STYCZEŃ 2025

NOWE TECHNOLOGIE (2025) – LEGISLACJA I REGULACJA W POLSCE I UNII EUROPEJSKIEJ (OD A DO Z)

Traple
Konarski
Podrecki
& Wspólnicy

TKP

SPIS TREŚCI

1. Auta autonomiczne....3
2. Blockchain....4
3. Chmura obliczeniowa....5
4. Cyberbezpieczeństwo....6
5. Data Act (Akt w sprawie danych)....8
6. Dezinformacja w Internecie....9
7. Elektroniczny sport (e-sport)....11
8. Freedom Media Act (Akt o wolności mediów)....12
9. Generatywna sztuczna inteligencja....13
10. Handel elektroniczny (e-commerce)....14
11. Influencer marketing....16
12. Internet rzeczy (IoT)....17
13. Komunikacja elektroniczna....18
14. Lotnicze prawo (drony)....19
15. Media cyfrowe....21
16. Ochrona małoletnich w Internecie....22
17. Patostreaming....23
18. Reklama w Internecie....23
19. Reklama polityczna w Internecie....25
20. Sztuczna inteligencja....26
21. Usługi zaufania (Rozporządzenie eIDAS-2) 28
22. Własność intelektualna (Internet)....30
23. Wolność słowa w Internecie (dyrektywa anty-SLAPP)....32
24. Zarządzanie danymi (Akt w sprawie zarządzania danymi)....33

1. Auta autonomiczne

Autonomiczny pojazd to samochód wyposażony w zaawansowane systemy technologiczne, które umożliwiają mu poruszanie się bez udziału kierowcy. Zgodnie ze standardową skalą autonomizacji pojazdów, opracowaną przez Stowarzyszenie Inżynierów Motoryzacyjnych (SAE), wyróżnić należy **sześć poziomów autonomii pojazdów**. W chwili obecnej w Unii Europejskiej dostępne są w sprzedaży samochody o drugim poziomie autonomii (zaawansowane systemy wspomagania kierowcy). Równocześnie prowadzone są prace i testy dotyczące wyższych poziomów autonomii, w tym poziomu czwartego (wysoka automatyzacja) oraz poziomu piątego (pełna automatyzacja). W ramach poziomu czwartego samochód może samodzielnie się prowadzić w większości sytuacji, ale wymaga interwencji kierowcy w bardziej skomplikowanych warunkach, np. przy ekstremalnej pogodzie. Natomiast na poziomie piątym pojazd jest w pełni autonomiczny i nie wymaga obecności kierowcy. Na tym poziomie samochód może samodzielnie poruszać się w dowolnych warunkach, na każdej drodze. Na chwilą obecną przyjmuje się, że autonomiczne pojazdy poziomu 4. lub 5. zaczną się pojawiać na europejskich drogach do 2030 roku.

Podstawowym aktem prawnym w Unii Europejskiej dotyczącym aut autonomicznych jest **Rozporządzenie wykonawcze Komisji (UE) 2022/1426 z dnia 5 sierpnia 2022 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/2144 w odniesieniu do jednolitych procedur i specyfikacji technicznych w zakresie homologacji typu systemu zautomatyzowanej jazdy (ADS) pojazdów w pełni zautomatyzowanych (Dz.U. UE L 221)**. Rozporządzenie to określa szczegółowe wymagania techniczne i proceduralne, które muszą spełnić systemy zautomatyzowanej jazdy (ADS), aby pojazdy wyposażone w takie systemy mogły uzyskać homologację i tym samym być dopuszczone do ruchu.

Rozporządzenie 2022/1426 stanowi ważny krok w kierunku dopuszczenia do eksploatacji aut autonomicznych, ale nie jest jedyną regulacją dotyczącą tego rodzaju pojazdów. Konieczne jest bowiem **dostosowanie innych jeszcze przepisów, w tym przede wszystkim o ruchu drogowym**. Niektóre państwa członkowskie Unii Europejskiej wprowadziły w związku z tym regulacje dotyczące testowania i, w ograniczonym zakresie, użytkowania samochodów autonomicznych (np. Holandia, Niemcy, Szwecja).

W Polsce, **w dniu 9 grudnia 2024 r. opublikowany został projekt nowelizacji Prawa o ruchu drogowym**, przygotowany przez Ministerstwo Infrastruktury. Zmiana Prawa o ruchu drogowym przewiduje możliwość wykorzystania dróg na potrzeby prac testowych **pojazdów zautomatyzowanych**, tj. pojazdów zbudowanych do samodzielnego poruszania się przez określony czas, jednak wymagających interwencji kierowcy, oraz **w pełni zautomatyzowanych**, tj. pojazdów autonomicznych niewymagających nadzoru kierowcy. Każdy podmiot, który będzie chciał uruchomić testy pojazdów autonomicznych, będzie musiał uzyskać zezwolenie i uprawnienie „organizatora prac testowych". Zezwolenie na prowadzenie prac testowych wydawać będzie Krajowy Koordynator Prac Testowych, w drodze decyzji administracyjnej na pisemny wniosek organizatora prac testowych.

Uchwalenie nowelizacji prawa o ruchu drogowym, dotyczące testów pojazdów autonomicznych, jest planowane w 2025 roku, a proponowane zmiany mają wejść w życie po upływie 6 miesięcy od dnia ogłoszenia ustawy.

2. Blockchain

Z uwagi na kompleksowe wykorzystanie technologii blockchain, która może być między innymi wykorzystywana w energetyce, finansach czy ochronie zdrowia, aktualnie **nie planuje się uchwalenia w Unii Europejskiej czy Polsce kompleksowej regulacji prawnej dotyczącej jej stosowania.**

W obecnym stanie prawnym, blockchain jako taki **nie ma charakteru odrębnej instytucji prawnej**, ale jest **technologią**, której wykorzystanie w określony sposób czy w określonym sektorze może skutkować zastosowaniem konkretnych regulacji prawnych. Przykładem jest **regulacja prawna kryptoaktywów, które stanowią jedno z najważniejszych zastosowań technologii blockchain** w sektorze finansowym. Technologie rozproszonego rejestru (DLT), której blockchain jest najpowszechniejszym typem, służą bowiem do ewidencji własności aktywów. W tym zakresie zastosowanie znajdują przepisy Rozporządzenia Parlamentu Europejskiego i Rady 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów i zmieniającego dyrektywę (UE) 2019/1937 (Dz.U. UE L 150/1), zwane **rozporządzeniem MiCA**. Część z tych przepisów zaczęła obowiązywać od **30 czerwca 2024 roku (art. 149 ust. 1), a pozostałe od dnia 30 grudnia 2024 roku (art. 149 ust. 2)**. Istotny wpływ na rozwój technologii blockchain w sektorze finansowym ma również Rozporządzenie nr 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operational Resilience Act, DORA), którego przepisy zaczynają obowiązywać w dniu **17 stycznia 2025 r**. (Dz.U. UE L 333/1). Zakłada się bowiem, że wymogi określone w **DORA** stwarzają szansę na budowę bardziej stabilnego i bezpiecznego ekosystemu finansowego opartego na tej technologii.

Pewne wycinkowe regulacje prawne dotyczące blockchain zostały przyjęte także w polskim systemie prawnym. Przykładowo **w art. 30031 § 3 oraz art. 3281 § 3 Kodeksu spółek handlowych**, umożliwiono spółkom akcyjnym oraz prostym spółkom akcyjnym prowadzenie rejestru akcjonariuszy w formie rozproszonej i zdecentralizowanej bazy danych, a zatem z wykorzystaniem technologii blockchain.

Poza przepisami rozporządzeń MiCA oraz DORA, w 2025 roku nie zaczną obowiązywać przepisy nowych aktów prawnych znajdujących zastosowanie do blockchain.

3. Chmura obliczeniowa

Zarówno **w Unii Europejskiej, jak i w Polsce nie planuje się uchwalenia aktu prawnego całościowo regulującego świadczenie usług i korzystanie z chmury obliczeniowej.**

W praktyce, w projektach chmury obliczeniowej zastosowanie znajdują przepisy następujących aktów prawnych:

1. przepisy ustawy o krajowym systemie cyberbezpieczeństwa (KSC),
2. przepisy o ochronie danych osobowych (RODO),
3. przepisy sektorowe (m.in. usługi finansowe, life science, public),
4. przepisy dotyczące praw własności intelektualnej (prawo autorskie, ustawa o ochronie baz danych),
5. przepisy prawa cywilnego (m. in odpowiedzialność za wykonanie umów o świadczenie usług chmury obliczeniowej).

Istotne znaczenie odgrywają również **wytyczne organów nadzorczych** (np. Komunikat Urzędu Komisji Nadzoru Finansowego z 23 stycznia 2020 r. dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej) lub **organów władzy wykonawczej**. W tym ostatnim kontekście, warto wspomnieć, że w dniu 23 października 2024 r. podjęta została uchwała Rady Ministrów nr 127 **zmieniająca uchwałę RM z dnia 11 września 2019 r. w sprawie inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (MP 2024 poz. 908). Zmieniona uchwała Rady Ministrów obowiązuje od dnia 29 października 2024 r.** i ma kluczowe znaczenie dla realizacji projektów chmury obliczeniowej w sektorze publicznym.

