of illegal content unacceptable on platforms. It stems from Art. 14(1) DSA that a user has the right to be informed in detail about any policy that is applicable to

[49] N.P. Suzor et al., *What do We Mean When We Talk about Transparency? Toward Meaningful Transparency in Commercial Content Moderation*, "International Journal of Communication" 2019, vol. 13, p. 1527.

[50] E. Goldman, op. cit., p. 58.

[51] As provided for in Art. 28b(1) AVMSD.

[52] Art. 28b(3) (a): Platforms need also to inform in their terms of service about the rules on commercial communications provided for users.

[53] It is pointed that Art. 5(1) of the Regulation 2021/784 was a direct inspiration for the DSA – J.P. Quintais et al., *Enforcement of Terms of Service*, "German Law Journal" 2023, vol. 24, no. 5, p. 890, https://doi.org/10.1017/glj.2023.53.

content, especially content not compliant with the terms of service. Such a policy may constitute 'community guidelines' and, in fact, merge information about illegal and unwanted content. User should also be informed about different tools and measures used for content moderation. Tools and measures typically include those listed in the legal definition of content moderation, such as demotion, demonetisation, disabling of access to, or removal of content (Art. 3(t) DSA). It is clear that from the regulatory perspective, users should be able to learn, from the clear and unambiguous language and plain and intelligible text of the T&C, which content shall be restricted and what content restrictions tools are applied.[54] In practice, many terms and conditions are complex documents. Therefore, additional requirements for VLOPs and VLOSEs include publishing the T&C in official languages of all Member States, and offering "a concise and easily readable summary of the main elements of the terms and conditions" (Art. 14(5) DSA).

The level of detail demanded from the T&C can also be inferred from Art. 17(3) (e) DSA on explanatory statements for moderating decisions. Information provided to the user *ex-ante*, before any content is uploaded, should explain what may happen after the content is published in violation of law and T&C. Ideally, explanatory statements should 'join the dots' for a particular user, explaining what happened *ex post* in a particular situation.

The DSA does not expressly answer the call for an online platform service to align their policies with the international human rights standards. The standards for freedom of expression should play a leading role in the area of content moderation.[55] The DSA, however, obliges platforms "to act in a diligent, objective and proportionate manner in applying and enforcing restrictions (…)" that were described in the T&C, "with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service" (art. 14(1) DSA). It is reasonable to expect that restrictions and content moderation policies need to be drafted in accordance with fundamental rights standards in the EU, and that terms of services should be reviewed to comply with these standards.

In the area of freedom of expression and copyright, more detailed provisions of the CDSM impose on OCSSPs an obligation to "inform their users in their terms and conditions that they can use works and other subject matter under exceptions or limitations to copyright and related rights provided for in Union law" (Art. 17(9) *in fine*). This may be an example of important information that should be provided based on harmonized national laws. To become truly relevant, this information should enable the user to post content including citations or parodies, despite the risks it may create for platforms, and along with the guidance that only manifestly illegal content should be subject to automated moderation. Otherwise, general

[54] Additionally, standards in templates, designs and processes of communication with the users on restrictions resulting from T&C should be promoted by the Commission, Art. 44(1) (b) DSA.

[55] J.P. Quintais et al., *Enforcement of terms of service*, pp. 881–882.

information on the possibility of relying on applicable limitations and exceptions is likely to remain an empty promise for users.

Ad b) Statement of reasons

To ensure transparency of the decisions in the area of content moderation, the online platform provider should inform both the user who reported illegal content and the user who was affected with the decision restricting the visibility or availability of content. According to Art. 16(4)–(6) DSA, the reporting user should first receive confirmation that the 'notice' was received, and then information on the decision of the hosting service provider, including information about whether automated means were used in the process and about the possibility for redress. A recipient of the service who is affected by a content moderation decision[56] imposing the restrictions listed in Art. 17(1) (a)–(d) should receive a clear and specific statement of reasons, notwithstanding if the decision was based on the ground that the content was illegal, or if it was incompatible with the T&C. The obligation to provide a statement of reasons does not extend to content moderated based on orders (Art. 9 DSA), nor to a high-volume deceptive content[57] and is limited to instances when the service provider knows the electronic contact details of a user.

An explanatory statement to a user needs to include information on the type of restriction applied, and also information concerning the facts and circumstances relied upon in taking moderation decisions. It should be clear to a user whether content was removed, access to content was disabled, demoted or some other visibility restriction, such as a shadow ban, was applied. Equally, it should be evident whether demonetization, in the form of suspending, terminating or restricting payments was applied, or whether an account or the provision of a service as such was terminated or suspended. Though not clearly indicated in the DSA, explaining precisely which content caused moderation decision should be considered as part of facts and circumstances relevant for the decision. Where relevant, the host provider should inform whether the decision was based on the notice based on its voluntary, own-initiative investigation. The restriction of this obligation to unclear situations when it is 'relevant' deserves critique. As the risks for content moderation are indicated mostly in the area of platforms' voluntary activities, this information is likely to be relevant for users in the case of their filing a complaint. As Art. 24(5) obliges online platforms to submit statements of reasons to be included in the

[56] In practice, it narrows the category of recipients of the service to those who make information accessible, and not only 'seek information', unless seeking information could reasonably trigger, for example, suspension or termination of a service. This provision is primarily applicable to registered users, as they create an account with contact details to publish content. There is, however, no express requirement to be a registered user.

[57] Commonly referred to as 'spam'.

publicly available databases,[58] to foster platform accountability this information should always be considered 'relevant'[59] in the case of online platforms. When the decision was made based on the fact that content was illegal, an explanatory statement needs to include a reference to the legal grounds, with an explanation of why the information was found to be illegal. In the event of a decision being based on the platform's terms of service, relevant contractual grounds must be indicated and explained. The exemplary decisions reported in the EU database indicate deficiencies to meaningfully inform users about moderation of their content. For example, under the heading "facts and circumstances" and "explanations of why content is considered as incompatible on that ground" precisely the same information is sometimes provided. Additionally, a general clause indicating more than one basis on which to find the content to be violating the terms of service is cited.[60] No details explaining why a particular content was removed, in the event of it being automatically detected and in the process of a partially automated decision, can be inferred from a published statement. Information on whether automated means were used in the process of identifying and in taking the moderation decision should be provided where applicable. This provision should be interpreted in line with the calls for high standards of transparency in the areas of risks to fundamental rights, as always applicable, if any automated means were used in the moderation process. Satisfying the minimum requirements provided for in the DSA results in scant information: "yes" or "no" answers to questions of whether automated means were used, and "yes," "no" or "partially" in the case of decisions taken. This information may be relevant both for the accountability to general public and for further appeal. Clear and user-friendly information on the possibilities of redress for a user constitutes the final mandatory element of an explanatory statement. An obligation to provide an explanatory statement is applicable from the day of imposition of a restriction, albeit without any deadline. In practice, it should happen automatically with the content moderation decision, otherwise it may hinder the redress possibilities, which are restricted in time.

Ad c) Reporting obligations

As already indicated, statements of reason provided by online platforms are published in an online transparency database that offers analytics and statistics, as well as opens up the data for research and analysis. This solution forms part of the transparency obligations linked to ensuring public accountability of online platforms and fosters an in-depth discussion on content moderation systems based on

[58] *DSA Transparency Database*, op. cit.

[59] This would leave some scope to consider when such information is not relevant in the case of pure hosting, without the dissemination of information to the public.

[60] See https://transparency.dsa.ec.europa.eu/statement/17541329612 (accessed: 3.4.2025).

the relevant data. This framework includes creating a publicly accessible database, including one on the terms of service,[61] and reporting obligations.

The basic reporting obligations are set out in Art. 15 DSA, with higher expectations for online platforms in Art. 23, and additional obligations for VLOPs and VLOSEs in Art. 42. Regularly submitted, publicly available reports provided on the template annexed in Commission Regulation[62] are the main tool to ensure transparency under the DSA. These reports are available to any interested users. Their significance lies in providing a bigger and, hopefully, systemic picture of content moderation mechanisms. All providers of intermediary services need to provide, on a yearly basis, clear, easily comprehensible, publicly available reports on any content moderation they engaged in (Art. 15(1)). A substantial part of the reporting obligations concern numbers, such as numbers of orders received from public authorities, numbers of notices submitted based on Art. 16(1), numbers of notices processed with automated means, or the number of complaints received via internal complaint handling systems. Online platforms are additionally required to report on a number of disputes submitted to out-of-court dispute settlement (ODS) bodies and about the suspensions caused by either frequently providing manifestly illegal content or manifestly unfounded notices or internal complaint.[63]

Numbers can certainly inform us about the scale of content moderation, and any use made of newly tailored notice-and-action mechanisms. Even the basic reporting requirements go beyond numbers, demanding, for example, information on "any use made of automated means for the purpose of content moderation, including a qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible rate of error of the automated means used in fulfilling those purposes, and any safeguards applied" (Art. 15(1) (e)). VLOPs and VLOSEs should provide more detailed information on human moderators and the "qualifications and linguistic expertise" of the persons carrying out moderating activities, as "well as the training and support given to such staff," and indicators for accuracy related to automated means (Art. 42(1) DSA). It is a challenge to ensure that reported massive amounts of data from all intermediary service providers are presented in a comprehensible manner, open for analytics and comparisons. A unified template serves this purpose, yet it may simplify the reporting process by requiring numbers in areas where the DSA could be read as requiring more. Accuracy and the error rate for the use of automated means by VLOPs is a good

[61] See https://platform-contracts.digital-strategy.ec.europa.eu/ (accessed: 3.4.2025).

[62] Commission Implementing Regulation (EU) 2024/2835 of 4 November 2024 laying down templates concerning the transparency reporting obligations of providers of intermediary services and of providers of online platforms under Regulation (EU) 2022/2065 of the European Parliament and of the Council (OJ L, 2024/2835, 5.11.2024).

[63] Additional obligations on protection against misuse of a service are included in Art. 23 DSA.

example. It should be expected that users learn more about how online platforms determine accuracy and error rates of their algorithmic tools. The reporting template includes reporting the "contextual information," which may constitute one of the tools to address the broader problem of better understanding of content moderation as "mass speech administration."[64] This brings the analysis to the ultimate question of who will analyse the data on content moderation, and how it will impact assessment of the compliance with due diligence obligations, provided that effective protection of fundamental rights, including freedom of expression, is one of the main objectives of the DSA?

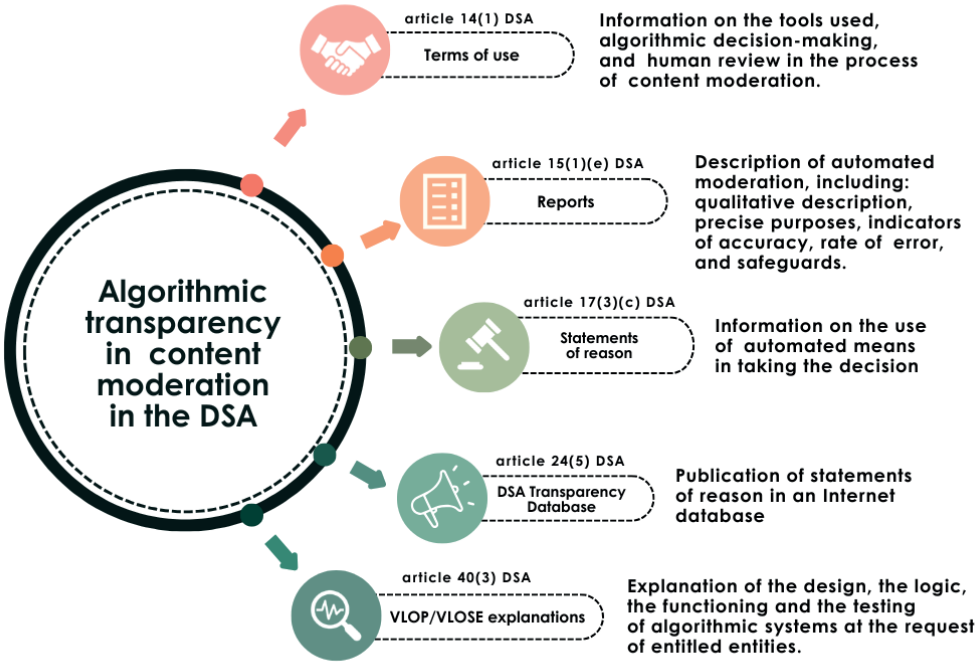


Figure 3: Algorithms in moderation – information obligations

Firstly, transparency should demonstrate compliance with the DSA due diligence framework, and primarily the DSCs and the European Commission are responsible for its supervision and enforcement.[65] Furthermore, transparency is important for individual users, especially as information needed to seek redress,

[64] E. Douek, *Content Moderation as Systems Thinking*, "Harvard Law Review" 2022, vol. 136, no. 2, p. 528.
[65] Enforcement issues are subject to discussion in Chapter V.

and for the accountability of platforms. In the latter context, the DSA includes content moderation systems in the list of factors that may impact systemic risk (Art. 34(2) (b)) in the context of VLOP operations. The risk that voluntary content moderation affects the freedom to receive and impart information with over-blocking, or automatic removal of legitimate content and unsatisfactory error rates, should be considered among systemic risks, as the DSA indicates not only the risk of spreading illegal content, or negative effects on electoral process, but also the risk of "actual or foreseeable negative effects for the exercise of fundamental rights", including freedom of expression. If it is a potential systemic risk,[66] it should be identified by VLOPs and mitigation measures should be applied. The deficiencies in this area may also be revealed in audit reports, on how due diligence obligations are complied with (Art. 37(1) DSA). Furthermore, the Commission and DSCs should be mindful of the risk to freedom of expression when analysing submitted data. As observed, some reported data may conceal grave problems, for example, if the low rate of internal complaint or dispute heard by out-of-court dispute settlement mechanisms was to indicate that all content moderation decisions are balanced or justified.[67] The Commission and DSCs are tasked with overseeing DSA compliance, and promoting best practices, also in the form of codes of conduct, which should help tackle systemic risks. Based on the publicly available information, and information accessed only by vetted researchers, the general public may be informed by researchers and civil society organizations about the risks linked to the functioning of online platforms. Ultimately, the user can make the decision not to use a service, as indicated by the European Declaration on Digital Rights and Principles for the Digital Decade. "Everyone should be able to effectively and freely choose which online services to use, based on objective, transparent, easily accessible and reliable information."[68] However, this seems utopian in the case of very large services with a massive audience that have become the infrastructure for communication of a modern society.

2.4. Conclusions

To conclude, we should start by reflecting on the main problem that the DSA attempts to solve. Is it the problem of ensuring that online environment is safe from illegal or harmful content? Or is it the problem of too much discretion of online

[66] Acting according to Art. 34 DSA.

[67] M. Senftleben, *Guardians of the UGC Galaxy – Human Rights Obligations of Online Platforms, Copyright Holders, Member States and the European Commission Under the CDSM Directive and the Digital Services Act*, "Journal of Intellectual Property, Information Technology and E-Commerce Law" 2023, vol. 14, no. 3, pp. 436–437, https://ssrn.com/abstract=4683206.

[68] Art. 10 of the European Declaration on Digital Rights and Principles for the Digital Decade.

platforms to moderate speech? Ensuring safety and predictability is definitely the first objective on the list. The framework for protecting fundamental rights, also prominent in the DSA, is fairly broad: from fighting illegal content to ensure no violations for human dignity, to privacy and freedom of expression. To empower users, platforms are obliged to provide certain functionalities, making it easy to submit a notice, which we have discussed here as a "right to report," but also to facilitate the submission of complaints. The safety of the platform environment is further fostered with favourable frameworks for voluntary content moderation. There is no doubt that the DSA increases content moderation, yet at the same time, it increases control over content moderation, including voluntary moderation by platforms.

As the risks for freedom of expression are identified particularly in the area of moderation based on internal policy,[69] the maximum safeguards implemented with regard to illegal content should apply to the moderation of content incompatible with the T&C. To minimize the risk of abuses, the requirements for "sufficiently precise and adequately substantiated notices" and the obligation to notify a user that has posted the content in question should also apply in the case of notices based on non-compliance of content with the terms of service. It should be underlined that platforms rely extensively on their own terms of service, as, apart from content that is manifestly illegal under EU law,[70] it may prove difficult to assess in the instantaneous and massive process of moderation which content is not compliant with the laws of a Member State, for example, as defamation or content harmful for minors.

To counter the risk of over-moderation, the DSA affords users the right to information, notwithstanding if moderation is based on the illegality or incompatibility of content with the T&Cs. This right to be informed is derived from consumer protection policy, but also extends to business users and other potentially affected parties (Art. 17(1)). This right translates into obligations to inform about content moderation policies, and to inform about activities affecting one's freedom to receive and impart information in the form of explanatory statements. Interpretation of the obligations in the area of providing information should ensure that users can appeal effectively against the platform's decision, or lodge substantiated complaints with DSCs. It is therefore important that users are able to learn why and how a particular piece of content was restricted, why the service provider found the content to have violated T&Cs, and whether the decision was taken after human review. The DSA's provisions, interpreted in the light of an objective of user empowerment and protection of fundamental rights, oblige platform service providers to be specific

[69] This type of moderation is voluntary but welcome from the perspective of the EU's regulatory approach.

[70] Such as child pornography.

in justifying their decisions. It is more difficult to clarify what information should be provided to the user regarding the algorithmic content information and human review in the particular case. Here, rather than being empowered, users are asked to trust regulatory authorities that have broader and structured access to information about algorithmic content moderation.

Chapter III

The principle of consumer protection under the Digital Services Act – mapping consumer benefits

3.1. The Digital Services Act and EU consumer law

Even if its purpose is expressed in such a general way (see remarks on Art. 1(1) DSA and Rec. 3 of its preamble, presented here in Chapter I), it is not difficult to identify the consumer dimension of the DSA under modern EU law. For that, at least one of the key principles of EU primary law, enshrined in Art. 12 TFEU, should be considered to be relevant. It states that consumer protection requirements shall be taken into account in the process of defining and subsequently implementing other Union policies and activities. The last revision of the EU treaties in 2009 moved this provision, previously known as Art. 153(2) Treaty establishing the European Community (TEC),[1] to Part One of the TFEU, where it is placed among the European Union's principles as the 'horizontal clause'.[2] This modification must be seen as an expression of the enhanced importance and autonomy of the consumer protection policy,[3] which is further confirmed in CFREU, where the principle of consumer protection (Art. 38) closes the catalogue of provisions contained in its Chapter IV (Solidarity), without, however, raising consumer protection to the status of a fundamental right within the meaning of Art. 52(2) CFREU.[4]

Today, this undoubted advancement of the principle of consumer protection, which may be described, without exaggeration, as a manifestation of 'constitutionalisation', represents a certain standard in the EU legal order, and the DSA may also be assessed in terms of its fulfilment. The EU legislator has, by and large, made

[1] Consolidated version 2002 (OJ C 325, 24.12.2002, pp. 33–184).

[2] In the context of horizontal clauses, the literature rightly points out that their inherently vague construction, which refers collectively to protected interests, may prove difficult in the event of an attempt to enforce it in a particular case due to the lack of possibility of its simple translation into legally recognised (justiciable) rights – cf. S. Weatherill, *Law and Values in the European Union*, Oxford 2016, p. 135 et seq.

[3] S. Weatherill, *Consumer Policy*, in: P. Craig, G. de Búrca (eds.), *The Evolution of EU Law*, 3rd ed., Oxford 2021, p. 875.

[4] I. Benöhr, *EU Consumer Law and Human Rights*, Oxford 2013, p. 63; N. Reich, H.-W. Micklitz, *Economic Law, Consumer Interests and EU Integration*, in: N. Reich et al. (eds.), *European Consumer Law*, 2nd ed., Cambridge, Antwerp, and Portland 2014, p. 14; S. Weatherill, *Law and Values*…, p. 136 et seq.

this task easier by specifying precisely in the description of the DSA's objective what (and thus whom) the regulation of a safe, predictable and trustworthy online environment is intended to serve, stating at the same time that this environment is to be a space that will "facilitate innovations" and one in which "the fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected" (Art. 1(1) DSA). The preamble of the DSA (Rec. 1 and 4) emphasises this specific combination of two dimensions: one focused on innovation (stimulating innovation, introducing innovative digital services) and the other emphasizing the status of citizens of digital society, expressed by reference to the fundamental rights guaranteed in the CFREU.

The latter component is comprehensive since, in addition to the principle of consumer protection explicitly invoked in Art. 1(1) DSA, it also encompasses the freedom of expression and of information, the freedom to conduct business, and the right to non-discrimination (Rec. 3 of the DSA preamble). Taken together, all that elements are helpful in reading the phrase "safe, predictable and trustworthy online environment." From this perspective, consumer rights (cf. Art. 169(1) TFEU) are not an isolated element of this regulation, but should be viewed as one of many points of reference to the provisions of the DSA, namely those relating directly to consumer protection, as well as those which often only indirectly, but still visibly, affect the legal status of the consumers of digital services.

***The relationship between the DSA and the consumer* acquis.** Article 2(4) (f) DSA states that the DSA is without prejudice to "Union law in the field of consumer protection and product safety." Regarding consumers, in an open-ended catalogue it mentions two EU regulations and two directives, and while Regulation (EU) 2017/2394[5] and Directive 2013/11/EU[6] are particularly relevant from the perspective of the enforcement of consumer rights, the other two pieces of legislation deal with product safety issues.[7] Moreover, as provided in Article 2(4) (f) DSA, the relationship of the DSA to specific EU consumer law provisions will remain dynamic and, among other things, it will allow it to be separated from such regulations that govern other aspects of the provision of intermediary services in the internal market (e.g. contracts for the supply of digital content and digital services in the context of Directive (EU) 2019/770[8]). Furthermore, it justifies taking into account provisions

[5] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 (OJ L 345, 27.12.2017, pp. 1–26).

[6] Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR) (OJ L 165, 18.6.2013, pp. 63–79).

[7] However, Directive 2001/95/EC (OJ L 11, 15.1.2002, pp. 4–17) referred to in this provision, has been repealed following the entry into force of Regulation (EU) 2023/988 (OJ L 135, 23.5.2023, pp. 1–51).

[8] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (OJ L 136, 22.5.2019, pp. 1–27).

specifying and complementing the scope of the DSA. Such a role may be attributed, for example, to Directive 2005/29/EC[9] or the aforementioned provisions for the enforcement of consumer rights. The dynamics of the relationship between these two Directives and *vis-à-vis* the DSA are illustrated by the specific provisions of the DSA discussed in Sections 3.3 and 3.4 below. Section 3.2 addresses the basic concepts pertaining to individuals and entities caught up in the DSA's regulatory framework. The focus, however, is on the consumer.

3.2. Consumers in the Digital Services Act

As a framework regulation harmonising the conditions for the provision of intermediary services, the DSA represents a new approach when compared to the solutions adopted in Directive 2000/31/EC[10] at the beginning of the digital era. Both the DSA and the Directive impose a number of obligations on businesses – providers of information society services – and focus on the providers of intermediary services. However, an important novel aspect introduced in this respect under the DSA is its differentiation of obligations put on intermediaries according to their position in the online environment, and particularly the degree of their impact measured by the number of active recipients of the service (see Art. 3(p) and (q) and Rec. 77 DSA). This is manifested, in particular, in the differentiation of due diligence standards developed for businesses (providers of intermediary services) covered by the provisions of the various sections of the DSA's Chapter 3 (Art. 11–48). A list of these opens with obligations imposed on all providers of intermediary services (Section 1), while other sections introduce further provisions relating to subsequent subcategories of these regulated entities.

Architecture of the DSA. The way in which the core provisions of the DSA are framed can be viewed as a concentric arrangement consisting of several contiguous sets (layers) of provisions that shape the obligations of a particular group of regulated entities. The core of this arrangement is formed by obligations applicable to all intermediary service providers. Subsequent sets, moving outwards from the centre, form successive rules applicable to providers of hosting services, then to providers of online platforms, online B2C platforms, up to additional rules addressed to providers of very large online platforms (VLOPs) and very large online search engines (VLOSEs).

[9] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) (OJ L 149, 11.6.2005, pp. 22–39).

[10] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ L 178, 17.7.2000, pp. 1–16).

The way these provisions focus on professional market players is evident. At the same time, it makes it possible to regard the various sets of such obligations from the perspective of the other participants of the Internet environment, namely, the broad category of **recipients of the service** (Ger. *Nutzer*, Fr. *destinataires des services*). For the purposes of the DSA, this concept is defined in its Art. 3(b) and explained in Rec. 2 of its preamble as including 'business users, consumers and other users'. This explanation, much more than the legal definition, highlights the diverse nature of that category of participants of the online environment (users). It corresponds to the specificities of the multisided (triangular) business models typical of online platforms today. Moreover, the inclusion of consumers alongside business users[11] within the concept of service recipients requires equal treatment of those two categories as functionally arising from their mutual dependence and their position *vis-à-vis* the intermediary, and the online platform, in particular.

