

dr Iga Małobęcka-Szwast

Uniwersytet Warszawski, Wydział Prawa i Administracji, Katedra Prawa Europejskiego
(ORCID: <https://orcid.org/0000-0002-4719-4899>)

Zwodnicze interfejsy w świetle DSA i innych aktów prawa unijnego – wielopoziomowy zakaz

Słowa kluczowe: *dark patterns, zwodnicze interfejsy, DSA, DMA, akt w sprawie sztucznej inteligencji*

Celem artykułu jest przedstawienie, w jaki sposób działania legislacyjne podejmowane na poziomie unijnym przeciwdziałają praktykom typu *dark patterns* (zwodniczym interfejsom), a także jakie są między nimi relacje i jak skutecznie egzekwować wielopłaszczyznowy zakaz stosowania zwodniczych interfejsów, który wyłania się z dokonanego przeglądu. Chociaż zwodnicze interfejsy można oceniać przez pryzmat różnych regulacji, w artykule skupiono się przede wszystkim na: akcie o usługach cyfrowych, RODO, dyrektywie o nieuczciwych praktykach handlowych, akcie o rynkach cyfrowych, akcie w sprawie sztucznej inteligencji, akcie w sprawie danych oraz dyrektywie w sprawie umów o usługi finansowe zawieranych na odległość. W celu stawienia czoła wyzwaniom związanym z wielopoziomowym zwalczaniem zwodniczych interfejsów oraz wzajemnym nakładaniem się na siebie omawianych regulacji autorka postuluje wprowadzenie konkretnych proceduralnych mechanizmów współpracy między organami i instytucjami odpowiedzialnymi za ich egzekwowanie – zarówno na poziomie krajowym, jak i unijnym.

1. Wprowadzenie

Zwodnicze interfejsy (ang. *dark patterns*)¹ nie są nową koncepcją, choć relatywnie od niedawna pod tym pojęciem pojawiają się w debacie publicznej i akademickiej dotyczącej bezpiecznego i godnego zaufania środowiska cyfrowego (internetowego)². Te oszukańcze praktyki są zwykle wykorzystywane przez przedsiębiorców działających online po to, by manipulować zachowaniami użytkowników i skłaniać ich do podejmowania decyzji i wyborów, które leżą w interesie tych przedsiębiorców. W ostatnich latach o praktykach typu *dark patterns* jest coraz głośniejsze – w UE przede wszystkim za sprawą działań podejmowanych przez unijne i krajowe instytucje i organy zajmujące się ochroną danych i ochroną konsumentów, które mają na celu zwalczanie zwodniczych interfejsów w środowisku cyfrowym, ale również działań regulacyjnych podejmowanych przez unijnego prawodawcę.

Unijne instytucje, świadome negatywnych skutków, jakie zwodnicze interfejsy niosą ze sobą dla różnych uczestników

rynków cyfrowych, ale także dla rozwoju całej gospodarki cyfrowej w UE, podejmują działania legislacyjne, których celem jest rozwiązanie problemu zwodniczych interfejsów³. Pierwszym aktem prawnym, który wprost posługuje się pojęciem zwodniczych interfejsów, jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z 19.10.2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)⁴ (motyw 67), który z pewnością przyczynił się do popularyzacji samego pojęcia, ale też samego problemu, który za tym pojęciem stoi. Nie jest to jednak jedyny akt prawa unijnego, którego celem jest zwalczanie zwodniczych interfejsów. Celem artykułu jest przedstawienie, w jaki sposób działania legislacyjne podejmowane na poziomie unijnym⁵ przeciwdziałają praktykom typu *dark patterns*, a także jakie są między nimi relacje i jak skutecznie egzekwować wielopłaszczyznowy zakaz stosowania zwodniczych interfejsów, który

1 Pojęcie *dark patterns* na tyle upowszechniło się w języku prawniczym i debacie publicznej na temat tego zjawiska, że będzie stosowane zamiennie z tłumaczeniem tego pojęcia na język polski – zwodnicze interfejsy.

2 OECD, *Dark commercial patterns*. OECD Digital Economy Papers, No. 336, OECD 2022, s. 9, https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/10/dark-commercial-patterns_9f6169cd/44f5e846-en.pdf (dostęp: 4.03.2025 r.).

3 M.R. Leiser, C. Santos, *Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface*, „European Journal of Law and Technology” 2024/1.

4 Dz.Urz. UE L 277, s. 1, ze zm. – dalej DSA.

5 Niniejszy artykuł odnosi się wyłącznie do aktów prawa unijnego i nie odnosi się polskich aktów prawnych, w tym ustaw implementujących akty prawa unijnego. Analizy polskiego porządku prawnego z perspektywy tego, jak odnosi się do praktyk określanych pojęciem *dark patterns*, dokonała K. Szota, *Dark patterns a ochrona konsumenta w świetle polskiego prawa*, Warszawa 2022.

wylania się z dokonanego przeglądu⁶. Chociaż zwodnicze interfejsy można oceniać przez pryzmat różnych regulacji, poniżej skupiam się przede wszystkim na: akcie o usługach cyfrowych, RODO⁷, dyrektywie o nieuczciwych praktykach handlowych⁸, akcie o rynkach cyfrowych⁹, akcie w sprawie sztucznej inteligencji¹⁰, akcie w sprawie danych¹¹ oraz dyrektywie w sprawie umów o usługi finansowe zawieranych na odległość¹².

2. Pojęcie i rodzaje zwodniczych interfejsów

Pojęcie *dark patterns* nie jest nowe – ukuł je w 2010 r. Amerykanin Harry Brignull, *UX designer*, aby zbiorczo określić „sztuczki stosowane w witrynach internetowych i aplikacjach, które powodują, że robisz rzeczy, których nie miałeś na myśli, np. kupujesz coś lub rejestrujesz się gdzieś”¹³. Pierwszym aktem prawnym, który wprost wspomina o zwodniczych interfejsach, wprowadzając ich definicję, jest DSA. Czini to przy tym nie w tekście głównym aktu (w art. 3 poświęconym definicjom), lecz w jego preambule, więc nie jest to typowa definicja legalna. Zgodnie z motywem 67 DSA zwodnicze interfejsy na interfejsach internetowych platform internetowych to praktyki, które w istotny sposób zniekształcają lub ograniczają, celowo lub w praktyce, zdolność odbiorców usługi do dokonywania niezależnych i świadomych wyborów lub podejmowania takich decyzji. Praktyki te mogą być wykorzystywane w celu nakłonienia odbiorców usługi do niepożądanego zachowania lub do podejmowania niepożądanych decyzji, które mają dla nich negatywne skutki. Podobną definicję zawiera motyw 41

dyrektywy 2023/2673, która jest jednak dostosowana do celu regulacyjnego tego aktu (tj. ochrony konsumentów przy zawieraniu umów o usługi finansowe na odległość).

Definicja zwodniczych interfejsów pojawia się również w różnych dokumentach unijnych, które uwzględniają specyfikę obszaru regulacyjnego, do którego się odnoszą. Dla przykładu, w raporcie *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation*¹⁴, który poświęcony jest nieuczciwym praktykom rynkowym, wskazano, że *dark patterns* to pojęcie, które jest powszechnie stosowane w odniesieniu do praktyk w interfejsach cyfrowych, które sterują, oszukują, wymuszają lub manipulują konsumentami, aby dokonywali wyborów, które często nie leżą w ich najlepszym interesie.

Z kolei Europejska Rada Ochrony Danych w swoich wytycznych 3/2022 w sprawie tzw. *deceptive design patterns* (zwodnicze wzorce projektowe) w interfejsach platform społecznościowych¹⁵ poddała analizie nieco odmienne pojęcie od *dark patterns* (tj. *deceptive design pattern*)¹⁶ w węższym kontekście interfejsów platform społecznościowych. Wytyczne przedstawiają definicję zwodniczych wzorców projektowych (ang. *deceptive design patterns*), z uwzględnieniem znaczenia tej praktyki dla prawa ochrony danych osobowych. Zwodnicze wzorce projektowe zdefiniowane są tam jako interfejsy i ścieżki użytkownika realizowane na platformach mediów społecznościowych, które próbują wpłynąć na użytkowników, aby podejmowali niezamierzone, niedobrowolne i potencjalnie szkodliwe dla siebie decyzje, które są często sprzeczne z interesami użytkowników, ale zgodne z interesami platform mediów społecznościowych, w zakresie przetwarzania ich danych osobowych. Takie praktyki mają na celu wpływanie na zachowanie użytkowników i mogą utrudniać im skuteczną ochronę danych osobowych oraz dokonywanie świadomych wyborów.

Z kolei OECD posługuje się pojęciem zwodniczych wzorców (handlowych) (ang. *dark (commercial) patterns*) na określenie szerokiej gamy praktyk powszechnie spotykanych w interfejsach internetowych użytkownika, które sprawiają, że konsumenci dokonują wyborów, które mogą nie leżeć w ich najlepszym interesie, w tym poprzez wykorzystywanie uprzedzeń

6 Przegląd unijnych aktów prawnych, które mogą dotyczyć wybranych zwodniczych interfejsów, znajduje się np. w OECD, *Dark commercial...*, s. 68–71.

7 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1 ze zm.) – dalej RODO.

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

9 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z 14.09.2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym oraz zmiany dyrektyw (UE) 2019/137 i (UE) 2020/1828 (akt o rynkach cyfrowych) (Dz.Urz. UE L 265, s. 1) – dalej DMA.

10 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13.06.2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz.Urz. UE L 2024/1689) – dalej AIA.

11 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z 13.12.2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) (Dz.Urz. UE L 2023/2854) – dalej akt w sprawie danych.

12 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2023/2673 z 22.11.2023 r. zmieniająca dyrektywę 2011/83/UE w odniesieniu do umów o usługi finansowe zawieranych na odległość oraz uchylająca dyrektywę 2002/65/WE (Dz.Urz. UE L 2023/2673) – dalej dyrektywa 2023/2673.

13 Zob. <https://www.deceptive.design/> (dostęp: 26.02.2025 r.); M.R. Leiser, W. Yang, *Illuminating manipulative design: From 'dark patterns' to information asymmetry and the repression of free choice under the Unfair Commercial Practices Directive*, „Loyola Consumer Law Review” 2023/3, s. 484.

14 F. Lupiáñez-Villanueva, A. Boluda, F. Bogliacino, G. Liva, L. Lechardoy, T. Rodríguez de las Heras Ballell, *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation*, 2022, s. 20, <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418> (dostęp: 5.08.2024 r.).

15 Guidelines 3/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, Version 2.0, przyjęte 14.02.2023 r. (brak oficjalnej polskiej wersji językowej), https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf (dostęp: 4.03.2025 r.) – dalej wytyczne EROD.

16 Po konsultacjach publicznych pierwotne wytyczne EROD zostały zaktualizowane w celu odzwierciedlenia otrzymanych uwag, w tym na temat zastąpienia w tytule pojęcia *dark patterns* szerszym pojęciem *deceptive design patterns*, które w ocenie EROD lepiej oddaje różnorodność pojawiających się zwodniczych praktyk. Wytyczne w wersji skierowanej do konsultacji publicznych nosiły nazwę: Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them, Version 1.0, przyjęte 14.03.2022 r., s. 8, https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf (dostęp: 5.08.2024 r.).

konsumentów. Zazwyczaj mają one na celu skłonienie konsumentów do oddania większej ilości pieniędzy, danych osobowych lub czasu, uwagi, niż jest to pożądane.

Powyższy przegląd najczęściej przywoływanych definicji pokazuje, że do dziś brak jest jednej uniwersalnej definicji zwodniczych interfejsów, a każda z nich uwzględnia kontekst regulacyjny aktu prawnego lub dokumentu, w którym się znajduje. Na tym tle warto jednak poczynić kilka uwag co do rozumienia pojęcia zwodniczych interfejsów. Po pierwsze, praktyki typu *dark patterns* mogą być kierowane nie tylko do odbiorców usług w rozumieniu DSA lub konsumentów. Odbiorcami takich praktyk może być każda osoba fizyczna wchodząca w interakcję z zasobami dostępnymi w internecie (np. poprzez odwiedzenie strony internetowej), niezależnie od swojego profesjonalnego lub nieprofesjonalnego charakteru – taką osobę możemy określić mianem użytkownika¹⁷. Nie ma zatem znaczenia, czy osoba taka jest konsumentem, czy przedsiębiorcą, czy jest odbiorcą usług świadczonych przez platformy internetowe w rozumieniu DSA, czy odbiorcą innych usług świadczonych przez internet. W konsekwencji, by objąć pojęciem zwodniczych interfejsów jak najszersze grono potencjalnych odbiorców takich praktyk, lepiej posługiwać się pojęciem osoby fizycznej lub użytkownika.

Po drugie, choć większość zwodniczych interfejsów przejawia się w interfejsach użytkownika, co odzwierciedlone jest w przywołanych powyżej definicjach, to niektóre – te najbardziej podstępne i trudne do wykrycia – można znaleźć na poziomie architektury systemu (w literaturze określa się je mianem *darkest patterns*)¹⁸. Takie praktyki są zwykle trudniej dostrzegalne dla użytkownika i charakteryzują się wyrafinowaną podstawą algorytmiczną. Są zaprojektowane w taki sposób, aby wykorzystywać uprzedzenia poznawcze, personalizować doświadczenia poprzez hiper-nakłanianie (ang. *hyper-nudging*) i działać zarówno na poziomie indywidualnym, jak i zbiorowym, często poza bezpośrednią percepcją użytkowników¹⁹. Stąd warto, by rozważając problem zwodniczych interfejsów, ujmować go szerzej, jako praktykę, która nie ogranicza się wyłącznie do interfejsów internetowych²⁰. Takie podejście jest również bliskie unijnemu prawodawcy, który w AIA ewidentnie zmierzał do uregulowania tych najbardziej wyrafinowanych zwodniczych interfejsów opartych na systemach sztucznej inteligencji, które nie są objęte definicją z DSA²¹ (zob. art. 5 ust. 1 lit. a AIA).

W konsekwencji, modyfikując definicję zawartą w motywie 67 DSA w świetle powyższych uwag, na potrzeby niniejszego artykułu można przyjąć, że **zwodnicze interfejsy to praktyki, które w istotny sposób zniekształcają lub ograniczają, celowo lub w praktyce, zdolność użytkowników do dokonywania niezależnych i świadomych wyborów lub podejmowania takich**

decyzji, które mogą być wykorzystywane w celu nakłaniania ich do niepożądanego zachowania lub do podejmowania niepożądanych decyzji, które mają dla nich negatywne skutki.