Jeżeli chodzi o **nowe akty i regulacje prawne dotyczące chmury obliczeniowej, a które mają zacząć obowiązywać lub nad którymi prace mają być kontynuowane w 2025 roku**, to wskazać należy na:

1. Rozporządzenie Unii Europejskiej nr 2023/2854 **(Akt w sprawie danych)**, w szczególności w części dotyczącej postanowień dotyczących zmiany dostawcy usługi chmurowej (zob. pkt 5 poniżej),
2. **nowelizację ustawy o świadczeniu usług drogą elektroniczną**, na podstawie której mają zostać ustanowione organy nadzorcze odpowiedzialne za przestrzeganie przepisów unijnego rozporządzenia nr 2022/2065 pt. Akt w sprawie usług cyfrowych (AUC). Chmura obliczeniowa stanowi bowiem usługę hostingu w rozumieniu tego aktu prawnego i związku z tym dostawcy usług chmurowych muszą również spełnić wymagania określone w AUC, a w przypadku niewykonania tych obowiązków będą ponosili odpowiedzialności określone w nowelizacji ustawy o świadczeniu usług drogą elektroniczną, włącznie z możliwością nałożenia kar pieniężnych przez Prezesa UKE jako organu nadzorczego.

Warto również śledzić prowadzone przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) prace legislacyjne dotyczące **systemu dobrowolnej certyfikacji usług chmurowych.**

Komisja Europejska pracuje również nad opracowaniem zbioru zasad oraz wytycznych dotyczących zamówień publicznych na usługi przetwarzania danych **(EU Cloud Rulebook)**. Wytyczne mają zawierać zalecenia w zakresie podstawowych kryteriów dotyczących usług przetwarzania danych, które mają być brane pod uwagę przez organy sektora publicznego podczas procesu przetargowego.

4. Cyberbezpieczeństwo

Od dnia 28 sierpnia 2018 roku w Polsce obowiązuje **ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (KSC)**, która wdrożyła do polskiego porządku prawnego tzw. dyrektywę NIS-1 (Dz.U. z 2024 r. poz. 1077).

Ustawa o krajowym systemie cyberbezpieczeństwa była pierwszym aktem prawnym w tym zakresie w Polsce i stworzyła podstawy prawne dla cyberbezpieczeństwa na poziomie krajowym. W KSC wprowadzono podział na operatorów usług kluczowych, tj. podmioty świadczące usługi o krytycznym znaczeniu dla prawidłowego funkcjonowania państwa (np. w sektorze energetycznym), oraz dostawców usług cyfrowych, do których między innymi zaliczono dostawców usług chmury obliczeniowej czy internetowych platform handlowych.

Mając na względzie nowe wyzwania związane z cyberzagrożeniami, prawodawca unijny doprowadził do **uchwalenia dyrektywy NIS-2**, która zastąpiła dotychczasową dyrektywę NIS-1. Jej implementacja do systemów prawnych poszczególnych państw Unii Europejskiej **miała nastąpić do dnia 17 października 2024 roku, polski ustawodawca nie dotrzymał jednak tego terminu i w chwili obecnej nadal prowadzone są prace nad nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa, która ma dostosować przepisy tej ustawy do wymogów prawnych NIS-2.** Zgodnie z deklaracjami Ministerstwa Cyfryzacji, **przepisy znowelizowanej ustawy o KSC mają zacząć obowiązywać w pierwszym półroczu 2025 roku** (w projekcie nowelizacji przewidziany został miesięczny okres vacatio legis).

Zgodnie z dyrektywą NIS-2, dotychczasowy podział na operatorów usług kluczowych oraz dostawców usług cyfrowych został zastąpiony **podziałem na podmioty kluczowe i podmioty ważne**, nakładając na nie jednocześnie szereg nowych obowiązków. Co więcej, zmienione zostały kryteria kwalifikacji podmiotów, które zostaną objęte obowiązkami przewidzianymi w znowelizowanej ustawie o KSC, a także określona została nowa procedura umieszczenia podmiotów w wykazie podmiotów kluczowych lub ważnych. W nowelizacji przewidziano włączenie do krajowego systemu cyberbezpieczeństwa dodatkowych branż, które do tej pory nie były nim objęte (np. zarządzanie usługami ICT, produkcja, przetwarzanie i dystrybucja żywności). W konsekwencji znowelizowana ustawa o KSC stosować się będzie do kilkudziesięciu tysięcy podmiotów Polsce.

Do najważniejszych obowiązków nałożonych na podmioty kluczowe i ważne zaliczyć należy **obowiązek wprowadzenia odpowiednich środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług.** W nowelizacji określono również obowiązki raportowania incydentów cyberbezpieczeństwa sektorowemu CSIRT (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego). Na podmiotach zgłaszających incydent spoczywają również obowiązki sprawozdawcze – okresowe oraz końcowe -z obsługi incydentu.

Tego rodzaju sprawozdania mają się przyczynić do wyciągnięcia odpowiednich wniosków, między innymi przez zespoły CSIRT, i do poprawy ogólnego poziomu cyberbezpieczeństwa. W nowelizacji wprowadzono również nowy środek prawny – polecenie zabezpieczające, które wydawać ma minister właściwy do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego. W projekcie ustawy znalazły się również przepisy dodatkowe, które nie wynikają z implementacji dyrektywy NIS-2. Chodzi w szczególności o przepisy dotyczące uznania danego podmiotu za dostawcę wysokiego ryzyka.

Istotną zmianą, w stosunku do dotychczasowego stanu prawnego, jest **rozbudowanie w nowelizacji uprawnień organów nadzorczych.** W przypadku podmiotów kluczowych może mieć on zarówno charakter prewencyjny, jak i następczy, a w przypadku podmiotów ważnych – tylko następczy. W nowelizacji ustawy o KSC przewidziano możliwość nakładania na obie te kategorie podmiotów **wysokich kar pieniężnych** za naruszenie przepisów ustawy. Karze pieniężnej może **również podlegać kierownik podmiotu kluczowego lub ważnego** (do 600% jego wynagrodzenia).

Nowelizacja ustawy o KSC nie jest jedynym aktem prawnym z zakresu cyberbezpieczeństwa, który ma zacząć obowiązywać w 2025 r. Wymienić w związku z tym należy również:

1. Rozporządzenie Unii Europejskiej nr 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operational Resilience Act, **DORA**). Rozporządzenie to ma na celu zwiększenie odporności sektora finansowego na cyberataki i inne zagrożenia technologiczne. Wprowadza ono nowe, bardziej rygorystyczne wymagania dotyczące bezpieczeństwa cyfrowego dla instytucji finansowych i ich dostawców usług IT.

2. Dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz.U. L 333), tzw. **Dyrektywa CER**. Jest to unijny akt prawny, który ma na celu zwiększenie odporności podmiotów krytycznych na różnego rodzaju zagrożenia. Te zagrożenia mogą mieć charakter naturalny (np. katastrofy naturalne), technologiczny (np. cyberataki) czy też pochodzić z działań człowieka (np. sabotaż). Dyrektywa CER powinna zostać implementowana do polskiego porządku prawnego do 17 października 2024 r. Polski ustawodawca nie dotrzymał jednak tego terminu i prowadzona są w związku nadal prace nad **zmianą ustawy o Zarządzaniu Kryzysowym.**

3. Rozporządzenie Unii Europejskiej nr 2024/2847 w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 **(Akt o cyberodporności).**

5. Data Act (Akt w sprawie danych)

Akt w sprawie danych to unijne rozporządzenie, które ma na celu stworzenie jednolitego rynku danych w Europie. Jego pełna nazwa to Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2023/2854 z dnia 13 grudnia 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). **Jego głównym celem jest zapewnienie szerszego dostępu do danych i ich wykorzystania między różnymi uczestnikami rynku, a także zwiększenie konkurencji na rynku danych. Przepisy rozporządzenia dotyczą zarówno danych osobowych, jak nieosobowych.**

Zgodnie z art. 50 Aktu w sprawie danych, jego przepisy zaczną **obowiązywać w dniu 12 września 2025 r.**, z tym, że przepisy ustanawiające nowe wymogi w zakresie projektowania i wytwarzania urządzeń Internetu rzeczy (IoT) będą miały zastosowanie do produktów **wprowadzonych na rynek po 12 września 2026 r**. Rozporządzenie zostanie uzupełnione **polską ustawą wdrażającą, nad którą obecnie trwają prace legislacyjne w Ministerstwie Cyfryzacji.** Ustawa ta będzie między innymi określać mechanizmy nadzoru i egzekwowania przepisów Aktu w sprawie danych, w tym organ nadzorczy i sankcje za naruszenie przepisów.

Akt w sprawie danych ma charakter horyzontalny. Jego przepisy stosuje się do wszystkich sektorów gospodarki. Reguluje on wymianę danych między przedsiębiorstwami (B2B), między przedsiębiorstwami a konsumentami (B2C) oraz między przedsiębiorstwami a administracją publiczną (B2G).