The DSA's specific provisions reflect the distinction drawn between consumers and other service recipients, and this approach is continued below, where the provisions applicable directly to consumers (Section 3) and the provisions that affect consumers indirectly (Section 4) are discussed separately. The mapping of consumer benefits that accompany the two subsequent sections assumes a correlation between the obligations imposed on intermediaries and the rights of service recipients, especially consumers. This coupling between an obligation and a right, typical for the private-law perspective, requires taking account of the specificities of the tripartite relationship occurring in the online platform environment. An example that demonstrates the necessity of identifying the recipients of a service on a case-by-case basis can be found in one of the very large online platforms (LinkedIn),[12] which, although used by individuals, predominantly serves purposes connected with their professional activity. Thus, against the background of the legal definition of Art. 3(c) DSA, its provisions that are applicable exclusively to consumers (mainly in a B2C relationship) may not apply to that service, while the provisions that serve the interests of other service recipients will continue to apply, and not be only restricted to a sub-group of consumers.

Definition of a 'consumer'. The wording of Art. 3(c) DSA differs only slightly from the definitions fund in classic EU consumer legislation (e.g. Directive 2011/83/EU,[13] Directive 2005/29/EC or Regulation (EU) 2017/2394). This similarity

[11] The DSA does not define this concept, but Regulation (EU) 2019/1150 (OJ L 186, 11.7.2019, pp. 57–79) does so, which, following Art. 2(4) DSA, may be seen as complementing it in this regard. In this context, the notions of 'business user' and 'end-user' as defined in Art. 2 DMA are of note (see Chapter IV Section 4.4).

[12] Their up-dated list is published on https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (accessed: 3.4.2025).

[13] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (OJ L 304, 22.11.2011, pp. 64–88).

is not at all surprising, as it allows for a consistent demarcation of this group of individuals, for which EU law provides a specific protection regime. This in turn enables the implementation of the EU consumer policy as expressed by the phrase "what is illegal offline should be illegal online" (cf. Chapter I).

In several cases discussed below (cf. Section 3.3), the DSA contains provisions that expressly refer to consumers. However, it should be strongly emphasised that such provisions will not constitute the only field of application of the consumer *acquis*. Indeed, wherever the DSA refers to 'recipients of a service' without explicitly delimiting which subcategory of users is concerned, each factual situation will require a careful assessment to decide whether it warrants recourse to the consumer regime. The functional interconnection of several subcategories of users, as well as the potential interaction between them, may also transform into an EU standard of protection for the recipients of services in the information society. In the evolution of such a standard, the high level of consumer protection consistently implemented by the European Union may play a significant role.

Taking into account the legal definition under the DSA regime, the consumer remains *homo economicus passivus*. This makes it possible to distinguish a consumer from other users (service recipients), particularly business users, as well as those who pursue objectives in the online environment that fall outside the economic context (political, charitable activities, etc.). Further nuancing of this concept, taking into account the dynamism and variability of the roles that recipients of information society services may play, for example, will remain the role of case law. Some of the key CJEU's rulings adopted so far[14] may certainly serve as relevant points of reference. There is no doubt that only the practical application of the DSA will show how much of its architecture, including the specific relationships between actors involved in the digital services market, ought to be reflected in the context of consumer protection.

The DSA's characteristic perspective of combining the principle of consumer protection with fundamental rights strongly encourages a deepened and continuing discussion on the need to reconceptualize the consumer concept by considering the specific conditions of the digital environment[15] and also the civic dimension,[16] expressed by the concept of information society.

---

[14] Cf. the judgment of CJEU of 25 January 2018 in case C-498/16, *Maximilian Schrems v Facebook Ireland Limited* (ECLI:EU:C:2018:37), concerning the assessment of the legal status of a user of a private social media account in a jurisdictional context, and the judgement of CJEU of 8 June 2023 in case C-570/21, *I.S., K.S. v YYY*, relating to the concept of a consumer in a specific contractual context (dual-purpose contracts).

[15] S. Umit Kucuk, *Consumerism in the Digital Age*, "Journal of Consumer Affairs" 2016, vol. 50, no. 3, p. 533, https://doi.org/10.1111/joca.12101.

[16] I. Benöhr, op. cit., p. 173; N. Helberger et al., *Digital Consumers and the Law: Towards a Cohesive European Framework*, Alphen aan den Rijn, 2013, p. 8 et seq.; L. McShane, C. Sabadoz, *Rethinking the Concept of Consumer Empowerment: Recognizing Consumers as Citizens*, "International Journal of Consumer Studies" 2015, vol. 39, no. 5, p. 547, https://doi.org/10.1111/ijcs.12186.

3.3. Provisions of the DSA dedicated to consumer protection on B2C platforms

3.3.1. Consumer exception within the liability for hosting services

Alongside completely new rules governing the provision of intermediary services, the DSA also includes provisions that update the existing measures. This is the case with the liability standard for providers of intermediary services, originally formulated in Directive 2000/31/EC in respect of electronic commerce. Some of its provisions, in a modernised version, have been incorporated into the DSA as Art. 4–6 and 8, while their counterparts from Directive 2000/31/EC have been repealed by Art. 89 DSA.[17] Undoubtedly, this fosters the development of a uniform regulatory standard across the EU.

The conditions accompanying the exception of liability of providers of intermediary services stipulated in the DSA largely repeat the legislative solutions set out in Directive 2000/31/EC. However, as regards Art. 6 DSA, which relates to the exception of liability of hosting providers, a new provision has been introduced that takes into account consumers' interests, including the right to effective protection of their economic interests and the right to information contained in the requirement of transparency and safety of the online environment emphasised in the DSA. This new solution, included in Art. 6(3) DSA, occupies a special place in the cascading structure of this provision. While paragraph 1 sets out the grounds for the exception of liability of a provider of hosting services, paragraphs 2 to 3 introduce a second level of exemption (counter-exception), indicating instances where it is precisely the exception under paragraph 1 that does not apply and, as a result, establishing the liability of the hosting provider.

The effect of the consumer exception under Art. 6(3) DSA will be the possible liability of an intermediary service provider. This liability, however, as expressly stated in the provision, will not apply to each category of intermediaries but only to providers of online platforms enabling consumers to conclude distance contracts with traders (so-called B2C platforms). From the perspective of the current legislation on the liability for online services, Art. 6(3) DSA may be assessed as beneficial for consumers using such platforms, as this is where the risk of violation of their interests should be reduced in the most effective way. At the same time, in its overall design, this provision identifies the obligations of B2C platforms, formulated in separate DSA provisions and concern, in particular, the traceability of traders (see Section 3.3.2). Indeed, attributing liability to a B2C platform will be possible once the conditions under Art. 6(3) DSA have been met. A significant condition among

[17] As a consequence, the relevant provisions adopted as a result of the implementation of this Directive in the EU Member States have also ceased to apply and have been replaced by the DSA provisions directly applicable in domestic legal systems.

these is the manner in which a B2C platform "presents a given piece of information or otherwise enables the conclusion of a given transaction."

Impact of case law. The mechanism for the liability of an intermediary service provider, which emerges from the wording of this provision, is not entirely new. It corresponds to solutions developed much earlier under EU legislation on consumer rights in the event of a sale of consumer goods.[18] In the 2016 judgment in case C-149/15 (*Wathelet*)[19] concerning the sale of a second-hand car to a consumer, basing on the then-applicable provisions of Directive 1999/44/EC,[20] the CJEU ruled that the seller's liability ought to have been extended to an intermediary-trader who had failed to duly inform the consumer that the goods sold were owned by a natural person. This judgment is currently cited[21] as a model solution that has been used in the digital environment under the provisions of the DSA and constitutes another confirmation of the EU's moving in the direction adopted in its consumer policy and expressed by the policy guideline "what is illegal offline should be illegal online."

The benchmark of the 'average consumer'. The practices of B2C platforms under Art. 6(3) DSA are examined using the criterion of the 'average consumer', from whose perspective the assessment of the transparency of transactions concluded on the platform and the traceability of the businesses involved will be made. The consumer's potential belief that the information at issue has been provided either by the online platform itself or by traders (recipients of the service) acting under its authority or control will determine how liability is attributed to the platform and not to the trader remaining in the B2C relationship with the consumer. The concept of the 'average consumer' derives from CJEU case law, from which, at a legislative level, it was anchored in Directive 2005/29/EC as a benchmark for the prohibition of unfair commercial practices. Transferring it to the DSA means extending its scope of application within the activities of intermediary service providers, thus confirming the value attributed to it in the literature as "the measure of all things."[22] At the same time, it may provide an impetus for the further development of this criterion, precisely taking into account the specific nature of the online environment and, in particular, the relationships involving consumers in that environment.

---

[18] Cf. M. Dregelies, *Verbraucherschutz im Digital Services Act*, "Verbraucher und Recht" 2023, no. 5, p. 176.

[19] Judgment of CJEU of 9 November 2016, Case C-149/15, *Sabrina Wathelet v Garage Bietheres & Fils SPRL* (ECLI:EU:C:2016:840).

[20] Repealed under the provisions of Directive (EU) 2019/771 (the 'Omnibus Directive') (OJ L 136, 22.5.2019, pp. 28–50) the adoption of which, in turn, had served largely to implement the EU's Digital Single Market strategy.

[21] H. Schulte-Nölke, *The EU Digital Services Act and EU Consumer Law*, in: A. De Franceschi, R. Schulze (eds.), *Harmonizing Digital Contract Law: The Impact of EU Directives 2019/770 and 2019/771 and the Regulation of Online Platforms: A Handbook*, Baden-Baden 2023, p. 708.

[22] H.-W. Micklitz, *Unfair Commercial Practices and Misleading Advertising*, in: N. Reich et al. (eds.), *European Consumer Law*, op. cit., p. 94. In the context of the application of these provisions to platforms defined as *social media*, see: M. Dregelies, op. cit., p. 178.

3.3.2. Due diligence of B2C platforms towards consumers

Within the structure of Chapter 3 of the DSA, which sets out the due diligence obligations imposed on providers of intermediary services, there are additional provisions of a separate section (Section 4: Art. 29–32 DSA) for providers of B2C online platforms, allowing consumers to conclude distance contracts with traders.[23]

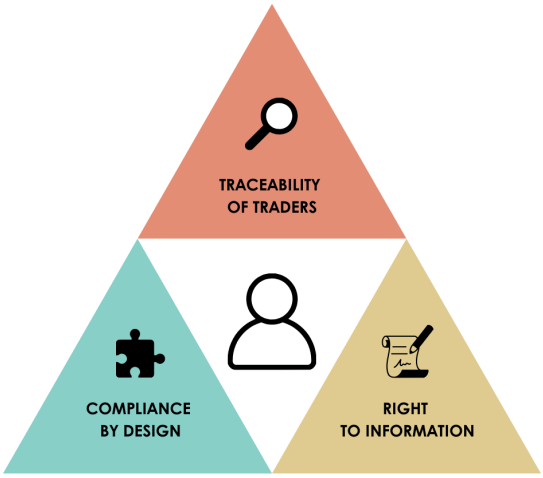


Figure 4: New due diligence rules for B2C online platforms

Article 29 DSA excludes the application of the provisions contained in this Section to certain categories of traders, namely micro and small enterprises.[24] A solution of this kind is not present in classic EU consumer legislation, where the idea of harmonising certain aspects of market operation, including the digital single market, while maintaining a high level of consumer protection, benefits businesses, particularly small and medium-sized enterprises sector.[25] The DSA, on the other hand, justifies this exclusion by the need to avoid disproportionate burdens (Rec. 57 of the preamble), at the same time emphasising that service providers who benefit from this exclusion may fulfil the obligations of this section on a voluntary basis. It may be questioned at this point to what extent the mechanism of market competition

[23] In the terminological context within EU consumer law, it is worth pointing to the concept of 'online marketplace' introduced by the aforementioned Omnibus Directive into Directive 2005/29/EC. This concept covers both B2C and C2C online platforms. It is thus broader than the one used in the DSA, although, at the same time, no legal definition of the term 'B2C online platform' will be found in it, but only a definition of the term 'online platform' (Art. 3(i) DSA). Cf. the term 'provider of an online marketplace' as defined by Art. 3(14) of Regulation (EU) 2023/988 (OJ L 135, 23.5.2023, pp. 1–51).

[24] An analogous exception has been envisaged under Section 3 of Chapter 3 – see Art. 19 DSA.

[25] Cf. Rec. 3 and 10 of Directive (EU) 2019/771.

will generate sufficient pressure to comply with the higher (more consumer-friendly) standards emerging from the current wording of the DSA provisions to bridge the differences in the treatment of consumers.

The essential obligations of B2C online platforms are formulated in Art. 30–32 DSA. Viewed from a systematic perspective, each article introduces a new obligation, hence there are three new rules of due diligence for B2C platforms. They can be seen in the Figure 4, and are centred on the consumer. The impact of each article on consumer's interests (rights) in the online environment is discussed below.

Traceability of traders. Article 30 DSA fits directly into the objective of transparency in the online environment. Primarily, it is intended to ensure that traders can use B2C online platforms "only to promote messages about products or services or to offer services or products to consumers located within the Union," and, in a way, excludes the use of B2C platforms for other purposes that extend beyond the rather fluid boundaries of market transactions.[26]

First and foremost, this concerns the relationship between the platforms and traders operating on those platforms (P2B), and requires the former to obtain (for tracing purposes) information about those traders as provided for in Art. 30(1) (a)–(d) DSA and, additionally, to make "best efforts" to assess whether this information is reliable and complete (Art. 30(2) DSA). These two paragraphs demonstrate an unquestionable reinforcement of the "know your business customer" (KYBC) rule, developed in the provisions of Directive 2000/31/EC. Their counterparts in B2C-relationships are the information requirements of Directive 2011/83/EU or Directive 2005/29/EC, but naturally without the concomitant verification obligation, which is only required in a P2B relationship. It should be added that the due diligence requirement described here is to be implemented at an early stage, prior to the use of the platform services by the trader.[27]

There are measures set out in that provision for the B2C platforms that support trader traceability, securing a timely delivery and the accuracy of the required information. These measures – refusal of permission to use the platform, a request to rectify deficiencies, or suspension of services to a trader – depends on the specific situation. At the same time, traders are entitled to defend their interests in accordance with the complaint procedures available to recipients of services under Art. 20–21 DSA.

The EU consumer is an indirect beneficiary of the mechanism described above.[28] Through it, the consumer obtains an additional level (within the P2B relationship)

[26] The phenomena occurring outside this area include political advertising which has recently been regulated in the EU by Regulation (EU) 2024/900 (OJ L, 2024/900, 20.3.2024).

[27] For traders already using B2C online platform services Art. 30(2) (2) DSA provides a time limit to comply with the new obligations, which expired 12 months after the date of applicability of the DSA, i.e. after 17 February 2024.

[28] Only part of the information on a given trader obtained by the provider of the online platform is subject to direct availability to the public "at least on the interface of the platform" (Art. 30(7) DSA).

for the verification of information that is relevant at the pre-contractual stage on the platform, irrespective of the information requirements that traders are obliged to meet in a direct B2C relationship. This undoubtedly serves to protect the customer's interests in the event of a potential dispute with the trader. At the same time, the obligation of the online platform provider to store such information for a period limited to 6 months after the end of the P2B contractual relationship does not materially weaken the pro-consumer nature of Art. 30 DSA, because, as indicated in Section 3.3.1 above, it applies without prejudice to other provisions of EU consumer law.[29]

Compliance by design. Both the significance of these provisions enshrined in consumer law and the importance of product safety rules under EU law are further manifested in the obligation referred to in Art. 31 DSA. As in the case of trader traceability, this provision applies to P2B relationships, requiring online platforms to design and organise their web interface in such a way as to enable traders operating on the platform to comply with their pre-contractual information obligations under EU law. In this respect, the DSA refers to Regulation (EU) 2019/1020[30] along with other relevant legislation (cf. Rec. 74), a list of which is currently supplemented by Regulation (EU) 2023/988.

At the same time, Art. 31(2) DSA sets out the minimum requirements for several categories of information (e.g. marks identifying the trader or information on labelling and marking of products). In no case, however, does the compliance in the design phase result in a general obligation for B2C online platforms to monitor the products or services offered on these platforms. This approach corresponds with Art. 8 DSA: providers of the B2C online platforms are only required to make 'reasonable efforts' (Art. 31(3)) to check whether products or services offered through them have been identified as illegal. The source of such checks may be the modified EU Rapid Information System, for example, whose abbreviated name 'RAPEX' has been renamed 'Safety Gate' under Regulation (EU) 2023/988.[31]

The obligation to ensure compliance by design is very similar (albeit slightly less elaborate) in structure to the first obligation (trader traceability) in Section 4 of Chapter 3 of the DSA. From the consumer's perspective, its undoubted merit is its reinforcement of those EU law provisions which specify the consumer rights to particular information and which also protect consumers' health or life in terms of product safety.[32] The design and organisation of technology (software) expressed in

[29] Complementary traceability obligations for traders are introduced by Regulation (EU) 2023/988 – cf. Rec. 58 of its preamble.

[30] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No. 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, pp. 1–44).

[31] The obligation to use this portal for product safety was introduced by Art. 22 of Regulation (EU) 2023/988.

[32] M. Dregelies, op. cit., p. 179.

a particular web interface which forms the architecture of the platform itself is thus, according to Art. 31 DSA, intended to reinforce the effectiveness of the generally applicable law. It is reasonable to consider this provision in conjunction with other provisions of the DSA relating to the design and organisation of web interfaces and the services provided by the users of platform providers (Art. 25, 28, 34–35 DSA).

Right to information. The catalogue of due diligence rules addressed to B2C online platforms closes with Art. 32 DSA. It formulates a concrete obligation for the provider of an online platform to react in the event of becoming aware that a trader has offered an illegal product or service through the platform. This response is to provide consumers who have purchased an illegal product or service with three types of information concerning the fact that the product or service is illegal, the identity of the trader, and any appropriate remedies (Art. 32(1) DSA). Obviously, such communication may be implemented *ex post* only, which renders this obligation different from the mechanisms provided for in Art. 30 and 31. Additionally, the necessary condition in this respect requires the provider of the B2C platform to have the consumers' contact details. If, however, the provider does not have such data, a variant of this obligation in the form of making the aforementioned information public and easily accessible on the web interface of the B2C platform in question becomes relevant (Art. 32(2) DSA).

Construed in this way, this obligation may be regarded as correlating with the right to information to be realised in a P2C relationship. Unlike the two above-discussed due diligence rules on B2C platforms, the latter provision creates the most direct instrument for consumers to exercise their right to information and to protect themselves against illegal goods or services that may harm their economic interests. The relevance of this obligation may be assessed within the DSA as an important addition to the tools to combat illegal content.[33] As defined in Art. 3(h) DSA, and explained in Rec. 12 of its preamble, the concept of illegal content should "broadly reflect the existing rules in the non-Internet environment," which can be understood straightforwardly as the implementation of the goal of EU digital consumer policy (see Chapter I Section 1.4). Examples of information relating to illegal content, products, services, and activities are listed in the aforementioned recital of the DSA's preamble. The right to information under Art. 32 DSA is also an important complement to the existing, mainly administrative, instruments on product safety, in particular, those recently introduced that are dedicated to the activities of online platforms.[34]

[33] Ibidem, p. 180, where both the difficulty of investigating the state of knowledge of a B2C online platform regarding the illegality of a product or service, as well as the temporal limitation of the binding of the platform to the obligation concerned are pointed out and critically examined (see Art. 32(1), subparagraph 2 DSA).

[34] Cf. Art. 35 of Regulation (EU) 2023/988.

3.4. Selected DSA provisions from the consumer perspective

Taking into account the structure of the DSA, in particular, its provisions setting out the obligations of intermediary service providers (see Section 3.2 above), wherever the beneficiaries of these obligations will be service recipients, consumers will also benefit from such mechanisms for a transparent and secure online environment. The previous Section reviewed those mechanisms dedicated explicitly to consumers. Here, the focus will be on selected provisions of the DSA which are not narrowly applied to consumers, but by protecting all users, still indirectly serve their interests. This selection is underpinned mainly by the possibility of linking the provisions discussed below with typical sources of consumer law, e.g. provisions on contractual clauses or on advertising practices, as well as addressing the vulnerability of specific groups of consumers (protection of minors).

3.4.1. Terms and conditions of the services

Article 14 DSA is an instrument which both impacts on the contractual freedom of intermediary service providers and seeks more effective protection of users, particularly with regard to their freedom of expression in the digital environment. It formulates a particular standard for communicating restrictions imposed in relation to the use of the services offered.

At its core is the obligation to provide information on all policies, procedures, measures and tools used for content moderation (Art. 14(1) sentence 2 DSA), which must be interpreted in conjunction with its very broad legal definition for "content moderation" in Art. 3(t) DSA. At the same time, the substantive layer of this obligation is complemented by a supplementary layer – the requirement to formulate such information in a specific manner, using intelligible, user-friendly and unambiguous language (Art. 14(1) sentence 3 DSA).

It is not the purpose of the discussion here to present the entirety of this elaborate provision, let alone its interrelationship with other provisions of the DSA or other EU legislation. What is worth emphasising, however, is its importance as an attempt to balance the interests of the various actors in the information society. Its 'civic' dimension is highlighted particularly by Art. 14(4) DSA's reference to the rights and legitimate interests of all parties involved, including those outlined in the CFREU. Taking a somewhat narrower consumer law perspective, several points deserve to be addressed.

"User-friendly". Firstly, with regard to the protection of service recipients, and thus also consumers, Art. 14 DSA, in conjunction with its Art. 3(u), in which the 'terms and conditions' are defined, introduces new requirements for assessing information obligations intended to compensate for the information asymmetry typical

in a B2C relationship.[35] In many older but also more recent provisions on consumer contracts (e.g. Directive 93/13/EEC,[36] Directive 2011/83/EU),[37] the requirement of "clear, comprehensive language"[38] is reiterated. However, the phrase used in the DSA is much more elaborate, in particularly its premise of 'user-friendliness' relating to the language formulating the required information. Alongside Art. 14, it appears in several other DSA provisions (cf. Art. 12(1), 16(1), 41(1)), as within the EU legal framework for the functioning of the digital society.[39] This indicates the scope of applying this requirement, making Art. 14 DSA *lex specialis* with regard to similar EU law provisions. At the same time, its use, in addition to the other traditional ones, suggests a different meaning, which, in the context of the user-platform relationship, may be understood as a need to adjust the linguistic form of communication, thus corresponding with user expectations in the colloquial sense. At the same time, in strict terms, it may also be seen as an expression of the validity of the general principle of good faith, which aligns with the principle of trust accentuated in the DSA.

Unfair terms. Secondly, contractual clauses established by providers of indirect services concerning restrictions imposed in connection with the use of their services will be assessed through the prism of the provisions aimed at eliminating unfair T&C in consumer contracts. For that, EU Member States' legislation resulting from the implementation of Directive 93/13/EEC is applicable. This will be of particular relevance in the event of a change in the T&C (Art. 14(2) DSA), which may, after all, also relate to content moderation restrictions. Infringements of the transparency rules provided for in this respect in the DSA will, in the context of consumer protection, be enforceable precisely based on the unfair contract terms regime,[40] which specifically allows courts to determine whether the clause in question is binding on the consumer (Art. 6 of Directive 93/13/EEC). Such a potential court ruling could consequently lead to significant differences in the

[35] M. Husovec, *Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules*, "Berkeley Technology Law Journal" 2023, vol. 38, no. 3, p. 918, https://doi.org/10.15779/Z38M902431.

[36] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, pp. 29–34).

[37] It is worth noting that outside the field of consumer law, the transparency principle applies to the field of personal data protection – cf. Rec. 58 of Regulation (EU) 2016/679 (OJ L 119, 4.5.2016, pp. 1–88).

[38] The standard of 'simplicity' and 'comprehensibility' is here linked to the principle of transparency understood as a subcategory of good faith – see comments on Directive 93/13/EEC: H.-W. Micklitz, *Unfair Terms in Consumer Contracts*, in: N. Reich, H.-W. Micklitz (eds.), *European Consumer Law*, op. cit., p. 143. Nowadays, in this context, it is worth noting the voluntary ISO standard for plain language published on 23 June 2023 as ISO 24495-1:2023 "Plain language Part 1: Governing principles and guidelines".

[39] Cf. Art. 1(5) and (44–45) of Regulation (EU) 2024/1183 (OJ L, 2024/1183, 30.4.2024), as well as Rec. 7 and 52 of Regulation (EU) 2022/868 (OJ L 152, 3.6.2022, pp. 1–44).