Do tej pory brak jest również jednej powszechnie przyjętej taksonomii zwodniczych interfejsów²² (choć mając na względzie szybki postęp technologiczny, stworzenie taksonomii odpornej na przyszłe zmiany wydaje się niemożliwe i niecelowe). Zwykle wyróżnia się 7 głównych kategorii, które mogą obejmować więcej niż jeden rodzaj zwodniczych interfejsów:

- 1) **wymuszone działanie** (ang. *forced action*) – to praktyki obejmujące wymuszanie podjęcia określonych działań przez użytkownika w celu uzyskania dostępu do określonej funkcjonalności lub treści. W szczególności użytkownik może zostać zmuszony do rejestracji w usłudze, pomimo że nie jest ona konieczna (ang. *forced registration*), lub może zostać zmuszony do ujawnienia większej ilości danych osobowych, niż jest to konieczne do pełnego korzystania z danej usługi. Innym przykładem jest pozyskiwanie i wykorzystywanie informacji o kontaktach użytkownika, w tym bez jego zgody, w celu korzystania z usługi (ang. *friend spamming* albo *social pyramid*);
- 2) **ingerencja w interfejs** (ang. *interface interference*) – zwodnicze interfejsy obejmujące różne formy ingerencji w interfejs, które mają na celu skłonienie użytkownika do podjęcia działań korzystnych dla firmy. Przykłady obejmują: zasłanianie ważnych informacji (ang. *hidden information*), domyślne zaznaczanie opcji korzystnych dla firmy (ang. *preselection*), tworzenie fałszywej hierarchii poprzez nadawanie wizualnego pierwszeństwa opcjom korzystnym dla firmy (ang. *false hierarchy*), wyświetlanie obniżonej ceny w odniesieniu do pierwotnej wprowadzającej w błąd lub fałszywej wyższej ceny (ang. *misleading reference pricing*), stosowanie podchwytliwych pytań lub/i dwuznacznego języka (np. podwójne przeczenia; ang. *trick wording*), ukrywanie reklam (ang. *disguised ads*), wykorzystywanie emocji w celu nakłaniania użytkowników do odstąpienia od dokonania określonego wyboru (ang. *toying with emotions*, np. zawstydzanie, wzbudzanie u użytkownika poczucia winy, ang. *confirms shaming*);
- 3) **nagabywanie** (nękanie) (ang. *nagging*) – to zwodnicze interfejsy obejmujące powtarzające się prośby do użytkownika o zrobienie czegoś, co leży w interesie firmy, np. powtarzające się prośby o włączenie powiadomień lub wyrażenie zgody na śledzenie lokalizacji;
- 4) **przeszkadzanie** (ang. *obstruction*) – to zwodnicze interfejsy, które utrudniają użytkownikowi wykonanie zadania lub uzyskanie dostępu do informacji, z zamiarem zniechęcenia go do działania. Przykładem może być ułatwianie rejestracji w usłudze lub wyrażenie zgody na ustawienia ingerujące w prywatność, przy jednoczesnym utrudnianiu rezygnacji z usługi (ang. *hard to cancel*) lub wyboru ustawień bardziej przyjaznych dla prywatności, np. poprzez wprowadzenie dłuższej ścieżki kliknięć w przypadku opcji niepreferowanych przez firmę. Inne przykłady obejmują utrudnianie lub uniemożliwianie usunięcia konta lub informacji o użytkowniku albo zapobieganie porównywaniu różnych ofert i cen (ang. *price comparison prevention*);

17 Zob. podobnie M.R. Leiser, C. Santos, *Dark Patterns*...

18 M.R. Leiser, *Dark patterns: The case for regulatory pluralism between the European Union's consumer and data protection regimes* [w:] *Research handbook on EU data protection law*, red. E. Kosta, R. Leenes, I. Kamara, Cheltenham 2022, s. 242; M. Leiser, *Psychological Patterns and Article 5 of the AI Act: AI-Powered Deceptive Design in the System Architecture and the User Interface*, „Journal of AI Law and Regulation” 2024/1, s. 8.

19 M.R. Leiser, C. Santos, *Dark Patterns*... Z tego względu niektórzy autorzy postulują, by zamiast pojęcia *dark patterns* posługiwać się szerszym pojęciem *deceptive design* – zob. M. Leiser, *Psychological Patterns*..., s. 9.

20 W takiej sytuacji można się zastanawiać, czy wciąż zasadne jest posługiwanie się polskim pojęciem zwodniczych interfejsów. Wydaje się, że bardziej trafne byłoby posługiwanie się pojęciem „zwodnicze wzorce projektowe”, tłumacząc angielskie pojęcie *dark patterns*.

21 M. Leiser, *Psychological Patterns*..., s. 8,

22 OECD, *Dark commercial*..., s. 9–11. Przegląd proponowanych taksonomii zwodniczych interfejsów pojawiających się w literaturze – zob. OECD, *Dark commercial*..., s. 53.

- 5) **przemycanie** (ang. *sneaking*) – to zwodnicze interfejsy, które mają na celu ukrycie, zamaskowanie lub opóźnienie ujawnienia informacji istotnych dla decyzji konsumenta, w szczególności w odniesieniu do kosztów, które musi ponieść. Pojęcie to obejmuje takie praktyki, jak: dodawanie nowych i potencjalnie znaczących nieopcjonalnych opłat do całkowitej ceny, gdy konsument jest bliski sfinalizowania zakupu, przemycanie produktu do koszyka konsumenta bez jego zgody, np. za pomocą pola wyboru na poprzedniej stronie (ang. *sneaking into basket*) lub automatyczne odnawianie zakupu (subskrypcji), w tym po okresie próbnym, bez wyraźnej zgody konsumenta – praktyka określana jako ukryta subskrypcja (ang. *hidden subscription*) lub wymuszona ciągłość (ang. *forced continuity*);
- 6) **(fałszywy) dowód społeczny** (ang. *social proof*) – to praktyki, które przywołują dowód społeczny po to, by użytkownik podjął decyzję na podstawie zachowań (opinii) innych użytkowników. Przykłady obejmują powiadomienia o aktywności innych konsumentów lub odwołania do ich ostatnich zakupów (np. „użytkownicy, którzy kupili towar X kupili również towar Y”). Takie powiadomienia o aktywności lub opinii mogą być niezgodne z prawdą lub mogą wprowadzać w błąd – wtedy mamy do czynienia z fałszywym dowodem społecznym (ang. *fake social proof*);
- 7) **(fałszywa) pilność** (ang. *(fake) urgency*) – to praktyki, które nakładają prawdziwe lub fałszywe ograniczenia czasowe lub ilościowe na transakcję w celu wywarcia presji na użytkownika po to, by dokonał zakupu. Przykłady obejmują komunikaty o niskich stanach magazynowych, wysokim popycie (ang. *low stock / high demand message*) lub licznikach czasu pokazujących czas trwania wskazania wygasającej oferty lub rabatu (ang. *countdown timer*)²³. Jeżeli takie komunikaty są nieprawdziwe, mamy do czynienia z fałszywą pilnością (ang. *fake urgency*) lub fałszywym niedoborem (ang. *fake scarcity*).

Zwodnicze interfejsy można również dzielić według ich formy.

W literaturze wskazuje się, że zwodnicze interfejsy mogą być:

- 1) **strukturalne** (np. ukrycie istotnych informacji w słabiej widocznym miejscu, domyślne zaznaczenie checkboxa ze zgodą),
- 2) **graficzne** (np. uwypuklenie pożądanego przez przedsiębiorcę opcji poprzez zastosowanie bardziej rzucającego się w oczy koloru lub pogrubionej czcionki, stosowanie niezrozumiałych czy nieintuicyjnych oznaczeń graficznych w elementach takich jak przyciski, suwaki, widżety),
- 3) **tekstowe** (np. zastosowanie niejasnego języka lub trudnych do zrozumienia komunikatów takich jak podwójna negacja) oraz
- 4) **dźwiękowe** (np. użycie efektu dźwiękowego kojarzonego z zakończeniem danej czynności sukcesem czy stosowanie rozpraszającej muzyki w tle)²⁴.

W praktyce budowa zwodniczego interfejsu często łączy w sobie więcej niż jedną formę zwodniczego interfejsu i więcej niż jeden typ praktyk.

23 OECD, *Dark commercial...*, s. 10–11; F. Lupiáñez-Villanueva, A. Boluda, F. Bogliacino, G. Liva, L. Lechardoy, T. Rodríguez de las Heras Ballell, *Behavioural study...*, s. 30 (tłumaczenie własne).

24 K. Araczeńska [w:] *Akt o usługach cyfrowych. Komentarz*, red. M. Gumularz, LEX 2024, art. 25.

W tym kontekście warto również przytoczyć wyniki badania i akcji kontrolnej stron internetowych w UE, które pokazują, jak powszechne jest zjawisko zwodniczych interfejsów w powyższym przedstawionym rozumieniu²⁵. Badanie przeprowadzone techniką tajemniczych klientów na zlecenie Komisji Europejskiej wykazało, że tego typu praktyki są coraz częściej stosowane przez dostawców platform internetowych (w szczególności sklepy internetowe) niezależnie od usług czy produktów, które oferują, czy od ich wielkości. Zgodnie z badaniem 97% najpopularniejszych stron internetowych i aplikacji używanych przez konsumentów w UE wykorzystywało co najmniej jeden zwodniczy interfejs. Najbardziej rozpowszechnione były: 1) ukryte informacje/fałszywa hierarchia, 2) wstępna selekcja, 3) dokonywanie, 4) trudne odwołania oraz 5) wymuszona rejestracja²⁶.

Z kolei na początku 2023 r. Komisja Europejska i krajowe organy ochrony konsumentów zrzeszone w sieci współpracy w zakresie ochrony konsumentów opublikowały wyniki szerokiej akcji kontrolnej stron internetowych związanych z handlem detalicznym (sklepy internetowe). Wynika z nich, że 148 z 399 badanych sklepów internetowych należących do sprzedawców detalicznych oferujących produkty z różnych sektorów stosowało jedną z trzech poniższych praktyk manipulacyjnych, które mają skłaniać konsumentów do podjęcia decyzji, które mogą nie leżeć w ich najlepszym interesie (tj. zwodnicze interfejsy): 1) fałszywe liczniki odmierzające czas, podające terminy zakupu konkretnych produktów, które nakłaniają i wywierają presję na klientów do zakupu produktu; 2) ukrywanie istotnych informacji o produkcie lub usłudze za pomocą bardzo małej czcionki, niekontrastujących kolorów lub umieszczanie istotnych informacji w mniej widocznym miejscu (takie jak informacje dotyczące kosztów dostawy, składu produktów lub dostępności tańszej opcji); 3) interfejsy internetowe zaprojektowane w taki sposób, aby skłonić konsumentów do dokonania zakupu, wykupienia abonamentu lub dokonania innego wyboru (od subskrypcji po droższe produkty lub opcje dostawy) poprzez stosowanie określonej grafiki albo używanie określonych sformułowań²⁷.

Poniżej analizie zostaną poddane wybrane unijne akty prawne, których celem jest zwalczanie zwodniczych interfejsów w rozumieniu przyjętym w tym artykule.

3. Akt o usługach cyfrowych

Akt o usługach cyfrowych – DSA – który jest stosowany w pełni od 17.02.2024 r., wprost odnosi się do zwodniczych interfejsów w motywie 67 i zakazuje ich stosowania przez platformy internetowe w art. 25. Choć art. 25 DSA nie posługuje się pojęciem zwodniczych interfejsów, tak jak robi to związany z tym przepisem motyw 67 DSA, to z treści tego przepisu jasno wynika, że zakazuje on dostawcom platform internetowych stosowania zwodniczych interfejsów. Stosownie do tego przepisu dostawcy platform internetowych nie mogą projektować,

25 Przegląd różnych badań przeprowadzonych na przestrzeni ostatnich lat przez podmioty w różnych krajach znajduje się w OECD, *Dark commercial...*, s. 54–64.

26 F. Lupiáñez-Villanueva, A. Boluda, F. Bogliacino, G. Liva, L. Lechardoy, T. Rodríguez de las Heras Ballell, *Behavioural study...*, s. 6, 45.

27 *Ochrona konsumentów: manipulacyjne praktyki internetowe wykryte w 148 z 399 skontrolowanych sklepów internetowych*, komunikat prasowy z 30.01.2023 r., https://ec.europa.eu/commission/presscorner/detail/pl/ip_23_418 (dostęp: 5.08.2024 r.).

organizować ani obsługiwać swoich interfejsów internetowych²⁸ w sposób, który wprowadza w błąd odbiorców usługi lub nimi manipuluje lub w inny istotny sposób zakłóca lub ogranicza zdolność odbiorców ich usługi do podejmowania wolnych i świadomych decyzji.

Zgodnie z DSA do takich praktyk należą m.in.:

- 1) projektowanie w sposób podstępny możliwości dokonywania wyborów w celu nakłonienia odbiorców usługi do działań, które przynoszą korzyści dostawcy platform internetowych, lecz które mogą nie leżeć w interesie odbiorców usługi;
- 2) prezentowanie wyborów w sposób nienaturalny, np. poprzez wyraźniejsze eksponowanie pewnych opcji przy pomocy elementów wizualnych, dźwiękowych lub innych, kiedy odbiorca usługi jest proszony o podjęcie decyzji;
- 3) wielokrotne zwracanie się do odbiorcy usługi o dokonanie wyboru, jeżeli takiego wyboru już dokonano;
- 4) znacznie bardziej uciążliwą procedurę anulowania usługi niż jej wybór;
- 5) utrudnianie dokonywania pewnych wyborów bądź też sprawianie, że ich dokonanie jest bardziej czasochłonne niż w przypadku innych wyborów;
- 6) bezzasadne utrudnianie zaprzestania zakupów lub wypisania się z danej platformy internetowej umożliwiającej konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość;
- 7) dezorientowanie odbiorców usługi poprzez zachęcanie ich do podejmowania decyzji dotyczących transakcji lub poprzez domyślne ustawienia, które są bardzo trudne do zmiany, a zatem powodowanie nieracjonalnej stroniowości procesu podejmowania decyzji przez usługobiorcę w sposób, który zniekształca i ogranicza jego autonomię, podejmowanie decyzji i wybór (motyw 67 DSA).

Nie jest to jednak katalog zamknięty, a Komisja Europejska może wydawać wytyczne dotyczące stosowania powyższego zakazu do konkretnych praktyk (art. 25 ust. 3 DSA), w szczególności większego eksponowania niektórych wyborów, gdy odbiorca usługi jest proszony o podjęcie decyzji, wielokrotnego żądania od odbiorcy usługi dokonania wyboru, gdy wyboru takiego już dokonał, w szczególności przez pokazywanie wyskakujących okienek, które zakłócają środowisko użytkownika, czy sprawiania, że procedura zrezygnowania z usługi jest trudniejsza niż procedura jej subskrypcji. Prawodawca unijny wyjaśnia przy tym w motywie 67 DSA, że zakaz stosowania zwodniczych interfejsów nie uniemożliwia dostawcom platform internetowych nawiązywania bezpośredniej interakcji z odbiorcami usługi i oferowania im nowych lub dodatkowych usług. Legalne praktyki (np. reklamowe), które są zgodne z prawem unijnym, nie powinny same w sobie być uznawane za zwodnicze interfejsy.

Głównym celem zakazu wprowadzonego w art. 25 DSA jest ochrona odbiorców usług, w szczególności ich zdolności do dokonywania wolnych i świadomych wyborów (autonomii decyzyjnej) przy korzystaniu z interfejsów internetowych platform²⁹. Przez eliminowanie z rynku nieuczciwych prak-

tyk art. 25 DSA służy także budowaniu zaufania do platform internetowych i szerzej – środowiska internetowego³⁰. Należy jednocześnie podkreślić, że zakaz stosowania zwodniczych interfejsów w rozumieniu DSA nie ogranicza się do stosunków konsumenckich, lecz obejmuje on także sytuacje, w których adresatem manipulacji są podmioty profesjonalne, prowadzące działalność gospodarczą. Jak słusznie wskazuje się w literaturze, takie podejście jest zgodne z ogólnymi założeniami DSA, które obejmuje ochroną wszystkie podmioty korzystające z usług pośrednictwa (wszystkich odbiorców usług), niezależnie od ich profesjonalnego lub nieprofesjonalnego działania oraz innych właściwości³¹.

Omawiany zakaz stosowania zwodniczych interfejsów z DSA w oczywisty sposób krzyżuje się z innymi unijnymi aktami prawnymi, w szczególności dotyczącymi ochrony danych osobowych i ochrony konsumentów. Stosowanie zwodniczych interfejsów przez platformy internetowe może bowiem naruszać również inne akty prawne, w szczególności RODO oraz dyrektywę 2005/29/WE o nieuczciwych praktykach rynkowych³².