W Akcie w sprawie danych doszło do **wzmocnienia uprawnień użytkowników w zakresie dostępu i wykorzystania danych generowanych przez urządzenia tzw. Internetu rzeczy.** Rozporządzenie w szczególności przyznaje użytkownikom większą kontrolę nad danymi generowanymi przez produkty, które posiadają. Oznacza to, że użytkownicy będą mogli łatwiej przenosić swoje dane do innych usługodawców oraz decydować, kto może mieć do nich dostęp. Obecnie dostęp do takich danych mają często wyłącznie producenci urządzeń, co uniemożliwia użytkownikom korzystanie z konkurencyjnych usług posprzedażowych lub naprawczych. Rozporządzenie wymaga, aby inteligentne urządzenia były projektowane i wytwarzane w taki sposób, aby dane generowane w wyniku korzystania z nich były domyślnie łatwo, bezpiecznie oraz, w razie potrzeby, bezpośrednio z poziomu urządzenia dostępne dla użytkownika oraz dla innych podmiotów przez niego wskazanych.

Dla relacji B2B istotne znaczenie ma **określenie w Akcie w sprawie danych postanowień umownych dotyczących dostępu i wykorzystania danych, które zostały uznane za nieuczciwe.** Przepisy te mają przede wszystkim chronić interesy mikro-, małych i średnich przedsiębiorstw, które mają słabszą pozycję negocjacyjną. Mają one bezwzględnie obowiązujący charakter i strony nie mogą ich wyłączyć w drodze umowy.

Akt w sprawie danych wprowadza również ułatwienia przy zmianie dostawcy usług chmurowych. Należy przy tym podkreślić, że dotyczy to również dostawców spoza UE, o ile świadczą usługi klientom na terytorium Unii Europejskiej. Przepisy te dotyczą również sytuacji zmiany usługi chmury na lokalną infrastrukturę ICT.

Prawa klienta i obowiązki dostawcy usługi przetwarzania danych w odniesieniu do zmiany dostawcy takich usług lub do przeniesienia do lokalnej infrastruktury ICT mają zostać jasno określone w umowie zawartej na piśmie, a dostawca usług przetwarzania danych udostępnia taką umowę klientowi przed jej podpisaniem. Proces przełączania usługi i przekazania danych do nowego dostawcy ma przebiegać szybciej i sprawniej, a wprowadzone w tym zakresie obowiązki mają zmniejszyć uzależnienie klientów od jednego dostawcy usług chmurowych. Od wejścia w życie Aktu w sprawie danych obniżeniu uległy koszty zmiany dostawcy, **a od 12 stycznia 2027 r. opłaty te mają być nienakładane.** W rozporządzeniu wprowadzono również standardy interoperacyjności danych i usług przetwarzania danych.

W Akcie w sprawie danych wprowadzono **również regulację umożliwiającą organom sektora publicznego dostęp i wykorzystanie danych, którymi dysponuje sektor prywatny.** Uzyskanie dostępu do danych prywatnych będzie możliwe tylko w nadzwyczajnych przypadkach, np. kiedy dane są niezbędne, aby skutecznie reagować na skutki klęsk żywiołowych, a potrzebnych danych nie da się na czas pozyskać w inny sposób.

6. Dezinformacja w Internecie

Dezinformacja to świadome rozpowszechnianie nieprawdziwych lub wprowadzających w błąd informacji, mające na celu podważanie zaufania do instytucji, społeczeństw i konkretnych ludzi. Działania dezinformacyjne podejmowane są z różnych powodów – głównie dla realizacji celów politycznych i/lub chęci osiągnięcia zysku ekonomicznego. Ich wynikiem może być wywołanie:

1. szkody publicznej (np. naruszenie demokratycznego procesu wyborczego),
2. szkody osobowej (np. naruszenie dobrego imienia konkretnej osoby fizycznej lub prawnej).

Zwalczaniu dezinformacji ma przede wszystkim służyć unijne rozporządzenie nr 2022/2065 pt. **Akt o usługach cyfrowych (AUC)**, nakładające w tym zakresie obowiązki na tzw. dostawców usług pośrednich (pośredników internetowych). Na gruncie AUC wyróżnić można dwa podstawowe sposoby zwalczania dezinformacji:

1. jako nielegalne treści w rozumieniu AUC,
2. jako treści szkodliwe społecznie, rodzące ryzyka określone w AUC.

Nielegalne treści w rozumieniu AUC to treści sprzeczne z prawem Unii Europejskiej (np. treści wzywające do terroryzmu) lub treści sprzeczne z prawem krajowym. W tym ostatnim przypadku chodzi zarówno o przepisy prawa publicznego (np. zabronione przepisami karnymi treści nawołujące do nienawiści na tle różnic narodowościowych, etnicznych, rasowych), jak i przepisy prawa prywatnego (np. treści stanowiące naruszenie dóbr osobistych na gruncie kodeksu cywilnego). **Obowiązek moderowania, w tym usunięcia, treści nielegalnych mają wszyscy pośrednicy internetowi.**

Treści szkodliwe to z kolei treści, które nie są formalnie bezprawne, ale są społecznie niepożądane. Obowiązek ich moderowania, w tym usunięcia, nałożony został tylko na określoną grupę pośredników internetowych, stanowiących na gruncie AUC tzw. bardzo duże platformy internetowe (VLOP) lub bardzo duże wyszukiwarki internetowe (VLOSE). W rozporządzeniu wskazano przy tym na konkretne przypadki tzw. ryzyk systemowych, którym powinny zapobiegać VLOP i VLOSE. Chodzi tu między innymi o „ryzyko faktycznego lub przewidywalnego negatywnego wpływu na procesy demokratyczne, dyskurs obywatelski i procesy wyborcze, a także na bezpieczeństwo publiczne czy negatywnego wpływu na ochronę zdrowia publicznego małoletnich oraz poważne negatywne konsekwencje dla fizycznego i psychicznego dobrostanu osoby, lub na przemoc ze względu na płeć" (motyw nr 83 i 84).

Możliwość zwalczania dezinformacji w Internecie, z wykorzystaniem powyższych instytucji prawnych, określonych w Akcie o usługach cyfrowych, zaktualizują się z chwilą uchwalenia ustawy wdrażającej AUC, tj. nowelizacji ustawy o świadczeniu usług drogą elektroniczną. Ma to nastąpić **w pierwszej połowie 2025 roku. Zwalczaniu dezinformacji służą również przepisy rozporządzenia Unii Europejskiej nr 2024/900 o reklamie politycznej** (zob. pkt 19 poniżej).

Niezależnie od środków prawnych ustanowionych w AUC oraz rozporządzeniu o reklamie politycznej, dezinformację można **również zwalczać na podstawie ogólnych przepisów Kodeksu cywilnego** (np. art. 23 k.c.) lub **Kodeksu karnego** (np. art. 212, 256-257 k.k.). W przypadku gdy źródłem tego rodzaju informacji jest dziennikarz, zastosowanie mogą ewentualnie znaleźć również przepisy **ustawy - Prawo prasowe**, w szczególności art. 12, zgodnie z którym „dziennikarz jest zobowiązany zachować szczególną staranność i rzetelność przy zbieraniu i wykorzystaniu materiałów prasowych, a w szczególności sprawdzać zgodność z prawdą uzyskanych wiadomości lub podać ich źródło". Warto wspomnieć, że w polskim systemie prawnym mamy również jeden przepis prawny „dedykowany" tego rodzaju sytuacjom. Chodzi w szczególności o przepis zwalczający rozpowszechnianie nieprawdziwych informacji w związku z kampanią wyborczą. Zgodnie z **art. 111 §1 ustawy - Kodeks wyborczy** kandydatowi przysługuje m.in. prawo do wniesienia do sądu okręgowego wniosku o wydanie orzeczenia zakazu rozpowszechniania takich informacji. Wniosek taki ma zostać rozpoznany w ciągu 24 godzin w postępowaniu nieprocesowym. Równie szybki jest termin na wniesienie zażalenia na takie rozstrzygnięcie i jego rozpatrzenia przez sąd apelacyjny, a publikacja sprostowania, odpowiedzi lub przeprosin powinna nastąpić najpóźniej w ciągu 48 godzin, na koszt zobowiązanego (art. 111 § 3 i 4).

7. Elektroniczny sport (e-sport)

W systemie prawnym Unii Europejskiej nie obowiązuje, a także nie planuje się uchwalenia kompleksowej regulacji prawnej dotyczącej e-sportu. Pewne aspekty działalności w zakresie sportu elektronicznego są natomiast regulowane wycinkowo w poszczególnych państwa UE (np. we Francji).

W polskim systemie prawnym **definicja legalna „sportu" zawarta jest w art. 2 ust. 1 ustawy o sporcie** (tj. Dz.U. z 2024 r. poz. 1488). Zgodnie z art. 2 ust. 1a ustawy o sporcie, „za sport uważa się również współzawodnictwo oparte na aktywności intelektualnej, którego celem jest osiągnięcie wyniku sportowego". Polski ustawodawca jednoznacznie dopuścił więc możliwość kwalifikacji gier umysłowych jako „sportu" w znaczeniu prawnym. Co więcej, w uzasadnieniu do projektu nowelizacji ustawy o sporcie z 2017 r. wprost wskazano, że również sporty elektroniczne realizują cele, które stawiane są „sportowi", stwarzając „możliwość rozwoju intelektualnego, wzmacniając relacje społeczne, sprzyjając socjalizacji uczestników oraz dodając pewności siebie" (Druk Sejmowy nr 1410 z 16 marca 2017 r.). Należy w związku z tym stwierdzić, że **w polskim systemie prawnym e-sport stanowi sport w rozumieniu prawnym.** Dotyczy zarówno turniejów rozgrywanych online, jak i offline (tzw. turnieje LAN-owe).