[40] H. Schulte-Nölke, op. cit., p. 710 et seq., who refers to the changes in the wording of the provision in question proposed during the legislative process concerning the DSA proposal.

legal position of consumers and other service recipients whose interests Art. 14 is intended to serve.

With regard to the protection of minors referred to in Art. 14(3) DSA, see the comments in Section 3.4.3 below.

3.4.2. Online advertising

The broad definition of the term "advertising" provided in Art. 3(r) DSA remains consistent with the approach to information society services which are not confined exclusively to the market paradigm ("irrespective of whether for commercial or non-commercial purposes…"). The latter paradigm prevailed in Directive 2000/31/EC, which can be seen when comparing the definition of the "commercial information" under Art. 2(f) (*vis-à-vis* Art. 3(w) DSA) with the broad understanding of "advertising" under the DSA (cf. Rec. 68–69 of its preamble). The fact that the DSA puts considerably more emphasis on advertising than the Directive confirms a certain degree of maturity of the former, especially when it is considered together with the provisions of the DMA on online advertising services.[41]

From the perspective of the transparency of communication in the online environment, the provision addressed to online platforms is extremely important for the consumer, as it sets out the obligations to identify certain information as advertising or commercial information (Art. 26(1) and (2) DSA). This provision, combined with the prohibition of advertising based on profiling with the use of sensitive data (Art. 26(3) DSA), illustrates perfectly the strong correlation in today's electronic communication environment of the regimes safeguarding the economic interests of consumers as actors in the market with those safeguarding personal data.

In terms of providers of VLOPs and VLOSEs, the DSA goes further by codifying in Art. 39 an even higher standard of transparency applicable to advertising practices, expressed in the obligation to establish and make available to the public a particular resource in the form of a repository (Ger. A*rchiv*, Fr. *registre*) of the minimum information relating to the advertisement provided. At the same time, the advertising systems used by this category of intermediary service providers constitute a separate factor under Art. 34–35 DSA, which must be taken into account when assessing or mitigating the systemic risk (see Rec. 79 et seq.).

Against the background of the extensive consumer advertising law in the EU[42] today, within which the provisions of a general nature (Directive 2005/29/EC) may be distinguished from the more dispersed, often fragmented sectoral regulations,[43]

[41] See Chapter IV Section 4.4.3.

[42] Its origins may be found in the Community case law developed on the basis of the freedoms enshrined in the Treaties, identified in EU terminology under classic formulas (e.g. *Cassis de Dijon*, *Keck*, *Mars*).

[43] These concern specific products (e.g. food, medicinal products), means of dissemination (e.g. audiovisual media services), or specific content. The latter category includes the provisions of Regulation (EU)

it may be concluded that the DSA constitutes an important addition to the current regime relating to online advertising. Given the multiple functions of advertising as both an informational and a persuasive tool to influence audience behaviour, in the digital environment these provisions have been rightly placed alongside the prohibition of deceptive interfaces (*dark patterns*) referred to in Article 25 DSA[44] and the provision on the use of the systems of recommendation through online platforms as provided for in Art. 27 DSA.

Even if the DSA, as a regulation with a horizontal scope of impact on online intermediaries, limits the notion of advertising to the information presented "by an online platform on its online interface" (Art. 3(r)), and as such does not regulate online advertising comprehensively, given the position of platforms in the digital environment, especially those designated as VLOPs and VLOSEs, the indicated provisions of the DSA play an important role in safeguarding the consumer's right to be informed. Their scope of application will not extend to businesses expressly excluded under Art. 19 DSA, which in turn may lead to the emergence of different standards of due diligence in advertising practices. The doubts which appear in this context seem analogous to those hinted at above when discussing Art. 29 DSA (see Section 3.3.2).

3.4.3. Protection of minors

Another consumer issue raised with regard to the DSA stems from the special treatment of one group of service recipients, namely minors. This question may be regarded as indicative of the implementation of consumer policy goals developed at the early stage of shaping the regulatory framework of the information society,[45] as well as in contemporary EU *soft law*.[46] At the same time, it expresses the EU's increased attention to children's rights,[47] also in the specific context of digital transformation.[48]

2024/900 on political advertising and the proposed rules on environmental marketing (see European Commission, Proposal for a Green Claims Directive, COM(2023) 166 final, Brussels, 22.3.2023).

[44] This provision refers to the design and organisation of online interfaces, which makes it possible to combine it with the previously discussed Art. 31 DSA addressed to B2C online platforms (see Section 3.3.2). At the same time, Art. 25(2) DSA clearly separates the prohibition contained in paragraph 1 from the provisions of Directive 2005/29/EC as well as Regulation (EU) 2016/679 (see Rec. 67–68 of the preamble of the DSA).

[45] See Rec. 4 of the Council Resolution of 19 January 1999 (OJ 1999/C 23/01) emphasizing the importance of "protection of children against unsuitable content" within the issues consumers are particularly concerned by on the verge of a digital era.

[46] See European Commission, New Agenda…, op. cit., pp. 21–22, where the interests of children and minors are included within particularly vulnerable groups of consumers.

[47] See European Commission, EU Strategy on the Rights of the Child (COM(2021) 142 final, Brussels, 24.3.2021), p. 19, where the then draft of the DSA was directly referred to.

[48] In the European Declaration on Digital Rights and Principles for the Digital Decade, the need to protect and empower children and young people in the online environment is highlighted under Chapter 5: Safety, Protection and Empowerment, especially in Art. 20–22.

The provisions of the DSA relating to this group of users of information society services feature an increased standard of due diligence expected of the providers of intermediary services, as illustrated by Art. 14(3) DSA, addressed to all intermediary service providers (see the comments in Section 3.4.1). The standard of transparency provided for in Art. 14(1) DSA has even been strengthened by the introduction of a requirement to 'explain' the conditions and restrictions, combined with a requirement of the comprehensibility of such explanations tailored to an audience consisting precisely of minors. Apart from the lack of a definition of the term 'minor' in EU law,[49] the obligation stipulated in Art. 14(3) DSA is not sufficiently precise, mainly due to the wording used to identify the intermediary service it aims to cover. Indeed, it will only be valid if such a service "is targeted primarily at minors or if it is used predominantly by minors." This, however, is only very perfunctorily explained in Rec. 46 of the preamble to the DSA.

A much clearer formula has been used in Art. 28 DSA, which is one of the provisions addressed to "providers of online platforms accessible to minors." Yet this provision, like Art. 14(3) DSA, is relatively general. After all, the obligation to ensure a high level of privacy, safety and protection of minors does not depart from the presumption of a high level of consumer protection under Art. 169(1) TFEU or Art. 38 of the CFREU. On the other hand, the requirement on online platforms to achieve this objective by "putting in place appropriate and proportionate measures," as stipulated in Art. 28(1) DSA, leaves platforms with a wide margin of discretion, whose boundaries will only potentially be limited by the Commission guidelines listed in Art. 28(4) DSA.

In the same way, as with the relationship between Art. 14(1) and (3) DSA in respect of advertising on platforms, the scope of prohibiting profiling-based advertisements under Art. 26(3) DSA is further reinforced in subsequent Art. 28(2) DSA, which is a consequence of the absence of a restriction regarding the use of special categories of personal data. The severity of this rigour is 'diluted' by the requirement regarding the status of the recipient of the service as a minor (Art. 28(2) DSA), since it has to be read in conjunction with the absence of an obligation to process additional personal data by the platform providers in order to identify the service recipient as a minor (Art. 28(3) DSA).

Given these criticisms and also the fact that the provisions indicated are by no means exhaustive in terms of the protection of minors contained in the DSA,[50]

[49] Council of Europe, European Union Agency for Fundamental Rights, *Handbook on European Law Relating to the Rights of the Child*, Luxembourg 2022, p. 19, https://data.europa.eu/doi/10.2811/610564 (accessed: 3.4.2025).

[50] Explicit references relating to this group of service recipients are included in the provisions addressed to VLOPs and VLOSEs concerning the assessment and mitigation of systemic risk – see Art. 34–35 DSA. See also the awareness campaign conducted under the 'Digital Europe' Programme (DIGITAL), https://www.betterinternetforkids.eu/policy/digitalservicesact (accessed: 3.4.2025).

the DSA constitutes an important step forward by approaching the problem of protecting this particularly vulnerable group of users in the digital environment. At the same time, this regulatory approach may appear similar to that provided by the EU data protection regime (see, in particular, Regulation (EU) 2016/679). After all, the DSA does not limit itself to treating minors solely as consumers in a market (economic) context. This is an obvious consequence of the objective enshrined in its Article 1, and is related to the fact that neither the GDPR nor the DSA is a classic consumer protection regulation (see the comments in Section 3.1 of this chapter).

As regards the protection of vulnerable groups of consumers, however, the DSA proves to be insufficient. While it rightly emphasises the need to protect minors, it almost[51] ignores the interests of those recipients of services who are exposed to certain risks on account of their age (seniors) and who, in view of the rapid digitisation, should also be supported by the EU legislator in achieving a coherent vision of the information society.

3.5. Conclusions

The DSA is undoubtedly a legal instrument responding to the challenges of modern information society within a digital platform economy, in which the providers of intermediary services play a key role, which is turn involves specific responsibilities. It modernises the existing EU rules relating to e-commerce by recognising the interests of consumers distinguished among the recipients of intermediary services. However, in doing so, it does not create a new concept of consumer, but reinforces existing EU *acquis* regarding consumer protection, and in particular builds on the aspiration expressed in EU primary law to ensure a high level of consumer protection in the internal market.

In each case, particular due diligence obligations imposed on providers of indirect services need to be correlated with rights, among which, from the perspective of consumer protection, the right to safety and the right to information (transparency) come to the fore. These protections are implemented through various provisions forming the specific architecture of the DSA which, in this sense, contribute to empowering both consumers and other service recipients.

Specific provisions of the DSA, whether directly addressed to consumers on B2C online platforms or applicable to all recipients of services, and thus creating certain benefits for consumers as well, frequently confirm in a very clear way the implementation of the EU consumer policy guideline expressed in the phrase "what is illegal offline, should be illegal online." Consequently, it is necessary to recognise

[51] Cf. the notion of "average consumer" as adopted in Art. 6(3) DSA precising the boundaries of the liability of online platforms (Chapter III Section 3.3.1).

the dynamic, multifaceted relationship connecting the DSA with the existing *acquis consummateur*. This, however, does not immediately make the DSA a standard instrument of consumer protection law: on the contrary, it tends to justify the need for a new perspective on the legal situation of consumers in the digital environment, the legal framework of which is subject to increasing and intensive development in the EU.

Chapter IV

Rights granted upon digital markets participants by the Digital Markets Act

4.1. Introduction

As discussed in Chapter I (Introduction), the DMA is significantly inspired by EU Competition Law regarding both its regulatory nature and the extent to which the DMA's substantive content is informed by earlier Commission decisions enforcing Art. 102 TFEU. We also outlined that in the course of preparatory works on DSA, the Commission primarily referred to the DMA as "the New Competition Tool," which, on one hand, would rely on the same regulatory engine, but on the other, would be addressed to the largest market players in digital sector only.

At the same time, the DMA and EU competition law differ in their substance. Understanding the differences between the two helps to appreciate how obligations imposed on big tech companies under the DMA may be regarded as rights granted upon users of platform services provided by those companies.

4.2. Key similarities and differences between the DMA and competition law

The first difference concerns subject matter and scope of application. Competition law applies to certain conduct occurring in any given market. Its scope of application is therefore horizontal (or, universal) and not limited to any specific business or legal areas.

Digital markets. On the contrary, the DMA is sector-specific in the sense that it applies to conduct occurring in digital markets, i.e. markets for products and services provided by means of, or through, information society services.[1] More precisely, DMA provisions apply to core platform services[2] provided or offered by gatekeepers.

[1] Art. 1(4) DMA.

[2] The definition on core platform services is provided in Art. 2(2) DMA and includes online intermediation services; online search engines; online social networking services; video-sharing platform services; number-independent interpersonal communications services; operating systems; web browsers; virtual assistants; cloud computing services and online advertising services.

Secondly, competition law applies to undertakings[3] and, with respect to Art. 102 TFEU, to undertakings holding a dominant position in a given market. Dominance is regarded as "a position of economic strength enjoyed by an undertaking, which enables it to prevent effective competition being maintained on the relevant market by affording it the power to behave to an appreciable extent independently of its competitors, customers, and ultimately of its consumers."[4] It is identified by assessing an undertaking's market power, including its market share and market position as well as that of competitors.[5]

Gatekeepers. On the other hand, the DMA is addressed to a precise type of undertaking, namely, gatekeepers. Following Art. 2(1) and 3 DMA, these are undertakings which provide core platform services and are designated as gatekeepers in a dedicated procedure. An undertaking shall be designated a gatekeeper when it meets all the following conditions[6]:

– it has a significant impact on the internal market[7];

– it provides a core platform service which is an important gateway for business users to reach end users[8]; and

– it enjoys an entrenched and durable position in its operations, or it is foreseeable that it will enjoy such a position in the near future.[9]

Thirdly, EU competition law is founded on rather general prohibitions mainly focusing on anti-competitive agreements and abuse of a dominant position. These concepts are then specified in open catalogues of anti-competitive practices specified in Art. 101–102 TFEU. However, competition law has a degree of flexibility in determining, case by case, whether certain conduct falls within the scope of these prohibitions or not. While this approach has clear merits (including the potential to

[3] For every entity engaged in an economic activity. regardless of their legal status and the way in which they are financed, see the judgment of CJEU of 23 April 1991, Case C-41/90, *Klaus Höfner and Fritz Elser v Macrotron GmbH* (ECLI:EU:C:1991:161); R. Whish, D. Bailey, *Competition Law*, Oxford 2021, p. 85.

[4] Judgments of CJEU: of 14 February 1978, Case 27/76, *United Brands Company and United Brands Continentaal BV v Commission of the European Communities* (ECLI:EU:C:1978:22), para. 65; of 13 February 1979, Case 85/76, *Hoffmann-La Roche & Co. AG v Commission of the European Communities* (ECLI:EU:C:1979:36); of 3 July 1991, Case C-62/86, *AKZO Chemie BV v Commission of the European Communities* (ECLI:EU:C:1991:286).

[5] See more in Communication from the Commission, Guidance on the Commission's enforcement priorities in applying Art. 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (OJ C 45, 24.2.2009, pp. 7–20), para. 9 et seq.

[6] Art. 3(1)–(2) DMA.

[7] This criterion is based on financial results obtained by given undertaking. The threshold amounts to turnover of EUR 7.5 billion in each of the last three financial years or average market capitalisation of at least EUR 75 billion in the last financial year. Additionally, to have a significant impact on the internal market, an undertaking needs to provide core platform services in at least three Member States.

[8] This criterion translates into at least 45 million monthly active end users established or located in the Union and at least 10,000 yearly active business users established in the Union.

[9] The condition of durability is met if an undertaking meets the thresholds of end and business users for three years.

identify new forms of infringement or abuse), it has significant implications for the timing and dynamics of proceedings, in which each conduct needs to be assessed against the general infringement criteria.

Precise obligations and prohibitions. At the same time, Art. 5–7 DMA introduce a comprehensive list of precise obligations and prohibitions addressed to gatekeepers. Some are directly inspired by the Commission's decisional practice under Art. 102 TFEU, in which it identified the anti-competitive effects of such practices as self-preferencing or unfair use data available to platforms.

The DMA prohibits gatekeepers from processing, combining or cross-using personal data of end users in certain ways. To avoid further lock-in effects, gatekeepers are also prohibited from preventing business users from offering the same products or services to end users through other platforms. When competing with their business users, gatekeepers shall not use any data that is not publicly available and is generated or provided by those business users during their presence on a given platform. These are just some examples of the precise obligations and prohibitions specified in the DMA. For a comprehensive discussion on these obligations (and how they translate into the rights of business users and end users), see Section 4.5 of the present chapter.

Fourthly, as discussed above, competition law in enforced *ex post*, which requires complex proceedings from the Commission.

Ex-ante *enforcement*. The DMA takes a different approach by introducing *ex-ante* enforcement measures. As follows from Art. 8(1) DMA, these are gatekeepers that shall ensure and demonstrate compliance with the substantive obligations laid down in the regulation being discussed. Additionally, under Art. 11 DMA, gatekeepers shall submit to the Commission, and update annually, compliance reports demonstrating what gatekeepers have done in order to comply with DMA obligations. Under Art. 15 DMA, they shall also submit independently prepared audited descriptions of any techniques used by the gatekeepers in profiling consumers.

The Commission supervises gatekeepers' compliance with DMA obligations. This matter is detailed in Chapter V with regard to DSA and DMA enforcement.

Some authors argue that the DMA's substantive scope is not novel, as it is largely concerns codifying and clarifying prohibitions that already exist in the competition law framework. However, it is generally accepted that the principal added value of the DMA resides in its procedural rather than its substantive aspects. As discussed in this section, the DMA provides enforcers with a new toolbox, allowing them to overcome the limitations of competition law.[10]

[10] O. Andriychuk, *Do DMA Obligations for Gatekeepers Create Entitlements for Business Users?*, "Journal of Antitrust Enforcement" 2023, vol. 11, no. 1, p. 126.

4.3. The Digital Markets Act as a source of platform users' rights

4.3.1. Direct effect of EU competition law

When discussing whether a particular EU primary or secondary law provision may constitute a source of rights granted upon individuals, we evaluate its direct effect. This discussion stems from the earlier days of EU law, when the debate concerned whether the Treaties (and legal acts adopted on their basis) are sources of rights and obligations imposed only on Member States (as is usually assumed in public international law, to which the Treaties belong) or whether individuals may also be addressees of these provisions. Thus, the principle of direct effect means that individuals can derive rights from EU law and can invoke these rights directly in proceedings before national courts.[11]

This principle is often confused with direct applicability, which means that certain pieces of EU legislation are applied in national legal orders in precisely the same shape in which they were introduced by Union legislature. However, provisions that are directly applicable will usually be directly effective, on condition they grant any rights in a clear, precise and unconditional manner.

The direct effect of competition law has been confirmed by the Court of Justice in its settled case law.[12] There is no doubt that the main competition law provisions are directly effective in horizontal relations (among individuals), thus parties to national court proceedings may make competition law claims before these courts. These claims can include e.g. allegations of the invalidity of anti-competitive agreements or action for damages regarding a loss resulting from the application of excessive prices by a party to such anti-competitive agreement.

4.3.2. Direct effect of the DMA

It remains a matter of debate whether the DMA creates any rights (or, entitlements) for business and end users, because this regulation does not include positive rights for these users.[13] On the other hand, this question can be addressed from the perspective of EU law's principle of direct effect.

---

[11] See the judgment of CJEU of 5 February 1963, Case 26/62, *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration* (ECLI:EU:C:1963:1); and subsequent case law regarding the principle of direct effect.

[12] Judgments of CJEU: of 30 January 1974, Case 127/73, *Belgische Radio en Televisie and société belge des auteurs, compositeurs et éditeurs v SV SABAM and NV Fonior* (ECLI:EU:C:1974:6); of 20 September 2001, Case C-453/99, *Courage Ltd v Bernard Crehan and Bernard Crehan v Courage Ltd and Others* (ECLI:EU:C:2001:465).

[13] O. Andriychuk, op. cit., p. 129.

There is no doubt that the DMA, as an EU Regulation, is directly applicable and also enjoys direct effect.[14] Thus, it constitutes a source of rights granted to individuals (business users or end users), which can be invoked directly by those individuals before national courts. Indeed, Rec. 42 DMA reads that to attain the DMA's principal objectives (regarding fairness and contestability of digital markets), it is important to safeguard the right of business users and end users to raise concerns about unfair practices by gatekeepers with any relevant administrative or other public authorities, including national courts.

The direct effect of the Regulation in question is also confirmed by the system of close cooperation between the Commission (the main DMA enforcer) and national courts, as assumed in Art. 39 DMA.

Since the Commission has extensive insight into digital markets (gathered from compliance reports, independent audits, market investigations and presumably data and information provided by third interested parties or complainants), under Art. 39(1) DMA, national courts may request from the Commission any information it possesses or an opinion on a particular case. Although the limits of that provision still need to be verified in practice (e.g. given the confidential nature of some of that information), it clearly confirms that national courts may be vital actors in ensuring the effectiveness of rights granted on users under the DMA.

The Commission will certainly be proactively interested in matters regarding how national courts apply the DMA. In this context, Art. 39(2) DMA obliges Member States to share with the Commission copies of any judgments by national courts issued on the application of this regulation. Additionally, under Art. 39(3) DMA, the Commission may join proceedings before national courts as an *amicus curiae*.

As a result, an infringement of the DMA by a gatekeeper can be subject to private action brought by individuals suffering harm resulting from that misconduct. Since neither the DMA nor any other piece of EU legislation introduces any procedure before national courts for DMA infringements, national procedural laws regulate these matters. Their exact provisions may therefore determine the characteristics and content of exact claims that may be made in such proceedings (e.g. damages, cease-and-desist, interim orders).

To further confirm the DMA's direct effect, Art. 42 DMA extends the applicability of the Representative Actions Directive[15] to representative actions brought

[14] A. Komninos, *Private Enforcement of the DMA Rules before the National Courts*, 5.4.2024, p. 5, http://dx.doi.org/10.2139/ssrn.4791499; F. Bostoen, *Understanding the Digital Markets Act*, "Antitrust Bulletin" 2023, vol. 68, no. 2, p. 303; D. Geradin, *Ensuring DMA Compliance: What Are the Business Users' Options?*, The Platform Law Blog, 28.11.2023, https://theplatformlaw.blog/2023/11/28/ensuring-dma-compliance-what-are-the-business-users-options/ (accessed: 3.4.2025); K. Bania, D. Geradin, S. Huijts, *7 March Is DMA D-Day: What Does This Mean?*, The Platform Law Blog, 7.3.2024, https://theplatformlaw.blog/2024/03/07/7-march-is-dma-d-day-what-does-this-mean/ (accessed: 3.4.2025).

[15] Directive 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, pp. 1–27).

against infringements of DMA provisions by gatekeepers, whereas Art. 43 DMA confirms that the provisions of the EU Whistleblowing Directive[16] shall apply to the reporting of all breaches of the DMA, as well as to the persons reporting such breaches.

A more detailed discussion regarding private enforcement of the DMA appears in Chapter V, which deals with DSA and DMA enforcement. At the same time, it can be argued that the lack of precise DMA provisions on direct effect and private enforcement might undermine the effectiveness of users' rights.[17]

4.4. Beneficiaries of the Digital Markets Act

4.4.1. Introduction

As discussed above, "traditional" commercial relations regularly involve two parties – a seller and a purchaser. In the digital sphere, the marketplace gains more importance, as it is organised and controlled by platforms who often have gatekeeper status.[18] On the one hand, such platforms are merely intermediaries between sellers and purchasers. On the other, however, due to the characteristics outlined in Chapter I, gatekeepers acquire specific power and ability to shape market conditions and structure, impacting the behaviour of other users of a given platform.

In the first set of designation decisions from September 2023, the Commission identified six gatekeepers.[19] These include:

– Alphabet (with respect to: Google Play, Google Maps, Google Shopping, Google Search, YouTube, Android Mobile, Alphabet's online advertising service and Google Chrome)[20] regarding the following core platform services: search, intermediation, ads, video sharing, browser and operating system;

[16] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (OJ L 305, 26.11.2019, pp. 17–56).

[17] R. Podszun, *From Competition Law to Platform Regulation – Regulatory Choices for the Digital Markets Act*, "Economics" 2023, vol. 17, no. 1, article 20220037, p. 10.

[18] See the definition of a gatekeeper in Section 4.2 of the present chapter.

[19] See: https://digital-markets-act.ec.europa.eu/gatekeepers_en; note that this list may be further extended and thus, in May 2024, the Commission designated Booking.com as a gatekeeper and continued its proceedings with respect to designation of social network service X (former Twitter).

[20] Commission Decision of 5 September 2023 designating Alphabet as a gatekeeper pursuant to Art. 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (Cases DMA.100011 – Alphabet – OIS Verticals, DMA.100002 – Alphabet – OIS App Stores; DMA. 100004 – Alphabet – Online search engines; DMA.100005 – Alphabet – Video sharing; DMA.100006 – Alphabet – Number-independent interpersonal communications services; DMA.100009 – Alphabet – Operating systems, DMA.100008 – Alphabet – Web browsers; DMA.100010 – Alphabet – Online advertising services) (OJ C, 2023/549, 27.10.2023).