Regułę rozstrzygania zbiegów między tymi przepisami i DSA zawiera art. 25 ust. 2 DSA³³. Wyjaśnia on, że DSA nie ma zastosowania do praktyk objętych dyrektywą 2005/29/WE o nieuczciwych praktykach rynkowych lub RODO, ograniczając zakres swojego zastosowania i przyznając tym aktom pierwszeństwo stosowania. Warto jednak wskazać, że takie ukształtowanie wzajemnych relacji między DSA a RODO i dyrektywą 2005/29/WE w art. 25 DSA może rodzić więcej problemów interpretacyjnych i jurysdykcyjnych niż w sytuacji jego braku. Stąd słusznie poddaje się art. 25 ust. 2 DSA krytyce i wskazuje, że przepis ten może prowadzić do niepewności prawnej³⁴. Przede wszystkim nie jest jasne, jak należy interpretować sformułowanie, że zakazu z art. 25 ust. 1 DSA nie stosuje się do praktyk, które są „objęte” dyrektywą 2005/29/WE i RODO. Dla przykładu prawie każda praktyka w sektorze cyfrowym wiąże się z przetwarzaniem danych osobowych i jako taka może zostać uznana za „objętą” RODO. Analogicznie duża część praktyk w sektorze cyfrowym dotyczy relacji między przedsiębiorcami i konsumentami i mogłaby zostać uznana za „objętą” dyrektywą 2005/29/WE. Taka interpretacja jest jednak błędna, prowadziłaby bowiem do faktycznego wniosku, że art. 25 ust. 1 DSA w praktyce (prawie) nigdy nie znajdzie zastosowania. Dlatego należy raczej przyjąć stanowisko, że wyłączenie z art. 25 ust. 2 DSA odnosi się wyłącznie do praktyk zakazanych na mocy dyrektywy 2005/29/WE lub RODO³⁵.

Oznacza to, że jeżeli dana praktyka typu *dark patterns* dostawcy platformy internetowej narusza przepisy RODO, to jej legalność będzie oceniana przez krajowy organ nadzorczy zgodnie z wymogami RODO, a nie DSA³⁶. Podobnie, jeżeli

28 Interfejs internetowy oznacza oprogramowanie komputerowe, w tym stronę internetową lub jej część, oraz aplikacje, w tym aplikacje mobilne (art. 3 lit. m DSA).

29 K. Araczeńska [w:] *Akt...*, art. 25; M. Barudi [w:] *Digital Services Act: DSA. Kommentar*, red. R. Müller-Terpitz, M. Köhler, München 2024, art. 25, s. 306.

30 M. Namysłowska, A. Jabłonowska [w:] *Akt o usługach cyfrowych. Komentarz*, red. D. Lubasz, M. Namysłowska, LEX 2024, art. 25; zob. również motyw 3 DSA.

31 M. Grochowski [w:] *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, red. M. Grochowski, Legalis 2024, art. 25 DSA; M. Namysłowska, A. Jabłonowska [w:] *Akt...*, art. 25.

32 W Polsce implementowana w drodze ustawy z 23.08.2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym (Dz.U. z 2023 r. poz. 845 ze zm.).

33 M. Grochowski [w:] *Rynek...*, art. 25.

34 M. Namysłowska, A. Jabłonowska [w:] *Akt...*, art. 25.

35 Podobnie M. Namysłowska, A. Jabłonowska [w:] *Akt...*, art. 25.

36 Przykłady takich praktyk zawarte zostały we wspomnianych już wytycznych EROD.

dana praktyka będzie naruszać krajowe ustawy implementujące dyrektywę o nieuczciwych praktykach rynkowych, zastosowanie znajdują przepisy tych ustaw, egzekwowane przez właściwe organy ds. ochrony konsumentów.

Artykuł 25 ust. 2 DSA i przyjęta ww. interpretacja tego przepisu nie rozwiąże jednak wszystkich problemów z nakładaniem się zakresów zastosowania przepisów omawianych w tym artykule. Nie zawsze da się bowiem jednoznacznie zakwalifikować daną praktykę jako naruszającą „tylko” RODO, „tylko” dyrektywę 2005/29/WE, „tylko” DSA, „tylko” DMA itd. Najczęściej w sektorze cyfrowym praktyka typu *dark patterns* będzie wchodziła w zakres zastosowania więcej niż jednego aktu prawnego³⁷, a podobnych reguł kolizyjnych jak ta zawarta w art. 25 ust. 2 DSA nie znajdziemy w pozostałych aktach prawnych³⁸.

Z praktycznym zastosowaniem art. 25 ust. 2 DSA możemy mieć do czynienia na gruncie sprawy X. Działając na podstawie omawianych przepisów, 12.07.2024 r. Komisja Europejska³⁹ poinformowała X (wcześniej Twitter) o swoim wstępnym stanowisku, że narusza on DSA w obszarach związanych z zwodniczymi interfejsami, przejrzystością reklam i dostępem naukowców do danych. W kontekście zwodniczych interfejsów Komisja uważa, że X projektuje i obsługuje swój interfejs dla zweryfikowanych kont z niebieskim znaczkiem (*blue checkmark*) w sposób, który nie odpowiada praktyce branżowej i wprowadza użytkowników w błąd. Fakt, że każdy może zapisać się i zapłacić, aby uzyskać taki „zweryfikowany” status, negatywnie wpływa na zdolność użytkowników do podejmowania swobodnych i świadomych decyzji dotyczących autentyczności kont i treści, z którymi wchodzi w interakcję, w szczególności że istnieją dowody na to, iż usługa „zweryfikowanego konta” jest nadużywana w celu oszukiwania użytkowników⁴⁰. Choć taki zarzut nie został jak dotąd podniesiony, to wydaje się, że wskazana praktyka mogłaby również zostać uznana za praktykę wprowadzającą w błąd w zakresie, w jakim użytkownicy nie są w sposób jasny i jednoznaczny informowani o istotnych cechach usługi (art. 6 ust. 1 lit. b dyrektywy 2005/29/WE).

Mając na względzie uwagi poczynione powyżej, słuszność należy przyznać stanowisku prezentowanemu w literaturze, zgodnie z którym realny wpływ zakazu z art. 25 ust. 1 DSA na zwalczanie zwodniczych interfejsów w sektorze cyfrowym jest ograniczony⁴¹. Po pierwsze, omawiany zakaz znajduje zastosowanie jedynie do platform internetowych (stosunkowo

wąsko) zdefiniowanych w art. 3 lit. i DSA⁴², a nie do wszystkich podmiotów, które mogą stosować zwodnicze interfejsy w środowisku internetowym⁴³. Po drugie, chroni on jedynie odbiorców usług dostawców platform internetowych, czyli osoby fizyczne lub prawne korzystające z usługi danego dostawcy platformy internetowej, w szczególności w celu poszukiwania informacji lub udostępnienia jej (art. 3 lit. b DSA). Po trzecie, o czym szerzej będzie poniżej, problemy interpretacyjne może rodzić niejasny art. 25 ust. 2 DSA, który ustanawia regułę rozstrzygania zbiegów między DSA a RODO i dyrektywą 2005/29/WE. Po czwarte, art. 25 ust. 1 DSA ogranicza się wyłącznie do takich zwodniczych interfejsów, które znajdują odzwierciedlenie w interfejsach internetowych w rozumieniu art. 3 lit. m DSA. Tym samym te bardziej wyrafinowane techniki manipulacyjne wbudowane w architekturę systemu pozostawione są poza zakresem zastosowania DSA⁴⁴. Ze względu na ten bardzo ograniczony zakres zastosowania DSA tym większą rolę w zwalczaniu zwodniczych interfejsów mają do odegrania pozostałe regulacje omawiane w niniejszym artykule.

4. Ogólne rozporządzenie o ochronie danych

Dane osobowe już od lat odgrywają istotną rolę w rozwoju podmiotów z sektora cyfrowego, których modele biznesowe opierają się na przetwarzaniu olbrzymiej ilości danych osobowych⁴⁵. Nie dziwi zatem, że takie podmioty (najczęściej platformy internetowe) stosują różne praktyki typu *dark patterns* po to, aby zbierać i przetwarzać najszerszy możliwy zakres danych osobowych zasadniczo w dowolnym celu. Stosowanie zwodniczych interfejsów w tym kontekście może naruszać RODO w zakresie, w jakim wpływają one na zachowanie osób, których dane dotyczą, w sposób, który może utrudniać im skuteczną ochronę ich danych osobowych oraz dokonywanie świadomych wyborów dotyczących przetwarzania ich danych osobowych.

Europejska Rada Ochrony Danych, dostrzegając problem zwodniczych interfejsów dla ochrony danych osobowych, przyjęła wytyczne 3/2022 w sprawie tzw. *deceptive design patterns* (zwodnicze wzorce projektowe) w interfejsach platform społecznościowych. Oprócz przywoływanej już definicji zwodniczych wzorców projektowych (ang. *deceptive design patterns*) wytyczne EROD zawierają konkretne przykłady zwodniczych wzorców projektowych, jak również praktyczne zalecenia dla dostawców, projektantów i użytkowników platform społecznościowych dotyczące tego, jak rozpoznawać i unikać zwodniczych wzorców projektowych w interfejsach mediów społecznościowych, które naruszają RODO.

Pomimo iż wytyczne odnoszą się wprost wyłącznie do praktyk na platformach społecznościowych, to mają one znaczenie

37 Obrazuje to np. tabela zawarta w raporcie z badania przeprowadzonego na zlecenie Komisji Europejskiej, choć nie obejmuje ona wszystkich przepisów omawianych w niniejszym artykule; zob. F. Lupiáñez-Villanueva, A. Boluda, F. Bogliacino, G. Liva, L. Lechardoy, T. Rodríguez de las Heras Ballell, *Behavioural study...*, s. 61–70.

38 Zwykle pojawia się w nich sformułowanie, zgodnie z którym dany akt „pozostaje bez uszczerbku dla” określonych aktów, przy czym nie jest jasne, jak należy interpretować taki przepis w razie kolizji z przepisami innych aktów (zob. np. motyw 7 i 9 aktu w sprawie danych czy motyw 12 DMA).

39 Z racji tego, że X został wskazany jako bardzo duża platforma internetowa, sprawa prowadzona jest przez Komisję Europejską (a nie krajowego koordynatora ds. usług cyfrowych); zob. *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*, komunikat prasowy z 25.04.2023 r., https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413 (dostęp: 5.08.2024 r.).

40 *Commission sends preliminary findings to X for breach of the Digital Services Act*, komunikat prasowy z 12.07.2024 r., https://ec.europa.eu/commission/presscorner/detail/en/IP_24_3761 (dostęp: 5.08.2024 r.).

41 M. Leiser, *Psychological Patterns...*, s. 9; M.R. Leiser, C. Santos, *Dark Patterns...*

42 Zgodnie z tym przepisem „platforma internetowa” oznacza usługę hostingu, która na żądanie odbiorcy usługi przechowuje i rozpowszechnia publicznie informacje, chyba że takie działanie jest nieznaczną lub wyłącznie poboczną cechą innej usługi lub nieznaczną funkcją głównej usługi, i że względów obiektywnych i technicznych nie można z niej skorzystać bez takiej innej usługi, a włączenie takiej cechy lub funkcji w taką inną usługę nie jest sposobem na obejście stosowania DSA.

43 Dla przykładu większość indywidualnych sklepów internetowych nie jest objęta definicją platformy internetowej z DSA.

44 M. Leiser, *Psychological Patterns...*, s. 9.

45 Zob. np. I. Małobęcka-Szwast, *Big Data and the Abuse of a Dominant Position by Data-Driven Online Platforms under EU Competition Law*, Warszawa 2021, s. 1–53.

dla całego sektora cyfrowego i stanowią wskazówkę w zakresie tego, w jaki sposób zwodnicze interfejsy mogą naruszać RODO⁴⁶. Praktyki typu *deceptive design pattern* pojawiają się bowiem nie tylko w ramach platform społecznościowych, ale – jak wspomniano już powyżej – również w ramach innych platform, witryn czy w aplikacjach. W tym kontekście warto podkreślić, że choć co prawda wytyczne EROD nie są prawem wiążącym, to w praktyce mają istotne znaczenie dla interpretacji przepisów o ochronie danych przez organy nadzorcze, które wchodzą w jej skład. Stanowią one również praktyczną wskazówkę dla podmiotów zaangażowanych w przetwarzanie danych osobowych.

W ocenie EROD stosowanie zwodniczych wzorów projektowych może naruszać takie przepisy RODO jak:

- 1) zasadę rzetelnego i przejrzystego przetwarzania danych osobowych (art. 5 ust. 1 lit. a),
- 2) zasadę przejrzystego informowania (art. 12),
- 3) zasadę rozliczalności (art. 5 ust. 2),
- 4) zasadę minimalizacji danych i ograniczenia celu (art. 5 ust. 1 lit. b i c),
- 5) wymogi dotyczące ochrony danych w fazie projektowania i domyślnej ochrony danych (art. 25),
- 6) wymogi dotyczące zgody (art. 4 pkt 11 i art. 7),
- 7) obowiązki informacyjne (art. 13 i 14),
- 8) przepisy RODO dotyczące korzystania z praw przez podmioty danych (art. 15–22)⁴⁷.