Kwalifikacja prawna sportu jako sportu elektronicznego pociąga za sobą istotne skutki prawne, które podzielić można na dwie, podstawowe grupy:

1. możliwość skorzystania z rozwiązań przewidzianych w ustawie o sporcie (np. finansowanie, dotacje, stypendia sportowe etc., przyznawane przez jednostki samorządu terytorialnego). Należy jednak podkreślić, że zdecydowana większość możliwości prawnych określonych w ustawie o sporcie wymaga – dodatkowo utworzenia polskiego związku sportowego, o czym decyduje minister właściwy do spraw kultury fizycznej (art. 7 ust. 2 ustawy o sporcie). Do chwili obecnej, nie utworzono jednak w Polsce związku sportów elektronicznych.
2. rozwiązania przewidziane w innych jeszcze ustawach (np. zwolnienie z podatku dochodowego od nagród, w przypadku gdy jednorazowa wartość nagrody nie przekracza 2.000 złotych (art. 21 ust. 1 pkt 68 ustawy o podatku dochodowym od osób fizycznych).

Oprócz wyżej wymienionych przepisów, do sportu elektronicznego znajdują zastosowania aktów prawnych, które nie są „dedykowane" do tego rodzaju działalności, w tym przede wszystkim ustawa o prawie autorskim. **W 2025 roku nie są planowane żadne zmiany legislacyjne dotyczące tych przepisów.**

8. Freedom Media Act (Akt o wolności mediów)

W dniu 17 kwietnia 2024 r. opublikowane zostało rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2024/1083 z dnia 11 kwietnia 2024 r. w sprawie ustanowienia wspólnych ram dla usług medialnych na rynku wewnętrznym i zmiany dyrektywy 2010/13/UE (Europejski Akt o Wolności Mediów). **Większość przepisów rozporządzenia zacznie obowiązywać od dnia 8 sierpnia 2025** r.

Zasadniczym celem rozporządzenia jest **ochrona pluralizmu mediów oraz niezależności redakcyjnej zarówno mediów prywatnych, jak i publicznych. Rozporządzenie ma w szczególności zabezpieczać prywatnych, jak i publicznych dostawców usług medialnych przed ingerencjami politycznymi w decyzje redakcyjne, a także chronić dziennikarzy i ich źródła.** Na państwa Unii Europejskiej nałożono także obowiązek rozdzielania środków publicznych na reklamę lub inne usługi świadczone przez media zgodnie z obiektywnymi kryteriami i w sposób niedyskryminujący. Na mocy rozporządzenia powołano również **Europejską Radę Usług Medialnych.**

Europejski Akt o Wolności Mediów wymaga uchwalenia przepisów krajowych, wdrażających jego postanowienia. W Polsce prace te nadzoruje Ministerstwo Kultury i Dziedzictwa Narodowego.

Zgodnie z **założeniami nowej ustawy medialnej**, która była poddana konsultacjom społecznym, ma ona regulować następujące, podstawowe obszary:

1. finansowanie mediów publicznych,
2. reformę Krajowej Rady Radiofonii i Telewizji,
3. powoływanie władz mediów publicznych,
4. pluralizm mediów.

Uchwalenie nowej ustawy medialnej planowane jest w 2025 roku.

9. Generatywna sztuczna inteligencja

Systemy sztucznej inteligencji można podzielić na:

1. **„tradycyjną" AI**, która koncentruje się na wykrywaniu wzorców, podejmowaniu decyzji, doskonaleniu analityki, np. klasyfikowaniu danych, tworzeniu modelu predykcyjnych etc.
2. **„generatywną" AI**, która wykorzystywana jest do tworzenia treści, obrazów, dźwięków czy kodów programów komputerowych.

Znaczenie prawne wyżej wymienionego podziału jest następujące:

1. dodatkowe obowiązki w Akcie w sprawie sztucznej inteligencji w zakresie tworzenia i korzystania z generatywnej sztucznej inteligencji (art. 50) – zob. pkt 20 poniżej;
2. dodatkowe, szczególne problemy i ryzyka prawne związane z korzystaniem z generatywnej AI.

Jeżeli chodzi ryzyka prawne związane z korzystaniem z generatywnej sztucznej inteligencji, to w pierwszej kolejności wymienić należy **ryzyka prawne związane z przepisami prawa autorskiego** (zob. pkt 22 poniżej).

Do innych ryzyk należy zaliczyć między innymi:

1) **ryzyko naruszenia postanowień umów z kontrahentami.** Należy w szczególności zweryfikować, czy **umowa lub inne ustalenia z kontrahentem nie wykluczają użycia AI**, ewentualnie w jakim zakresie pozwalają lub zakazują jej użycia lub wykorzystania efektów jej pracy.

2) **ryzyko naruszenia poufności danych** (np. objętych tajemnicą przedsiębiorstwa) - zgodnie z postanowieniami warunków korzystania z produktów i usług dostawców rozwiązań generatywnej sztucznej inteligencji (np. chatbotów), ich dostawcy zastrzegają sobie prawo wykorzystywania treści przetwarzanych w ramach udostępnianych użytkownikowi narzędzi na potrzeby „utrzymania, rozwijania i ulepszania swoich technologii". Mowa tu nie zarówno o danych wejściowych („input"), jak i danych wyjściowych („output"). Oznacza to, że użytkownik, wprowadzając do np. chatbota dane stanowiące tajemnicę przedsiębiorstwa lub objęte zobowiązaniem do zachowania poufności, przekazuje te dane dostawcy do bliżej niesprecyzowanego użytku.

3) **ryzyko braku merytorycznej poprawności danych** - wyniki otrzymywane z narządzi generatywnej sztucznej inteligencji mogą być wadliwe. Wyraźnie zastrzegają to w warunkach usług dostawcy, podkreślając, że użytkownik wykorzystuje je na „własne ryzyko i odpowiedzialność."

Odnośnie sztucznej inteligencji – zob. również pkt 20 poniżej.

10. Handel elektroniczny (e-commerce)

Na system przepisów prawnych regulujących prowadzenie handlu elektronicznego w Polsce składają się obowiązujące już od lat, następujące akty prawne:

1) ogólne przepisy dotyczące świadczenia usług elektronicznych (relacje B2B i B2C)
   a) ustawa o świadczeniu usług drogą elektroniczną („uśude")
2) przepisy dotyczące transakcji elektronicznych (relacje B2B i B2C)
   a) sposób zawarcia umów online (kodeks cywilny)
   b) forma czynności prawnych (kodeks cywilny, rozporządzenie eIDAS)
   c) rozporządzenie UE o usługach pośrednictwa internetowego
3) przepisy dotyczące ochrony konsumenta w handlu elektronicznym (relacje B2C)
   a) ustawa o prawach konsumenta
   b) ustawa o ochronie konkurencji i konsumentów
   c) ustawa o informowaniu o cenach towarów i usług
   d) ustawa o przeciwdziałaniu nieuczciwym praktykom rynkowym
   e) przepisy kodeksu cywilnego dotyczące tzw. klauzul abuzywnych
4) przepisy dotyczące ochrony przedsiębiorcy w umowach z platformami internetowymi (relacje B2B).

Poza nowelizacją ustawy o świadczeniu usług drogą elektroniczną (zob. pkt 15 poniżej) oraz nowelizacją rozporządzenia eIDAS (zob. pkt 21 poniżej), w 2025 r. nie jest planowana zmiana wyżej wymienionych przepisów.

W 2024 r. zaczęły natomiast obowiązywać **dwa nowe akty prawne, odnoszące się do handlu elektronicznego:**

1. ustawa z dnia 23 maja 2024 r. o zmianie ustawy o wymianie informacji podatkowych z innymi państwami oraz niektórych innych ustaw (Dz.U. z 2024 r. poz. 879), która implementowała do polskiego systemu prawnego przepisy unijnej **dyrektywy DAC-7.**
2. Rozporządzenie Parlamentu Europejskiego i Rady nr 2023/988 w sprawie ogólnego bezpieczeństwa produktów, Dz.U. UE, L 135/1 **(General Product Safety Regulation, GPRS)**.

Celem uchwalenia dyrektywy DAC-7 jest przeciwdziałanie zjawiskom uchylania się od opodatkowania w związku z transakcjami elektronicznymi realizowanymi poprzez platformy cyfrowe, a także zwiększenie dostępności dla administracji podatkowych danych o dochodach uzyskiwanych ze sprzedaży prowadzonej za pośrednictwem określonych platform cyfrowych. Adresatami obowiązków określonych w nowych przepisach są **operatorzy takich platform, a więc podmioty, które w ramach umowy ze sprzedawcami (użytkownikami platformy) udostępniają im platformę albo jej część, tak aby za pośrednictwem tej platformy można było dokonywać odpłatnych transakcji (np. sprzedaży towarów w internetowych serwisach aukcyjnych).** Operatorem platformy w rozumieniu znowelizowanej ustawy o wymianie informacji podatkowych nie będzie natomiast podmiot, który dokonuje z wykorzystaniem platformy transakcji wyłącznie we własnym imieniu i na własną rzecz (np. sklep internetowy).