– Amazon (with respect to Marketplace and Amazon Advertising)[21] regarding intermediation and ads;

– Apple (with respect to AppStore, iOS and Safari[22] and further iPadIOS) regarding intermediation, browser and operating system;

– ByteDance (with respect to TikTok)[23] regarding social network core platform service;

– Meta (with respect to Facebook Marketplace, Facebook, Instagram, WhatsApp, Messenger and Meta Ads)[24] regarding social networks, number-independent interpersonal communication services, intermediation and ads;

– Microsoft (with respect to LinkedIn and Windows PC OS)[25] regarding social network and operating system core platform services.

Platforms, or gatekeepers, serve two types of customers. Firstly, business users offer their services or products to consumers on gatekeepers' marketplaces. Thus, they are customers to a platform (receiving a given marketplace service) and service providers to consumers. In this second role, they often compete with gatekeepers on these downstream markets. For instance, Apple has been designated by the Commission as a gatekeeper in such fields as providing its online intermediation service, the App Store. At the same time, it is present on the App Store with its music streaming application, Apple Music. Parallelly, business users such as Spotify, an independent music streaming application, are present in the App Store and reach consumers with their offer while remaining in competition with Apple Music.

---

[21] Commission Decision of 5 September 2023 designating Amazon as a gatekeeper pursuant to Art. 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (Cases DMA.100018 Amazon – online intermediation services – marketplaces; DMA.100016 Amazon – online advertising services) (OJ C, 2023/905, 15.11.2023).

[22] Commission Decision of 5 September 2023 designating Apple as a gatekeeper pursuant to Art. 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (Cases DMA.100013 Apple – online intermediation services – app stores; DMA.100025 Apple – operating systems and DMA.100027 Apple – web browsers) (OJ C, 2023/548, 27.10.2023).

[23] Commission Decision of 5 September 2023 designating ByteDance as a gatekeeper pursuant to Art. 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (Case DMA.100040 ByteDance – Online social networking services) (OJ C, 2023/552, 27.10.2023).

[24] Commission Decision of 5 September 2023 designating Meta as a gatekeeper pursuant to Art. 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (Cases DMA.100020 Meta – online social networking services; DMA.100024 Meta – number-independent interpersonal communications services; DMA.100035 Meta – online advertising services; DMA.100044 Meta – online intermediation services – marketplace) (OJ C, 2023/1092, 23.11.2023).

[25] Commission Decision of 5 September 2023 designating Microsoft as a gatekeeper pursuant to Art. 3 of Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector (Cases DMA.100017 Microsoft – online social networking services; DMA.100023 Microsoft – number-independent interpersonal communications services; DMA.100026 Microsoft – operating systems) (OJ C, 2023/549, 27.10.2023).

Secondly, there are end users that are at the same time customers to both platforms (from whom end users receive search services, social media or any other core platform service) and business users (receiving offers on specific services or products).

In such a setting, when gatekeepers are not constrained by any other market players in core platform services, they may be incentivised to engage in conduct harming business users (e.g. through 'self-preferencing', i.e. reducing the visibility of business users' offer to the benefit of their own offer) as well as end users (e.g. by use of algorithms giving visibility preference to sponsored search results over more accurate ones).

Therefore, understanding the characteristics and scope of rights introduced in the DMA requires considering the features and roles of both types of platform service users. These rights can be now invoked (enforced) with respect to gatekeepers and areas as identified in the designation decisions.

4.4.2. Business users

Article 2(21) DMA defines a business user as any natural or legal person acting in a commercial or professional capacity using core platform services for the purpose of, or in the course of, providing goods or services to end users.

As discussed, business users play a dual role on digital platforms in performing their economic activities. Firstly, they offer goods or services to their customers as in any other commercial model. Secondly, however, they do so via online platforms served by gatekeepers. Therefore, any engagement in presenting an offer or concluding a transaction with an end user is conditional on becoming the gatekeeper's customer.

Given the characteristics of digital (or online platforms) sector already discussed, business users are largely dependent on gatekeepers when conducting their activities online. The T&C, as well as the actual performance of platform services significantly impact business users' visibility in the marketplace, their ability to reach consumers with their offer and, in consequence, the profitability of the business.

Following this market power asymmetry, regardless of their efforts, business users will generally be unable to question in an effective manner the conditions imposed on them by gatekeepers. In the event of gatekeepers being present on downstream markets and competing there with business users, they gain a significant competitive advantage based on a number of different factors (from access to data related to market behaviours or regarding the commercial performance of their downstream competitors through to the capacity to navigate streams of end users' attention based on offerings' visibility algorithms).

Such unequal competition, accompanied by a lack of specific regulation, may incentivise gatekeepers to adopt unfair practices against business users. In the long run, such practices may change the market structure by eliminating certain business users from the market, with their market position consequently being taken over by gatekeepers. In other words, gatekeepers may leverage the market power they enjoy on a given market to another market where they are only starting to develop their presence. In turn, such a restriction of competition will result in limiting consumers' choices as well as reducing the quality (reliability) of the services offered by the gatekeeper in that new market.

This can be illustrated using the example of the *Google Shopping* case. Google already enjoyed a very significant position in the market for general search services. Under the Google Shopping brand it had also entered a new market for comparison shopping services (CSS), in which some other market players were already present. However, by granting significant preference to its own service over other CSS providers in presenting search results on the general online search service, Google managed to strengthen Google Shopping's position in the CSS market and gradually (but significantly) restrict the presence of other CSS providers. Eventually, if nowadays consumers want to compare prices of goods or services available online, they will use Google search service and only rarely rely on other providers of such price comparison websites. Having such limited alternatives, consumers cannot be sure whether they are indeed being presented with the best offer or if specific visibility algorithms are influenced by non-objective factors.

The definition of business users does not depend on any other factors or thresholds. Thus, this category will be very broad and may range from small and medium-sized enterprises up to large multinational companies. Moreover, online platforms (including VLOPs under the DSA or gatekeepers under the DMA) or other intermediaries can be the business users of other core online platform services provided by gatekeepers. This includes such examples as Spotify being a business user on App Store (provided by Apple being a designated gatekeeper) or Facebook and Instagram applications (by Meta, designated as a gatekeeper with regard to social networks) being the business users of either iOS or Google Android, run by Apple and Alphabet (Google) respectively, designated as gatekeepers for operating systems services.

4.4.3. End users

The end user is defined by Art. 2(20) DMA as any natural or legal person using core platform services other than as a business user. End users can be assimilated with consumers or final customers, as they act on platforms in capacities other than

commercial or professional and within their presence they only receive (and not offer) goods or services offered by other parties.

While many DMA substantive provisions seem to focus on strengthening business users' position *vis-à-vis* gatekeepers, end users' welfare remains a key foundation of the DMA. Several gatekeepers' obligations are justified in the DMA's preamble, covering the need to improve or ensure adequate choice for end users. This applies, for instance, to the access of other service providers to certain operating systems (Rec. 57 DMA) or access to data, as well as encouraging multi-homing among different platforms (Rec. 59 DMA).

Safeguarding end users' choice (and therefore rights) is directly linked to the DMA's principal goals. Indeed, Rec. 107 DMA reads that the objectives of that regulation include ensuring "a contestable and fair digital sector in general and core platform services in particular, with a view to promoting innovation, high quality of digital products and services, fair and competitive prices, as well as a high quality and choice for end users in the digital sector."

End users therefore assume a dual consumer role: they purchase goods or services from business users on online platforms, but at the same time, they are non-commercial users of these platforms, interested in obtaining access to different categories of content (that can be both commercial and non-commercial).

It is not the DMA's goal to protect consumers (end users) from unfair practices undertaken by their immediate commercial partners (business users), as other acts of EU consumer law cover this aspect. Therefore, potential claims that end users base on the DMA will be raised against gatekeepers. However, the threefold nature of the digital sector (and the role of business users in that setting) impacts the sphere of consumers' rights and contributes to the conclusion that end users may invoke their DMA rights against gatekeepers. For instance, Art. 5(3) DMA prohibition for gatekeepers to prevent business users from offering the same products or services to end users through third-party online platforms seems to be equally invocable by business or end users.

4.5. Rights included in the DMA

4.5.1. Gatekeepers' obligations

As outlined in this chapter, Art. 5–7 DMA introduce a set of obligations and prohibitions addressed to gatekeepers. In that sense, they form the DMA's substantive part.

The obligations included in Art. 5 DMA are considered to be "self-executing," whereas Art. 6–7 DMA introduce obligations that may be further specified by the

Commission in a delegated act, which may impose measures that the gatekeeper concerned is to implement in order to effectively comply with these obligations.[26]

While some authors question whether these obligations translate automatically into users' entitlements,[27] we assume that given the DMA's direct effect, it can be regarded as source of rights granted upon business and end users. However, the nature of these obligations will determine two aspects.

The first is whether one may indeed derive rights from all of these obligations. In this context, we follow the conclusion that all specific substantive provisions meet the requirements of direct effect and can be regarded as sources of rights for business users or platform users.[28]

The second aspect concerns which type of users (business, end or both) may benefit from specific rights when invoking them before national courts or authorities. Provisions proclaiming gatekeepers' obligations are rather lengthy and often employ technical wording. In this section, we divide them into obligations corresponding with rights enjoyed by (1) both types of users and (2), predominantly business users.[29]

Within that division, we identify groups of obligations and rights that have similar subject matter or features (e.g. use of data) in order to discuss them in a more thematic way. It follows from this division that we consider most of the rights introduced by the DMA to cover both end users and business users. However, in practical cases, it might transpire that courts or authorities do not follow this suggested approach and take a different view with respect to the beneficiaries of a specific provision.

4.5.2. Rights enjoyed by both business as well as end users

4.5.2.1. Use and access to users' data

The DMA chiefly focuses on the use of and access to data by gatekeepers and other market participants. Indeed, one may claim that today's competition in digital markets is "all about data" and many market flaws in the digital sector stem from gatekeepers having access to data otherwise unavailable. This includes data of business users present on a given platform or generated by them (e.g. market strategies), as well as that of end users (e.g. customers behaviour).

[26] Art. 8 DMA, see also: F. Bostoen, op. cit., pp. 280–281.

[27] O. Andriychuk, op. cit.

[28] A. Komninos, op. cit., p. 5.

[29] While the DMA includes rights dedicated solely to end users, these are correlated with similar business users' rights (see example of Art. 5(4) and (5) DMA discussed under anti-steering section). Due to this close functional link, we categorise these rights as being granted to both types of users.

Certainly, following the gatekeepers' dual role discussed earlier (marketplace organisers and active participants, at the same time), they obtain access to data not available to other users and from which one may read a wealth of competitively sensitive information. This leads to classical information asymmetries, providing gatekeepers with an unprecedented competitive advantage over business users, since gatekeepers will always be able to see sensitive information on their competitors' market performance (clients portfolio, sales data, pricing policy, other aspects of market behaviour). At the same time, gatekeepers obtain advantages over end users, as they might direct their interest to particular offers in a scope and manner not attainable under conventional market circumstances.

In this context, Art. 5(2) (a) DMA prohibits processing, for the purpose of online advertising, personal data of end users that are using other business users' services on a given gatekeeper's platform. Art. 5(2) (b) and (d) DMA proclaim prohibition of combining personal data from a given core platform service provided by a gatekeeper (e.g. social media) with other data obtained from either other gatekeeper's services (e.g. marketplace) or from third-party services (e.g. online store). Finally, Art. 5(2) (c) prohibits gatekeepers from cross-using personal data from the relevant core platform service in other services provided separately by the gatekeeper (for instance, data obtained from an online search engine may not be used in other services such as online maps, e-mail accounts etc.).

Data negative obligations (or prohibitions) are elaborated in Art. 6 DMA. Its paragraph 2 prohibits the use of business users' data to compete with these users. This prohibition applies to data not publicly available and which is generated by business users on a given platform or result from their presence in that platform.

Further, Art. 6(9) DMA ensures end users' data portability. This means that end users, at their request and free of charge, are able to obtain and transfer elsewhere (e.g. to other operating system or other social media service) data that they generated by using gatekeeper's platform. Similarly, under Art. 6(10) DMA, business users are granted access to self-generated data from a given core platform service.

Additionally, Art. 6(11) DMA requires that any third-party providing online search engines may request access to data regarding ranking, query, click and views in relation to free and paid search generated by end users on that party's online search engines. This access needs to be granted on fair, reasonable and non-discriminatory terms.

Figure 5 summarises key users' rights reflected in obligations on the use and processing of data by gatekeepers.

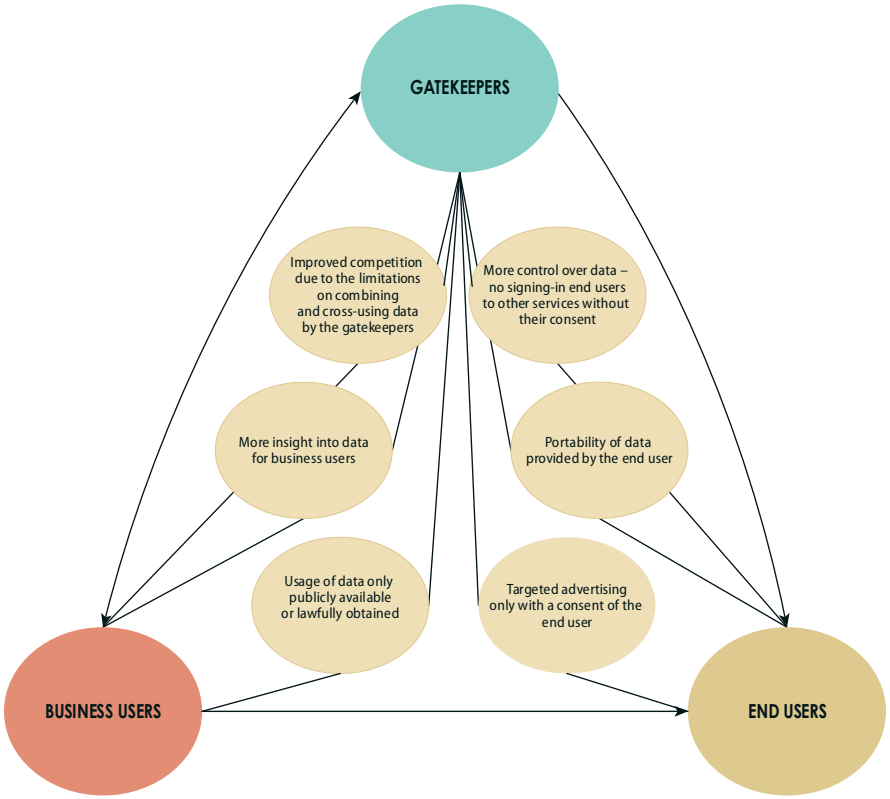


Figure 5: Key users' rights regarding use of data

4.5.2.2. Interoperability and similar rights

Interoperability is one of key factors ensuring that competition is not distorted by high entry barriers imposed by incumbents (or gatekeepers) and that markets therefore remain contestable. It guarantees that if new software or an online service (e.g. online application) is developed, it will be available to users of the main operating systems, for example.

In this context, Art. 6(7) DMA obliges gatekeepers to ensure effective interoperability with and access to (with the aim of granting interoperability) hardware and software features accessed or controlled via the operating system or virtual assistant to the same extent as they are available to services or hardware provided by the gatekeeper. Thus, providers of hardware and providers of services shall obtain access free of charge to markets arising from ecosystems created by gatekeepers.

The interoperability obligation is also reflected in Art. 6(6) DMA, which prohibits gatekeepers from restricting, technically or otherwise, the ability of end users to switch between different software applications and services that are accessed by when using the gatekeeper's core platform services.

Article 6(3) and (4) DMA further seeks to ensure access for third-party service providers. The former provision requires that when using a gatekeeper's operating system, end users may easily uninstall any software applications that are not essential for that system or the device on which they are installed to function. It also requires that end users may easily change any default settings on the operating system, virtual assistant and web browser of the gatekeeper that direct or steer end users towards products or services provided by the gatekeeper. By having the possibility to easily uninstall gatekeeper's applications, end users will have incentive to use competing apps provided by third parties, or business users.

As the second step in that context, Art. 6(4) DMA provides for a gatekeeper to allow and technically enable the installation and effective use of third-party software applications or software application stores using, or interoperating with, its operating system, and allow those software applications or software application stores to be accessed by means other than the relevant core platform services of that gatekeeper.

Moreover, Art. 5(7) DMA guarantees that both end users and business users are free to decide on the cross-use and interoperability of given online services with services provided by gatekeepers. More specifically, the provision enables users to act on gatekeepers' platforms independently of their services such as web browser engines, identification services or payment services.

4.5.2.3. NI-ICS interoperability

Article 7 DMA is devoted entirely to the obligation for gatekeepers to ensure interoperability of number-independent interpersonal communications services (NI-ICS). NI-ICS are understood as interpersonal communications services that do not connect with publicly assigned numbering resources, namely, a number or numbers in national or international numbering plans, or which do not enable communication with a number or numbers in national or international numbering plans.[30] Examples of such NI-ICS include Messenger, WhatsApp, Signal or Telegram.

As explained in Rec. 64 DMA, the lack of interoperability allows gatekeepers that provide NI-ICS to benefit from strong network effects, which contributes to the weakening of contestability. Moreover, gatekeepers often provide NI-ICS as part of their platform ecosystems (such as historically Messenger for Facebook or

[30] Art. 2(7) Directive 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, pp. 36–214).

Direct Messages for Instagram), which constitutes another significant entry barrier in those markets.

Therefore, Art. 7 DMA requires that when a gatekeeper provides NI-ICS that are listed in the designation decision, it shall make the basic functionalities of its NI-ICS interoperable with the NI-ICS of other providers offering or intending to offer such services in the Union. More specifically, a gatekeeper shall make at least the following basic functionalities interoperable where the gatekeeper itself provides those functionalities to its own end users.

Firstly, following the listing in the designation decision, gatekeepers ensure end-to-end text messaging between two individual end users, as well as the sharing of images, voice messages, videos and other attached files in end-to-end communication between two individual end users. Secondly, within two years of designation, gatekeepers ensure the same for group chats (i.e. end-to-end text messaging within groups of individual end users plus the sharing of images, voice messages, videos and other attached files in end-to-end communication between a group chat and an individual end user). Thirdly, within four years of designation, gatekeepers ensure end-to-end voice and video calls between two individual end users as well as between a group chat and an individual end user.

4.5.2.4. Cross-platform access to content, anti-steering and tying

Articles 5(4) and (5) DMA prohibit so-called 'anti-steering' and 'supporting' measures being imposed by gatekeepers. Firstly, business users may, free of charge, communicate and promote offers to end users acquired via gatekeeper's platforms or through other channels, and to conclude contracts with those end users, regardless of whether they use the core platform services of the gatekeeper for that purpose. Offers communicated by business users via gatekeepers' platforms may include conditions different to those proposed by these business users on gatekeepers' platforms.

Equally, end users have the right to access and use services content, subscriptions, features or other items through gatekeeper's core platform by using a business user's software application, including situations where those end users acquired such items from the relevant business user without using the core platform services of the gatekeeper.

In line with Art. 5(8) DMA, gatekeepers shall not place conditions on end users or business users in terms of using, accessing, signing up for or registering with any of gatekeepers' core platform services upon the requirement that they subscribe to or register with other core platform services provided by these gatekeepers. Therefore, gatekeepers are prohibited from leveraging their market power in a given core platform service on another service by artificially increasing the number of

users (which would strengthen the network effects and may eliminate competition among these services).

4.5.2.5. Most Favoured Nation

The DMA also includes another measure inspired by general competition law and corresponding with the rights conferred upon both business and end users. Art. 5(3) DMA stipulates that gatekeepers shall not prevent business users from offering the same products or services to end users through third-party platforms or through their own direct online sales channel at prices or conditions that differ from those offered through the online intermediation services of the gatekeeper. Such practices are often referred to as most favoured nation (MFN) clauses, meaning that granting an advantage to one party equates with granting the same advantage to the other.

Such attempts to hinder the visibility of other platforms or channels of distribution clearly seek to further concentrate a given market around one gatekeeper and eliminate competition.

4.5.2.6. Effectiveness and termination

The general effectiveness of users' rights is secured by two other DMA provisions. While these have different subject matter, they do include horizontal safeguards for both business users and end users.

Firstly, Art. 5(6) DMA states that gatekeepers may not, directly or indirectly, prevent or restrict business users or end users from raising any issue of non-compliance with the relevant law by the gatekeeper with any relevant public authority (including national courts) related to any practice of the gatekeeper.

Secondly, Art. 6(13) DMA prohibits gatekeepers from introducing disproportionate general conditions for terminating the provision of any core platform services (e.g. effective terminating the user's account on social media service cannot be subject to excessive conditions). In this context, gatekeepers also need to ensure that the conditions of termination can be exercised without undue difficulty.

4.5.3. Business users' rights

4.5.3.1. Self-preferencing

Article 6(5) DMA prohibits self-preferencing by gatekeepers. They shall not treat their own services and products more favourably, in ranking and related indexing

and crawling, than similar services or products offered by a third party. Moreover, the gatekeeper shall apply transparent, fair and non-discriminatory conditions to such ranking.

Self-preferencing is particularly harmful in terms of enhancing negative market tendencies in the digital sector, as outlined in this chapter. It may lead to further vertical integration of gatekeepers, leveraging their power on other markets and thus restricting competition. It was also one of the first practices identified and prohibited by the Commission when enforcing EU competition law in the *Google Shopping* case. The course of self-preferencing practices is explained in the Figure 6.

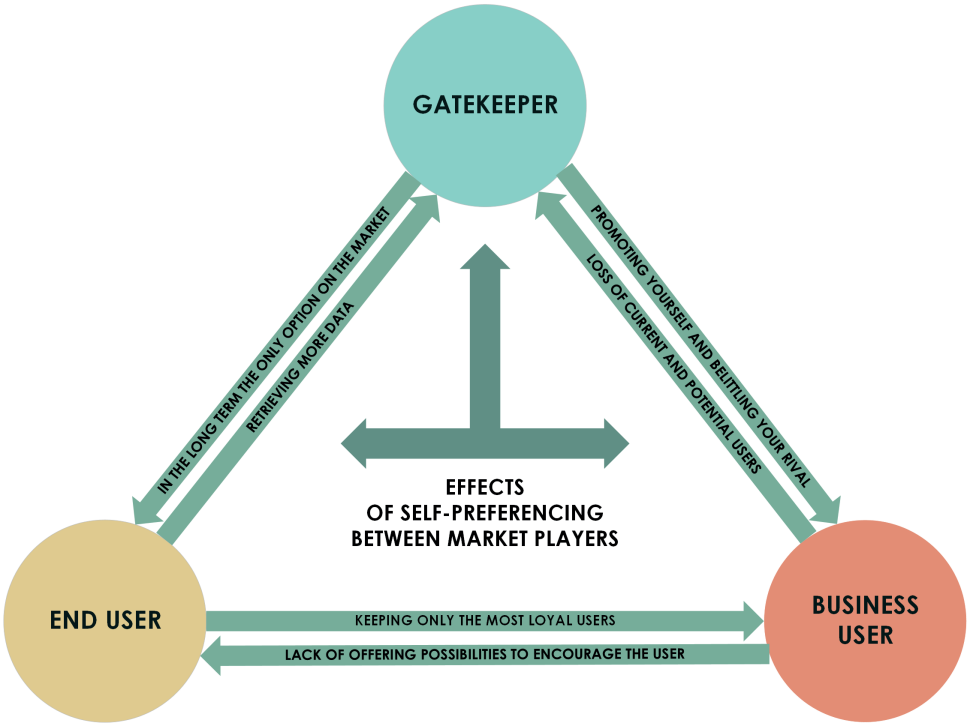


Figure 6: Self-preferencing

4.5.3.2. Access to application stores on FRAND conditions

Article 6(12) DMA requires a gatekeeper to apply fair, reasonable, and non-discriminatory (FRAND) general conditions of access for business users to its software application stores, online search engines and online social networking services listed in the designation decision.

4.5.3.3. Online advertising

The other two obligations concern the gatekeeper's capacity to provide online advertising services. In terms of information, gatekeepers enjoy a particular advantage over advertisers and publishers regarding such aspects as actual reach and the effectiveness of specific online advertising tools. As a result, this market has become particularly non-transparent for market players other than gatekeepers. Thus, Art. 5(9) and (10) DMA provides specific obligations (and respective rights) regarding advertisers' (and publishers') access to information on a daily basis and free of charge, concerning each advertisement placed by the advertiser within the online advertising services provided by gatekeepers.

Article 6(8) DMA introduces further information obligations for gatekeepers when providing online advertising services. It requires a gatekeeper to provide advertisers and publishers (upon their request and free of charge) with access to the gatekeeper's performance measuring tools and the data necessary for advertisers and publishers to carry out their own independent verification of the advertisements inventory, including aggregated and non-aggregated data.