Do głównych rodzajów praktyk typu *deceptive design pattern* EROD zalicza:

- 1) **przeładowywanie (przeciążenie) treścią** (ang. *overloading*), czyli zasypywanie użytkowników masą próśb, informacji, opcji lub możliwości, aby skłonić ich do udostępnienia większej ilości danych lub zaakceptowania pewnych praktyk dotyczących przetwarzania i wykorzystania ich danych, wbrew ich uzasadnionym oczekiwaniom. Taka praktyka może przyjąć trzy formy i naruszać następujące przepisy RODO: a) **ciągłe zachęcanie** (ang. *continuous prompting*), czyli nakłanianie użytkowników do podania większej ilości danych osobowych, niż jest to konieczne do celów przetwarzania, lub wyrażenia zgody na inne wykorzystanie ich danych poprzez wielokrotne proszenie użytkowników o podanie danych lub wyrażenie zgody na nowy cel przetwarzania (naruszenie art. 5 ust. 1 lit. b, art. 7 w zw. z art. 4 pkt 11, art. 7 ust. 2 RODO); b) **labirynt prywatności** (ang. *privacy maze*), czyli utrudnianie użytkownikom uzyskania określonych informacji lub skorzystania z przysługujących im praw poprzez przedstawianie zbyt wielu stron i informacji, w których nie mogą oni łatwo znaleźć szukanych informacji, np. na temat skorzystania z prawa do wycofania zgody (naruszenie 5 ust. 1 lit. a, art. 12 ust. 1 i 2, art. 7 w zw. z art. 4 pkt 11 RODO); c) **zbyt wiele opcji** (ang. *too many options*), czyli przedstawianie użytkownikom zbyt wielu opcji do wyboru. Liczba dostępnych opcji sprawia, że użytkownicy nie są w stanie dokonać żadnego wyboru

lub pomijają niektóre ustawienia, które mogą dotyczyć preferencji w zakresie ochrony danych (naruszenie art. 5 ust. 1 lit. a, art. 12 ust. 1 RODO);

- 2) **pomijanie** (ang. *skipping*), czyli zaprojektowanie interfejsu lub ścieżki użytkownika w taki sposób, aby użytkownik zapomniał lub nie myślał o kwestiach związanych z ochroną danych osobowych. Taka praktyka może przyjąć dwie formy i naruszać następujące przepisy RODO: a) **praktyka typu *deceptive snugness***⁴⁸, czyli domyślnie stosowanie funkcji i opcji najbardziej inwazyjnych dla danych osobowych (naruszenie art. 25 ust. 1, art. 4 pkt 11, art. 6); b) **spójrz tam** (ang. *look over there*), czyli prezentowanie działań lub informacji związanych z ochroną danych w sposób, który konkuruje z innymi elementami (informacjami), mając na celu odwrócenie uwagi użytkownika (naruszenie: art. 5 ust. 1 lit. a, art. 12 ust. 1 i 2);
- 3) **zamieszanie** (ang. *stirring*), czyli wpływanie na wybór użytkowników poprzez odwoływanie się do ich emocji lub używanie wizualnych zachęt. Taka praktyka może przyjąć dwie formy i naruszać następujące przepisy RODO: a) **sterowanie emocjonalne** (ang. *emotional steering*)⁴⁹, czyli używanie sformułowań lub elementów wizualnych (takich jak styl, kolory, zdjęcia) w sposób, który ma wywołać u użytkowników albo pozytywne emocje, sprawiając, by czuli się oni nagrodzeni czy bezpieczni, albo negatywne emocje, tak by użytkownicy czuli się przestraszeni, winni lub ukarani (naruszenie art. 5 ust. 1 lit. a, art. 12 ust. 1 i 2, art. 8, art. 7 w zw. z art. 4 pkt 11); b) **ukryte na widoku** (ang. *hidden in plain sight*), czyli użycie stylu wizualnego lub techniki kontroli informacji lub ochrony danych, która zachęca użytkowników do korzystania z mniej restrykcyjnych, a tym samym bardziej inwazyjnych opcji w zakresie prywatności (naruszenie art. 5 ust. 1 lit. a, art. 7 w zw. z art. 4 pkt 11, art. 12 ust. 1 i 2);
- 4) **utrudnianie** (ang. *obstructing*), czyli utrudnianie lub blokowanie użytkownikom procesu pozyskiwania informacji na temat przetwarzania ich danych lub zarządzania ich danymi poprzez ograniczanie lub uniemożliwianie wykonania określonych czynności. Taka praktyka może przyjąć trzy formy i naruszać następujące przepisy RODO: a) **ślepy zaulek** (ang. *dead end*), czyli przekierowywanie użytkowników do niedziałających linków lub stron internetowych w sytuacji, gdy szukają oni informacji lub funkcji, za pomocą której mogą dokonywać zmian w ustawieniach swojej prywatności (naruszenie art. 12 ust. 1 i 2, art. 25 ust. 1); b) **dłużej niż to konieczne** (ang. *longer than necessary*), czyli wydłużanie ścieżki użytkownika w przypadku, gdy próbuje on aktywować opcje mniej inwazyjne dla ochrony danych w porównaniu do analogicznej ścieżki w przypadku opcji bardziej inwazyjnych (naruszenie art. 12 ust. 1 i 2, art. 21 ust. 1, art. 7 ust. 3, art. 25 ust. 1); c) **działanie wprowadzające w błąd** (ang. *misleading action*), czyli sytuacja, w której rozbieżność między informacjami a dostępnymi opcjami skłania użytkowników do zrobienia czegoś, czego nie zamierzają (naruszenie art. 12 ust. 1, art. 5 ust. 1 lit. a);

46 I. Małobęcka-Szwast, *Zwodnicze interfejsy (dark patterns) pod lupą unijnych instytucji*, 10.03.2023 r., <https://newtech.law/pl/zwodnicze-interfejsy-dark-patterns-pod-lupa-unijnych-instytucji/> (dostęp: 5.08.2024 r.).

47 Podejście EROD odzwierciedlone jest również w literaturze poprzedzającej przyjęcie wytycznych EROD – zob. np. M.R. Leiser, *Dark patterns...*, s. 240–269.

48 W ocenie autorki nie jest możliwe przetłumaczenie tego pojęcia na język polski w sposób pozwalający na oddanie jego sensu.

49 Jest to praktyka związana z praktyką typu *toying with emotions*, która opisana została poniżej w kontekście dyrektywy 2005/29/WE.

- 5) **zmiennosc (niespójność)** (ang. *fickle*), czyli zaprojektowanie interfejsu w sposób niespójny i nieprzejrzysty, co utrudnia użytkownikom zrozumienie natury przetwarzania, dokonanie właściwego wyboru dotyczącego ich danych oraz poruszanie się po różnych narzędziach kontroli ochrony danych. Taka praktyka może przyjąć cztery formy i naruszać następujące przepisy RODO: a) **brak hierarchii** (ang. *lacking hierarchy*), czyli sytuacja, w której informacje w zakresie ochrony danych są prezentowane bez hierarchii, na kilka różnych sposobów i wiele razy, przez co użytkownik nie rozumie, w jaki sposób jego dane są przetwarzane i jak może sprawować nad nimi kontrolę (naruszenie art. 12 ust. 1 i 2); b) **dekontekstualizacja** (ang. *decontextualising*), czyli umieszczenie informacji lub funkcji, za pomocą których użytkownik może kontrolować przetwarzanie danych osobowych na stronie pozbawionej kontekstu, nie dotyczącej ochrony danych (naruszenie art. 12 ust. 1 i 2); c) **niespójny interfejs** (ang. *inconsistent interface*), czyli stosowanie interfejsu, który nie jest spójny w różnych kontekstach (np. menu związane z ochroną danych nie wyświetla tych samych elementów na urządzeniach mobilnych i komputerach stacjonarnych) (naruszenie art. 12 ust. 1 i 2); d) **brak ciągłości językowej** (ang. *language discontinuity*), czyli prezentowanie informacji związanych z ochroną danych w innym języku niż język usługi, z której korzysta użytkownik (naruszenie art. 5 ust. 1 lit. a, art. 12 ust. 1, art. 13, 14);
- 6) **pozostawienie w ciemności (niewiedzy)** (ang. *left in the dark*), czyli zaprojektowanie interfejsu w taki sposób, aby ukryć informacje lub narzędzia kontroli ochrony danych lub pozostawić użytkowników w niepewności co do tego, jak przetwarzane są ich dane, jakie prawa im przysługują i jaki rodzaj kontroli mogą nad nimi sprawować. Taka praktyka może przyjąć dwie formy i naruszać następujące przepisy RODO: a) **sprzeczne informacje** (ang. *conflicting information*), czyli przekazywanie użytkownikom sprzecznych ze sobą informacji (naruszenie art. 5 ust. 1 lit. a, art. 12 ust. 1, art. 7 ust. 2 w zw. z art. 4 pkt 11); b) **niejednoznaczne sformułowania lub informacje** (ang. *ambiguous wording or information*), czyli używanie niejednoznacznych i niejasnych pojęć podczas przekazywania informacji użytkownikom (naruszenie art. 5 ust. 1 lit. a, art. 12 ust. 1, art. 7 ust. 2 w zw. z art. 4 pkt 11, art. 13)⁵⁰.

Zwykle określony zwodniczy interfejs łączy w sobie kilka ww. elementów (praktyk)⁵¹. Prawdopodobnie najczęściej występującym w praktyce zwodniczym interfejsem, który narusza RODO, ale też dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej⁵², są banery *cookie*, które prezentując

użytkownikom różne opcje w zakresie akceptacji lub odrzucenia plików *cookie* instalowanych na urządzeniach końcowych użytkowników i związanego z tym przetwarzania danych, nie robią tego w sposób neutralny, zgodny z RODO. Często banery *cookie* zaprojektowane są w sposób, który ma skłonić użytkownika wchodzącego na stronę internetową do wyrażenia zgody na wszystkie pliki *cookie* (np. poprzez uwypuklenie opcji „akceptuj wszystkie” albo poprzez wymóg, by odrzucenie wszystkich plików *cookie* odbywało się w bardziej skomplikowany sposób niż ich akceptacja)⁵³.

5. Dyrektywa 2005/29/WE

Stosowanie zwodniczych interfejsów w przyjętym w tym artykule rozumieniu wchodzi również w zakres przedmiotowy dyrektywy 2005/29/WE⁵⁴. Choć dyrektywa 2005/29/WE nie wspomina wprost o zwodniczych interfejsach (praktykach typu *dark patterns*), to Komisja Europejska w swoich wytycznych dotyczących wykładni i stosowania dyrektywy 2005/29/WE wprost odnosi się do praktyk typu *dark patterns* w sektorze cyfrowym⁵⁵ jako praktyk objętych dyrektywą 2005/29/WE⁵⁶. Dyrektywa 2005/29/WE ma bowiem zastosowanie do każdej „nieuczciwej praktyki handlowej”, która mieści się w zakresie przedmiotowym tej dyrektywy, niezależnie od jej klasyfikacji czy nazwy. Może być ona zatem wykorzystana do zakwestionowania uczciwości praktyki typu *dark patterns*, jeżeli jest ona stosowana w ramach stosunków handlowych między przedsiębiorcą a konsumentami i spełnia pozostałe przesłanki jej zastosowania.

Dyrektywa 2005/29/WE definiuje nieuczciwe praktyki handlowe, których stosowanie przez przedsiębiorców wobec konsumentów przed zawarciem transakcji handlowej dotyczącej produktu, w trakcie jej zawierania oraz po jej zawarciu jest zakazane w Unii Europejskiej. Definicja praktyki handlowej zawarta w art. 2 lit. d dyrektywy 2005/29/WE obejmuje „każde działanie przedsiębiorcy, jego zaniechanie, sposób postępowania, oświadczenie lub komunikat handlowy, w tym reklamę i marketing, bezpośrednio związane z promocją, sprzedażą lub dostawą produktu do konsumentów”. Trybunał Sprawiedliwości szeroko interpretuje tę definicję, wskazując, że dyrektywa cechuje się szczególnie szerokim zakresem przedmiotowym, obejmującym wszystkie praktyki handlowe mające bezpośredni związek z promocją, sprzedażą lub dostawą konsumentom jakiegoś produktu⁵⁷ (lub usługi)⁵⁸. Dyrektywa 2005/29/WE nie wymaga przy tym

⁵⁰ Wytyczne EROD, s. 65–71.

⁵¹ C. Bösch i in. dokonali przeglądu różnych praktyk typu *dark patterns*, które naruszają prywatność; zob. w artykule C. Bösch, B. Erb, F. Kargl, H. Kopp, S. Pfattheicher, *Tales from the dark side: Privacy dark strategies and privacy dark patterns*, „Proceedings on Privacy Enhancing Technologies” 2016/4, s. 237–254.

⁵² Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. WE L 201, s. 37 ze zm.) – dalej dyrektywa 2002/58/WE. Dyrektywa ta wymaga uzyskania zgody użytkownika końcowego na instalowanie plików *cookie* innych niż ściśle niezbędne na urządzeniu końcowym tego użytkownika (art. 5 ust. 3).

⁵³ Tę praktykę dobrze obrazują sprawy inicjowane przez organizację NOYB, która złożyła do organów nadzorczych w różnych państwach członkowskich ponad 226 skarg dotyczących zwodniczych banerów *cookie*, wymuszających zgodę użytkownika; zob. NOYB, 226 complaints lodged against deceptive cookie banners, 9.08.2022 r., <https://noyb.eu/en/226-complaints-logged-against-deceptive-cookie-banners> (dostęp: 5.08.2024 r.).

⁵⁴ M.R. Leiser, W. Yang, *Illuminating...*, s. 486; M. Brennecke, *Regulating dark patterns*, „Notre Dame Journal of International & Comparative Law” 2024/1, s. 46–47, art. 5.

⁵⁵ Zawiadomienie Komisji – Wytyczne dotyczące wykładni i stosowania dyrektywy 2005/29/WE Parlamentu Europejskiego i Rady dotyczącej nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym (Dz.Urz. UE C 526 z 2021 r., s. 1) – dalej jako wytyczne Komisji.

⁵⁶ Wytyczne Komisji, s. 99–102.

⁵⁷ Wyrok TS z 9.11.2010 r., C-540/08, Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG przeciwko „Österreich”-Zeitungsverlag GmbH, EU:C:2010:660, pkt 17 i 21.

⁵⁸ Wyrok TS z 19.09.2013 r., C-435/11, CHS Tour Services GmbH przeciwko Team4 Travel GmbH, EU:C:2013:574, pkt 27.

istnienia stosunku umownego czy zakupu produktu (usługi). Stąd praktyki handlowe mające na celu wyłącznie przyciągnięcie uwagi konsumenta, które nie skutkują zakupem, również są objęte zakresem dyrektywy 2005/29/WE⁵⁹. Przy tak szerokiej definicji jasne jest, że większość zwodniczych interfejsów rozumianych w sposób przyjęty w tym artykule, stosowanych w relacjach między przedsiębiorcami a konsumentami, mieści się w zakresie zastosowania dyrektywy 2005/29/WE (będą one bowiem zwykle praktykami handlowymi bezpośrednio związanymi z promocją, sprzedażą lub dostawą produktu do konsumentów)⁶⁰.

Zgodnie z klauzulą generalną zawartą w art. 5 ust. 2 dyrektywy 2005/29/WE praktyka handlowa jest nieuczciwa, jeżeli: 1) jest sprzeczna z wymogami staranności zawodowej⁶¹ oraz 2) w sposób istotny zniekształca lub może w sposób istotny zniekształcić zachowanie gospodarcze względem produktu przeciętnego konsumenta, do którego dociera bądź do którego jest skierowana, lub przeciętnego członka grupy konsumentów, jeżeli praktyka handlowa skierowana jest do określonej grupy konsumentów. Kolejne przepisy dyrektywy 2005/29/WE wskazują, że do nieuczciwych praktyk handlowych należą praktyki wprowadzające w błąd, które obejmują działania wprowadzające w błąd (art. 6) i zaniechania wprowadzające w błąd (art. 7), a także praktyki agresywne charakteryzujące się stosowaniem nękania, przymusu i bezprawnego nacisku (art. 8 i 9). Załącznik I do dyrektywy 2005/29/WE zawiera wykaz praktyk handlowych, które są zakazane w każdych okolicznościach (tzw. czarna lista).

Aby praktyka była nieuczciwa w rozumieniu art. 5–9 dyrektywy 2005/29/WE, musi ona powodować lub móc powodować podjęcie przez konsumenta decyzji dotyczącej transakcji, której inaczej by nie podjął. Z orzecznictwa TS wynika, że pojęcie decyzji dotyczącej transakcji należy interpretować szeroko: obejmuje ono nie tylko decyzję o zakupie lub odmowie zakupu produktu, lecz także decyzję bezpośrednio związaną z tą decyzją⁶². Na tym tle Komisja w swoich wytycznych wskazuje, że praktyka handlowa może zostać uznana za nieuczciwą nie tylko wówczas, gdy prawdopodobnie będzie skutkować podjęciem przez przeciętnego konsumenta decyzji o zakupie lub powstrzymaniu się od zakupu produktu (usługi), lecz także jeżeli prawdopodobnie będzie skutkować podjęciem przez konsumenta np. następujących decyzji:

- 1) o wejściu do sklepu;
- 2) o poświęceniu więcej czasu w internecie na realizację procesu rezerwacji;
- 3) o powstrzymaniu się od przejścia do innego usługodawcy lub innego produktu;
- 4) o kliknięciu w link lub reklamę online;
- 5) o kontynuowaniu korzystania z serwisu poprzez przeglądanie lub przewijanie.