Operator platformy ma **obowiązek przekazać drogą elektroniczną Szefowi Krajowej Administracji Skarbowej zbiorczą informację o sprzedawcach podlegających raportowaniu za okres sprawozdawczy (dany rok kalendarzowy).** Obowiązek ten nie dotyczy podmiotów sprzedających rzeczy okazjonalnie w trakcie okresu sprawozdawczego (mniej niż 30 transakcji za łączną kwotę do 2000 euro). Raportujący operator platformy po raz pierwszy będzie zobowiązany do spełnienia obowiązków sprawozdawczych w 2025 r.

Raportujący operator platformy ma również **obowiązek gromadzenia i weryfikacji informacji dotyczących swoich użytkowników oraz uznawania sprzedawcy za rezydenta danego państwa.** Operator platformy będzie także zobowiązany przechowywać informacje i dowody dotyczące realizowanych obowiązków przez okres 5 lat, licząc od końca roku, w którym upłynął termin przekazania informacji o sprzedawcach.

Szef Krajowej Administracji Skarbowej będzie uprawniony do przeprowadzenia kontroli w zakresie wykonywania powyższych obowiązków przez raportującego operatora platformy. Ich niewypełnienie zagrożone jest karą pieniężną w wysokości do 1.000.000 złotych, może również stanowić przestępstwo lub wykroczenie skarbowe.

W dniu 13 grudnia 2024 r. zaczęło z kolei obowiązywać unijne rozporządzenie 2023/988 w sprawie ogólnego bezpieczeństwa produktów (General Product Safety Regulation, GPRS). Celem GPSR jest zapewnienie wysokiego poziomu bezpieczeństwa produktów konsumenckich na rynku Unii Europejskiej, zwłaszcza w świetle zmian związanych z rozwojem nowych technologii oraz sprzedażą przez Internet. Zasadniczo GPSR obejmuje wszystkie produkty, których aspekty bezpieczeństwa nie zostały szczegółowo uregulowane w innych przepisach unijnych. Rozporządzenie ma zastosowanie do szerokiego katalogu produktów, które są dostarczane lub udostępniane za wynagrodzeniem lub bez, w tym w ramach świadczenia usługi. **Nowe przepisy dotyczą produktów przeznaczonych dla konsumentów, bez względu na to, czy są to produkty nowe, używane, naprawione lub odnowione. W ramach rozporządzenia usprawniono procedury zgłaszania niebezpiecznych produktów, a także wprowadzono nowe, bardziej efektywne procedury zgłaszania produktów niebezpiecznych.** Poszerzono zakres informacji przekazywanych konsumentom, a przedsiębiorcy zobowiązani zostali do przechowywania, przez określony czas, dokumentacji dotyczącej bezpieczeństwa produktów. Ustanowiono również szczególne obowiązki dostawców internetowych platform handlowych związane z bezpieczeństwem produktów sprzedawanych na tych platformach (art. 22).

W kontekście przepisów dotyczących handlu elektronicznego, należy również odnotować, że **w dniu 28 czerwca 2025 r. zacznie również obowiązywać ustawa z dnia 26 kwietnia 2024 r. o zapewnieniu spełniania wymagań dostępności niektórych produktów i usług przez podmioty gospodarcze (Dz.U. z 2024 r. poz. 731)**. Ustawa ma na celu usunięcie barier, które uniemożliwiają lub utrudniają osobom z niepełnosprawnościami korzystanie z produktów i usług dostępnych na rynku. Przepisy ustawy stosuje się między innymi do usług handlu elektronicznego (art. 3 ust. 2 pkt 6). Przedsiębiorcy oferujący tego rodzaju usługi są między innymi zobowiązani do zapewnienia odpowiedniej dostępności stron internetowych i aplikacji mobilnych, a także dokumentów. Muszą także umożliwić alternatywne sposoby komunikacji, takie jak opisane obrazy, napisy do filmów czy transkrypcje audio. Systemy informatyczne muszą być zgodne z popularnymi technologiami wspomagającymi, takimi jak np. czytniki ekranowe.

W podsumowaniu nowych przepisów dotyczących e-commerce warto **również wymienić nowelizację ustawy o świadczeniu usług drogą elektroniczną, w ramach której przewidziane jest ustanowienie organów nadzorczych, które między innymi będą odpowiedzialne za przestrzeganie przepisów Aktu o usługach cyfrowych, dotyczących funkcjonowania internetowych platform handlowych i umożliwiających konsumentom zawieranie umów z przedsiębiorcami na odległość (art. 29-32)**. Właściwym organem w tym zakresie ma być Prezes UOKiK. Przepisy te mają zostać uchwalone **w pierwszej połowie 2025 roku.**

11. Influencer marketing

Obecnie ani w Unii Europejskiej, ani w Polsce nie obowiązują przepisy prawne, które wprost regulują działalność influencerów.

Częstym zarzutem kierowanym pod adresem influencerów jest zaniechanie właściwego oznaczania materiałów reklamowych w mediach społecznościowych (transparentność). Może to skutkować uznaniem ich działalności za:

1. **kryptoreklamę** w rozumieniu art. 7 ust. 1 pkt 11 ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym – „nieuczciwą praktyką rynkową jest kryptoreklama, która polega na wykorzystywaniu treści publicystycznych w środkach masowego przekazu w celu promocji produktu w sytuacji, gdy przedsiębiorca zapłacił za tę promocję, a nie wynika to wyraźnie z treści lub z obrazów lub dźwięków łatwo rozpoznawalnych przez konsumenta”
2. **czyn nieuczciwej konkurencji** w rozumieniu art. 16 ust. 1 pkt 4 ustawy o zwalczaniu nieuczciwej konkurencji – „czynem nieuczciwej konkurencji w zakresie reklamy jest w szczególności wypowiedź, która, zachęcając do nabywania towarów lub usług, sprawia wrażenie neutralnej informacji”.

W związku z powyższym, warto wspomnieć o dwóch inicjatywach zrealizowanych w Polsce. Po pierwsze, **w 2022 r. Prezes UOKiK wydał rekomendacje dotyczące oznaczania treści reklamowych przez influencerów w mediach społecznościowych (https://uokik.gov.pl/influencer-marketing)**. Treść rekomendacji została skonsultowana z organizacjami branżowymi: IAB Polska, SAR i Radą Reklamy, oraz ośrodkami naukowymi: Uniwersytetem Warszawskim i Uniwersytetem im. Adama Mickiewicza w Poznaniu. Po drugie, w dniu 17 grudnia 2024 r. **Rada Reklamy uchwaliła Kodeks etycznego postępowania w branży influencer marketingu.**

W związku z działalnością influencerską warto również wspomnieć o **komunikacie KRRiT z dnia 12 stycznia 2022 roku**, zgodnie z którym działalność influencerów, polegająca na zarobkowej publikacji materiałów na platformach udostępniania video (np. YouTube), stanowi audiowizualną usługę medialną w rozumieniu ustawy o radiofonii i telewizji i w związku z tym podlega obowiązku zgłoszenia usług do wykazu Przewodniczącego KRRiTV, a także innym obowiązkom określonym w tej ustawie.

W 2025 roku nie jest planowane uchwalenie przepisów prawnych dotyczących działalności influencerskiej.

12. Internet rzeczy (IoT)

Zarówno w Unii Europejskiej, jak i w Polsce nie planuje się uchwalenia aktu prawnego całościowo regulującego świadczenie usług i korzystanie z chmury obliczeniowej.

W praktyce, w projektach chmury obliczeniowej zastosowanie znajdują przepisy następujących aktów prawnych:

1. przepisy ustawy o krajowym systemie cyberbezpieczeństwa (KSC),
2. przepisy o ochronie danych osobowych (RODO),
3. przepisy sektorowe (m.in. usługi finansowe, life science, public),
4. przepisy dotyczące praw własności intelektualnej (prawo autorskie, ustawa o ochronie baz danych),
5. przepisy prawa cywilnego (m.in. odpowiedzialność za wykonanie umów o świadczenie usług chmury obliczeniowej).

Istotne znaczenie odgrywają również **wytyczne różnych organów. Warto w związku z tym wymienić wytyczne Europejskiej Rady Ochrony Danych (EROD) nr 1/2020** dotyczące przetwarzania danych osobowych w kontekście pojazdów podłączonych do Internetu i aplikacji związanych z mobilnością (connected cars) oraz wytyczne Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) pt. “Guidelines for securing the Internet of Things (2020)”.

Jeżeli chodzi o akty prawne, które **zaczną obowiązywać w 2025 roku lub do przepisów których należy rozpocząć stopniowe dostosowanie,** to na rynek Internetu rzeczy wpływ będą miały przede wszystkim **trzy nowe regulacje**:

1. Rozporządzenie Unii Europejskiej pt. **Akt w sprawie danych,** w szczególności w zakresie zwiększenia uprawnień użytkowników urządzeń IoT (zob. pkt 5 powyżej),
2. Rozporządzenie Unii Europejskiej pt. **Akt w sprawie sztucznej inteligencji** (zob. pkt 20 poniżej),
3. Rozporządzenie Unii Europejskiej pt. **Akt o cyberodporności.**

Przepisy Rozporządzenia nr 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 **(Akt o Cyberodporności, Cyber Resilence Act, CRA)**, weszły w życie w dniu 10 grudnia 2024 r. (Dz.U. UE z 20.11.2024), ale **zasadnicza część regulacji zacznie obowiązywać dopiero od dnia 11 grudnia 2027 r.** (art. 71 ust. 2). Jest to pierwszy tego rodzaju akt prawny, który wprowadza obowiązkowe wymogi w zakresie cyberbezpieczeństwa dla produktów posiadających elementy cyfrowe (np. robotów, aplikacji mobilnych czy gier video). Będzie miał zastosowanie do wszystkich produktów, które są bezpośrednio lub pośrednio połączone z innym urządzeniem lub siecią.