4.6. Conclusions

The Digital Markets Act is part of the broader EU regulatory framework towards 'big tech companies'. It aims to improve contestability and fairness of digital markets and, consequently, ensure that these markets remain accessible for individuals willing to undertake and develop their businesses. Although the DMA belongs to the internal market legal framework, it takes significant inspiration from established practice in EU competition law.

Substantively, the DMA introduces precise rules addressed to the largest big tech companies, designated by the Commission as gatekeepers. As discussed in this chapter, specific obligations and prohibitions binding upon gatekeepers concern aspects such as the use of personal data or ensuring interoperability between different systems available in digital markets.

These obligations involve introducing (subjective) rights conferred upon the users of core platform services served by gatekeepers. Business users benefit from these rights in order to be able to offer, on fair and equal grounds, their goods and services in digital platforms, which became the main marketplace. At the same time, rights conferred upon end users (consumers) predominantly seek to ensure that end users obtain the appropriate choice, quality and prices of digital services.

Chapter V

Enforcement and judicial protection of users in the digital market

5.1. Introduction

Full effectiveness of is one of the key principles of EU legal order/system. According to the Court's established case law,[1] this principle requires that, in specific contexts, individuals are be able to invoke their rights derived from EU legislation or claim damages for infringement of these rights. In the former chapters, we discussed what rights are granted to users of online platforms from both the DSA and DMA, and full effectiveness of these rights depends on design of the legal framework for their enforcement. In other words, it depends on the scope and availability of legal measures, both substantive and procedural, allowing certain obligations to be executed from online platforms and specific users' rights to be claimed.

Essentially, enforcement might be performed in two ways: by public authorities or by individuals (users) themselves, who make certain claims in proceedings before national courts or through recourse to other available legal measures.

Public enforcement. Thus, by public enforcement we understand situations in which certain public authorities are granted competence to oversee legal obligations and to impose specific measures or to order particular behaviour, with a view to ensuring that a supervised entity (e.g. an online platform) complies fully with the law (either the DSA or DMA). Different legal acts have distinct enforcement systems: from centralised (e.g. sole competence by the European Commission), through hybrid (enforcement by both the Commission and national authorities), to decentralised (enforcement by national authorities only).

Private enforcement. When discussing private enforcement, we focus on users (individuals) who themselves derive certain rights from a legal act (DSA or DMA) and request that an online platform comply with that legislation. If such a request proves unsuccessful, private parties may wish to enforce their rights by initiating proceedings before national courts or through recourse to other methods, such

[1] See judgements of CJEU: of 9 March 1978, Case C-106/77, *Amministrazione delle Finanze dello Stato v Simmenthal SpA* (ECLI:EU:C:1978:49), para. 16; of 19 June 1990, Case C-213/89, *The Queen v Secretary of State for Transport, ex parte: Factortame Ltd and Others* (ECLI:EU:C:1990:257), para. 19; of 20 September 2001, Case C-453/99, *Courage Ltd v Bernard Crehan and Bernard Crehan v Courage Ltd and Others* (ECLI:EU:C:2001:465), paras. 25–26.

as alternative dispute resolution systems. In such proceedings, users may request a national court order enforcing certain behaviour upon an online platform, but they also may claim compensation of a loss incurred as a result of a DSA/DMA infringement.

Enforcement models vary across EU sector-specific legislation. For public enforcement, we may identify conferral of different powers upon the Commission or competent national authorities. In the latter case, the scope of their competence may be expressly regulated in EU legislation or be stipulated in national law. Private enforcement may also be regulated to a different extent depending on specific legislative area. In many instances, the scope of harmonisation is scarce, thus leaving considerable regulatory discretion for Member States and their national legal systems.

Therefore, in this chapter we discuss the following: public enforcement of the DMA with primary role of the European Commission; public enforcement of the DSA with exclusive competence of the Commission to enforce special obligations of VLOPs and VLOSEs and the key role of Digital Services Coordinators (DSCs) with respect to other platforms. We address different means of redress available to a user, and the role of the DSCs in different areas of ensuring compliance with due diligence obligations. We then move on to discuss the possibilities of private enforcement of both the DSA and DMA.

5.2. Public enforcement of the Digital Markets Act

5.2.1. Introduction

As discussed in Chapter IV (Rights granted upon digital markets participants by the Digital Markets Act), introducing *ex-ante* enforcement measures into the DMA is a key added value when compared to general competition rules. Indeed, enforcement of competition law takes place *ex post*, i.e. after the alleged infringement occurs, and is identified by a competent authority. However, that model is particularly ineffective in digital markets due to the dynamics and structure of this sector.[2]

Therefore, the DMA introduces a set of measures that seek to ensure that big tech companies are more proactive in terms of reporting their compliance to the Commission. It also equips the Commission with specific competences to conduct market investigations. As a consequence, the Commission obtains a more transparent overview of digital markets in "real time," instead of seeing the full picture only after the consequences of a given infringement occur.

[2] O. Andriychuk, *The Digital Markets Act: Tailoring the Tailors*, in: K. Tyagi, A.K. Sanders, C. Cauffman (eds.), *Digital Platforms, Competition Law and Regulation*, Oxford, New York, and Dublin 2024, p. 44 et seq.

Most enforcement measures correspond with the already discussed substantive part of the DMA, i.e. its Art. 5–7, which also constitute sources of rights for business and end users of gatekeepers' platform services. In this handbook, our focus is on users' rights, and we concentrate on this perspective when discussing enforcement measures.[3]

It is noteworthy that Art. 8 DMA provides for a general obligation for gatekeepers to "ensure and demonstrate" their compliance with Art. 5–7 DMA. Therefore, firstly, gatekeepers shall introduce all necessary measures ensuring effective compliance with specific obligations as well as with the DMA in general. Secondly, and as a consequence of the first point, gatekeepers also need to be able to demonstrate that they have implemented all the necessary measures and that these measures are indeed effective.

Within that framework, the Commission may initiate proceedings to verify gatekeeper compliance with their obligations, and also specify these obligations by adopting a particular implementing act.

At the same time, pursuant to Art. 8(3) DMA, gatekeepers may request the Commission to engage in consultations and verification if measures that gatekeepers intend to implement effectively secure compliance with the DMA. While the Commission enjoys discretion in deciding whether it engages in such a dialogue, the solution discussed here introduces a framework for good-faith cooperation and transparency in relations between gatekeepers and the authority.[4]

5.2.2. Specific elements of *ex-ante* enforcement

In this section, we discuss particular measures introduced by the DMA which seek to proactively ensure the transparency of gatekeepers' platforms *vis-à-vis* the Commission, platform users and the society.

Compliance reports. Article 11 DMA stipulates that gatekeepers shall provide the Commission with "a report describing in a detailed and transparent manner the measures it has implemented to ensure compliance with the obligations laid down in Art. 5, 6 and 7" of the DMA. The report must be submitted within 6 months of designation as a gatekeeper and then updated annually.

The aim of this measure is to ensure that the Commission, as the DMA's enforcer, has a complete and updated overview of the specific actions undertaken by

[3] For a comprehensive discussion regarding DMA enforcement, see ibidem; D. Zimmer, J.F. Göhsl, *Enforcement of the Digital Markets Act*, Verfassungsblog 2024, https://verfassungsblog.de/enforcement-of-the-digital-markets-act/ (accessed: 3.4.2025).

[4] It also is a novel solution when compared to general competition rules, which are based solely on self-assessment and under which one may not consult with the Commission compliance of the envisaged conduct.

the gatekeepers in response to their DMA obligations. The reports need to identify concrete obligations, on the one hand, and specific measures undertaken to ensure compliance, on the other. This allows the Commission to assess the efficiency of gatekeepers' endeavours in real time.

Gatekeepers also need to provide the Commission with non-confidential versions of the reports, which are made public.[5] As with transparency reports under the DSA, these versions of compliance reports ensure the transparency of gatekeepers' conduct towards the wider public. This facilitates better oversight and verification of a gatekeeper's DMA compliance by other organisations or individuals, including business or end users.

The first collection of compliance reports was submitted to the Commission in March 2024. Some gatekeepers received criticism for having delivered documents that are too brief and overly general.[6] Clearly, the Commission needs to work with gatekeepers on the appropriate approach towards these reports, even though it has already provided specific guidance in the procedural implementing regulation[7] and by proposing a compliance report template.[8]

Independent audits. Gatekeepers also have a specific transparency obligation with respect to any techniques they apply for profiling[9] consumers in their platform services. If gatekeepers engage in such conduct, they are required to submit an independently audited report to the Commission on that matter.

As in the case of compliance reports, audits regarding consumer profiling need to be submitted within 6 months of a gatekeeper being designated and updated annually. They also need to be accompanied with a non-confidential version that is shared publicly. Thus, users and any other parties may learn from the reports how their data is processed and verify compliance of this conduct with the DMA and other relevant legislation.

Compliance function. Furthermore, gatekeepers are obliged to introduce a compliance unit into their corporate structure. This needs to be endowed with sufficient

[5] See the Commission's dedicated website: https://digital-markets-act-cases.ec.europa.eu/reports/compliance-reports (accessed: 3.4.2025).

[6] See e.g. Apple's report containing only 12 pages of rather general statements: https://www.apple.com/legal/dma/dma-ncs.pdf (accessed: 3.4.2025).

[7] Commission Implementing Regulation (EU) 2023/814 of 14 April 2023 on detailed arrangements for the conduct of certain proceedings by the Commission pursuant to Regulation (EU) 2022/1925 of the European Parliament and of the Council (OJ L 102, 17.4.2023, pp. 6–19).

[8] Available at https://digital-markets-act.ec.europa.eu/legislation_en (accessed: 3.4.2025).

[9] Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements; as defined in Art. 4(4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, pp. 1–88).

independence, authority, stature, resources and access to the management body in order to monitor the gatekeeper's DMA compliance effectively. The compliance unit monitors and supervises gatekeeper compliance with the DMA, and reports its findings directly to the management body. Moreover, it cooperates with the Commission in ensuring that a gatekeeper fully complies with the DMA.

Market investigations. The Commission may conduct a market investigation in three specific instances: with a view to designating a gatekeeper; into systemic non-compliance by a gatekeeper; and investigating new services or new practices in digital sector. Users may submit observations in such proceedings, which may reinforce the effectiveness of their rights.

Non-compliance proceedings concern investigating whether a gatekeeper has infringed any of its substantive obligations as laid down in Art. 5–7 DMA. The Commission initiates the proceedings *ex officio*, but they can be inspired by inconsistencies in compliance reports, e.g. with complaints from platform users or observations that users attempt to enforce their rights privately before national courts. Article 27 DMA expressly encourages third parties, including business users, end users and competitors of gatekeepers, to inform the Commission about any alleged DMA non-compliance.

In other market investigation proceedings, the Commission may follow up on developments in the digital sector. Such developments may include identifying new core platform services (requiring a gatekeeper to be designated) or new anti-competitive types of conduct by gatekeepers.

5.2.3. Non-compliance proceedings and decisions

If *ex-ante* measures prove insufficient, the Commission may open proceedings with a view to adopting a non-compliance decision. Such matters are procedurally similar to general competition law cases. Thus, in the course of the proceedings, the Commission enjoys "regular" competences that allow for gathering relevant evidence, including powers to request information, carry out interviews and take statements, or conduct inspections (so-called 'dawn-raids').

Moreover, the Commission may impose interim measures in urgent cases arising from the risk of serious and irreparable damage to business or end users. By interim measures, the Commission may compel a gatekeeper to undertake any necessary conduct required to protect the other party's interests until the final decision is delivered.

Systemic non-compliance proceedings may be concluded with a decision that, contrary to preliminary concerns, the gatekeeper did in fact comply with the DMA. Alternatively, the Commission may adopt implementing acts (decisions) (1) imposing remedies on the gatekeeper; (2) imposing certain commitments on

the gatekeeper; or (3) declaring the gatekeeper's non-compliance with a given DMA provision.

Remedies may be imposed if, due to non-compliance, a gatekeeper has strengthened or extended its position in relation to the requirement to designate that gatekeeper. Remedies may include measures that are behavioural (i.e. requiring certain behaviour, such as granting access to application store for application developers) or structural (e.g. divestment of certain business) in nature.[10]

Commitments can be proposed by a gatekeeper in the course of non-compliance proceedings. In essence, they need to address preliminary concerns expressed by the Commission and ensure that the alleged non-compliance is brought to an end. As a result, the Commission may accept the proposed Commitments (or negotiate their exact shape with the gatekeeper) and include them in a decision binding upon the gatekeeper.

Non-compliance decisions are adopted when the Commission finds that a gatekeeper does not comply with: (1) obligations from Art. 5–7 DMA; (2) specific measures imposed on a gatekeeper; (3) remedies; (4) interim measures; or (5) commitments made legally binding upon that gatekeeper.

Fines. A non-compliance decision may include a fine of 10% of the gatekeeper's total worldwide turnover in the financial year preceding the decision. This 10% level, also used in competition law, is believed to be extremely high and to have a deterrent function. For repetitious infringements, the DMA foresees an increase in the fine of up to 20% of the gatekeeper's turnover.[11]

5.3. Public enforcement of the Digital Services Act

5.3.1. Competent authorities and Digital Services Coordinators

The DSA imposes several due diligence obligations with the aim of protecting users in relations with intermediary service providers. Those obligations were discussed in Chapters II and III, with a particular focus on protection in content moderation and consumer protection. Compared to Directive 2000/31/EC, whose Chapter 3 (Art. 16–20) was dedicated to tools for the effective implementation and application of provisions adopted by Member States in the context of its transposition into their

[10] For instance, it is expected that the Commission will order a structural remedy on Google in ad tech proceedings and thus require Google to divest its business in either publisher ad server or with its ad-buying tools; see: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3207 (accessed: 3.4.2025). The case is conducted on the basis of Art. 102 TFEU and not the DMA, although the essence of the structural remedies is the same in both types of proceedings.

[11] This solution follows recent observations that for some gatekeepers regular amounts in fines are insufficient deterrents and do not exceed the profits resulting from anti-competitive behaviour. To that effect, see https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1161 (accessed: 3.4.2025).

legal orders, in this regard, the DSA, specifically Chapter 4 (Art. 49–88), offers a significantly more extensive set of instruments, a substantial proportion of which are public enforcement tools. The responsibility for applying them falls simultaneously on the Member States and the Commission, which, as indicated in Art. 56(5) DSA, shall supervise and enforce the provisions of this Regulation in close cooperation, the latter one being further facilitated by the establishment of the European Board for Digital Services (EBDS).

Supervision of the service providers and enforcement of the DSA provisions is entrusted to competent authorities established by Member States. While a Member State may appoint one or more of the competent authorities, only one of them should be designated the Digital Service Coordinator.[12] The margin of discretion for Member States includes creating new authorities, or empowering existing ones. This approach follows that adopted already in the EU, with notable examples being the AVMSD or GDPR.[13] In Ireland and Italy media authorities were appointed as DSCs, and in other Member States this role was attributed to a new regulatory body.[14] In France, the fusion of CSA (Conseil Supérierur de l'Audiovisuel) – the authority responsible for audiovisual media) and l'Hadopi (Haute Autorité pour la Diffusion des Ouevres et la Protection de Droit sur l'Internet) resulted in the creation of Arcom: Autorité de la communication audiovisuelle et numérique.[15] Some states entrusted the leading role to telecom regulators, which is how it is envisaged in Polish law.[16] The states' obligation is to ensure that the DSC has sufficient technical, financial and human resources, is autonomous in managing its budget and acts impartially, transparently and in a timely manner. DSCs are obliged to act independently, without any instructions or external influence.[17]

DSCs form the European Board for Digital Services (EBDS), an advisory body with the objective of reinforcing the consistent and effective application of the DSA rules.[18] Because of the cross-border nature of intermediary services, a number of solutions were introduced to facilitate cooperation, particularly between the DSC

[12] Art. 49(1) and (2).

[13] Art. 30 of the AVMSD requires that a Member State to designate one or more national regulatory authorities, bodies or both that fulfil the conditions of impartiality and independence. Art. 51(1) GDPR also requires establishment of one or more independent public supervisory authorities.

[14] List of coordinators by Member State available at: https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs (accessed: 3.4.2025).

[15] Arcom, https://www.arcom.fr/nous-connaitre/decouvrir-linstitution (accessed: 3.4.2025).

[16] In Poland the proposal is to establish Office of Electronic Communications (Pol. Urząd Komunikacji Elektronicznej, UKE) as the DSC; see the current status of the legislatory work: https://legislacja.rcl.gov.pl/projekt/12383101/ (accessed: 3.4.2025).

[17] Art. 50 DSA; J. Jaursch, *Platform Oversight: Here Is What Strong Digital Coordinator Should Look Like*, in: J. van Hoboken et al. (ed.), *Putting the DSA into Practice: Enforcement, Access to Justice and Global Implications*, Berlin 2023, p. 98, https://verfassungsblog.de/wp-content/uploads/2023/02/vHoboken-et-al_Putting-the-DSA-into-Practice.pdf (accessed: 3.4.2025).

[18] Art. 61–62 DSA.

from the state of establishment of the ISP, and the DSC from the country of destination, [19] in the context of a general duty to cooperate.[20] The DSC from the country of establishment may request information from the other DSC in the framework of mutual assistance,[21] or can also initiate and lead joint-investigations.[22] The DSC of destination, suspecting that an ISP has infringed the DSA in a manner negatively affecting the recipients of the service, may request the DSC of establishment to take all the measures foreseen in the DSA to ensure compliance with the Regulation.[23] In cases where at least three countries are concerned, the EBDS may issue a similar request.

In the event of cross-border infringements, as is the case with VLOPs and VLOSEs, the primary role is attributed to the Commission.[24] The ultimate control over whether DSCs comply with the Regulation in their response to requests belongs to the Commission. Based on the referrals initiated by the EBDS, the Commission may request that the DSC reassess (review) the matter, notwithstanding its powers to refer the matter of non-compliance with the Regulation by a state to the CJEU.[25]

5.3.2. Supervision and enforcement powers

To ensure effective compliance (supervision) with the rules for providing digital services harmonized under the DSA and to enable responses to instances of non-compliance (enforcement), DSCs have been entrusted[26] with the competences specified in Art. 51–52 DSA. The first of these provisions distinguishes three types of DSC powers within investigation, enforcement and additional measures.

Investigation and enforcement. Powers related to investigative measures are intended to allow DSCs to obtain information related to suspected infringements of the DSA. For this purpose, under Art. 51(1) DSA, DSCs may resort to both personal sources (requests for relevant information or explanations) and material sources, including information storage mediums, which may require access to the premises of certain entities. In the area of enforcing the provisions of the DSA, the list of DSC powers includes administrative tools such as approving commitments

[19] Rec. 126–131 DSA.

[20] Art. 58 DSA.

[21] Art. 57 DSA.

[22] Art. 60 DSA.

[23] Art. 58 DSA.

[24] Art. 58(1); see Section 3.3.3 below for the Commission's specific competences to supervise VLOPs and VLOSEs.

[25] Art. 59 and Rec. 129 DSA.

[26] According to Art. 49(4) DSA, these powers also apply to any other competent authorities designated by Member States to implement the provisions of the DSA.

proposed by providers, orders to cease infringements, imposing fines or penalties, and adopting interim measures as indicated in Art. 51(2) DSA.

In turn, special types of powers include additional measures that serve as tools of the last resort (*ultima ratio*). They are provided for in cases where, despite the exhaustion of the powers mentioned above, "the infringement has not been remedied or is continuing and is causing serious harm" (Art. 51(3) DSA). In such cases, DSCs may require the provider to adopt and submit an action plan or even exercise their power to order the temporary restriction of access of recipients to the service (online interface) concerned by the infringement.

Procedure. Exercising the powers granted to the DSCs under the DSA in a procedural context, including the fundamental guarantees accompanying the state-citizen relationship, requires reference to the relevant provisions of national law (see the example of Poland below). Therefore, Art. 52(5)–(6) DSA only includes a reference to general principles, among which are those emphasizing the right to respect for private life, the right to defence, including the right to be heard and of access to file, and subject to the right to an effective judicial remedy.

Sanctions. As a complement to the powers of DSCs, both in terms of enforcement and investigative activities, they may also impose sanctions as foreseen in Art. 52 DSA. These take the form of fines and periodic penalty payments for specific infringements, up to a maximum amount relative to the annual global turnover or income of the intermediary service provider in question. As with the measures adopted by DSCs, sanctions must also meet the general requirements of being effective, proportionate and dissuasive, as specified under the relevant national provisions.

The case of Poland. According to the draft law still under legislative consideration in Poland, the role of the DSC is to be performed by the President of the Office of Electronic Communications. At the same time, the President of the Office of Competition and Consumer Protection[27] is foreseen as the competent authority. Following Art. 49(2) DSA, the latter will be entrusted with powers concerning the supervision of the obligations of B2C online platform providers under Art. 29–32 DSA (see remarks in Chapter III Section 3.3). It is also planned that a unified procedure implementing Art. 51–52 DSA for both competent authorities will be introduced, inspired in many aspects[28] by the extensive procedural rules currently governing the activity of the aforementioned authority.

[27] As present, this authority combines powers within the area of antitrust (anti-competitive agreements and merger control) with powers related to protecting collective consumer interests (violations of collective consumer interests and the use of unfair terms in consumer contracts) within its statutory competencies.

[28] It is worth noting that according to the draft law (cf. footnote 16 above), the common court currently specialized in competition and consumer protection matters (the Court of Competition and Consumer Protection based in Warsaw) will be empowered to hear appeals against administrative decisions of both competent authorities in matters concerning the application of the DSA.

5.3.3. Enforcement over VLOPs and VLOSEs

As the consequence of separate, harmonized due diligence obligations for VLOPs and VLOSEs the DSA introduces dedicated supervision, investigation, enforcement and monitoring tools for this category of service providers (Art. 64–83 DSA). These confirm the division of competences between the Commission[29] and the Member States, as set out in Art. 56 DSA. According to this model, the Commission holds a central position in supervising and enforcing the obligations imposed on VLOPs and VLOSEs. At the same time, this model is characterized by close cooperation between the entities involved.

The importance of cooperation among the institutions involved is evident in terms of developing expert knowledge and capabilities for the effective enforcement of the DSA. Article 64 provides for various forms of institutional collaboration between the Commission, the Board, DSCs, and, potentially, other relevant authorities. Given the other forms of expert activities provided for under the DSA,[30] including those related to specific due diligence obligations,[31] and the enforcement tools used by the Commission, it can be expected that this body of knowledge will be of particular value when assessing the practices of platforms and their users.

The investigatory powers granted to the Commission may be exercised either on the Commission's own initiative or following the request of the DSC. In the latter case, the DSA sets specific formal and substantive requirements for requests made by the DSC to the Commission for an assessment of a suspected infringement of the DSA by VLOPs or VLOSEs (Art. 65 DSA). In the event that it is the Commission who initiates proceedings,[32] a multilateral flow of information is provided, involving the Commission, VLOPs and VLOSEs, national coordinators, the EBDS, and other relevant authorities involved in the case (Rec. 148 of the preamble, Art. 66

[29] See the discussion on the effectiveness of this model, including the solutions adopted under other regulations in the area of digital transformation in the EU: A. Zhelyazkova, *Challenges in EU Law Enforcement and the Digital Age*, in: M. Scholten (ed.), *Research Handbook on the Enforcement of EU Law*, Cheltenham and Northampton 2023, p. 100; K. Söderlund, S. Larsson, *Enforcement Design Patterns in EU Law: An Analysis of the AI Act*, "Digital Society" 2024, vol. 3, article 41, p. 7.

[30] The requirement for expert knowledge accompanies various instruments of the DSA, including in the case of out-of-court dispute resolution bodies (Art. 21(3) (b)), 'trusted flaggers' (Art. 22(2)), auditing organizations (Art. 37(3)), and 'vetted researchers' (Art. 40(8)).

[31] In addition to the entities directly mentioned in the DSA, it is important to consider the Observatory on the Online Platform Economy, established in 2018 (Commission Decision of 26 April 2018, C(2018) 2393 final), referenced in Recital 137 of the DSA, as well as the European Centre for Algorithmic Transparency.

[32] The first such proceedings were started by the Commission in December 2023 against the provider of the X platform (formerly Twitter), and in 2024, against the providers of services such as TikTok, AliExpress, Facebook, Instagram and Temu– see references to Commission decisions and press releases on the dedicated website: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (accessed: 3.4.2025).