Ponadto w dyrektywie 2005/29/WE nie wymaga się wykazania, że zachowanie gospodarcze konsumenta (tj. jego decyzja dotycząca transakcji) zostało rzeczywiście zniekształcone – wystarczające jest wykazanie, że praktyka handlowa „prawdopodobnie” będzie mieć (tj. może mieć) taki wpływ na przeciętnego konsumenta. W tym kontekście warto zauważyć, że potencjał do zniekształcania decyzji transakcyjnych konsumentów (rozumianych w powyżej wskazany sposób) jest wpisany w przyjętą w tym artykule definicję zwodniczych interfejsów.

Mając na względzie powyższe uwagi, nie dziwi, że Komisja w swoich wytycznych wskazuje, że każda praktyka manipulacyjna typu *dark patterns*, która w istotny sposób zniekształca lub może w sposób istotny zniekształcić zachowanie gospodarcze przeciętnego konsumenta lub konsumenta podatnego na zagrożenia, może naruszać wymogi staranności zawodowej przedsiębiorcy⁶³ określone w art. 5 oraz art. 2 lit. h dyrektywy 2005/29/WE, może stanowić praktykę wprowadzającą w błąd (art. 6–7 dyrektywy 2005/29/WE) lub praktykę agresywną (art. 8–9 dyrektywy 2005/29/WE) w zależności od konkretnej zastosowanej praktyki typu *dark patterns*⁶⁴. Komisja w swoich wytycznych podaje również różne przykłady praktyk typu *dark patterns*, które ocenia z perspektywy przepisów dyrektywy 2005/29/WE. W ocenie Komisji następujące praktyki typu *dark patterns* można uznać za naruszające dyrektywę 2005/29/WE:

- 1) praktyki manipulacyjne polegające na zasłanianiu ważnych informacji lub uporządkowanie ich w taki sposób, aby promować konkretną opcję (ang. *hidden information, false hierarchy*), jak również stosowanie podchwytliwych pytań i dwuznacznego języka (np. podwójne przeczenie; ang. *trick wording*) w celu zmylenia konsumenta, mogą zostać zakwalifikowane jako działanie wprowadzające w błąd (art. 6 dyrektywy 2005/29/WE) lub jako zaniechanie wprowadzające w błąd (art. 7 dyrektywy 2005/29/WE) – powodują one bowiem, że informacje przekazywane przez przedsiębiorcę są dla konsumenta niezrozumiałe lub dwuznaczne;
- 2) praktyki polegające na wykorzystywaniu emocji w celu nakłonienia użytkowników do odstąpienia od dokonania określonego wyboru (ang. *toying with emotions*), takie jak wzbudzanie u konsumenta poczucia winy (ang. *confirmation bias*) może stanowić agresywną praktykę handlową (art. 8 dyrektywy 2005/29/WE) – polega ona bowiem na wywieraniu bezprawnego nacisku w celu zakłócenia procesu podejmowania decyzji przez konsumenta;
- 3) praktyki polegające na pomijaniu lub przekazywaniu informacji o cyklicznych opłatach abonamentowych czy subskrypcji w sposób nieprzejrzysty (np. pomijanie informacji o tym, że zapisując się na bezpłatną wersję próbną, konsument dokonuje subskrypcji), może stanowić działanie wprowadzające w błąd (art. 6 dyrektywy 2005/29/WE) lub zaniechanie wprowadzające w błąd (art. 7 dyrektywy 2005/29/WE) (ang. *hidden subscription, forced continuity*)⁶⁵;
- 4) praktyki polegające na domyślnym zaznaczeniu pól wyboru, np. w celu pobrania opłaty za dodatkowe usługi,

59 F. Lupiáñez-Villanueva, A. Boluda, F. Bogliacino, G. Liva, L. Lechardoy, T. Rodríguez de las Heras Ballell, *Behavioural...*, s. 70.

60 F. Lupiáñez-Villanueva, A. Boluda, F. Bogliacino, G. Liva, L. Lechardoy, T. Rodríguez de las Heras Ballell, *Behavioural...*, s. 70.

61 Zdefiniowanej w art. 2 lit. h dyrektywy 2005/29/WE jako standard dotyczący szczególnej wiedzy i staranności, których można w racjonalny sposób oczekiwać od przedsiębiorcy w jego relacjach z konsumentami, zgodnie z uczciwymi praktykami rynkowymi i/lub ogólną zasadą dobrej wiary w zakresie jego działalności.

62 F. Lupiáñez-Villanueva, A. Boluda, F. Bogliacino, G. Liva, L. Lechardoy, T. Rodríguez de las Heras Ballell, *Behavioural...*, s. 70; wyrok TS z 19.12.2013 r., C-281/12, Trento Sviluppo srl i Centrale Adriatica Soc. coop. arl przeciwko Autorità Garante della Concorrenza e del Mercato, EU:C:2013:859.

63 Komisja wskazuje, że rozumienie pojęcia wymogów staranności zawodowej w kontekście projektowania interfejsów można wyprowadzić w szczególności z zasad zaczerpniętych z norm międzynarodowych i kodeksów postępowania w zakresie etycznego projektowania takich interfejsów – zob. wytyczne Komisji, s. 101.

64 Wytyczne Komisji, s. 101.

65 Wytyczne Komisji, s. 58–59, 102.

mogą stanowić nieuczciwą praktykę handlową na ogólnych zasadach (art. 5 dyrektywy 2005/29/WE). Mogą one również naruszać art. 22 dyrektywy 2011/83/UE⁶⁶ w sprawie praw konsumentów⁶⁷.

Ponadto do praktyk typu *dark patterns* wyraźnie zabronionych w załączniku I do dyrektywy 2005/29/WE w każdych okolicznościach Komisja zalicza:

- 1) praktyki „przynęty i zamiany”, które obejmują oferowanie produktów po określonej cenie bez podania uzasadnionych powodów braku możliwości dostarczenia produktu lub oferowanie produktu, a następnie odmówienie przyjęcia zamówienia lub dostarczenia go w odpowiednim terminie z zamiarem promowania w zamian innego produktu (pkt 5 i 6 załącznika I);
- 2) stwarzanie pilnej potrzeby poprzez fałszywe twierdzenie, że produkt będzie dostępny tylko przez ograniczony czas lub że będzie on dostępny na określonych warunkach przez ograniczony czas (pkt 7 załącznika I) (ang. *fake urgency*). Dotyczy to np. fałszywych liczników czasu i informacji o ograniczonej ilości towaru na stronach internetowych;
- 3) podawanie nieścisłych informacji o warunkach rynkowych lub możliwości znalezienia produktu, z zamiarem nakłonięcia konsumenta do zakupu produktu na warunkach mniej korzystnych niż normalne warunki rynkowe (pkt 18 załącznika I);
- 4) twierdzenie, że konsument wygrał nagrodę, a następnie nieprzyznanie opisanych nagród lub ich odpowiedniego ekwiwalentu (pkt 19 i 31 załącznika I) lub fałszywe opisywanie produktu jako „darmowego” (pkt 20 załącznika I);
- 5) powtarzające się wtrącenia podczas normalnych interakcji w celu nakłonięcia konsumenta do zrobienia lub zaakceptowania czegoś (tj. nagabywanie, ang. *nagging*) mogą być równoznaczne z uporczywym i niechcianym namawianiem (nr 26 załącznik I)⁶⁸.

W tym kontekście warto przywołać wyrok C-102/20, StWL Städtische Werke Lauf a.d. Pegnitz⁶⁹, który dotyczył oceny zgodności praktyki polegającej na wyświetlaniu w skrzynce odbiorczej użytkownika usługi prowadzenia konta poczty elektronicznej wiadomości reklamowych w formie zbliżonej do prawdziwych wiadomości przesyłanych pocztą elektroniczną i w tym samym umiejscowieniu co one z dyrektywą 2002/58/WE⁷⁰

oraz dyrektywą 2005/29/WE. Trybunał uznał, że taka praktyka: po pierwsze, stanowi używanie poczty elektronicznej do celów marketingu bezpośredniego w rozumieniu art. 13 ust. 1 dyrektywy 2002/58/WE i jako takie wymaga spełnienia wymogów tam wskazanych (w tym konieczność wyrażenia zgody przez użytkownika), a po drugie, stanowi uporczywe i niechciane namawianie użytkowników usług prowadzenia konta poczty elektronicznej do zakupu produktów w rozumieniu pkt 26 załącznika I do dyrektywy 2005/29/WE, jeśli z jednej strony wyświetlanie tych wiadomości reklamowych ma charakter wystarczająco częsty i regularny, by uznać je za „uporczywe namawianie”, i z drugiej strony, w braku wyrażenia przez użytkownika zgody na wyświetlanie tej reklamy, może zostać uznane za „niechciane namawianie”. Sama Komisja w swoich wytycznych ów wyrok przywołuje w kontekście praktyki nagabywania (ang. *nagging*)⁷¹.

Z przywołanego wyroku, a także z uwag poczynionych powyżej płyną dwa bardziej ogólne wnioski: po pierwsze, dyrektywa 2005/29/WE jest regulacją wystarczająco elastyczna, by stosować ją do oceny praktyk typu *dark patterns*; po drugie, że wchodzi w interakcję z innymi unijnymi regulacjami (w tym przypadku: dyrektywą 2002/58/WE), które mogą być istotne dla oceny zgodności danej praktyki z dyrektywą 2005/29/WE (w tym przypadku wymóg wyrażenia zgody przez użytkownika wynikający z dyrektywy 2002/58/WE jest jednym z czynników wpływających na ocenę, czy dochodzi do „niechcianego namawiania”).

Powyżej wskazane praktyki są wyłącznie przykładami praktyk typu *dark patterns*, które mogą zostać uznane za nieuczciwe praktyki handlowe w rozumieniu dyrektywy 2005/29/WE. Kompleksowy przegląd różnych praktyk typu *dark patterns* i ich ocena z perspektywy dyrektywy 2005/29/WE jest przedmiotem m.in. przywoływanego już raportu *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation*, a także licznych artykułów⁷². Warto jednak podkreślić, że lista praktyk typu *dark patterns*, które pojawiają się w literaturze, nie jest wyczerpująca – wraz z rozwojem coraz to nowych technologii, praktyk manipulacyjnych i interfejsów internetowych mogą pojawiać się nowe praktyki, które również będą mieściły się w pojęciu zwodniczych interfejsów i mogą naruszać dyrektywę 2005/29/WE.

6. Dyrektywa 2023/2673

Omawiając zakaz stosowania zwodniczych interfejsów, warto również odnieść się pokrótce do dyrektywy 2023/2673, pomimo iż krajowe przepisy implementujące tę dyrektywę znajdą zastosowanie dopiero od 19.06.2026 r.⁷³ Jednym z celów dyrektywy 2023/2673 jest zapobieganie wykorzystywaniu przez przedsiębiorców, przy zawieraniu umów o świadczenie usług finansowych na odległość, zwodniczych interfejsów na interfejsach internetowych. Dyrektywa zmierza do osiągnięcia tego celu poprzez wprowadzenie nowego art. 16e do dyrektywy

66 Zgodnie z tym przepisem zanim konsument zostanie związany umową lub ofertą, przedsiębiorca powinien uzyskać wyraźną zgodę konsumenta na każdą dodatkową płatność należną oprócz uzgodnionego wynagrodzenia za główne obowiązki umowne przedsiębiorcy. Jeżeli przedsiębiorca nie otrzymał wyraźnej zgody konsumenta, lecz założył jej istnienie poprzez stosowanie domyślnych opcji, które konsument musi odrzucić w celu uniknięcia dodatkowej płatności, konsument ma prawo do zwrotu tej płatności.

67 Dyrektywa Parlamentu Europejskiego i Rady 2011/83/UE z 25.10.2011 r. w sprawie praw konsumentów, zmieniająca dyrektywę Rady 93/13/EWG i dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca dyrektywę Rady 85/577/EWG i dyrektywę 97/7/WE Parlamentu Europejskiego i Rady (Dz.Urz. UE L 304, s. 64) – dalej dyrektywa 2011/83/UE; zob. Wytyczne Komisji, s. 101.

68 Wytyczne Komisji, s. 101–102.

69 Wyrok TS z 25.11.2021 r., C-102/20, StWL Städtische Werke Lauf a.d. Pegnitz GmbH przeciwko eprimo GmbH, EU:C:2021:954.

70 Jak już wspomniano, dyrektywa ta wymaga uzyskania zgody użytkownika końcowego na instalowanie plików *cookie* innych niż ściśle niezbędne na urządzeniu końcowym tego użytkownika (art. 5 ust. 3).

71 Wytyczne Komisji, s. 102.

72 Zob. np. M.R. Leiser, M.M. Caruana, *Dark Patterns: Light to be Found in Europe's Consumer Protection Regime*, „Journal of European Consumer and Market Law” 2021/6, s. 237–251; M.R. Leiser, W. Yang, *Illuminating...*, s. 484–528.

73 Państwa członkowskie mają czas do 19.12.2025 r. na implementację dyrektywy 2023/2673.

2011/83/UE. Nowy przepis zasadniczo powiela treść art. 25 DSA i w wielu miejscach się do niego odwołuje⁷⁴.

Zgodnie z nowym art. 16e ust. 1 dyrektywy 2011/83/UE, nie naruszając przepisów dyrektywy 2005/29/WE i RODO, państwa członkowskie zapewniają, by przy zawieraniu umów o usługi finansowe na odległość przedsiębiorcy nie mogli projektować, organizować ani obsługiwać swoich interfejsów internetowych, zdefiniowanych w art. 3 lit. m DSA, w sposób, który wprowadza w błąd konsumentów będących odbiorcami ich usługi lub nimi manipuluje lub w inny istotny sposób zakłóca lub ogranicza zdolność tych konsumentów do podejmowania wolnych i świadomych decyzji. W szczególności państwa członkowskie zobowiązane są do przyjęcia środków, które zgodnie z prawem Unii dotyczą co najmniej jednej z następujących praktyk stosowanych przez przedsiębiorców: a) wyróżnianie pewnych możliwości wyboru, kiedy konsumenci będący odbiorcami ich usługi są proszeni o podjęcie decyzji; b) wielokrotne żądanie od konsumentów będących odbiorcami ich usługi dokonania wyboru, gdy wyboru takiego już dokonał, w szczególności przez pokazywanie wyskakujących okienek, które zakłócają środowisko użytkownika; lub c) sprawianie, że procedura zrezygnowania z usługi jest trudniejsza niż procedura jej subskrypcji⁷⁵. Przepis ten ma na celu zagwarantowanie, że przedsiębiorcy nie będą wykorzystywać braku obiektywizmu konsumentów (ang. *consumer biases*) poprzez „konfigurowanie interfejsów internetowych w sposób, który może zaburzyć lub ograniczyć zdolność konsumenta do podjęcia swobodnej, samodzielnej i świadomej decyzji lub dokonania swobodnego, samodzielnego i świadomego wyboru”⁷⁶.

Powiązany z omawianym przepisem motyw 41 dyrektywy 2023/2673 zawiera definicję zwodniczych interfejsów analogiczną do tej zawartej w motywie 67 DSA. Stosownie do tego motywu zwodnicze interfejsy na interfejsach internetowych przedsiębiorców to praktyki, które w istotny sposób zniekształcają lub ograniczają, celowo albo w praktyce, zdolność konsumentów będących odbiorcami usług finansowych do dokonywania niezależnych i świadomych wyborów lub podejmowania takich decyzji. Dotyczy to w szczególności umów o usługi finansowe zawieranych na odległość. Takie praktyki mogą być stosowane przez przedsiębiorców, by przekonać konsumentów będących odbiorcami świadczonej przez nich usługi do niepożądanego zachowania lub niepożądanych decyzji, które mogą mieć dla nich negatywne konsekwencje.