13. Komunikacja elektroniczna

Prawo komunikacji elektronicznej (PKE) zostało uchwalone w Polce w dniu 12 lipca 2024 r. w związku obowiązkiem implementacji Dyrektywy nr 2018/1972 o Europejskim Kodeksie Łączności Elektronicznej (Dz.U. z 2024 r. poz. 1221). PKE uchyliło dotychczasowe Prawo telekomunikacyjne (PT). Przepisy te w istotnej części zaczęły obowiązywać od dnia **10 listopada 2024 r.**

Dla rynku nowych technologii jedna z najistotniejszych zmian, wprowadzonych w Prawie komunikacji elektronicznej, polega na **objęciu jego przepisami podmiotów świadczących tzw. usługi interpersonalne, w stosunku do których do tej pory przepisy Prawa telekomunikacyjnego nie stosowały się.** Chodzi w szczególności o dostawców: poczty elektronicznej, komunikatorów internetowych oraz czatów grupowych.

W Prawie komunikacji elektronicznej połączono również dotychczasowe przepisy dotyczące prowadzenia **marketingu elektronicznego**, a znajdujące się do tej pory w ustawie o świadczeniu usług drogą elektroniczną (art. 10) oraz prawie telekomunikacyjnym (art. 172). Obecnie są one w całości uregulowane w przepisach PKE (art. 398).

Niezależnie od powyższego, w ustawie - Prawo komunikacji elektronicznej przejęto szereg, wcześniej już obowiązujących, przepisów Prawa telekomunikacyjnego, a dotyczących przedsiębiorców świadczących usługi telekomunikacyjne (obecnie usługi komunikacji elektronicznej). Równocześnie jednak **dokonano modyfikacji części z tych obowiązków (np. w zakresie treści warunków umów) oraz wprowadzono względnie zupełnie nowe rozwiązania.** Przykładem jest obowiązek uzyskania uprzedniej zgody abonenta na uruchomienie usługi fakultatywnego obciążania rachunku, tzw. **direct billing** (art. 349 PKE).

Przedsiębiorca, który umożliwia klientowi korzystanie z usług dodatkowych przez doliczenie kwoty zakupy do rachunku (np. subskrypcji, gier online, płatnych treści premium), jest zobowiązany do:

1. informowania klienta o wszelkich kosztach, przed dokonaniem transakcji
2. wprowadzenia mechanizmów potwierdzających zgodę użytkownika na obciążenie jego rachunku.

Direct billing ma chronić klientów przed przypadkowymi zakupami oraz nieświadomymi opłatami, jednocześnie zwiększając odpowiedzialność przedsiębiorców za przejrzystość oferowanych usług.

W razie niewykonania lub nienależytego wykonania większości obowiązków ustanowionych w Prawie komunikacji elektronicznej, Prezes UKE będzie mógł nałożyć na przedsiębiorców komunikacji elektronicznej **karę pieniężną w wysokości do 3% przychodu osiągniętego przez tego przedsiębiorcę w poprzednim roku kalendarzowym (art. 446 ust. 1).**

W kontekście komunikacji elektronicznej, należy również podkreślić, że w 2024 roku weszły w życie kolejne przepisy **ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej** (tj. Dz.U. z 2024 r. poz. 1803).

W art. 3 ustawy wskazano na cztery przykłady zakazanych nadużyć w komunikacji elektronicznej, w szczególności:

1. generowanie sztucznego ruchu,
2. smishing, a więc wysłanie krótkiej wiadomości tekstowej (SMS), w której nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego zachowania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego lub instalacji oprogramowania,
3. CLI spoofing, a więc nieuprawnione posłużenie się lub korzystanie przez użytkownika lub przedsiębiorcę telekomunikacyjnego, wywołującego połączenie głosowe, informacją adresową wskazującą na osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej inną niż ten użytkownik lub przedsiębiorca telekomunikacyjny, służące podszyciu się pod inny podmiot, w szczególności w celu wywołania strachu, poczucia zagrożenia lub nakłonienia odbiorcy tego połączenia do określonego zachowania, zwłaszcza do przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji oprogramowania,
4. nieuprawniona zmiana informacji adresowej - niezgodne z prawem modyfikowanie informacji adresowej uniemożliwiające albo istotnie utrudniające ustalenie, przez uprawnione podmioty lub przedsiębiorców telekomunikacyjnych uczestniczących w dostarczaniu.

Przykładem obowiązku nałożonego na przedsiębiorców komunikacji elektronicznej w zwalczaniu wyżej wymienionych nadużyć jest przewidziany w art. 6 ustawy wymóg blokowania krótkich wiadomości tekstowych (SMS) wyczerpujących znamiona smishingu.

Na przedsiębiorców komunikacji elektronicznej, którzy nie wypełniają nałożonych na nich obowiązków, może zostać nałożona **kara pieniężna** (art. 27 ust. 3), w wysokości, co do zasady, maks. 3% przychodu osiągniętego w poprzednim roku kalendarzowym (art. 28 ust. 1).

14. Lotnicze prawo (drony)

W obecnym stanie prawnym **wykorzystywanie dronów jest regulowane zarówno przepisami prawa unijnego, jak i prawa polskiego.**

Z punktu widzenia prawa Unii Europejskiej kluczowe znaczenie mają następujące akty prawne:

1. **Rozporządzenie wykonawcze Komisji (UE) 2019/947** – dotyczy głównie zasad wykonywania operacji dronami,
2. **Rozporządzenie delegowane Komisji (UE) 2019/945** – dotyczy przede wszystkim klas systemów BSP (bezzałogowych systemów powietrznych),
3. dokument ***Easy Access Rules for UAS*** (wskazówki i wyjaśnienia stosowania przepisów wynikających z rozporządzeń wykonawczych nr 945 i 947),
4. dokument ***Guidelines for UAS operations in the open and specific category – Ref to Regulation (EU) 2019/947.***

Wyżej wymienione dokumenty Unii Europejskiej nie regulują jednak wszystkich kwestii związanych z wykorzystywaniem dronów. Konieczne jest w związku z tym wydanie przez poszczególne państwa Unii Europejskiej odpowiednich przepisów krajowych. Ponieważ proces przyjęcia w Polsce odpowiedniej nowelizacji prawa lotniczego bardzo się wydłużył, Prezes Urzędu Lotnictwa Cywilnego wprowadził tzw. **Wytyczne Prezesa ULC** regulujące część tych zasad. Są to:

1. Wytyczne nr 6/2024 Prezesa Urzędu Lotnictwa Cywilnego z dnia 20 maja 2024 r. **w sprawie wyznaczania stref geograficznych dla systemów bezzałogowych statków powietrznych** (Dz.U. Urzędu Lotnictwa Cywilnego, poz. 22),
2. Wytyczne nr 7/2024 Prezesa Urzędu Lotnictwa Cywilnego z dnia 20 maja 2024 r. **w sprawie sposobów wykonywania operacji przy użyciu systemów bezzałogowych statków powietrznych** w związku z wejściem w życie przepisów rozporządzenia wykonawczego Komisji (UE) nr 2019/947 z dnia 24 maja 2019 r. w sprawie przepisów i procedur dotyczących eksploatacji bezzałogowych statków powietrznych (Dziennik Urzędowy Urzędu Lotnictwa Cywilnego, poz. 23).

Na podstawie wyżej wymienionych przepisów, **korzystanie z dronów w Polsce jest już dopuszczalne, przy spełnieniu określonych w nich warunków.**
W dniu 5 listopada 2024 r. Rada Ministrów przyjęła **projekt ustawy o zmianie ustawy – Prawo lotnicze oraz niektórych innych ustaw.** W nowelizacji dokonano wyszczególnienia trzech kategorii operacji bezzałogowymi statkami powietrznymi (BSP):

1. operacja „otwarta”,
2. operacja „szczególna”,
3. operacja „certyfikowana”.

Nowy podział wynika z przepisów UE i został dokonany w oparciu o analizę ryzyka wykonywanych operacji lotniczych.

Kategoria „otwarta” przeznaczona ma być dla operacji wykonywanych w warunkach widzialności wzrokowej (VLOS), o najniższym ryzyku. Niskie ryzyko zapewnione zostanie dzięki jasnym wytycznym, określającym między innymi dopuszczalne masy startowe bezzałogowych statków powietrznych, ich wyposażenie, prędkości lotu, maksymalną energię kinetyczną uderzenia oraz odległość od pojedynczych osób i zgromadzeń osób.

W kategorii „szczególnej” operacje zostaną ściśle określone i będą mogły być wykonywane na podstawie zezwolenia wydawanego przez Prezesa Urzędu Lotnictwa Cywilnego.

Operacja „certyfikowana” będzie najwyższą kategorią dopuszczenia do lotu bezzałogowego statku powietrznego. Aby wykonywać operacje w tej kategorii, konieczne będzie posiadanie certyfikowanego systemu BSP, który uzyskał wpis do rejestru cywilnych statków powietrznych.