DSA). This process is supported by the information exchange system ("AGORA") established under Art. 85 DSA.[33]

Enforcement actions. The basic instruments that the DSA provides to the Commission for enforcing the obligations of VLOPs and VLOSEs are essentially similar to the tools known from EU competition law (see Art. 18–21 and 23–26 of Council Regulation (EC) No. 1/2003[34]), as well as provisions concerning digital markets that, along with the DSA, formed a single regulatory package known as the Digital Services Package (see Art. 20–34 DMA).[35] The EU legislator adjusts this model of centralized enforcement of EU provisions to the architecture of the DSA (see Chapter III Section 3.2), particularly with regard to systemic risks stemming from the design, functioning and use of VLOPs' or VLOSEs' services.

Consequently, the Commission may demand to be provided with information related to suspected infringements based on Art. 67 DSA. This provision specifies, among other aspects, those entities to which the Commission may direct such a request, as well as its form (either through a simple request or a decision).[36] Article 68 DSA, in turn, empowers the Commission to receive interviews and statements, which facilitates investigative activities related to suspected infringements. Equally important is the power granted in Art. 69 DSA and clarified in the implementing act[37] to conduct inspections on the premises of VLOP or VLOSE concerned, as well as other persons mentioned in Art. 67(1) DSA.

The variety of decisions the Commission is entitled to adopt while enforcing the DSA against VLOPs and VLOSEs includes typical tools such as interim measures (Art. 70) or commitments[38] (Art. 71). These decisions may be adopted during the proceedings. The criteria for non-compliance decisions are defined in Art. 73 DSA. Sanctioning tools include decisions imposing fines (Art. 74) or periodic penalty payments (Art. 76), depending on the nature of the infringement, with unlimited jurisdiction by the CJEU (Art. 81).

---

[33] See Commission Implementing Regulation (EU) 2024/607 of 15.2.2024 on the practical and operational arrangements for the functioning of the information sharing system pursuant to Regulation (EU) 2022/2065 of the European Parliament and of the Council (Digital Services Act) (OJ L, 2024/607, 16.2.2024).

[34] Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (OJ L 1, 4.1.2003, pp. 1–25).

[35] As discussed in Chapter IV.

[36] Cf. the information on the official website (footnote 32 above), indicating specific cases of proceedings initiated by the Commission.

[37] See Commission Implementing Regulation (EU) 2023/1201 of 21 June 2023 on detailed arrangements for the conduct of certain proceedings by the Commission pursuant to Regulation (EU) 2022/2065 of the European Parliament and of the Council (Digital Services Act) (OJ L 159, 22.6.2023, pp. 51–59).

[38] For the first time, the Commission issued such a decision under the DSA regarding the TikTok – see the press release of Commission from 8 May 2024, TikTok Commits to Permanently Withdraw TikTok Lite Rewards Programme from the EU to Comply with the Digital Services Act, https://ec.europa.eu/commission/presscorner/detail/en/IP_24_4161 (accessed: 3.4.2025).

Unique to the DSA is the enhanced supervision system established under Art. 75, which aims to eliminate infringements of the additional obligations related to systemic risk management imposed on VLOPs and VLOSEs in Art. 33–43 DSA. The enhanced supervision is mandatory and is linked to a non-compliance decision as adopted according to Art. 73 DSA. As part of this mechanism, the VLOP or VLOSE concerned shall be obliged to draw up and communicate an action plan to the DSC, the Commission, and the EBDS, setting out the necessary measures which are sufficient to terminate or remedy the infringement.

Monitoring actions. In addition to supervision, investigation and enforcement, the DSA places particular emphasis on monitoring the effective implementation and compliance with its provisions. For this purpose, Art. 72 DSA empowers the Commission[39] to issue orders to provide access to the databases and algorithms of a VLOP or VLOSE concerned, or to impose an obligation on these entities to retain specific documents. Monitoring actions also allow the Commission to appoint external experts and auditors assisting and providing specific knowledge to the Commission, which aligns with the institutional cooperation model established in Art. 64 DSA.

The aspect of cooperation also appears in the form of a separate competence granted to the Commission to submit requests to the DSC or national courts to take action under Art. 51(3) DSA. This provision – previously mentioned in the context of discussing the powers of the DSC – introduces an *ultima ratio* tool. Its application by the Commission is governed by the rules set out in Art. 82 DSA. This may result in the preliminary ruling procedure (see Art. 82(3) DSA, which refers to Art. 267 TFEU), involving national courts. Additionally, this provision addresses the consistency of national court rulings with Commission decisions, particularly those from proceedings initiated under the DSA. This mechanism of cooperation with national courts is likely to have been modelled on Art. 16(2) of the previously mentioned Council Regulation (EC) No. 1/2003. It was also utilized in Art. 39(5) DMA. In all these cases, the aim is to ensure the harmonised application and enforcement of EU law.

5.3.4. Users' disputes with online platforms and the role of DSCs

DSCs play the vital role in the **structural framework for remedies** available to the user and in reinforcing the users' position, particularly in the platform environment.

We can analyse the role of a DSC: (1) from the perspective of a user as any individual or entity entitled to report illegal content according to Art. 16 DSA; (2) from the perspective of a service recipient, whose content or activity has been restricted by platforms; and (3) from the perspective of a consumer whose right to safety and to information has been violated. Under the DSA's **means of redress**

[39] As specified in Commission Implementing Regulation (EU) 2023/1201.

include internal complaint mechanisms, entitlement to refer the dispute to an out-of-court dispute settlement body, or compensation claims in national courts (Figure 7). The DSA also ensures **the right to lodge a complaint to a DSC** in the state of establishment or location of a recipient.

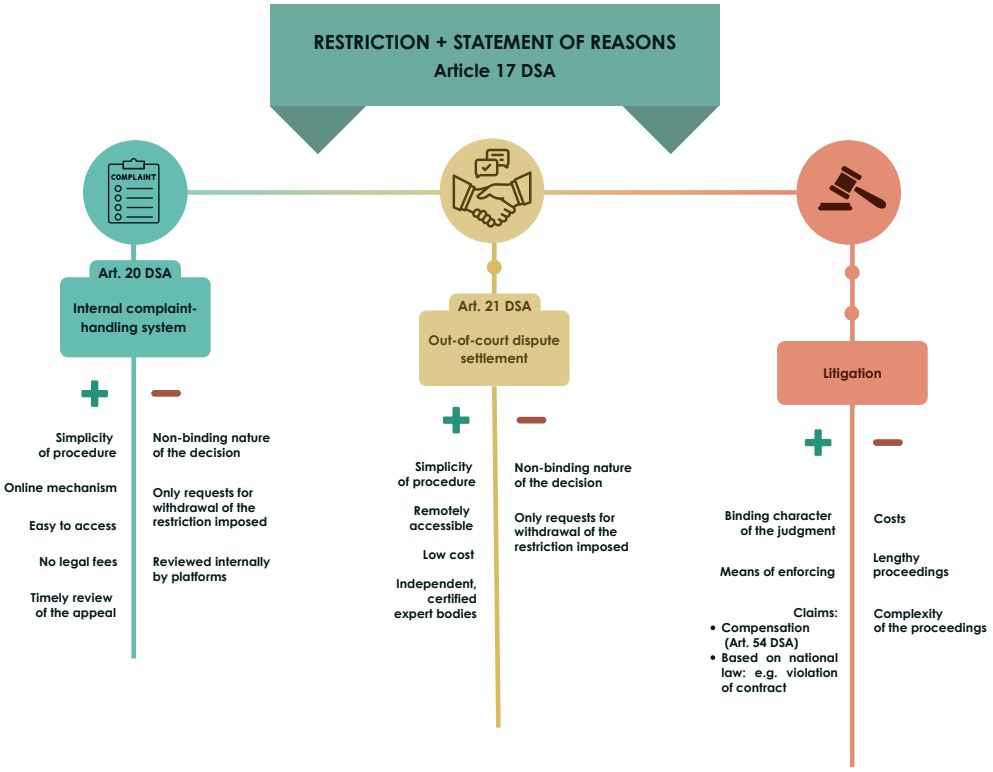


Figure 7: Remedies for users

In the context of remedies, the DSA refers to: (1) 'service recipients' in Art. 20 and 21 including individuals or entities who submitted notices (according to Art. 16)[40]; (2) a 'service recipient or any body, organisation or association mandated to exercise the rights conferred by this Regulation'[41] Art. 53 in the context of the right to lodge a complaint; and (3) only to a 'service recipient' in Art. 54 addressing compensation claims. Therefore, **any user who has reported illegal content** can complain to the platform under the same conditions as service recipients, and if that user is affected by the decisions listed in Art. 20(1) DSA, he or she is entitled to select any out-of-court dispute settlement body.

[40] D. Lubasz underlines that the right to report illegal content is not and cannot be restricted only to service recipients, D. Lubasz, M. Namysłowska (eds.), *Akt o usługach cyfrowych. Komentarz*, Warsaw 2024, p. 400.

[41] Art. 86 DSA.

Only online platforms, and not all hosting service providers, are obliged to establish internal complaint-handling mechanisms, and only their decisions can be questioned in the out-of-court proceedings. In their capacity as a supervisory authority with enforcement powers, DSCs should react if **notice and action mechanisms or internal complaint mechanisms are not in place**. Art. 16 and 20 DSA list the conditions that these mechanisms need to fulfil. It is in the scope of the powers of a DSC to assess whether notice and action mechanisms are easy to access, user-friendly, and allow for purely electronic and adequately substantiated submissions.[42] Similar conditions were established for internal complaint mechanisms.[43] In the area of ensuring safer space and protecting illegal content, DSCs are tasked with awarding the status of a **'trusted flagger'** to an expert entity whose notices are given priority and processed without undue delays.[44] In the field of protecting users from platforms discretionary decisions, the DSC's role is to **certify out-of-court dispute settlement (ODS) mechanisms**.

In the certification process, the DSC assesses whether the applicant meets the requirements, firstly, of impartiality and independence, including the financial independence of the body and its members,[45] and secondly, of being able to solve the disputes swiftly, efficiently and in cost-effective manner, according to clear, fair, and publicly accessible rules of procedure compliant with the applicable law.[46] The certification process aims at ensuring reliable, expert and easily accessible means of redress for users, independent of platforms. DSCs assess whether the applicant body has relevant expertise in relation to an area of illegal content, such as content protected by intellectual property rights, or what is generally referred to as 'hate speech', or expertise in the area of enforcing the T&C of one or more types of platforms.[47] DSCs therefore contribute to shaping the system of out-of-court means of redress for disputes with platforms. Opinions are divided over whether these bodies would ensure adequate protection in the area of fundamental rights.[48] Theoretically, their role could be vital, as such mechanisms are independent of platforms, accessible and expert in nature. The certified bodies have an obligation to report to DSCs, and in their reports DSCs should identify any systemic or sectoral shortcomings or difficulties and may make recommendations and identify best practices to improve the

[42] Art. 16(1) DSA. According to Art. 56(3) DSA, the Commission also has the power to oversight and enforcement of this Regulation over VLOPs and VLOSEs, other than as specified in Chapter 3, Section 5.

[43] Art. 20(1) DSA.

[44] Art. 22(1) DSA.

[45] Remuneration is granted at the level not linked to the outcome of the proceedings.

[46] The list of all conditions is included in Art. 21(3) DSA.

[47] Art. 20(3) (b) DSA.

[48] See: J.P. Quintais et al., *Discussion Report. The Role of Fundamental Rights in Out-of-Court Dispute Settlement under art. 21 DSA*, November 2024, pp. 2–6, https://www.user-rights.org/media/50/download/Discussion%20Report%20No.%202%20-%20Article%2021%20-%20Academic%20Advisory%20Board.pdf?v=1&inline=1 (accessed: 3.4.2025).

functioning of the body. For a user this means that the public authority is monitoring the adequate functioning of the system. On the other hand, dispute settlement bodies have no power to impose a binding settlement on the parties.[49]

Supervision of **the reporting obligations** is vested primarily upon the DSCs.[50] Not publishing reports or not including relevant data such as the number of notices submitted according to Art. 16 amounts to an infringement of the DSA. A DSC should also be the one to assess whether the information submitted in the report, for example, with regard to the use of automated tools for content moderation[51] complies with the requirements set in the DSA. The systematic analysis of different reports and data, such as publicly available statement of reasons, is not a clear obligation of DSCs, it is, however, desirable. Other entities like researchers, trusted flaggers or NGOs may contribute to this analysis. DSCs have the power to **grant the status of a 'vetted researcher'**, and address a reasoned request to VLOPs and VLOSEs to grant researchers access to data for the purpose of research contributing to the analysis of systemic risks in the EU.[52]

Every service recipient has the **right to lodge a complaint to a DSC**. Those filing notices under Art. 16 are not indicated in Art. 53. It is thus unclear whether submitting the notice under Art. 16 results in gaining the status of a 'service recipient'.[53] Consumers belong to the category of 'service recipients' and can lodge the complaints on infringements of the DSA, including the provisions of Section 4 addressing special obligations of B2C platforms.

The DSA formulates basic requirements that a DSC assesses the complaint, and may transfer it to other competent authority (such as a consumer protection authority[54]) or to a DSC of establishment. Both parties have the right to be heard and receive appropriate information in the course of the proceedings initiated with the complaint. The details of the procedure should be indicated in national law. The DSA is silent on the type of action or response that should be provided by a DSC. As the DCS is the relevant authority for all matters relating to supervision and enforcement, it can certainly use its investigative and discretionary powers while

[49] Art. 21(2) DSA.

[50] Basic reporting obligations are imposed in Art. 15 with additional obligations for online platforms, and VLOPs and VLOSEs. According to Art. 56(3), the Commision has powers to supervise and enforce other obligations than those laid down in Section 5 of Chapter 3 DSA.

[51] Art. 15(1) (e) DSA.

[52] Art. 40(4) and (8) and Art. 34 DSA.

[53] This could be sustained with the argument that such a user is using the service functionality, thus using a service with respect to information that he or she finds illegal. In the case of a hosting service provider violating Art. 16(4) and failing to confirm the receipt of the notice, not reacting, and a user considering that the host provider and failing to act diligently, non-arbitrarily and objectively (Art. 16(6)) Art. 20 and 21 would not apply, and the user should be entitled to alert the DSC with official complaint according to Art. 53, as a service recipient.

[54] This would be the case of the Office of Competition and Consumer Protection (Pol. Urząd Ochrony Konkurencji i Konsumentów, UOKiK) in consumer matters.

acting proportionately, considering the nature, gravity, recurrence and duration of infringement. This is implied by the obligation to report on a number of complaints received and oversee their follow-up.[55]

The complaint may address obvious infringements of the DSA, such as a lack of internal complaint mechanisms, but also individual matters such as complaints that service provider did not act in a diligent, timely and non-arbitrary manner and infringed Art. 14(4) or Art. 20(4) in the area of complaints. This may pose a challenge to an administrative authority. As it was explained by the Irish DSC, Comisiún na Meán, the DSC's role is not one of a judge.[56] A DSC is tasked, however, with assessing whether the intermediary service provider acted diligently, and the right to lodge a complaint concerning individual matters is a directly effective right granted by the Regulation.

5.4. Private enforcement of the Digital Services Act

The effectiveness of the rights of service recipients that may be identified under the DSA based on the set of harmonized due diligence obligations imposed on intermediary service providers depends on the appropriate selection of legal tools available for the proper enforcement these obligations. In the context of EU consumer policy (see Chapter I), reference can be made to the general right to redress and the right to be heard, which will fully apply in the digital environment. For all recipients of the services, of similar significance is the right to an effective remedy and to a fair trial (Art. 47 CFREU), as well as similar fundamental rights derived from national legal systems and specified in the form of particular enforceable rights and individual remedies in national legislation.

The provisions of Chapter 4 of the DSA outline an enforcement model based primarily on public instruments (*public enforcement*). However, *private enforcement* should be treated as complementary, potentially providing legal tools to ensure compliance with the rules governing the provision of digital services. There is no doubt that the implementation of several obligations set out in the DSA will be of particular importance for the practical exercising of users' rights pursued through *private enforcement*. In this context, one can point to the obligation for intermediary service providers to designate a single point of contact for service recipients (Art. 12 DSA), the notice and action mechanisms concerning providers of hosting service, including online platforms (Art. 16 DSA), and the obligations applicable to providers of online platforms to ensure service recipients have access to an inter-

[55] Art. 55(1) DSA.

[56] Comisiún na Meán, Complaints guide, https://www.cnam.ie/general-public/report-complain/something-i-saw-or-experienced-online/what-can-i-report/#whatyoucantreport (accessed: 3.4.2025).

nal complaint-handling system combined with an out-of-court dispute resolution mechanism (Art. 20–21 DSA).

Compensation claims. Among the *private enforcement* tools, Art. 54 DSA plays a central role. It provides the basis for compensation claims for infringements by providers of their obligations under this regulation. In comparison with a similar provision in the data protection regime (Art. 82 of Regulation (EU) 2016/679)[57], Art. 54 DSA is a much less detailed normative structure. The right to claim compensation is granted to service recipients (users)[58] against intermediaries, while using the concepts of "damage" and "loss."[59] For the proper enforcement of such claims, reference is made to the rules and procedures deriving from the applicable national law. Moreover, Rec. 121 DSA explains that such compensation should not affect other possibilities of redress available under consumer protection rules. The introduction of this provision into the DSA as an independent basis for compensation claims is undoubtedly a significant step in strengthening the rights of digital service users, and is understood as one of the goals of EU digital policy. However, it should be emphasized that the effectiveness of claims under Art. 54 DSA will require the application of specific tools under domestic legal systems (e.g. regimes for contractual and tort liability, rules of civil procedure), while respecting the principles of direct applicability and direct effect.

Remedies for consumer protection. The importance of national and EU law within the framework of *private enforcement* of obligations of service providers set out in the DSA is particularly evident in terms of consumer law. In this domain, existing consumer protection regulations adopted by Member States, following EU legislation (see remarks in Chapter III of this book), are essential. These may include instruments derived from Directive 2005/29/EC, recently amended by the 'Omnibus Directive',[60] mainly in response to the emergence of digital environments. An

[57] Only recently, under this regulation, have the rules for determining compensation by national courts been clarified within the framework of CJEU *case law*, see the judgment of CJEU of 4 May 2023 in Case C-300/21, *UI v* Österreichische *Post AG* (ECLI:EU:C:2023:370). It seems that Art. 54 DSA will require such clarification from the CJEU.

[58] No distinction was made here between recipients of services being consumers or businesses, although the proposal for this provision was accompanied by arguments focused on consumer protection, as indicated by the opinion of the European Economic and Social Committee (EESC), Opinion. Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, INT/929-EESC-2021, 27.4.2021, point 4.2.

[59] Given the need for a uniform interpretation of these concepts under EU law, as well as the practice of the EU legislation adopting different terminology, as demonstrated by the example of Art. 82 of Regulation (EU) 2016/679, it is important to take into account the ongoing discussion regarding compensation claims under private law in the EU: Ch. von Bar, The Notion of Damage, in: A. Hartkamp et al. (eds.), *Towards a European Civil Code*, 4th ed., Alphen aan den Rijn and Nijmegen 2011, p. 387; M. Bussani, V. Palmer, *The Frontier between Contractual and Tortious Liability in Europe: Insights from the Case of Compensation for Pure Economic Loss*, in: A. Hartkamp et al. (eds.), *Towards a European Civil Code*, op. cit., p. 946.

[60] Member States were obliged to introduce proportionate and effective legal remedies available to consumers harmed by unfair commercial practices. These remedies may include the right to claim com-

example here is the case initiated in Germany by a local non-governmental organization against the provider of the digital platform (Etsy) concerning obligations under Art. 30 DSA.[61]

It should be noted that the activity of individual service recipients, as well as organizations representing their interests (e.g. as consumers or businesses), in enforcing specific provisions of the DSA, is decisive from the perspective of *private enforcement*. Also helpful in this regard are the actions of a particular category of entities known as trusted flaggers, both in connection with their standing to submit notifications under Art. 16 DSA and the related reporting obligations (Art. 22(3) DSA).

Representative actions. In the area discussed here, instruments in the form of representative (class) actions play a significant role. In response to the digital transformation, the European Union has adopted new consumer protection tools in the form of Directive (EU) 2020/1828,[62] which is based on the principle of minimum harmonization. In national legal systems, as exemplified by Poland,[63] these provisions have been introduced to allow for the various claims within the representative proceedings available both for consumers and businesses. In the context of digital services, where simultaneous violations of the interests of many users may stem from particular uniform practices of a service provider, national tools such as class actions used in *private enforcement* scenario can be applied in conjunction with the DSA provisions, especially in cases involving small claims that may be considered as not being effective if handled by individual users.

Moreover, the DSA seems to encourage this explicitly by granting recipients of intermediary services "at least (…) the right to mandate a body, organisation or association to exercise the rights conferred by this Regulation" in Art. 86 (Rec. 149) DSA. This allows recipients' rights to be further strengthened, thereby reinforcing the enforcement of the DSA. It refers particularly to those rights related to submitting notices, challenging the decisions taken by providers of intermediary services, and lodging complaints against the providers for infringing the DSA, to be exercised by specialized organizations acting on behalf of recipients (see Rec. 149 DSA).

Remedies for digital users. From the perspective of EU law, consumers, including those on the digital markets, have access to significantly more developed tools for enforcing their rights under the DSA regime compared to other categories of service recipients, such as professional users and their business customers (B2B). The latter will largely rely on the instruments available under national law, such as

---

pensation for damage and, where relevant, the right to request a price reduction or the termination of the contract (see Rec. 16 of the Omnibus Directive).

[61] Zentrale zur Bekämpfung unlauteren Wettbewerbs, Wettbewerbszentrale klagt gegen Etsy, 8.4.2024, https://www.wettbewerbszentrale.de/wettbewerbszentrale-klagt-gegen-etsy/ (accessed: 3.4.2025).

[62] OJ L 409, 4.12.2020, pp. 1–27.

[63] J. Mucha, *From Recipe to Reality: The Polish Way of Collective Redress*, "ERA Forum" 2024, vol. 25, p. 97.

contractual or tort liability regimes. In this context, there is a noticeable trend in national law towards expanding the scope of consumer protection, particularly in relation to small businesses.[64] The provisions of the DSA may therefore potentially serve as a catalyst towards developing harmonized standards for protecting of the rights of all categories of service recipients. Combined with the potential "Brussels effect," the DSA may thus contribute to promoting high standards of protection for users of digital services worldwide.

5.5. Private enforcement of the Digital Markets Act

5.5.1. Systemic background

The DMA and safeguarding user's rights. Private enforcement of rights included in the DMA is not introduced in that Regulation itself. Therefore, one may ask whether individuals, end users and business users, in particular, may invoke provisions of Art. 5–7 DMA in proceedings against gatekeepers before national courts at all.

There are some sceptical views regarding the DMA's capacity to be privately enforced. However, the dominant view is that DMA is a source of rights granted to individuals and may be enforced privately. We discussed some of the arguments supporting that position in Chapter IV.

Effective protection of business users and end users by national courts is already placed at the very heart of the DMA's objectives in its preamble. Its Recital 42 reads that "it is important to safeguard the right of business users and end users […] to raise concerns about unfair practices by gatekeepers raising any issue of non-compliance […] with any relevant administrative or other public authorities, including national courts."

Article 39 DMA is the key provision in this context, as it regulates cooperation between the Commission and national courts when applying DMA substantive legislation. In the first place, it establishes a framework for exchanging information between the Commission and the courts. This allows national courts to use valuable material gathered by the Commission (e.g. in market investigations) for the purposes of hearing private enforcement claims.

Article 39 DMA also allows the Commission to act as *amicus curiae* before national courts in cases regarding the application of the DMA. Thus, the Commission

[64] An example of this in Polish law is the application of certain provisions of the Civil Code of 23 April 1964 (consolidated version Journal of Laws of 2024 item 1061) regarding consumer protection (including those related to unfair contract terms) to individuals conducting business activity, as a result of regulatory changes adopted in 2019. By comparison, in German law, the Verbandsklagenrichtlinienumsetzungsgesetz of 2023 (BGBl. I Nr. 272 S. 1) stipulates that small businesses (Ger. *kleine Unternehmen*) should be treated as consumers in the context of class actions regime set out in that legal act.

may submit written observations in such proceedings and, if allowed by a court, make oral observations as well.

This provision also contains an important coherence rule requiring that national courts shall not issue a decision which runs counter to a decision adopted by the Commission under the DMA. They shall also avoid giving decisions which would conflict with one contemplated by the Commission in proceedings it has already initiated. This is without prejudice to the competence to ask preliminary questions under Art. 267 TFEU.[65]

The Digital Markets Act also addresses private enforcement matters in its Art. 42. This provision refers to representative actions and confirms the applicability of Directive 2020/1828 to the representative actions brought against DMA infringements committed by gatekeepers. Representative actions are discussed in Section 5.4 of the present chapter.