W motywie 41 dyrektywy 2023/2673 zauważa się, że choć DSA zakazuje dostawcom usług pośrednich prowadzonym platformy internetowe korzystania ze zwodniczych interfejsów przy projektowaniu i organizacji ich interfejsów internetowych, to dyrektywa 2023/2673 powinna zobowiązywać państwa członkowskie do tego, by uniemożliwiały przedsiębiorcom oferującym usługi finansowe na odległość korzystanie z takich zwodniczych interfejsów przy zawieraniu umów na takie usługi. W tym kontekście unijny prawodawca wyjaśnia, że przepisy DSA i dyrektywy 2023/2673 uzupełniają się – mają one bowiem zastosowanie do przedsiębiorców działających w różnym charakterze.

Jednocześnie nowe przepisy zastrzegają, że ze względu na swoją złożoność i nieodłączne poważne ryzyka, usługi finansowe mogą wymagać dalszych szczegółowych wymogów w odniesieniu do zwodniczych interfejsów. Z tego względu państwa członkowskie – w drodze odstępstwa od pełnego poziomu harmonizacji – mają możliwość przyjęcia lub utrzymania bardziej rygorystycznych przepisów w tym zakresie, pod warunkiem że takie przepisy są zgodne z prawem Unii (zob. nowy art. 16e ust. 2). Taka możliwość jest jednocześnie zgodna z art. 3 ust. 9 dyrektywy 2005/29/WE w odniesieniu do nieuczciwych praktyk handlowych związanych z usługami finansowymi, który przewiduje, że w ramach usług finansowych państwa członkowskie mogą też nakładać wymogi o charakterze bardziej restryktywnym lub nakazowym (motyw 41 dyrektywy 2023/2673).

7. Akt w sprawie sztucznej inteligencji

Systemy sztucznej inteligencji mogą zostać wykorzystane przy projektowaniu jeszcze bardziej wyrafinowanych zwodniczych interfejsów, które będą wpływać na wybory użytkowników – zarówno konsumentów, jak i podmiotów profesjonalnych. W literaturze wskazuje się, że związek między sztuczną inteligencją a zwodniczymi interfejsami opiera się na zdolności systemów sztucznej inteligencji do analizowania i wykorzystywania ludzkiej psychologii w sposób, który jest zarówno podprogowy, jak i potencjalnie szkodliwy⁷⁷.

Akt w sprawie sztucznej inteligencji – AIA – który wszedł w życie 1.08.2024 r., ma na celu m.in. promowanie upowszechniania zorientowanej na człowieka i godnej zaufania sztucznej inteligencji (AI), przy jednoczesnym zapewnieniu wysokiego poziomu ochrony zdrowia, bezpieczeństwa, praw podstawowych zapisanych w Karcie, przed szkodliwymi skutkami systemów AI w Unii oraz wspieraniu innowacji (art. 1 ust. 1 AIA). W tym celu AIA definiuje systemy AI (art. 3 pkt 1 AIA) i ustanawia zharmonizowane przepisy dotyczące wprowadzania ich do obrotu, oddawania do użytku ich oraz wykorzystywania w UE. Akt w sprawie sztucznej inteligencji wprowadza proporcjonalne, oparte na ryzyku podejście do regulacji systemów AI, które nakłada stopniowalny system wymogów i obowiązków w zależności od poziomu ryzyka stwarzanego dla zdrowia, bezpieczeństwa i praw podstawowych⁷⁸. Stosując to podejście, AIA klasyfikuje wszystkie systemy AI według czterech poziomów ryzyka:

- 1) niedopuszczalne ryzyko, które prowadzi do zakazanych praktyk w zakresie AI (art. 5);
- 2) wysokie ryzyko, z którym wiąże się stosowanie szczegółowych obowiązków określonych w AIA (w szczególności art. 8–27);
- 3) ograniczone ryzyko, które prowadzi do konieczności realizacji określonych obowiązków w zakresie przejrzystości (art. 50);
- 4) minimalne ryzyko, w przypadku którego zainteresowane strony są zachęcane do dobrowolnego tworzenia kodeksów postępowania (art. 95).

74 M. Brenncke, *Regulating dark...*, s. 49.

75 W tym zakresie przepis ten zasadniczo powiela treść art. 25 ust. 3 DSA.

76 Wniosek – dyrektywa Parlamentu Europejskiego i Rady zmieniająca dyrektywę 2011/83/UE w zakresie umów o usługi finansowe zawieranych na odległość oraz uchylająca dyrektywę 2002/65/WE, COM(2022) 204 final, s. 3.

77 M. Leiser, *Psychological Patterns...*, s. 10.

78 Zob. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> (dostęp: 26.02.2025 r.).

Akt w sprawie sztucznej inteligencji odnosi się do problemu zwodniczych interfejsów w szczególności w art. 5, który reguluje zakazane praktyki w zakresie AI i w motywie 29. Motyw 29 AIA zauważa, że techniki manipulacyjne oparte na AI mogą być wykorzystywane w celu nakłaniania osób do niepożądanych zachowań lub w celu wprowadzania ich w błąd poprzez skłanianie ich do podejmowania decyzji w sposób, który podważa i ogranicza ich autonomię, decyzyjność i swobodę wyboru. Jak wskazuje się w literaturze, AIA ma szansę przyczynić się do zwalczania tych najbardziej wyrafinowanych, trudnych do wykrycia, a tym samym prawdopodobnie najbardziej szkodliwych zwodniczych interfejsów (określanych mianem *darkest patterns*), które opierają swoje działanie na systemach sztucznej inteligencji wbudowanych w architekturę systemu i działają poza świadomością użytkownika⁷⁹. Do takich praktyk należą np. manipulacje sensoryczne, czyli takie praktyki, które angażują zmysły w sposób, który często omija naszą świadomość, prowadząc do formy psychologicznej manipulacji (np. komunikaty podprogowe i wykorzystanie niezauważalnych dźwięków lub dźwięków w tle o częstotliwościach, które wywołują pożądane reakcje użytkownika), czy manipulacje algorytmiczne, czyli takie praktyki, które wykorzystując algorytmy adaptacyjne i ukryty nadzór nad działaniami użytkownika, dostosowują prezentowane mu treści i interakcje na podstawie indywidualnych danych behawioralnych, subtelnie kierując uwagę użytkownika w stronę pewnych wyborów i z dala od innych⁸⁰. Jak wspomniano powyżej, takie praktyki pozostają poza zakresem zastosowania DSA, a zastosowanie do nich regulacji takich jak dyrektywa 2005/29/WE czy RODO z pewnością będzie rodzić wyzwania⁸¹.

W art. 5 ust. 1 lit. a AIA unijny prawodawca zdecydował się na wprowadzenie zakazu praktyki w zakresie AI polegającej na wprowadzaniu do obrotu, oddawaniu do użytku lub wykorzystywaniu systemu AI, który stosuje techniki podprogowe będące poza świadomością danej osoby (takie jak bodźce dźwiękowe, bodźce będące obrazami lub materiałami wideo, których nie można dostrzec, ponieważ bodźce takie wykraczają poza świadomą ludzką percepcję – motyw 29), lub celowe techniki manipulacyjne lub wprowadzające w błąd, czego celem lub skutkiem jest dokonanie znaczącej zmiany zachowania danej osoby lub grupy osób poprzez znaczące ograniczenie ich zdolności do podejmowania świadomych decyzji, powodując tym samym podjęcie przez nie decyzji, której inaczej by nie podjęły, w sposób, który wyrządza lub może wyrządzić u niej, u innej osoby lub u grupy osób poważną szkodę.

Artykuł 5 ust. 1 lit. b AIA zakazuje z kolei „wprowadzania do obrotu, oddawania do użytku lub wykorzystywania systemu AI, który wykorzystuje słabości osoby fizycznej lub określonej grupy osób ze względu na ich wiek, niepełnosprawność lub szczególną sytuację społeczną lub ekonomiczną, którego celem lub skutkiem jest dokonanie znaczącej zmiany zachowania danej osoby lub osoby należącej do tej grupy w sposób, który wyrządza lub może z uzasadnionym prawdopodobieństwem wyrządzić u tej osoby lub u innej osoby poważną szkodę”.

Zarówno art. 5 ust. 1 lit. a, jak i lit. b AIA mają na celu uniemożliwienie systemom sztucznej inteligencji korzystania

z technik podprogowych, które w znacznym stopniu manipulują zachowaniem użytkowników i powodują poważne szkody. Oba zakazy posługują się jednak przy tym niejednoznacznymi pojęciami, które mogą być różnie interpretowane. M. Leiser zauważa w szczególności, że nie jest jasne, co znaczy „technika podprogowa” i kiedy jest ona „poza świadomością danej osoby” – ustalenie granicy między świadomym a podświadomym wpływem może okazać się niemożliwe dla organów regulacyjnych bez jasnych wytycznych. Trudności mogą się wiązać również z interpretacją pojęcia poważnej szkody – co prawda motyw 29 wskazuje, że chodzi w tym zakresie w szczególności o szkody mające wystarczająco istotny niepożądany wpływ na zdrowie fizyczne, psychiczne lub na interesy finansowe, ale i tak pole do różnych interpretacji wskazanych w motywie 29 pojęć pozostaje. Niełatwe może okazać się również wykazanie związku przyczynowego między techniką podprogową a poważną szkodą, co jest wymogiem stwierdzenia odpowiedzialności za naruszenie ww. zakazów. M. Leiser obawia się, że zwodnicze interfejsy, które stopniowo zmieniają zachowanie użytkownika, mogą nie spełniać wymogu związku przyczynowego lub może być on szczególnie trudny do ustalenia⁸². Z powyższych względów wydaje się, że szczególnie istotną rolę w zapewnieniu skuteczności ww. zakazów w zwalczaniu tych najbardziej podstępnych zwodniczych interfejsów odegrają organy odpowiedzialne za egzekwowanie nowych przepisów.

Motyw 29 podkreśla, że zakazy dotyczące praktyk w zakresie AI określone w art. 5 ust. 1 lit. a i b AIA stanowią uzupełnienie przepisów zawartych w dyrektywie 2005/29/WE, w szczególności przepisu zakazującego stosowania we wszelkich okolicznościach nieuczciwych praktyk handlowych powodujących dla konsumentów szkody ekonomiczne lub finansowe, niezależnie od tego, czy praktyki te stosuje się za pomocą systemów AI, czy w innym kontekście. Motyw 29 wskazuje również – analogicznie jak czyni to motyw 67 DSA – że powszechne i zasadne praktyki handlowe, np. w dziedzinie reklamy, które są zgodne z mającym zastosowanie prawem, nie powinny być same w sobie uznawane za szkodliwe praktyki manipulacyjne oparte na AI.

8. Akt o rynkach cyfrowych

Akt o rynkach cyfrowych – DMA – w art. 5–7 nakłada na wyznaczonych strażników dostępu szereg obowiązków, które mają zapewnić uczciwość i kontestowalność rynków cyfrowych. Strażnicy dostępu to duże przedsiębiorstwa internetowe o ugruntowanej pozycji, które świadczą podstawowe usługi platformowe⁸³ będące ważnym punktem dostępu, za pośrednictwem którego użytkownicy biznesowi docierają do użytkowników końcowych⁸⁴. Unijny prawodawca świadomy istotnej roli interfejsów w skutecznej realizacji tych obowiązków wprowadził również odpowiednie zakazy w art. 13 ust. 4 i 6 DMA,

82 M. Leiser, *Psychological Patterns...*, s. 17–18.

83 Katalog podstawowych usług platformowych został wskazany w art. 2 pkt 2 DMA.

84 Do tej pory Komisja Europejska jako instytucja odpowiedzialna za egzekwowanie DMA wskazała 7 strażników dostępu (we wrześniu 2023 r.: Apple, Alphabet, Meta, Amazon, Microsoft i ByteDance, a w maju 2024 r.: Booking.com) i 24 podstawowe usługi platformowe, które objęte są DMA – zob. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328 (dostęp: 26.02.2025 r.) oraz https://ec.europa.eu/commission/presscorner/detail/en/IP_24_2561 (dostęp: 26.02.2025 r.).

79 M.R. Leiser, *Dark patterns...*, s. 242; M. Leiser, *Psychological Patterns...*, s. 8.

80 M. Leiser, *Psychological Patterns...*, s. 10–11.

81 M.R. Leiser, C. Santos, *Dark Patterns...*

które mają przeciwdziałać obchodzeniu głównych obowiązków przewidzianych w tym rozporządzeniu. Choć DMA nie posługuje się pojęciem zwodniczych interfejsów, nie ulega wątpliwości, że przepisy te odnoszą się właśnie do takich praktyk, które mogą zagrozić skuteczności obowiązków wskazanych w art. 5–7 DMA⁸⁵.

Zgodnie z art. 13 ust. 4 DMA strażnik dostępu nie może dopuszczać się zachowań, które w jakikolwiek sposób utrudniają skuteczne wypełnianie obowiązków ustanowionych w art. 5, 6 i 7, niezależnie od tego, czy zachowanie to ma charakter umowny, handlowy, techniczny lub jakikolwiek inny lub czy polega na stosowaniu technik behawioralnych lub projektowaniu interfejsu. Z kolei art. 13 ust. 6 DMA przewiduje, że strażnik dostępu nie może pogarszać warunków ani obniżać jakości podstawowych usług platformowych świadczonych na rzecz użytkowników biznesowych lub użytkowników końcowych, którzy zdecydowali się skorzystać z praw lub możliwości wyboru ustanowionych w art. 5, 6 i 7, ani sprawiać, że korzystanie z tych praw lub możliwości będzie nadmiernie utrudnione, w tym poprzez oferowanie użytkownikom końcowym możliwości wyboru w sposób nieobiektywny, bądź też przez osłabianie autonomii, procesów decyzyjnych lub swobody wyboru użytkowników końcowych lub użytkowników biznesowych za pośrednictwem struktury, projektu, funkcji lub sposobu działania interfejsu użytkownika lub jego części. Motyw 70 DMA jako przykład takich zakazanych zachowań wskazuje projekt stosowany przez strażnika dostępu, przedstawianie użytkownikom końcowym opcji wyboru w sposób, który nie jest neutralny, lub wykorzystywanie struktury, funkcji lub sposobu obsługi interfejsu użytkownika lub jego części w celu osłabienia lub ograniczenia autonomii użytkownika, jego możliwości podejmowania decyzji lub wyboru.

Zakaz stosowania zwodniczych interfejsów pojawia się również w kontekście zakazu wyrażonego w art. 5 ust. 2 DMA. W uproszczeniu, przepis ten zakazuje strażnikom dostępu łączenia danych osobowych z różnych źródeł, chyba że użytkownikowi końcowemu zapewniono możliwość dokonania konkretnego wyboru i wyraził on zgodę w rozumieniu RODO. Powiązany z tym przepisem motyw 37 wskazuje, że strażnicy dostępu nie powinni projektować, organizować lub obsługiwać swoich interfejsów internetowych w sposób, który w drodze wprowadzenia w błąd, manipulacji lub w inny sposób istotnie zakłóca lub ogranicza zdolność użytkowników końcowych do swobodnego wyrażenia zgody. W szczególności strażnicy dostępu nie mogą skłaniać użytkowników końcowych częściej niż raz w roku do wyrażenia zgody do tego samego celu przetwarzania danych, w odniesieniu do którego nie wyrazili oni pierwotnie zgody lub ją cofnęli.