Nowym rozwiązaniem ma być również **możliwość wyznaczania w przestrzeni powietrznej stref geograficznych, które mogą ograniczyć lub wykluczyć wykonywanie operacji z użyciem systemów BSP**. Chodzi o wyeliminowanie zagrożeń dla bezpieczeństwa, prywatności czy środowiska naturalnego, które wynikają z wykonywania operacji BSP. Wyznaczanie stref geograficznych zostanie powierzone Polskiej Agencji Żeglugi Powietrznej (PAŻP).

Nowe rozwiązania mają – co do zasady - wejść w życie po 14 dniach od ogłoszenia w Dzienniku Ustaw, **uchwalenie wyżej wymienionej nowelizacji prawa lotniczego planowane jest w 2025 roku.**

15. Media cyfrowe

W 2025 roku uchwalone mają być dwa akty prawne dotyczące mediów cyfrowych:

1. **nowa ustawa medialna**, która implementuje postanowienia Europejskiego Aktu o Wolności Mediów (zob. 8 punkt powyżej),
2. **nowelizacja ustawy o świadczeniu usług drogą elektroniczną,** która stanowi tzw. ustawę wdrażającą rozporządzenie unijne pt. Akt o usługach cyfrowych.

AUC jako rozporządzenie unijne jest aktem bezpośrednio stosowanym i każde z państw członkowskich zobowiązane jest do zapewnienia jego skutecznego stosowania w swoim porządku prawnym poprzez przyjęcia właściwych przepisów wewnętrznych. W AUC przekazano do uregulowania na poziomie krajowym obowiązek wyznaczenia organu pełniącego rolę koordynatora do spraw usług cyfrowych, tj. regulatora odpowiadającego za przestrzeganie przepisów rozporządzenia w Polsce oraz nadanie mu odpowiednich uprawnień z tym związanych.

Ostatnia wersja projektu nowelizacji ustawy o świadczeniu usług drogą elektroniczną pochodzi z dnia 13 grudnia 2024 r. Zgodnie z nią (art. 15a) ust. 1 projektu), **organami właściwymi w sprawach z zakresu AUC mają być:**

1. **Prezes UOKIK** – w zakresie przepisów dotyczących dostawców platform internetowych umożliwiających konsumentom zawieranie z przedsiębiorcami umów zawieranych na odległość oraz innych spraw dotyczących ochrony konsumentów określonych w AUC,
2. **Prezes UKE** – w pozostałym (przeważającym) zakresie.

Równocześnie wskazano Prezesa Urzędu Komunikacji Elektronicznej (UKE) jako organ pełniący funkcję koordynatora do spraw usług cyfrowych w Polsce (art. 49 ust. 1 AUC). Przy Prezesie UKE ma zostać powołana Krajowa Rada do Spraw Usług Cyfrowych.

W nowelizacji ustawy o świadczeniu usług drogą elektroniczną określono również takie zagadnienia jak:

1. nakazy podjęcia działań przeciwko nielegalnym treściom, nakazy usunięcia ograniczeń nałożonych przez dostawcę usług hostingu oraz nakazy udzielenia informacji,
2. zasady certyfikacji podmiotów do spraw pozasądowego rozstrzygania sporów,
3. zasady przyznawania statusu zaufanego podmiotu sygnalizującego i tzw. zweryfikowanego badacza,
4. określenie zasad dotyczących skarg na dostawców usług pośrednich,
5. określenie zasad odpowiedzialności cywilnej dostawców usług pośrednich i postępowania przed sądami,
6. zasady nakładania kar pieniężnych nakładanych w oparciu o przepisy AUC,
7. przepisy zmieniające inne akty prawne.

Uchwalenie nowelizacji ustawy o świadczeniu usług drogą elektroniczną **planowane jest w pierwszej połowie 2025 r., a jej przepisy mają wejść w życie po upływie 30 dni od dnia ogłoszenia.**

16. Ochrona małoletnich w Internecie

Ministerstwo Cyfryzacji pracuje obecnie nad **projektem ustawy o ochronie małoletnich przed treściami szkodliwymi w Internecie.**

13 grudnia ub. r., podczas Kongresu OSE (Ogólnopolska Sieć Edukacyjna) poświęconego tematyce ochrony małoletnich w Internecie, Ministerstwo Cyfryzacji zaprezentowało kluczowe założenia planowanej ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w Internecie.

Najważniejsze założenia projektowanej legislacji:

1)ustawa ma objąć ochroną osoby małoletnie, czyli osoby, które nie ukończyły 18. roku życia,

2)dostawcy usług świadczonych drogą elektroniczną będą mieli obowiązek przeprowadzenia w ich usługach analizy ryzyka w zakresie prawdopodobieństwa dostępności treści szkodliwych dla małoletnich. W założeniach projektodawców ma to wzmocnić odpowiedzialność i świadomość dostawców usług w zakresie treści, jakie oferują w ramach swojej działalności,

3)ustawa nałoży szczególne obowiązki na te podmioty, w których usługach świadczonych drogą elektroniczną znajdują się treści pornograficzne,

4)dostawcy usług (stron, platform internetowych itp.), w ramach których dostępne będą treści pornograficzne, zostaną zobowiązani do dokonywania weryfikacji wieku w celu uniemożliwienia małoletnim dostępu do tych treści,

5)przez weryfikację wieku należy rozumieć mechanizmy i narzędzia pozwalające na skuteczne ustalenie pełnoletności, wyłączając możliwość weryfikacji wieku poprzez deklarację użytkownika co do jego wieku oraz szacowanie wieku,

ustawa nie obejmie komunikatorów internetowych ani poczty elektronicznej, zatem nie będzie możliwe skanowanie treści indywidualnych wiadomości,

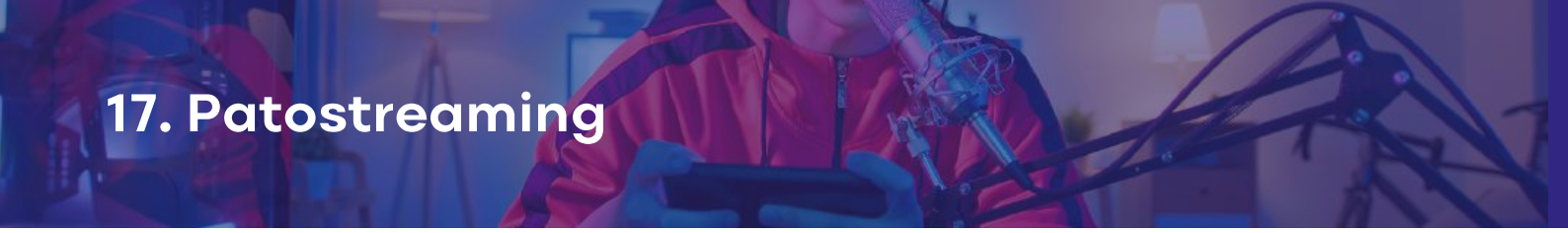
7)wprowadzony zostanie rejestr domen, zawierających treści pornograficzne, do których dostęp nie jest zabezpieczony weryfikacją wieku; rejestr będzie prowadzony przez NASK-PIB (w ramach już prowadzonego przez Instytut rejestru),

8)przedsiębiorcy telekomunikacyjni zostaną zobowiązani do blokowania dostępu do domen znajdujących się w rejestrze,

9)dostawca niezgadzający się z wpisem do rejestru będzie mógł wnieść sprzeciw, który będzie rozpatrywany przez Prezesa Urzędu Komunikacji Elektronicznej,

10)Prezes UKE zyska uprawnienia kontrolne oraz możliwość nakładania administracyjnych kar pieniężnych na podmioty niewywiązujące się z obowiązków wskazanych w ustawie.

Prace nad projektem ustawy o ochronie małoletnich przed treściami szkodliwymi w Internecie mają być kontynuowane 2025 roku.



17. Patostreaming

W 2024 roku dużo mówiło się w Polsce o sprawach zaliczanych do kategorii **patostreamingu** - publicznego transmitowania i rozpowszechniania w Internecie treści audiowizualnych prezentujących przemoc, agresję i zachowania patologiczne, co rodzi poważne zagrożenia społeczne oraz moralne. W Sejmie poprzedniej kadencji podjęto w związku z tym próbę uchwalenia nowego przepisu karnego, „dedykowanego" do tego rodzaju czynów (nowy art. 255b. § 1 Kodeks karny). Przepis ten jednak nie został ostatecznie uchwalony.

W dniu **12 grudnia 2024 r. Rzecznik Praw Obywatelskich (RPO) skierował pismo do Ministra Sprawiedliwości, wskazując na potrzebę podjęcia kolejnej próby wprowadzenia do polskiego prawa karnego przepisów dotyczących patrostreaming.**

Zdaniem RPO należy zaproponować penalizację prezentowania treści przemocowych małoletnim, na wzór rozwiązania funkcjonującego na gruncie art. 200 § 3 k.k. w odniesieniu do treści o charakterze pornograficznym. Według RPO należy również rozważyć wprowadzenie typu kwalifikowanego przestępstwa polegającego na nawoływaniu do popełnienia przestępstwa (art. 255 k.k.), z uwagi na cel osiągnięcia korzyści majątkowej przez sprawcę. Wprowadzenie typu kwalifikowanego miałoby skutecznie uzupełnić regulację dotyczącą nawoływania do przestępstwa i objąć działania patostreamerów, którzy monetyzują swoje transmisje, zachęcając do przemocy i innych przestępstw.