Implications of competition law private enforcement. Discussions about the possibility and scope of DMA private enforcement may recall similar past discussions with respect to the private enforcement of competition law. It follows from the Court's established case law that since competition rules are intended to give rise to the rights of individuals, these individuals have the right to seek compensation for a loss caused by competition law infringement.[66] These conclusions have been confirmed expressly with respect to the application of competition rules in the digital sector.[67]

The line of case law discussed here was one of the factors leading to the adoption of Directive 2014/104/EU on Antitrust Damages Actions.[68] The Damages Directive harmonises certain rules of national laws with respect to bringing claims for damages resulting from competition law infringements. Among other effects, it harmonises rules on the use of evidence gathered by competition authorities, quantifying damage or establishing the presumption of an infringement if it was declared in a competition authority's decision.

However, the Damages Directive's scope of application was not extended at EU level to DMA infringements. At the same time, Member States have the autonomy

[65] Indeed, it will be very interesting to see if national courts would be willing to test the boundaries of that limitation and ask the Court of Justice about possible deviations from the Commission's decisions in private enforcement actions, balancing the express DMA provision with the national court's powers to apply EU law directly.

[66] Indeed, it results from the principle of full effectiveness of competition rules that "national courts whose task it is to apply the provisions of [Union] law in areas within their jurisdiction must ensure that those rules take full effect and must protect the rights which they confer on individuals"; see Case C-453/99, *Courage v Crehan*, paras. 19, 25–26.

[67] See judgment of CJEU of 18 April 2024, Case C-605/21, *Heureka Group a.s. v Google LLC*, (ECLI:EU:C:2024:324), para. 61.

[68] Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union (OJ L 349, 5.12.2014, pp. 1–19).

to do this in their national laws implementing the Damages Directive. For instance, such a solution was adopted by Germany in the Gesetz gegen Wettbewerbsbeschränkungen (Act against Restraints of Competition).[69]

5.5.2. What rights can be enforced and how

As outlined in Chapter IV, substantive obligations for gatekeepers are introduced in Art. 5–7 DMA and further translate into rights of individuals, specifically business and end users. Thus, the provisions can be privately enforced before national courts.

For instance, a business user may seek compensation if a gatekeeper fails to unlock its app distribution ecosystem or uses publicly unavailable data generated by the customers of those business users. End users could bring claims against a gatekeeper if they cannot easily uninstall a given software application from the operating system or when a gatekeeper fails to ensure effective data portability outside its platform service.

Given that neither the DMA nor the Damages Directive contain specific rules regarding the private enforcement of Art. 5–7 DMA, this matter is subject to the national laws of Member States. Thus, they are free to decide on specific substantive and procedural aspects of bringing such claims (regulatory autonomy), as long as the general principles of effectiveness and equivalence are obeyed.

Lack of DMA private enforcement rules at the EU level may be challenging for both gatekeepers and users claiming their rights. For business and end users, lack of clear rules in a given jurisdiction may act as discouragement from bringing any claims. These aspects can lead to what is termed 'forum shopping', where claimants and defendants search for the most favourable jurisdiction in which to settle their dispute. Despite the safeguards included in Art. 39 DMA, forum shopping could lead to fragmentation and incoherences in how the DMA is applied.

At the same time, practical examples show that violations of competition rules in the digital sector give rise to significant claims brought by individuals. For instance, in February 2024, over 30 media organisations from the EU brought a legal action against Google, in which they seek damages of more than 2 billion euros for the alleged infringements in online advertising business.[70]

---

[69] Art. 33 (1) of that act expressly reads that "Whoever violates […] Article 101 or Article 102 [TFEU] or Article 5, 6 or 7 of [DMA] (infringer) […] shall be obliged to the person affected to rectify the harm caused by the infringement […]."

[70] For more information see: https://adtechclaim.eu/ (accessed: 3.4.2025). The case follows up on an ad tech decision by the French Competition Authority, but also reflects the Commission's proceedings on the same matter.

5.6. Conclusions

As discussed in this chapter, the DSA and the DMA introduce certain novel solutions for regarding enforcement in their respective areas. For the DMA, the key change compared to general competition law is complementing the *ex-post* enforcement based on self-assessment with the *ex-ante* approach. In the DSA's field, the main novel aspect is the introduction of general due diligence obligations for platforms to ensure a transparent and safe online environment. These due diligence obligations also include a consumer protection perspective, which requires national competent authorities to be granted additional powers.

Enforcement of the DSA and the DMA demonstrates certain similarities, but significant differences also exist. Understanding these features is essential for users in terms of invoking their rights *vis-à-vis* online platforms.

The common approach in public enforcement may be mostly witnessed with respect to the largest digital companies, i.e. VLOPs (VLOSEs) under the DSA and gatekeepers under the DMA. In this context, precise lists of obligations included in both legal acts evolve into further compliance and transparency requirements. Thus, the Commission obtains better and ongoing insight of large platforms' actual conduct.

If large platforms do not comply with DSA or DMA provisions, the Commission may initiate proceedings with a view to ordering full compliance by a given online platform. It may also impose a fine or other measures upon non-compliant entities.

While the Commission remains the sole DSA and DMA enforcer with respect to the largest platforms, it may still cooperate with competent national authorities. The DSA requires that the Commission and the DSCs provide each other with mutual assistance and cooperate closely to ensure uniform application of that Regulation. Under the DMA, the Commission may ask national competition authorities for support both in market investigations and in exchanging relevant information regarding gatekeepers' conduct in a given Member State.

Such a centralised public enforcement system aims to strengthen users' rights. Indeed, Art. 53 DSA grants users the right to lodge a complaint against platforms with the DSCs, should they believe that a given DSA obligation had been infringed. While such a specific system is not foreseen in the DMA, users may lodge similar complaints with the Commission or national competition authorities on the basis of the general rules of EU and national laws.

Differences among the DSA and the DMA are most visible regarding application and enforcement with respect to smaller online platforms. While the DMA only applies to large ones (the gatekeepers), the DSA essentially covers all platform and intermediary services providers. To this end, the enforcement system is decentralised, as national DSCs are granted relevant competences. However, it should

be noted that in the other area discussed here, the DMA may be accompanied by general competition law when enforced by the Commission or national competition authorities against undertakings that do not meet the gatekeeper designation criteria.

Private enforcement. While private enforcement is expressly foreseen only in DSA (and its Art. 54), it results from EU law principles (and the principles of direct effect and full effectiveness, in particular) that users and other individuals may invoke both the DSA and DMA before national courts in order to claim their rights introduced by either piece of legislation. They may also claim compensation for a loss resulting from a DSA or DMA infringement.

In the context of the fundamental principles of effectiveness and direct effect, the question of which particular rules apply to such private actions is still open for discussion at the judicial or legislative level, as is the matter of which specific rules apply to such private actions. For the time being, due to the lack of any specific harmonisation in this field, private enforcement will be executed before national courts and under the national rules of Member States. These rules include both substantive (e.g. quantification of harm, limitation periods) and procedural aspects. Differences among Member States' legislation may lead to forum shopping (or, users and platforms seeking the most favourable jurisdiction), fragmentation and a less uniform application of the EU Regulations in question.

Conclusions

This handbook is dedicated to exploring users' rights in the Digital Services Package. The objectives of the DSA and the DMA need to correspond with the concept of the Digital Single Market. Based on how this concept is presented in EU soft law and in the framework of secondary EU law aiming to improve the functioning of the Single Market,[1] we elaborate on three key areas: (1) facilitating **business activities in the online environment**, as well as ensuring **fairness and contestability** in digital markets; (2) flows and access to the **core resources of information and data**; and (3) protection of **fundamental values and rights**, such as the right to receive and impart information or protection of consumers.

The objectives of the DSA include better functioning of the Single Market fostered by a uniform legal framework for liability exemptions of intermediary service providers with additional due diligence obligations. Thus, a safer, trusted and predictable online environment should become the space for communication between users in all areas of their economic and non-economic activities. The activities of online platforms that provide digital infrastructure for our daily communication are at the centre of our analysis. The feature that distinguishes online platforms from other intermediaries is their role in **disseminating the information**. Platforms' significant role in facilitating access to information is addressed with multiple due diligence obligations, including explanations that need to be provided in the terms of service, functionalities available to the users or reporting obligations. **For online platforms as business operators,** additional obligations do not necessarily "facilitate" the provision of services, but the DSA provides a uniform set of rules, while different national regimes are usually considered a barrier to cross-border activities. For users, the DSA definitely **enhances the right to information**, including information provided to consumers, particularly in terms of requirements related to what information should be provided to users and in which way.

The DSA **aims to reduce the risks** associated with our activities in social media, on content sharing platforms or in online marketplaces and deals primarily with the potential for spreading **illegal content and information** to the detriment of the users. In the area of content moderation, providing the functionalities for users to report unlawful content is a clear obligation on online platforms and implicates **the right to report** for anyone aware of illegal information hosted by the service

[1] Art. 114 TFEU is the legal basis for both the DSA and the DMA.

provider. It should be noted that in the DSA the concept of "illegal content" is very broad and encompasses not only the areas of criminal liability but any content that is not compliant with numerous rules in the EU or national law, regardless of the specific area of regulation is.

In Chapter II, we discussed the answers that the DSA provides regarding to risks that content moderation by online platforms poses **for fundamental rights**, such as by delegating the judicial function to platforms, lack of transparency or effective remedies. The DSA introduces **transparency obligations** related to clarifying an entity's own policy, statements of reasons provided to users and reports on content moderation and application of algorithmic tools. Ideally, new information revealed by online platforms or made available to the vetted researchers should serve better enforcement. To ensure effective protection of fundamental rights, **information provided to users** needs to include information on the remedies available. In the context of enforcement, the question still remains as to how to ensure not only that the information in reports or the statements of reasons is provided to users, but that it satisfies the conditions of being "meaningful and comprehensible" (Art. 15(1) (c) DSA), or "clear and easily comprehensible and as precise and specific as reasonably possible" (Art. 17(4) DSA).

The objective of bolstering the effectiveness of fundamental rights protection is also clear in the obligations imposed on the intermediaries to "act in a diligent, objective and proportionate manner in applying and enforcing the restrictions" in the area of content moderation, with due regard to "the fundamental rights of the recipients of the service, such as the freedom of expression, freedom and pluralism of the media" (Art. 14(4) DSA).

Focusing on platform-user relations, we note that **the concept of the user in the DSA** is based on the two fundamental, legally defined terms: a recipient of the service, and a consumer. A protective approach is implemented not only with relation to consumers, but also with respect to any natural or legal person providing or seeking information by means of intermediary services. Some "rights" should be ensured in the broadest possible way to anyone, an example being the right to report illegal content. **The effective protection for rights** is enhanced with by the possibility that complaints to the DSC can also be submitted by any body, organisation or association mandated to exercise the rights conferred by the DSA. **Consumers**, on the other hand, are addressed particularly in the context of **B2C relations on transactional platforms**.

A reliable platform environment should reinforce the high level of consumer protection as one of the EU's fundamental principles. In Chapter I of this handbook, we explained that when referring to the existing body of *acquis consommateur*, as well as recognizing the EU standards for consumer protection introduced prior to the digital era, the DSA seeks to protect the interests of users in online environments, in line with the latest EU policy developments in this field.

The due diligence requirements targeted at protecting consumer interests on B2C platforms, such as traceability of traders, compliance by design, and the right to information (Art. 28–32 DSA), essentially adhere to the classic informational paradigm that underpins modern consumer policy. Undoubtedly, these provisions strengthen the position of consumers, but as emphasized here in Chapter III, they may be seen as an attempt to reflect the specific nature of the complex transactional relationships within the digital environment of online platforms.

On the other hand, the consumer-related aspects present in other provisions of the DSA, such as those concerning terms of service, online advertising, or the protection of minors, while highly prominent, may be regarded as heralding a new approach to user protection in the context of the challenges facing the EU legislator in the digital era.

The realization of the concept of a Digital Single Market will not be possible without bolstering user rights and the corresponding obligations of intermediaries. To this end, the DSA has introduced an extensive set of tools for supervising, enforcing, and monitoring actions. In presenting this comprehensive set of tools, which predominantly takes the form of *public enforcement* but also includes elements of *private enforcement*, the importance of cooperation between the institutions responsible for implementing the DSA at both the EU and national level has been emphasized.

Against this background, the DMA's objective may seem more specific and market-oriented. As discussed in the book, the DMA predominantly seeks to address overall market flaws in digital sector and to restore the balance of market power between gatekeepers (who are very often VLOPs under the DSA at the same time) and users of online platforms provided by these largest market players. Thus, **the main objective of the DMA is to ensure contestability and fairness in digital markets**. While the DMA constitutes a piece of internal market legislation and expressly focuses on economic aspects, it is more often argued that it may also safeguard other objectives of a less economic nature (such as plurality in democratic society).

Regarding contestability, the Regulation introduces a number of obligations on gatekeepers, the aim of which is to facilitate new market entries and enhance competitive pressure exerted on gatekeepers by at least these potential entrants. Following the DMA's preamble, **fairness is defined as** a **balance between the rights and obligations of business users where the gatekeeper does not obtain a disproportionate advantage**. Therefore, while in methodological terms, the EU legislator mainly focuses on introducing publicly enforced obligations for gatekeepers, it stems from the DMA's key objective that this serves to enhance the rights and market power of both business users and end users, the gatekeepers' counterparties.

It also follows from specific provisions of the DMA discussed in this handbook that the **provision and enforcement of platform users' rights lies at the very heart of the Regulation**. These rights are reflected in gatekeepers' obligations, mostly

for the benefit of both types of platform users: business users and end users. They encompass several areas of market operation, i.e. interoperability between gatekeepers' platforms and other digital services, the processing and use of users' data by gatekeepers, unfair trading, and transparency requirements in online advertising.

Business users of platforms are believed to be the main beneficiaries of the DMA. These undertakings use platforms as a marketplace allowing them to conduct their business: present offers to customers and conclude transactions. The DMA seeks to ensure that these users remain independent of gatekeepers and that they are not usurped from the market by gatekeepers unfairly extending their market presence from platforms to more specific markets for given products or services.

However, the DMA impacts the position of end users as well. These are individuals who use platforms for non-commercial purposes, mostly as consumers. Firstly, it confers upon them specific entitlements (such as the right to easily uninstall applications from an operating system or to transfer their data from one platform service to another). Secondly, as with competition law, the DMA's overarching goal is to safeguard consumer choice and welfare, even if indirectly, through achieving other specific objectives, including imposing obligations on gatekeepers or rights upon business users.

Introducing a regulatory framework dedicated to the Digital Single Market marks a new stage of the development of Single Market law. The market reality is dynamic and founded on technological rather than legal development. Implementing the DSA and the DMA along with the introduction of necessary national laws complementing the enforcement structure should have been completed already. However, at the time of writing, still one Member State had not appointed Digital Services Coordinators – Poland. Some DSCs are already pointing to the importance of users', or consumers' rights.[2] What the user may expect from the public enforcement authorities, and when the individual claims and complaints should be viable options is of key importance. Initial experience demonstrates that there is greater transparency, for example, with the EU Transparency Database[3] for statements of reasons, or the transparency reports, particularly from VLOPs and VLOSEs.[4]

The end of 2025 brings the first report on the application of Art. 33 DSA and addressing how the DSA interacts with other EU legal acts regarding the Digital

[2] Irish DSC publishes the guide to complaints: Digital Services Act – Your right to complain, https://www.cnam.ie/onlinecomplaints/; German DSC lists users rights on its website: Rechte von Nutzern https://www.dsc.bund.de/DSC/DE/3Verbraucher/1VB/start.html; French DSC, ARCOM answers the question what the DSA means for me, from the user perspective, Qu'est-ce que ce règlement va changer pour moi?, https://www.arcom.fr/actualites/5-informations-retenir-sur-le-reglement-sur-les-services-numeriques-rsn-ou-digital-services-act-dsa (accessed: 3.4.2025).

[3] https://transparency.dsa.ec.europa.eu/ (accessed: 3.4.2025).

[4] https://digital-strategy.ec.europa.eu/en/policies/dsa-brings-transparency (accessed: 3.4.2025).

Single Market, particularly those prior to the DSA.[5] It will be followed by more comprehensive reports that evaluate the effects of the DMA in 2026[6] and the DSA in 2027.[7]

Furthermore, different activities aimed at observing, commenting and recommending the appropriate approach have been begun by academics.[8] Answers to the questions we pose in our handbook do not depend only on institutional reporting activities. They are linked to the degree to which the DSC and European Commission are involved in analysing the available data, researchers pushing forward the analysis of publicly available data, and data access in the specific framework of the DSA, and on the activity of users and their representatives. Therefore, this Handbook serves as an invitation to follow-up work.

---

[5] Art. 91(1) DSA.

[6] Art. 53(1) DMA.

[7] Art. 91(1) DSA.

[8] Such as the DSA Observatory, https://dsa-observatory.eu/ (accessed: 3.4.2025).

Sources

Wykaz źródeł

BIBLIOGRAPHY (BIBLIOGRAFIA)

Aldridge A., *Konsumpcja*, trans. M. Żakowski, Warsaw 2006.

Andriychuk O., *Do DMA Obligations for Gatekeepers Create Entitlements for Business Users?*, "Journal of Antitrust Enforcement" 2023, vol. 11, no. 1, pp. 123–132. https://doi.org/10.1093/jaenfo/jnac034

Angelopoulos Ch., *European Intermediary Liability in Copyright: A Tort Based Analysis*, PhD thesis, Universiteit van Amsterdam 2016, https://hdl.handle.net/11245/1.527223_

von Bar, Ch., *The Notion of Damage*, in: A. Hartkamp et al. (eds.), *Towards a European Civil Code*, 4th ed., Alphen aan den Rijn and Nijmegen 2011, pp. 387–400.

Benöhr I., *EU Consumer Law and Human Rights*, Oxford 2013.

Bostoen F., *Understanding the Digital Markets Act*, "Antitrust Bulletin" 2023, vol. 68, no. 2, pp. 263–306. https://doi.org/10.1177/0003603X231162998

Bussani M., Palmer V., *The Frontier between Contractual and Tortious Liability in Europe: Insights from the Case of Compensation for Pure Economic Loss*, in: A. Hartkamp et al. (eds.), *Towards a European Civil Code*, 4th ed., Alphen aan den Rijn and Nijmegen 2011, pp. 945–976.

Cauffman C., Goanta C., *A New Order: The Digital Services Act and Consumer Protection*, "European Journal of Risk Regulation" 2021, vol. 12, no. 4, pp. 758–774. https://doi.org/10.1017/err.2021.8

Chakravorti B., Tunnard Ch., Chaturvedi R.S., *Where the Digital Economy is Moving Fastest*, Harvard Business Review, Analytic Services, 9.2.2015, https://hbr.org/2015/02/where-the-digital-economy-is-moving-the-fastest (accessed: 3.4.2025).

de Cock Buning M. et al., *Consumer@Protection.EU: An Analysis of European Consumer Legislation in the Information Society*, "Journal of Consumer Policy" 2001, vol. 24, pp. 287–338. https://doi.org/10.1023/A:1013965627370

Dinwoodie G.B., *A Comparative Analysis of the Secondary Liability of Online Service Provoders*, in: G.B. Dinwoodie (ed.), *Secondary Liability of Internet Service Providers*, Cham 2017, pp. 1–72.

Dregelies M., *Verbraucherschutz im Digital Services Act*, "Verbraucher und Recht" 2023, no. 5, pp. 175–182.

Douek E., *Content Moderation as Systems Thinking*, "Harvard Law Review" 2022, vol. 136, no. 2, pp. 528–607.

de Elizalde F., *Fragmenting Consumer Law Through Data Protection and Digital Market Regulations: The DMA, the DSA, the GDPR, and EU Consumer Law*, "Journal of Consumer Policy" 2025, https://doi.org/10.1007/s10603-025-09584-3

Elkin-Koren N., Peerel M., de Gregorio D., *Social Media as Contractual Networks: A Bottom-up Check on Content Moderation*, "Iowa Law Review" 2022, vol. 107, pp. 987–1049, https://ilr.law.uiowa.edu/sites/ilr.law.uiowa.edu/files/2023-02/A2_ElkinKoren_DeGregio_Perel.pdf.
Gillespie T., *Custodians of the Internet: Platforms, Content Moderation and the Hidden Decisions That Shape Social Media*, New Haven and London 2018.
Goldman E., *Content Moderation and Remedies*, "Michigan Technology Law Review" 2021, vol. 28, no. 1, article 2. https://doi.org/10.36645/mtlr.28.1.content
Grochowski M. (ed.), *Rynek cyfrowy. Akt o usługach cyfrowych: Akt o rynkach cyfrowych. Komentarz*, Warsaw 2024.
Haimson O.L. et al., *Disproportionate Removals and Differing Content Moderation Experiences for Conservative, Transgender, and Black Social Media Users: Marginalization and Moderation Gray Areas*, "Proceedings of the ACM on Human-Computer Interaction" 2021, vol. 5, no. CSCW2, article 466. https://doi.org/10.1145/3479610
Hardin R., *Trust*, Cambridge 2006.
Hartkamp A. et al. (eds.), *Towards a European Civil Code*, 4th ed., Alphen aan den Rijn and Nijmegen 2011.
Helberger N.et al., *Digital Consumers and the Law: Towards a Cohesive European Framework*, Alphen aan den Rijn 2013.
Husovec M., *Accountable, Not Liable: Injunctions Against Intermediaries*, "TILEC Discussion Paper" 2016, no. 2016-012. http://dx.doi.org/10.2139/ssrn.2773768
Husovec M., *Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules*, "Berkeley Technology Law Journal" 2023, vol. 38, no 3, pp. 883–920. https://doi.org/10.15779/Z38M902431
van Hoboken J. et al. (eds.), *Putting the DSA into Practice: Enforcement, Access to Justice and Global Implications*, Berlin 2023, https://doi.org/10.17176/20230208-093135-0
Jaursch J., *Platform Oversight: Here Is What Strong Digital Coordinator Should Look Like*, in: J. van Hoboken et al. (eds.), *Putting the DSA into Practice: Enforcement, Access to Justice and Global Implications*, Berlin 2023, pp. 91–105.
Jhaver S., Bruckman A., Gilbert E., *Does Transparency in Moderation Really Matter?: User Behavior After Content Removal Explanations on Reddit*, "Proceedings of the ACM on Human-Computer Interaction" 2019, vol. 3, no. CSCW, article 150. https://doi.org/10.1145/3359252
Komninos A., *Private Enforcement of the DMA Rules before the National Courts*, 5.4.2024. http://dx.doi.org/10.2139/ssrn.4791499
Köndgen J., *Die Rechtsquellen des Europäischen Privatrechts*, in: K. Riesenhuber (ed.), *Europäische Methodenlehre:. Handbuch für Ausbildung und Praxis*, Berlin 2006.
Lessig L., *Code and Other Laws of Cyberspace*, New York 1999.
Lubasz D., Namysłowska M. (eds.), *Akt o usługach cyfrowych: Komentarz*, Warsaw 2024.
McShane L., Sabadoz C., *Rethinking the Concept of Consumer Empowerment: Recognizing Consumers as Citizens*, "International Journal of Consumer Studies" 2015, vol. 39, no. 5, pp. 544–551, https://doi.org/10.1111/ijcs.12186
Micklitz H.-W., *Unfair Commercial Practices and Misleading Advertising*, in: N. Reich et al. (eds.), *European Consumer Law*, 2nd ed., Cambridge, Antwerp, and Portland 2014.
Micklitz H.-W., *Unfair Terms in Consumer Contracts*, in: N. Reich et al. (eds.), *European Consumer Law*, 2nd ed., Cambridge, Antwerp, and Portland 2014.
Montagnani M.L., *Virtues and Perils of Algorithmic Enforcement and Content Regulation in the EU – A Toolkit for A Balanced Algorithmic Copyright Enforcement*, "Case Western Reserve

Journal of Law, Technology and Internet" 2019–2020, vol. 11, no. 1, pp. 3–49, https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=3767008 (accessed: 3.4.2025).
Mucha J., *From Recipe to Reality: The Polish Way of Collective Redress*, "ERA Forum" 2024, vol. 25, pp. 97–108, https://doi.org/10.1007/s12027-024-00790-z
Piech M., *Pośrednicy internetowi w prawie Unii Europejskiej: Rola i obowiązki wobec treści użytkowników*, Warsaw 2019.
Podszun R., *From Competition Law to Platform Regulation – Regulatory Choices for the Digital Markets Act*, "Economics" 2023, vol. 17, no. 1, art. 20220037. https://doi.org/10.1515/econ-2022-0037
Quintais J.P., Schwermer S.F., *The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?*, "European Journal of Risk Regulation" 2022, vol. 13, no. 2, 191–217. https://doi.org/10.1017/err.2022.1
Quintais J.P. et al., *Enforcement of Terms of Service*, "German Law Journal" 2023, vol. 24, no. 5, pp. 881–911. https://doi.org/10.1017/glj.2023.53
Reich N. et al., *European Consumer Law*, 2nd ed., Cambridge, Antwerp, and Portland 2014.
Reich N., Micklitz H.-W., *Economic Law, Consumer Interests and EU Integration*, in: N. Reich et al. (eds.), *European Consumer Law*, 2nd ed., Cambridge, Antwerp, and Portland 2014.
Rosati E. *The Digital Services Act and Copyright Enforcement: The Case of Article 17 of the DSM Directive*, in: M. Cappello (ed.), *Unravelling the Digital Services Actpackage*, Strasbourg 2021, pp. 63–78.
Riesenhuber K. (ed.), *Europäische Methodenlehre: Handbuch für Ausbildung und Praxis*, Berlin 2006.
Schulte-Nölke H., *The EU Digital Services Act and EU Consumer Law*, in: A. de Franceschi, R. Schulze (ed.), *Harmonizing Digital Contract Law: The Impact of EU Directives 2019/770 and 2019/771 and the Regulation of Online Platforms: A Handbook*, Baden-Baden 2023.
Senftleben M., *Guardians of the UGC Galaxy – Human Rights Obligations of Online Platforms, Copyright Holders, Member States and the European Commission Under the CDSM Directive and the Digital Services Act*, "Journal of Intellectual Property, Information Technology and E-Commerce Law" 2023, vol. 14, no. 3, pp. 435–452. https://ssrn.com/abstract=4683206
Söderlund K., Larsson S., *Enforcement Design Patterns in EU Law: An Analysis of the AI Act*, "Digital Society" 2024, vol. 3, article 41. https://doi.org/10.1007/s44206-024-00129-8
Suzor N.P. et al., *What do We Mean When We Talk about Transparency? Toward Meaningful Transparency in Commercial Content Moderation*, "International Journal of Communication" 2019, vol. 13, pp. 1526–1543.
Szpringer W., *Platformy cyfrowe i gospodarka współdzielenia: Problemy instytucjonalne*, Warsaw 2020.
Tyagi K., Sanders A.K., Cauffman C. (eds.), *Digital Platforms, Competition Law and Regulation: Comparative Perspectives*, Oxford, New York, and Dublin 2024.
Umit Kucuk S., *Consumerism in the Digital Age*, "Journal of Consumer Affairs" 2016, vol. 50, no. 3, pp. 515–538. https://doi.org/10.1111/joca.12101
Weatherill S., *Law and Values in the European Union*, Oxford 2016.
Weatherill S., *Consumer Policy*, in: P. Craig, G. de Búrca (eds.), *The Evolution of EU Law*, 3rd ed., Oxford 2021.
Whish R., Bailey D., *Competition Law*, Oxford 2021.
Wilman F., *Between Preservation and Qualification: The Evolution of the DSA's Liability Rules in Light of the CJEU's Case Law*, w: J. van Hoboken et al. (eds.), *Putting the DSA into Practice:. Enforcement, Access to Justice and Global Implications*, Berlin 2023, pp. 35–49.