Warto również wskazać na art. 13 ust. 5 DMA. Z racji tego, że dane (w szczególności dane osobowe) są jednym z kluczowych czynników decydujących o sile rynkowej przedsiębiorstw na rynkach cyfrowych, DMA wprowadza obowiązki, które mają na celu „uwolnienie” danych spod wyłącznej kontroli strażników dostępu i zapewnienie dostępu do nich użytkownikom biznesowym (np. art. 6 ust. 10, art. 6 ust. 11 DMA). W przypadku danych osobowych takie udostępnienie może

nastąpić pod warunkiem, że osoba, której dane dotyczą, wyrazi na to zgodę (art. 6 ust. 10 DMA). W praktyce taka zgoda może być zbierana przez użytkowników biznesowych wyłącznie za pośrednictwem strażnika dostępu, który ma bezpośrednią relację z osobą, której dane dotyczą. Z tego względu, by zapewnić skuteczność takim przepisom, art. 13 ust. 5 DMA wskazuje, że jeżeli przestrzeganie DMA wiąże się z koniecznością uzyskania zgody na zbieranie, przetwarzanie i udostępnianie danych osobowych oraz wykorzystywanie danych osobowych w ramach różnych usług, strażnik dostępu podejmuje konieczne działania, aby zapewnić użytkownikom biznesowym możliwość bezpośredniego uzyskania zgody na przetwarzanie tych danych w przypadkach, w których zgoda ta jest wymagana na mocy RODO lub dyrektywy 2002/58/WE, albo aby zapewnić przestrzeganie unijnych przepisów i zasad w zakresie ochrony danych i prywatności w inny sposób, w tym – w stosownych przypadkach – poprzez dostarczanie użytkownikom biznesowym należycie zanonimizowanych danych. Strażnik dostępu nie może doprowadzić do sytuacji, w której uzyskanie tej zgody przez użytkownika biznesowego będzie bardziej uciążliwe niż uzyskanie jej na potrzeby usług świadczonych przez samego strażnika dostępu, np. właśnie poprzez zastosowanie zwodniczych interfejsów, które będą sugerowały osobie, której dane dotyczą, by nie wyrażała ona zgody na takie udostępnienie jej danych użytkownikowi biznesowemu. Jeżeli strażnik dostępu obchodzi lub próbuje obchodzić którykolwiek z obowiązków określonych w art. 5, 6 lub 7 w jeden ze sposobów opisanych w art. 13 ust. 4, 5 i 6 DMA, Komisja może wszcząć postępowanie na podstawie art. 20 i przyjąć akt wykonawczy, o którym mowa w art. 8 ust. 2 DMA, aby określić środki, które strażnik dostępu ma wdrożyć w celu skutecznego wypełnienia swoich obowiązków na gruncie DMA (art. 13 ust. 7 DMA).

O ile zakaz stosowania zwodniczych interfejsów z DSA, dyrektywy 2005/29/WE i AIA ma na celu ochronę autonomii woli (autonomii decyzyjnej) odbiorców usług i odpowiednio konsumentów, o tyle zakazy stosowania zwodniczych interfejsów, które pojawiają się w DMA, mają na celu zapobieganie obchodzeniu głównych obowiązków przez strażników dostępu i w efekcie zapewnienie ich skuteczności. Odgrywają one zatem raczej rolę pomocniczą w stosunku do głównych zakazów i nakazów określonych w art. 5–7 DMA, ale również istotną – ich bezpośrednie sformułowanie w tekście tego aktu prawnego wyklucza podawanie przez strażników dostępu w wątpliwość zarzutów dotyczących obchodzenia obowiązków poprzez odpowiednie zaprojektowanie ich interfejsów.

9. Akt w sprawie danych

Akt w sprawie danych, który wszedł w życie 11.01.2024 r. i będzie stosowany co do zasady od 12.09.2025 r., to regulacja mająca na celu wzmocnienie unijnej gospodarki opartej na danych i wspieranie konkurencyjnego rynku danych poprzez zwiększenie dostępności i użyteczności danych (w szczególności danych przemysłowych), zachęcanie do innowacji opartych na danych i zwiększenie dostępności danych⁸⁶. W tym celu akt w sprawie danych wprowadza m.in. regulacje dotyczące udostępniania danych, uzyskanych lub wygenerowanych

85 K. Drążewski [w:] *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, red. M. Grochowski, Legis 2024, art. 13 DMA.

86 Zob. <https://digital-strategy.ec.europa.eu/pl/policies/data-act> (dostęp: 5.08.2024 r.).

w wyniku korzystania z produktu skomunikowanego lub usługi powiązanej, między użytkownikami, posiadaczami danych i osobami trzecimi. Akt w sprawie danych dotyczy w szczególności danych generowanych przez urządzenia podłączone do internetu (internet rzeczy). Dzięki tej regulacji produkty podłączone do internetu będą musiały być projektowane i produkowane w sposób umożliwiający użytkownikom łatwy i bezpieczny dostęp do generowanych danych, ich wykorzystywanie i udostępnianie.

Dla przykładu, zgodnie z art. 4 ust. 1 aktu w sprawie danych, użytkownicy produktów skomunikowanych mają prawo do uzyskania od posiadacza danych (np. producenta produktu) dostępu do danych generowanych przez korzystanie z tego produktu, jeżeli dane te nie są jeszcze bezpośrednio dostępne dla użytkownika. Użytkownicy mogą następnie udostępniać te dane dostawcom usług w zakresie napraw i konserwacji (osobom trzecim), wspierając konkurencję na rynku posprzedażowym (ang. *aftermarket*) (art. 5).

W tym kontekście akt w sprawie danych wprowadza zakaz stosowania zwodniczych interfejsów: zarówno przez posiadaczy danych, jak i osoby trzecie, które otrzymują dane od posiadacza danych na wniosek użytkownika. Ów zakaz wyrażony jest odpowiednio w art. 4 ust. 4 (w stosunku do posiadaczy danych) oraz art. 6 ust. 2 lit. a aktu w sprawie danych (w stosunku do osób trzecich).

Artykuł 4 ust. 4 aktu w sprawie danych przewiduje, że posiadacze danych nie utrudniają bezzasadnie użytkownikom dokonywania wyborów ani wykonywania praw na podstawie tego przepisu, w tym poprzez oferowanie użytkownikom wyboru w sposób nieneutralny lub poprzez podważanie lub ograniczanie autonomii, zdolności decyzyjnych lub wyborów użytkownika za pomocą struktury, projektu, funkcji lub sposobu działania interfejsu cyfrowego użytkownika bądź jego części. Analogiczny zakaz przewidziany jest w art. 6 ust. 2 lit. a aktu w sprawie danych w odniesieniu do osób trzecich, które otrzymują dane od posiadacza danych na wniosek użytkownika. Stosownie do tego przepisu osoba trzecia bezzasadnie nie utrudnia użytkownikom dokonywania wyborów i wykonywania praw na podstawie art. 5 i 6 aktu w sprawie danych, w tym poprzez oferowanie użytkownikom wyboru w sposób nieneutralny lub zmuszanie, wprowadzanie w błąd użytkownika lub manipulowanie nim, bądź podważanie lub ograniczanie autonomii, zdolności decyzyjnych lub wyborów użytkowników, w tym za pomocą cyfrowego interfejsu użytkownika lub za pomocą jego części.

Powiązany z powyższymi przepisami motyw 38 wyjaśnia, że osoby trzecie lub posiadacze danych nie powinni podczas projektowania swoich interfejsów cyfrowych stosować tzw. zwodniczych interfejsów. Motyw 38 definiuje przy tym zwodnicze interfejsy, ale w nieco odmienny sposób, niż czyni to DSA: „Zwodnicze interfejsy to techniki projektowe, które służą do wymuszania na konsumentach decyzji, które mają dla nich negatywne skutki, lub wprowadzenia konsumentów w błąd w celu skłonienia ich do takich decyzji. Te techniki manipulacji mogą być wykorzystywane, by skłonić użytkowników, w szczególności konsumentów podatnych na zagrożenia, do niechcianych zachowań, wprowadzić ich błąd poprzez nakłanianie do decyzji w sprawie udostępnienia danych lub też by nieobiektywnie wpłynąć na zdolności decyzyjne użytkowników usługi w sposób podważający lub ograniczający ich autonomię, zdolności decyzyjne i wybór”. Jednocześnie

motyw 38 zastrzega, że powszechne i uzasadnione praktyki handlowe zgodne z prawem unijnym nie powinny same w sobie być uznawane za zwodnicze interfejsy (podobnie jak czyni to motyw 67 DSA).

Z przywołanego motywu 38 wynika, że unijny prawodawca zdecydował się na odmienne, węższe zdefiniowanie zwodniczych interfejsów w akcie w sprawie danych niż ma to miejsce w DSA. Podczas gdy akt w sprawie danych wydaje się ograniczać cel zwodniczych interfejsów wyłącznie do „wymuszania na konsumentach decyzji, które mają dla nich negatywne skutki, lub wprowadzenia konsumentów w błąd w celu skłonienia ich do takich decyzji”, DSA nie ogranicza zakazu zwodniczych interfejsów wyłącznie do konsumentów (posługuje się pojęciem odbiorcy usługi, który może być zarówno osobą fizyczną, jak i osobą prawną). Nie jest również konieczne, żeby celem lub efektem zwodniczych interfejsów na gruncie DSA było podjęcie decyzji o negatywnych skutkach dla konsumenta – jak słusznie wskazuje się w literaturze, przepis ten chroni bowiem autonomię woli i nie jest ograniczony do przeciwdziałania jedynie negatywnym decyzjom odbiorców usługi w zakresie ich interesów gospodarczych⁸⁷. W końcu warto również zauważyć, że brzmienie definicji z motywu 38 wydaje się niekonsekwentne i sprzeczne z samym brzmieniem aktu w sprawie danych. Po pierwsze, przepisy art. 4 ust. 4 oraz 6 ust. 2 lit. a aktu w sprawie danych nie są ograniczone do konsumentów, a użytkowników, którymi mogą być zarówno osoby fizyczne, jak i osoby prawne⁸⁸. Po drugie, przepisy te nie wspominają o tym, że wprowadzone zakazy ograniczają się jedynie do celu, jakim jest wymuszanie na konsumentach decyzji, które mają dla nich negatywne skutki. Wręcz przeciwnie, przepisy te chronią – podobnie jak czyni to DSA – autonomię, zdolności decyzyjne i wybory użytkownika, o czym świadczy wprost treść tych przepisów⁸⁹. Wydaje się zatem, że definicję zwodniczych interfejsów w motywie 38 aktu w sprawie danych należy raczej uznać za legislacyjną pomyłkę, która nie znajduje odzwierciedlenia w treści przepisów, do których się odnosi (art. 4 ust. 4 i art. 6 ust. 2 lit. a aktu w sprawie danych).

10. Wnioski – wielopłaszczyznowy zakaz stosowania zwodniczych interfejsów i związane z tym wyzwania

Powyżej omówione regulacje są lub będą za niedługo egzekwowane przez różne krajowe i unijne instytucje i organy. Z pewnością doprowadzi to do niełatwych do rozstrzygnięcia problemów jurysdykcyjnych i wyzwań w stosowaniu unijnych zasad przez instytucje i organy właściwe do egzekwowania ww. przepisów, w szczególności zasady lojalnej współpracy⁹⁰ i zasady proporcjonalności.

W obszarze zwalczania zwodniczych interfejsów w Unii Europejskiej mamy do czynienia z czymś, co możemy

87 K. Araczevska [w:] *Akt...*, art. 25.

88 Zgodnie z art. 2 pkt 12 aktu w sprawie danych „użytkownik” oznacza osobę fizyczną lub prawną, która jest właścicielem produktu skomunikowanego lub której na podstawie umowy przekazane zostały tymczasowe prawa do korzystania z tego produktu skomunikowanego, lub która korzysta z usług powiązanych.

89 M. Brennecke, *Regulating dark...*, s. 51.

90 Zob. np. motyw 90 DMA.

określić mianem regulacyjnego patchworku (ang. *regulatory patchwork*)⁹¹. Omówione powyżej akty prawne zmierzają do zwalczania zwodniczych interfejsów w ramach swoich właściwości; jednocześnie unijny prawodawca, dostrzegając regulacyjne luki i ograniczenia w jednych regulacjach, decyduje się na wprowadzenie kolejnych aktów prawnych, które te luki w założeniu mają uzupełniać. Omówione przepisy prawa rodzą jednak wiele wątpliwości interpretacyjnych. Unijny prawodawca często – celowo lub nie – posługuje się nieścisłymi pojęciami i koncepcjami, które będą musiały zostać dookreślone w praktyce decyzyjnej tych organów, jak też sądów unijnych. Z jednej strony takie podejście wydaje się zrozumiałe, ponieważ zostawia tym organom i instytucjom pole do tego, by dostosowywać pojęcia z omawianych aktów do szybko postępujących zmian technologicznych mających wpływ na stosowanie zwodniczych interfejsów. Z drugiej strony ta nieścisłość i nieprecyzyjność może być wykorzystywana przez przedsiębiorców stosujących takie praktyki po to, by obchodzić ustanowione w unijnych przepisach zakazy i osiągać założone biznesowe cele. Jedno jest jednak pewne: właściwe organy i instytucje, a także sądy unijne, będą miały istotną rolę do odegrania w zapewnieniu skuteczności tego wielopłaszczyznowego zakazu zwodniczych interfejsów.

Warto podkreślić, że egzekwowanie większości z tych regulacji będzie powierzone różnym organom i instytucjom, zarówno na poziomie krajowym, jak i unijnym. Stąd – aby zakaz zwodniczych interfejsów wyrażony w tak licznych regulacjach nie pozostał iluzoryczny, konieczne jest postulowanie ścisłej współpracy między wszystkimi zaangażowanymi organami i instytucjami. W tym kontekście warto zauważyć, że z nachodzeniem na siebie zakresu zastosowania różnych regulacji prawnych w sektorze cyfrowym (w szczególności prawa konsumenckiego, ochrony danych czy prawa konkurencji) mamy do czynienia w praktyce nie od dziś, a w literaturze wskazuje się, że taka sytuacja umożliwia wykorzystanie mocnych stron jednego mechanizmu regulacyjnego przy jednoczesnym kompensowaniu jego słabości za pomocą innych instrumentów prawnych⁹². Prawo ochrony konsumentów, prawo ochrony danych osobowych, a także prawo ochrony konkurencji czy regulacje takie jak DSA mogą znajdować zastosowanie do tych samych praktyk⁹³, co w literaturze ocenia się raczej pozytywnie – właśnie ze względu na możliwość wzajemnego uzupełniania się różnych regulacji w zwalczaniu tych samych praktyk, szczególnie w sektorze cyfrowym⁹⁴.

Oczywiście takie podejście może rodzić problemy jurysdykcyjne, w szczególności mając na względzie fakt, że ww. regulacje są egzekwowane przez różne unijne i krajowe instytucje i organy⁹⁵, które dotychczas były krytykowane za działanie w wyodrębnionych silosach i brak współpracy. Problemy te powinno się jednak raczej zwalczać, wdrażając odpowiednie mechanizmy współpracy w duchu unijnej zasady lojalnej współpracy – zarówno na poziomie unijnym, jak i na poziomie państw członkowskich⁹⁶. Problem zbiegu różnych sankcji nakładanych przez różne organy i instytucje za tę samą praktykę można z kolei rozwiązać wspomnianą współpracą, jak również odpowiednim stosowaniem unijnej zasady proporcjonalności na etapie wymierzania sankcji przez odpowiedni organ lub instytucję, która zresztą wpisana jest w sposób egzekwowania omawianych przepisów⁹⁷.