Wilman F., *The Digital Services Act (DSA) – An Overview*, 16.12.2022. http://dx.doi.org/10.2139/ssrn.4304586

Zhelyazkova A., *Challenges in EU Law Enforcement and the Digital Age*, in: M. Scholten (ed.), *Research Handbook on the Enforcement of EU Law*, Cheltenham and Northampton 2023.

LEGAL ACTS IN CHRONOLOGICAL ORDER (AKTY PRAWNE W KOLEJNOŚCI CHRONOLOGICZNEJ)

Commission Implementing Regulation (EU) 2024/2835 of 4.11.2024 laying down templates concerning the transparency reporting obligations of providers of intermediary services and of providers of online platforms under Regulation (EU) 2022/2065 of the European Parliament and of the Council (OJ L, 2024/2835, 5.11.2024).

Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11.4.2024 amending Regulation (EU) No. 910/2014 as regards establishing the European Digital Identity Framework (OJ L, 2024/1183, 30.4.2024).

Regulation (EU) 2024/900 of the European Parliament and of the Council of 13.3.2024 on the transparency and targeting of political advertising (OJ L, 2024/900, 20.3.2024).

Commission Implementing Regulation (EU) 2024/607 of 15.2.2024 on the practical and operational arrangements for the functioning of the information sharing system pursuant to Regulation (EU) 2022/2065 of the European Parliament and of the Council (Digital Services Act) (OJ L, 2024/607, 16.2.2024).

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13.12.2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (OJ L, 2023/2854, 22.12.2023).

Commission Decision of 5.9.2023 designating Alphabet as a gatekeeper pursuant to Art. 3 DMA (Cases DMA.100011 – Alphabet – OIS Verticals; DMA.100002 – Alphabet – OIS App Stores; DMA. 100004 – Alphabet – Online search engines; DMA.100005 – Alphabet – Video sharing; DMA.100006 – Alphabet – Number-independent interpersonal communications services; DMA.100009 – Alphabet – Operating systems; DMA.100008 –- Alphabet – Web browsers, DMA.100010 – Alphabet – Online advertising services) (OJ C, 2023/549, 27.10.2023).

Commission Decision of 5.9.2023 designating Amazon as a gatekeeper pursuant Art. 3 DMA (Cases DMA.100018 Amazon – online intermediation services – marketplaces; DMA.100016 Amazon – online advertising services) (OJ C, 2023/905, 15.11.2023).

Commission Decision of 5.9.2023 designating Apple as a gatekeeper pursuant to Art. 3 DMA (Cases DMA.100013 Apple – online intermediation services – app stores; DMA.100025 Apple – operating systems and DMA.100027 Apple – web browsers) (OJ C, 2023/548, 27.10.2023).

Commission Decision of 5.9.2023 designating ByteDance as a gatekeeper pursuant to Art. 3 DMA (case DMA.100040 ByteDance – Online social networking services) (OJ C, 2023/552, 27.10.2023).

Commission Decision of 5.9.2023 designating Meta as a gatekeeper pursuant to Art. 3 DMA (Cases DMA.100020 Meta – online social networking services; DMA.100024 Meta – number-independent interpersonal communications services; DMA.100035 Meta – online advertising services; DMA.100044 Meta – online intermediation services – marketplace) (OJ C, 2023/1092, 23.11.2023).

Commission Decision of 5.9.2023 designating Microsoft as a gatekeeper pursuant to Art. 3 DMA (Cases DMA.100017 Microsoft – online social networking services; DMA.100023 Microsoft – number-independent interpersonal communications services; DMA.100026 Microsoft – operating systems) (OJ C, 2023/549, 27.10.2023).

Commission Implementing Regulation (EU) 2023/1201 of 21.6.2023 on detailed arrangements for the conduct of certain proceedings by the Commission pursuant to Regulation (EU) 2022/2065 of the European Parliament and of the Council (Digital Services Act) (OJ L 159, 22.6.2023, pp. 51–59).

Regulation (EU) 2023/988 of the European Parliament and of the Council of 10.5.2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC (OJ L 135, 23.5.2023, pp. 1–51).

Commission Implementing Regulation (EU) 2023/814 of 14.4.2023 on detailed arrangements for the conduct of certain proceedings by the Commission pursuant to Regulation (EU) 2022/1925 of the European Parliament and of the Council (OJ L 102, 17.4.2023).

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19.10.2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, pp. 1–102).

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14.9.2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, pp. 1–66).

Regulation (EU) 2022/868 of the European Parliament and of the Council, 30.5.2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (OJ L 152, 3.6.2022, pp. 1–44).

Directive (EU) 2020/1828 of the European Parliament and of the Council of 25.11.2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, pp. 1–27).

Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20.6.2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No. 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, pp. 1–44).

Directive (EU) 2019/1937 of the European Parliament and of the Council of 23.10.2019 on the protection of persons who report breaches of Union law (OJ L 305, 26.11.2019, pp. 17–56).

Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20.6.2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019, pp. 57–79).

Directive (EU) 2019/790 of the European Parliament and of the Council of 17.4.2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, pp. 92–125).

Directive (EU) 2019/771 of the European Parliament and of the Council of 20.5.2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC (OJ L 136, 22.5.2019, pp. 28–50).

Directive (EU) 2019/770 of the European Parliament and of the Council of 20.5.2019 on certain aspects concerning contracts for the supply of digital content and digital services (OJ L 136, 22.5.2019, pp. 1–27).

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11.12.2018 establishing the European Electronic Communications Code (Recast), (OJ L 321, 17.12.2018, pp. 36–214).

Directive (EU) 2018/1808 of 14.11.2018 Amending Directive 2010/13/EU on the Coordination of Certain Provisions Laid down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) in View of Changing Market Realities (OJ L 303, 28.11.2018, pp. 69–92).

Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12.12.2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No. 2006/2004 (OJ L 345, 27.12.2017, pp. 1–26).

Charter of Fundamental Rights of the European Union (OJ C 202, 7.6.2016, pp. 389–405).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.4.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, pp. 1–88).

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9.9.2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, pp. 1–15).

Directive 2014/104/EU of the European Parliament and of the Council of 26.11.2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union (OJ L 349, 5.12.2014, pp. 1–19).

Directive 2013/11/EU of the European Parliament and of the Council of 21.5.2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR) (OJ L 165, 18.6.2013, pp. 63–79).

Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12.12.2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, pp. 1–32).

Directive 2011/83/EU of the European Parliament and of the Council of 25.10.2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (OJ L 304, 22.11.2011, pp. 64–88).

Directive 2010/13/EU of the European Parliament and of the Council of 10.3.2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (OJ L 95, 15.4.2010, pp. 1–24).

Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17.6.2008 on the law applicable to contractual obligations (Rome I) (OJ L 177, 4.7.2008, pp. 6–16).

Treaty on the Functioning of the European Union of 13.12.2007 – consolidated version (OJ C 202, 7.6.2016, pp. 47–360).

Directive 2005/29/EC of the European Parliament and of the Council of 11.5.2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) (OJ L 149, 11.6.2005, pp. 22–39).

Council **Regulation (EC) No 1/2003** of 16.12.2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (OJ L 1, 4.1.2003, pp. 1–25).

Treaty establishing the European Community (Consolidated version 2002) (OJ C 325, 24.12.2002, pp. 33–184).

Directive 2001/95/EC of the European Parliament and of the Council of 3.12.2001 on general product safety (OJ L 11, 15.1.2002, pp. 4–17).

Directive 2000/31/EC of the European Parliament and of the Council of 8.6.2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ L 178, 17.7.2000, pp. 1–16).

Directive 1999/44/EC of the European Parliament and of the Council of 25.5.1999 on certain aspects of the sale of consumer goods and associated guarantees (OJ L 171, 7.7.1999, pp. 12–16).

Council **Directive 93/13/EEC** of 5.4.1993 on unfair terms in consumer contracts (OJ L 95, 21.4.1993, pp. 29–34).

SOFT LAW IN CHRONOLOGICAL ORDER (DOKUMENTY PRAWNIE NIEWIĄŻĄCE W KOLEJNOŚCI CHRONOLOGICZNEJ)

European Commission, Proposal for a directive of the European Parliament and of the Council on substantiation and communication of explicit environmental claims (Green Claims Directive), COM(2023) 166 final, Brussels, 22.3.2023.

European Declaration on Digital Rights and Principles for the Digital Decade (OJ C 23, 23.1.2023, pp. 1–7).

European Economic and Social Committee, Opinion. Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, INT/929-EESC-2021, 27.4.2021.

European Commission, EU strategy on the rights of the child, COM(2021) 142 final, Brussels, 24.3.2021.

European Commission, Communication from the Commission to the European Parliament and the Council. New Consumer Agenda Strengthening consumer resilience for sustainable recovery, COM(2020) 696 final, Brussels, 13.11.2020.

European Commission, 'Impact Assessment of the Digital Services Act', SWD (2020) 348 final, n.d.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Shaping Europe's Digital Future", COM(2020) 67 final, Brussels, 19.2.2020.

Commission Decision of 26.4.2018 on setting up the group of experts for the Observatory on the Online Platform Economy, C(2018) 2393 final, Brussels, 26.4.2018.

Commission Recommendation (EU) 2018/334 of 1.3.2018 on measures to effectively tackle illegal content online, C/2018/1177 (OJ L 63, 6.3.2018, pp. 50–61).

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *A Digital Single Market Strategy for Europe*, COM/2015/0192 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Online Platforms and the Digital Single Market Opportunities and Challenges for Europe, COM (2016) 288 final.

Communication from the Commission, Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (OJ C 45, 24.2.2009, pp. 7–20).
Council Resolution of 19.1.1999 on the Consumer Dimension of the Information Society (OJ of the EC 1999/C 23/01).
Commission of the EC, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions. Europe at the Forefront of the Global Information Society: Rolling Action Plan, COM(96) 607 final, Brussels, 27.11.1996.
Commission of the EC, Communication from the Commission. Priorities for Consumer Policy 1996–1998, COM(95) 519 final, Brussels, 31.10.1995.
Commission of the EC, Europe's Way to the Information Society. An Action Plan. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, COM(94) 347 final, Brussels, 19.7.1994.
Commission of the EC, Three Year Action Plan of Consumer Policy in the EEC (1990–1992), COM(90) 98 final, Brussels, 3.5.1990.
Commission of the EC, Communication from the Commission to the Council of 4.7.1985. The need for a new impetus for consumer protection policy, Bulletin of the European Communities, supplement 6/86, COM(85) 314 final.
Council Resolution of 14.4.1975 on a preliminary programme of the European Economic Community for a consumer protection and information policy (OJ C 92, 25.4.1975, pp. 1–16).

CASE LAW OF THE CJEU IN CHRONOLOGICAL ORDER (ORZECZNICTWO TSUE W KOLEJNOŚCI CHRONOLOGICZNEJ)

C-605/21, 18.4.2024, *Heureka Group a.s. v Google LLC* (ECLI:EU:C:2024:324).
C-639/23 P(R), Order of the Vice-President of the Court, 27.3.2024, *European Commission v Amazon Services Europe Sàrl* (ECLI:EU:C:2024:277).
C-570/21, 8.6.2023, *I.S. and K.S. v YYY.S.A.* (ECLI:EU:C:2023:456).
C-300/21, 4.5.2023, *UI v Österreichische Post AG* (ECLI:EU:C:2023:370).
C-401/19, 26.4.2022, *Republic of Poland v European Parliament and Council of the European Union* (ECLI:EU:C:2022:297).
C-682/18 and C-683/18, 22.6.2021, *Frank Peterson v Google LLC and Others and Elsevier Inc. v Cyando AG* (ECLI: EU:C:2021:503).
C-62/19, 3.12.2020, *Star Taxi App SRL v Unitatea Administrativ Teritorială Municipiul Bucureşti prin Primar General and Consiliul General al Municipiului Bucureşti* (ECLI:EU:C:2020:980).
C-500/18, 2.4.2020, *AU v Reliantco Investments LTD and Reliantco Investments LTD Limassol Sucursala Bucureşti* (ECLI:EU:C:2020:264).
C-390/18, 19.12.2019, *Criminal proceedings against X* (ECLI:EU:C:2019:1112).
C-18/18, 3.10.2019, *Eva Glawischnig-Piesczek v Facebook Ireland Limited* (ECLI:EU:C:2019:821).
C-498/16, 25.1.2018, *Maximilian Schrems v Facebook Ireland Limited* (ECLI:EU:C:2018:37).
C-434/15, 11.05.2017, Opinion of Advocate General Szpunar, *Asociación Profesional Elite Taxi v Uber Systems Spain, SL* (ECLI:EU:C:2017:364).
C-434/15, 20.12.2017, *Asociación Profesional Élite Taxi v Uber Systems Spain, SL* (ECLI: EU:C:2017:981).
C-149/15, 9.11.2016, *Sabrina Wathelet v Garage Bietheres & Fils SPRL* (ECLI:EU:C:2016:840).

C-484/14, 15.9.2016, *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* (ECLI:EU:C:2016:689).
C-360/10, 16.2.2012, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* (ECLI:EU:C:2012:85).
C-324/09, 12.7.2011, *L'Oréal SA and Others v eBay International AG and Others* (ECLI:EU:C:2011:474).
C-236/08 –C-238/08, 23.3.2010, *Google France SARL and Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA and Luteciel SARL (C-237/08) and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others (C-238/08)* (ECLI:EU:C:2010:159).
C-453/99, 20.9.2001, *Courage Ltd v Bernard Crehan and Bernard Crehan v Courage Ltd and Others* (ECLI:EU:C:2001:465).
C-62/86, 3.7.1991, *AKZO Chemie BV v Commission of the European Communities* (ECLI:EU:C:1991:286).
C-41/90, 23.4.1991, *Klaus Höfner and Fritz Elser v Macrotron GmbH* (ECLI:EU:C:1991:161).
C-213/89, 19.6.1990, *The Queen v Secretary of State for Transport, ex parte: Factortame Ltd and others* (ECLI:EU:C:1990:257).
85/76, 13.2.1979, *Hoffmann-La Roche & Co. AG v Commission of the European Communities* (ECLI:EU:C:1979:36).
106/77, 9.3.1978, *Amministrazione delle Finanze dello Stato v Simmenthal SpA* (ECLI:EU:C:1978:49).
27/76, 14.2.1978, *United Brands Company and United Brands Continentaal BV v Commission of the European Communities* (ECLI:EU:C:1978:22).
127/73, 30.1.1974, *Belgische Radio en Televisie and société belge des auteurs, compositeurs et éditeurs v SV SABAM and NV Fonior* (ECLI:EU:C:1974:6).
26/62, 5.2.1963, *NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration* (ECLI:EU:C:1963:1).

STUDIES, REPORTS, RECOMMENDATIONS (STUDIA, RAPORTY, REKOMENDACJE)

Council of Europe, *Content Moderation: Best Practices Towards Effective Legal and Procedural. Frameworks for Self-Regulatory and Co-regulatory Mechanisms of Content Moderation, Guidance Note Adopted by the Steering Committee for Media and Information Society (CDMSI) at Its 19th Plenary Meeting, 19–21 May 2021*, 2021, https://edoc.coe.int/en/internet/10198-content-moderation-guidance-note.html.
Council of Europe, European Union Agency for Fundamental Rights, *Handbook on European law relating to the rights of the child*, Luxembourg 2022, https://data.europa.eu/doi/10.2811/610564.
Guiding Principles on Business and Human Rights, Implementing the UN Protect-Respect-Remedy Framework, New York and Geneva 2011, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.
European Commision, *Shaping Europe's Digital Future*, Luxembourg 2020, https://eufordigital.eu/wp-content/uploads/2020/04/communication-shaping-europes-digital-future-feb2020_en_4.pdf.

European Commission: Directorate-General for Competition and Schweitzer H., *The New Competition Tool: Its Institutional Set Up and Procedural Design: Expert Study*, Brussels 2020, https://data.europa.eu/doi/10.2763/060011.
Flash Eubarometer 469. Report. Illegal Content Online, European Union, 4.6.2018, https://europa.eu/eurobarometer/surveys/detail/2201.
Kaye D., *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, Geneva 2018.
Pírková E., Pallero J., *26 Recommendation on Content Governance. A Guide for Lawmakers, Regulators and Company Policy Makers*, Access Now, 2020, https://www.accessnow.org/guide/guide-how-to-protect-human-rights-in-content-governance/.
Quintais J.P. et al., *Discussion Report: The Role of Fundamental Rights in Out-of-Court Dispute Settlement Under Art. 21 DSA*, November 2024.
Side-stepping rights. Regulating Speech by Contract. Policy Brief, London 2018, https://www.article19.org/wp-content/uploads/2018/06/Regulating-speech-by-contract-WEB.pdf.
Zimmer D., Göhsl J.F., *Enforcement of the Digital Markets Act*, Verfassungsblog 2024, https://verfassungsblog.de/enforcement-of-the-digital-markets-act/.

OTHERS
(INNE)

Apple's Non-Confidential Summary of DMA Compliance Report, 7.3.2024, https://www.apple.com/legal/dma/dma-ncs.pdf.
Bania K., Geradin D., Huijts S., *7 March Is DMA D-Day: What Does This Mean?*, The Platform Law Blog, 7.3.2024, https://theplatformlaw.blog/2024/03/07/7-march-is-dma-d-day-what--does-this-mean/.
Commission Fines Apple over €1.8 Billion over Abusive App Store Rules for Music Streaming Providers, European Union, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1161.
Commission Opens Formal Proceedings Against X Under the Digital Services Act 18.12.2023, European Union, https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6709.
Commission Sends Request for Information to X, European Union, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4953.
Commission Sends Statement of Objections to Google over Abusive Practices in Online Advertising Technology, European Union, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3207.
Communications Decency Act of 1995, Congress.gov, https://www.congress.gov/bill/104th-congress/senate-bill/314.
Compliance Reports, European Union, https://digital-markets-act-cases.ec.europa.eu/reports/compliance-reports.
Council of the European Union, Press release, 25.11.2021, https://www.consilium.europa.eu/pl/press/press-releases/2021/11/25/what-is-illegal-offline-should-be-illegal-online-council-agrees-on-position-on-the-digital-services-act/.
Council of the European Union, Press release, 5.8.2024, https://ec.europa.eu/commission/presscorner/detail/en/IP_24_4161.
Dang S., *Musk's X Aims to Hire 100 Content Moderators in Austin by End of Year*, Reuters, 27.1.2024, https://www.reuters.com/technology/musks-x-aims-hire-100-content-moderators-austin--by-end-year-2024-01-27/.

Découvrir l'institution, Arcom, https://www.arcom.fr/nous-connaitre/decouvrir-linstitution.
Digital Services Act Package, European Union, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.
Digital Services Coordinators, European Union, https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs.
DSA Transparency Database, European Union, https://transparency.dsa.ec.europa.eu/.
Dworkin E., *Elon Musk Wants a Free Speech Utopia: Technologists Clap Back*, The Washington Post, 18.4.2022, https://www.washingtonpost.com/technology/2022/04/18/musk-twitter--free-speech/.
Geradin D., *Ensuring DMA Compliance: What Are the Business Users' Options?*, The Platform Law Blog, 28.11.2023, https://theplatformlaw.blog/2023/11/28/ensuring-dma-compliance--what-are-the-business-users-options/.
Ortutay B., O'Brien M., The Associated Press, *Elon Musk Fires Outsourced Content Moderators Who Track Hate and Harmful Posts on* Twitter, Fortune, 14.11.2022, https://fortune.com/2022/11/13/twitter-elon-musk-fires-outsourced-content-moderators-track-hate-harmful.
Stay Loud. Know Your Rights, Bits of Freedom, 17.4.2024, https://www.jouwplatformrechten.nl/en/rights/moderation.
X Safety, *Freedom of Speech, Not Reach: An Update on our Enforcement Philosophy*, Blog X, 17.4.2023, https://blog.x.com/en_us/topics/product/2023/freedom-of-speech-not-reach--an-update-on-our-enforcement-philosophy.

Oddawany w ręce czytelników Handbook jest efektem pracy dydaktycznej i naukowej zespołu Katedry Jean Monnet Digital Single Market and the Free Flow of Information. W jego skład wchodzą pracownicy Wydziału Prawa i Administracji Uniwersytetu im. Adama Mickiewicza w Poznaniu: prof. UAM dr hab. Katarzyna Klafkowska-Waśniowska, dr Igor B. Nestoruk oraz dr Miłosz Malaga, będący ekspertami w zakresie prawa jednolitego rynku, mediów cyfrowych i prawa autorskiego oraz ochrony konsumenta i prawa konkurencji.

Celem publikacji jest wyjaśnienie i poddanie krytyce nowych unijnych rozporządzeń: Aktu o usługach cyfrowych i Aktu o rynkach cyfrowych. Analiza prowadzona jest z dwóch perspektyw: użytkowników platform, którzy rozumiani są jako korzystający z prawa do rozpowszechniania i otrzymywania informacji, jako konsumenci oraz jako tzw. użytkownicy biznesowi, a także skutecznej ochrony ich praw.

The Handbook is the result of teaching and scientific work by the team from the Jean Monnet Chair of the Digital Single Market and the Free Flow of Information. This team is composed of employees of the Faculty of Law and Administration at Adam Mickiewicz University in Poznań: Prof. UAM dr hab. Katarzyna Klafkowska-Waśniowska, Dr. Igor B. Nestoruk and Dr. Miłosz Malaga, who are experts in Single Market law, digital media and copyright law, as well as consumer protection and competition law.

The aim of the publication is to explain and critique the new EU Regulations: the Digital Services Act and Digital Markets Act. The analysis is conducted from two perspectives: platform users, who are understood as exercising their right to disseminate and receive information, as consumers, and then as 'business users', along with the effective protection of their rights.

ISBN 978-83-232-4438-7 (PDF)