W celu stawienia czoła wyzwaniom związanym z wielopoziomowym zwalczaniem zwodniczych interfejsów i wzajemnym nakładaniem się na siebie omawianych regulacji należy postulować wprowadzenie konkretnych mechanizmów proceduralnych – zarówno na poziomie krajowym, jak i na poziomie unijnym, które zinstytucjonalizują lub stworzą ramy dla omówionego powyżej postulatu współpracy. Dotychczasowe doświadczenia związane z egzekwowaniem różnych zakazów i nakazów w gospodarce cyfrowej w przeważającej mierze pokazują, że bez wprowadzenia konkretnych zmian w prawie taka współpraca niekoniecznie będzie miała miejsce.

Na poziomie krajowym taka współpraca mogłaby przyjąć formę obowiązkowego zasięgania opinii innego właściwego organu (właściwych organów) przez organ rozpatrujący sprawę w trakcie trwania postępowania, jeżeli wie, że takie praktyki mogą wchodzić w zakres również jego właściwości lub były badane przez taki organ w przeszłości (organ opiniujący). Aby przeciwdziałać ewentualnym zarzutom pod adresem takiej procedury co do potencjalnej ingerencji w niezależność poszczególnych organów, opinia wyrażona przez organ opiniujący nie miałaby charakteru wiążącego. Organ rozpatrujący sprawę mógłby się zatem nie zgodzić ze stanowiskiem organu opiniującego⁹⁸.

Ponadto, w przypadku praktyk typu *dark patterns* określonego podmiotu, które zostały już uprzednio uznane w prawomocnej decyzji za naruszenie określonej regulacji przez dany organ właściwy (np. w obszarze ochrony konsumentów), organ rozpatrujący daną praktykę z perspektywy odrębnych regulacji (np. DSA) na późniejszym etapie powinien być zobowiązany do zapoznania się z wcześniejszą decyzją danego organu i wziąć ją pod uwagę przy podejmowaniu własnej decyzji (w tym w szczególności w kontekście określania wysokości kar pieniężnych lub grzywien). Tego typu rozwiązanie pozwoli na uniknięcie ewentualnych rozbieżności między stanowiskami poszczególnych organów podejmujących decyzję na podstawie odrębnych regulacji i na pełniejszą realizację zasady proporcjonalności w kontekście kar pieniężnych lub grzywien.

91 M.R. Leiser, C. Santos, *Dark Patterns...*

92 M.R. Leiser, *Dark patterns...*, s. 268–269.

93 Zob. np. I. Małobęcka-Szwast, *Facebook enforcement „saga”: How to enforce competition, consumer, and data protection laws in the digital economy*, „Studia Iuridica” 2021, t. 89, s. 189–215.

94 Tak np. F. Zuiderveen Borgesius, N. Helberger, A. Reyna, *The perfect match? A closer look at the relationship between EU consumer law and data protection law*, „Common Market Law Review” 2017/5, s. 1427; M.R. Leiser, *Dark patterns...*, s. 255–256; I. Graef, S. van Berlo, *Towards smarter regulation in the areas of competition, data protection and consumer law: why greater power should come with greater responsibility*, „European Journal of Risk Regulation” 2021/3, s. 674; M. Botta, K. Wiedemann, *The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey*, „The Antitrust Bulletin” 2019/3, s. 428–444; I. Graef, *Blurring boundaries of consumer welfare: How to create synergies between competition, consumer, and data protection law in digital markets* [w:] *Personal data in competition, consumer protection, and intellectual property law: Towards a holistic approach?*, red. M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt, G. Surblytė-Namavičienė, Berlin 2018, s. 121–151.

95 Głównie krajowe organy nadzorcze, organy ochrony konsumentów i konkurencji, koordynatorów ds. usług cyfrowych i Komisję.

96 A. Reyna, *Breaking down silos in public enforcement: Lessons from consumer-facing markets*, 2021, <https://ssrn.com/abstract=3838697> (dostęp: 5.08.2024 r.).

97 M. Namysłowska, A. Jabłonowska [w:] *Akt...*, art. 25.

98 W odniesieniu do współpracy między organami nadzorczymi a organami ochrony konkurencji zob. I. Małobęcka-Szwast, *Oddziaływanie prawa ochrony danych osobowych (RODO) na prawo ochrony konkurencji i konsumentów*, „Monitor Prawniczy” 2020/23 (dodatek), s. 99–100.

Wprowadzenie takiego mechanizmu współpracy nie byłoby całkowicie rewolucyjnym rozwiązaniem w polskim systemie prawnym. Warto w tym zakresie wskazać na art. 106 Kodeksu postępowania administracyjnego⁹⁹, który reguluje zasady współdziałania organów administracji publicznej w przypadkach określonych w przepisach szczególnych¹⁰⁰. Zgodnie z art. 106 § 1 k.p.a., jeżeli przepis prawa uzależnia wydanie decyzji od zajęcia stanowiska przez inny organ (wyrażenia opinii lub zgody albo wyrażenia stanowiska w innej formie), organ administracji publicznej załatwiający sprawę może wydać decyzję dopiero po zajęciu stanowiska przez ten organ. Stosownie natomiast do art. 106a § 1 k.p.a. organ załatwiający sprawę może, z urzędu albo na wniosek strony lub organu, do którego zwrócono się o zajęcie stanowiska, zwołać posiedzenie, jeżeli przyczyni się to do przyspieszenia zajęcia stanowiska (posiedzenie w trybie współdziałania).

Bazując na rozwiązaniu przewidzianym w art. 106 k.p.a., należałoby postulować wprowadzenie do krajowych przepisów zwalczających zwodnicze interfejsy obowiązku wzajemnego zasięgnięcia opinii, jeżeli dana praktyka może naruszać przepisy więcej niż jednej ustawy. Analogicznie do art. 106a k.p.a., w razie potrzeby organ rozpatrujący sprawę mógłby zwołać wspólne posiedzenie z innym organem (organami), jeżeli usprawniłoby to zajęcie przez niego stanowiska i przyspieszyłoby załatwienie sprawy.

Z kolei na poziomie unijnym współpraca, która miałaby na celu wypracowanie jednolitego podejścia do oceny określonych praktyk typu *dark patterns* przez danego przedsiębiorcę w ramach UE, mogłaby być koordynowana przez Komisję Europejską. Mogłaby ona przyjąć formę zinstytucjonalizowanej współpracy lub współpracy organizowanej *ad hoc* na potrzeby określonej sprawy. Jako wzór zorganizowania takiej współpracy może posłużyć mechanizm kompleksowej współpracy między organami nadzorczymi przewidziany w art. 60–62 RODO, współpraca między organami ochrony konkurencji i Komisją Europejską w ramach Europejskiej Sieci Konkurencji (European Competition Network¹⁰¹) lub działanie grupy wysokiego szczebla ds. aktu o rynkach cyfrowych (art. 40 DMA).

W tym kontekście warto również wskazać, że już w 2016 r. Europejski Inspektor Ochrony Danych sugerował ustanowienie platformy koordynacyjnej służącej egzekwowaniu przepisów w środowisku cyfrowym w ramach UE (*Digital Clearing House*), która byłaby dobrowolną siecią zrzeszającą organy regulacyjne w ramach UE mającą na celu wymianę informacji, na zasadzie dobrowolności i w ramach swoich właściwych kompetencji, o możliwych nadużyciach w środowisku cyfrowym oraz najsukurszejszych sposobach radzenia sobie z nimi¹⁰². Kontynuując tę ideę, która nie przyniosła pierwotnie zakładanych rezultatów,

Europejski Inspektor Ochrony Danych ponownie w styczniu 2025 r. zaproponował utworzenie *Digital Clearinghouse 2.0*, forum dla zainteresowanych regulatorów mające na celu identyfikację obszarów zainteresowania międzyregulacyjnego w celu ułatwienia koordynacji i wymiany wiedzy, doświadczeń i zasobów między regulatorami (organami) odpowiedzialnymi za egzekwowanie przepisów o ochronie danych osobowych, aktu w sprawie danych, AIA, DSA, DMA i aktu w sprawie zarządzania danymi (DGA)¹⁰³. Ponadto EDPS zachęca Komisję Europejską do rozważenia przedłożenia nowego wniosku ustawodawczego w celu ułatwienia współpracy międzyregulacyjnej i wymiany informacji między właściwymi organami na temat trwających dochodzeń w ich odpowiednich dziedzinach. Przedłożenie takiego wniosku przez Komisję i przyjęcie przez Unię Europejską przepisów, które instytucjonalizowały współpracę między właściwymi organami w obszarze stosowania przepisów unijnych regulujących rynki i usługi cyfrowe, z pewnością przyczyniłyby się do bardziej efektywnego zwalczania praktyk typu *dark patterns*.

Abstract

dr Iga Małobęcka-Szwast

University of Warsaw, Faculty of Law and Administration,
Department of European Law
(ORCID: <https://orcid.org/0000-0002-4719-4899>).

Dark Patterns in light of the DSA and Other Acts of EU Law – a Multi-Level Prohibition

Keywords: *dark patterns*, DSA, DMA, AI Act

The objective of the article is to show how legislative actions taken at the EU level counteract dark pattern practices, what the relationships are between them and how to effectively enforce the multi-level prohibition on the use of dark patterns, which arises from the review. Although dark patterns can be evaluated from the point of view of various regulations, the article focuses primarily on: Digital Services Act (DSA), GDPR, Unfair Commercial Practices Directive, Digital Markets Act, Artificial Intelligence Act, Data Act and the Directive concerning financial services contracts concluded at a distance. The author calls for the introduction of specific procedural mechanisms of cooperation between the authorities and institutions responsible for their enforcement, both at the national and EU levels, in order to face the challenges of the multi-level defence against dark patterns and tackle the overlap of the regulations in question.

Bibliografia/References

- Araczeńska K. [w:] *Akt o usługach cyfrowych. Komentarz*, red. M. Gumularz, LEX 2024.
- Barudi M. [w:] *Digital Services Act: DSA. Kommentar*, red. R. Müller-Terpitz, M. Köhler, München 2024.
- 103 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z 30.05.2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz.Urz. UE L 152, s. 1). Zob. Europejski Inspektor Ochrony Danych, Towards a Digital Clearinghouse 2.0 – Concept Note, https://www.edps.europa.eu/system/files/2025-01/towards_a_digital_clearinghouse_2_0_january_2025_en_0.pdf (dostęp: 18.01.2025 r.).

99 Ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2024 r. poz. 572 ze zm.) – dalej k.p.a.

100 Jak wskazuje się w doktrynie, art. 106 k.p.a. nie stanowi podstawy prawnej współdziałania – taką podstawą są bowiem przepisy szczególne, które uzależniają wydanie decyzji od zajęcia stanowiska przez inny organ. Przepis ten określa jedynie zasady i tryb współdziałania, tj. dotyczy wyłącznie kwestii proceduralnych współdziałania; zob. A. Wróbel [w:] *Kodeks postępowania administracyjnego. Komentarz*, red. M. Jaśkowska, M. Wilbrandt-Gotowicz, A. Wróbel, LEX 2020, art. 106.

101 I. Małobęcka-Szwast, *Oddziaływanie...*, s. 100.

102 Europejski Inspektor Ochrony Danych, EDPS Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, 2016, s. 3, 15, https://edps.europa.eu/sites/edp/files/publication/16-09-23_big-data_opinion_en.pdf (dostęp: 18.01.2025 r.).

Bösch C., Erb B., Kargl F., Kopp H., Pfattheicher S., *Tales from the dark side: Privacy dark strategies and privacy dark patterns*, „Proceedings on Privacy Enhancing Technologies” 2016/4.
 Botta M., Wiedemann K., *The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey*, „The Antitrust Bulletin” 2019/3.

Brenncke M., *Regulating dark patterns*, „Notre Dame Journal of International & Comparative Law” 2024/1.

Drażewski K. [w:] *Rynek cyfrowy. Akt o usługach cyfrowych. Akt o rynkach cyfrowych. Rozporządzenie platform-to-business. Komentarz*, red. M. Grochowski, Legis 2024.

Graef I., *Blurring boundaries of consumer welfare: How to create synergies between competition, consumer, and data protection law in digital markets* [w:] *Personal data in competition, consumer protection, and intellectual property law: Towards a holistic approach?*, red. M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt, G. Surblytė-Namavičienė, Berlin 2018.

Graef I., van Berlo S., *Towards smarter regulation in the areas of competition, data protection and consumer law: why greater power should come with greater responsibility*, „European Journal of Risk Regulation” 2021/3.

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

Leiser M., *Psychological Patterns and Article 5 of the AI Act: AI-Powered Deceptive Design in the System Architecture and the User Interface*, „Journal of AI Law and Regulation” 2024/1.

Leiser M.R., *Dark patterns: The case for regulatory pluralism between the European Union's consumer and data protection regimes* [w:] *Research handbook on EU data protection law*, red. E. Kosta, R. Leenes, I. Kamara, Cheltenham 2022.

Leiser M.R., Caruana M.M., *Dark Patterns: Light to be Found in Europe's Consumer Protection Regime*, „Journal of European Consumer and Market Law” 2021/6.

Leiser M.R., Santos C., *Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation beneath the Interface*, „European Journal of Law and Technology” 2024/1.

Leiser M.R., Yang W., *Illuminating manipulative design: From 'dark patterns' to information asymmetry and the repression*

of free choice under the Unfair Commercial Practices Directive, „Loyola Consumer Law Review” 2023/3.

Lupiáñez-Villanueva F., Boluda A., Bogliacino F., Liva G., Lechardoy L., Rodríguez de las Heras Ballell T., *Behavioral study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation*, 2022, <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en/format-PDF/source-257599418> (dostęp: 5.08.2024 r.).

Małobęcka-Szwast I., *Big Data and the Abuse of a Dominant Position by Data-Driven Online Platforms under EU Competition Law*, Warszawa 2021.

Małobęcka-Szwast I., *Facebook enforcement „saga”: How to enforce competition, consumer, and data protection laws in the digital economy*, „Studia Iuridica” 2021, t. 89.

Małobęcka-Szwast I., *Oddziaływanie prawa ochrony danych osobowych (RODO) na prawo ochrony konkurencji i konsumentów*, „Monitor Prawniczy” 2020/23 (dodatek).

Małobęcka-Szwast I., *Zwodnicze interfejsy (dark patterns) pod lupą unijnych instytucji*, 10.03.2023 r., <https://newtech.law/pl/zwodnicze-interfejsy-dark-patterns-pod-lupa-unijnych-instytucji/> (dostęp: 5.08.2024 r.).

Namysłowska M., Jabłonowska A. [w:] *Akt o usługach cyfrowych. Komentarz*, red. D. Lubasz, M. Namysłowska, LEX 2024.

Reyna A., *Breaking down silos in public enforcement: Lessons from consumer-facing markets*, 2021, <https://ssrn.com/abstract=3838697> (dostęp: 5.08.2024 r.).

Szota K., *Dark patterns a ochrona konsumenta w świetle polskiego prawa*, Warszawa 2022.

Wróbel A. [w:] *Kodeks postępowania administracyjnego. Komentarz*, red. M. Jaśkowska, M. Wilbrandt-Gotowicz, A. Wróbel, LEX 2020.

Zuiderveen Borgesius F., Helberger N., Reyna A., *The perfect match? A closer look at the relationship between EU consumer law and data protection law*, „Common Market Law Review” 2017/5.

REKLAMA

Legal Alert

Korzystaj z nowoczesnego narzędzia marketingu prawniczego i zwiększ zasięg swojej kancelarii

 Wolters Kluwer

www.LEX.pl/legalalert

- ✓ Gotowe newsy eksperckie z 20 dziedzin prawa
- ✓ Platformę do wysyłki eleganckich mailingów
- ✓ Personalizowane treści dla klientów pisane przystępnym językiem
- ✓ Profesjonalny wizerunek Twojej kancelarii