Na chwilę obecną nie wiadomo jeszcze, czy Ministerstwo Sprawiedliwości uruchomi prace legislacyjne w kształcie proponowanym przez Rzecznika Praw Obywatelskich.

18. Reklama w Internecie

W przypadku reklamy w Internecie w 2025 roku następujące akty prawne będą miały kluczowe znaczenie:

1. **nowelizacja ustawy o świadczeniu usług drogą elektroniczną**, która wprowadzi organy nadzorcze odpowiedzialne za przestrzeganie przepisów Aktu o usługach cyfrowych (AUC). Dotyczy to również przepisów „reklamowych", określonych w AUC, a więc art. 26 ust. 1-3 oraz art. 28 ust. 2 AUC,
2. **Prawo komunikacji elektronicznej,** które między innymi ujednoliciło zasady prowadzenia marketingu elektronicznego (zob. pkt 13 powyżej),
3. **Rozporządzenie Unii Europejskiej nr 2024/29 dotyczące reklamy politycznej** (zob. pkt 19 poniżej).

Przed omówieniem najważniejszych przepisów dotyczących reklamy **internetowej w AUC, należy podkreślić, że z uwagi na zakres przedmiotowy AUC (art. 2 ust. 1), adresatami obowiązków określonych w art. 26 ust. 1 AUC są dostawcy usług platform internetowych działający w modelu dostawcy usług pośrednich (pośredników internetowych), a więc podmiotów przechowujących i publicznie rozpowszechniających informacje umieszczane przez użytkowników.**

Przykładem są serwisy społecznościowe czy platformy internetowe umożliwiające publiczne rozpowszechnianie przez użytkowników tych platform rożnego rodzaju treści (np. audio, video, pliki graficzne). Obowiązek określony w art. 26 ust. 1 AUC nie dotyczy więc podmiotów funkcjonujących wyłącznie w modelu dostawcy treści, a więc podmiotów decydujących o zamieszczaniu w Internecie własnych lub cudzych treści (np. internetowe serwisy informacyjne).

Zgodnie z art. 26 ust. 1 AUC dostawcy platform internetowych, którzy prezentują reklamy na swoich interfejsach internetowych, zapewniają, aby – w odniesieniu do każdej konkretnej reklamy prezentowanej każdemu indywidualnemu odbiorcy – odbiorcy usługi byli w stanie w sposób jasny, wyraźny, zwięzły i jednoznaczny oraz w czasie rzeczywistym uzyskać określone informację (np. o tym, w imieniu jakiej osoby fizycznej lub prawnej jest prezentowana reklama). **Obowiązek określony w art. 26 ust. 1 AUC jest niezależny od obowiązków informacyjnych określonych w innych aktach prawnych.** Przepis ten nie stosuje się do reklamy własnej dostawcy platformy internetowej.

Z kolei, zgodnie z art. 26 ust. 2 AUC, dostawcy platform internetowych zapewniają odbiorcom usługi funkcję umożliwiającą składanie oświadczenia, czy przekazywane przez nich treści są informacjami handlowym lub zawierają informacje handlowe. Celem powyższego przepisu jest zapewnienie transparentności w zakresie przekazywanych w ramach platform treści o charakterze informacji handlowych. Chodzi w szczególności o sytuacje, gdy na danej platformie, należącej do dostawcy A., przekazywane są informacje handlowe podmiotu B., z którymi z kolei mogą zapoznać się podmioty C., będące użytkownikami tej platformy.

W art. 26 ust. 3 i art. 28 ust. 2 AUC wprowadzono ograniczenia dotyczące tzw. reklamy targetowanej, opartej na profilowaniu danych wrażliwych w rozumieniu RODO lub danych osób małoletnich.

Zgodnie z art. 26 ust. 3 AUC dostawcy platform internetowych nie mogą prezentować odbiorcom usługi reklam opartych na profilowaniu, zgodnie z definicją w art. 4 pkt 4 RODO, z wykorzystaniem szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO. **Kategorie danych wrażliwych** zostały określone w art. 9 ust. 1 RODO i obejmują między innymi informacje ujawniające poglądy polityczne, przekonania religijne lub światopoglądowe czy dane dotyczące zdrowia, seksualności lub orientacji seksualnej. Zakaz z art. 26 ust. 3 AUC odnosi się wyłącznie do profilowania w rozumieniu art. 4 pkt 4 RODO, co oznacza, że nadal dopuszczalne jest np. prezentowanie reklamy internetowej dotyczącej produktów leczniczych, o ile nie jest ono oparte na zestawianiu informacji o zdrowiu osoby, której reklama jest wyświetlana. Z przetwarzaniem, w tym profilowaniem, danych wrażliwych mamy do czynienia przede wszystkim wówczas, gdy **wykorzystywane są dane tego rodzaju wprowadzone bezpośrednio przez odbiorcę do platformy internetowej** (np. na etapie zakładania konta użytkownika). W pewnych sytuacjach, do personalizacji reklam w oparciu o profilowanie danych wrażliwych może również dojść gdy, biorąc pod uwagę charakter, cel, kontekst przetwarzania, w szczególności możliwość ich połączenia przez dostawcę platformy z innymi danymi, w obiektywny sposób możliwe jest wywnioskowanie przynajmniej jednej z kategorii danych wskazanych w art. 9 ust. 1 RODO. Sytuacje te należy oceniać ***a casu ad casum.***

Zgodnie z treścią art. 28 ust. 2 AUC, dostawcy platform internetowych nie mogą prezentować na swoim interfejsie reklam opartych na profilowaniu, zgodnie z definicją w art. 4 pkt 4 RODO, z wykorzystaniem danych osobowych odbiorcy usługi, jeżeli wiedzą z wystarczającą pewnością, że odbiorca usługi jest małoletnim. Należy podkreślić, że **art. 28 ust. 2 AUC nie ustanawia bezwzględnego zakazu spersonalizowanej reklamy internetowej skierowanej do małoletnich użytkowników**, co oznacza, że dopuszczalne jest prezentowanie reklam internetowych małoletnim, o ile dostawca nie ma wystarczającej pewności, że konkretny użytkownik platformy jest małoletnim. **Dla przyjęcia, czy dostawca wie „z wystarczającą pewnością", że odbiorca usługi jest małoletnim, należy dokonać oceny, czy biorąc pod uwagę kontekst przetwarzania danych użytkownika, charakter platformy, dodatkowe informacje o użytkowniku, którymi dysponuje dostawca platformy, oraz wykorzystywane przez niego środki (np. metody weryfikacji lub szacowania wieku użytkowników), można w obiektywny sposób stwierdzić, że konkretny dostawca jest w stanie w dostatecznie wiarygodny sposób ustalić, że konkretny użytkownik jest małoletnim.** W świetle art. 28 ust. 3 AUC dostawca platformy internetowej nie jest również zobowiązany do przetwarzania dodatkowych danych osobowych (innych danych niż te, którymi dysponuje) w celu dokonania oceny, czy odbiorca usługi jest małoletnim, aby przestrzegać zakazu z art. 28 ust. 2 AUC.

19. Reklama polityczna w Internecie

W dniu 10 października 2025 r. zacznie obowiązywać zasadnicza część przepisów Rozporządzenia Parlamentu Europejskiego i Rady nr 2024/900 z dnia 13 marca 2024 r. w sprawie przejrzystości i targetowania reklamy politycznej (Dz.U. UE L. 2024/900).

Głównym celem uchwalenia **rozporządzenia o reklamie politycznej** jest zapewnienie przejrzystości i uczciwości w procesie wyborczym oraz ochrona obywateli przed manipulacją informacją, w tym dezinformacją.

Rozporządzenie wprowadza szereg regulacji, które mają znaczący wpływ na działalność w Internecie, szczególnie w kontekście kampanii wyborczych i debaty publicznej.

Oto kilka kluczowych rozwiązań, jakie wprowadzi rozporządzenie, kształtując cyfrową przestrzeń:

1. **Przezroczystość finansowania:** Platformy internetowe mają być zobowiązane do ujawniania informacji o podmiotach finansujących reklamy polityczne wyświetlane na ich stronach. Dzięki temu użytkownicy mogą łatwiej zidentyfikować, kto stoi za konkretnym przekazem.
2. **Oznaczenie reklam politycznych:** Reklamy polityczne mają być wyraźnie oznaczone, co ułatwi użytkownikom odróżnienie ich od innych treści.
3. **Ograniczenia dotyczące targetowania:** Platformy internetowe nie mogą kierować reklam politycznych do użytkowników na podstawie wrażliwych danych osobowych, takich jak przekonania polityczne, pochodzenie rasowe czy orientacja seksualna.
4. **Zwalczanie dezinformacji:** Rozporządzenie nakłada na platformy internetowe obowiązek podejmowania działań zmierzających do ograniczenia rozpowszechniania fałszywych informacji i treści wprowadzających w błąd.

Adresatami obowiązków określonych w rozporządzeniu o reklamie politycznej są:

1. **Reklamodawcy polityczni** - podmioty, które bezpośrednio lub pośrednio finansują lub zlecają tworzenie i rozpowszechnianie reklamy politycznej. Mogą to być partie polityczne, organizacje pozarządowe, ale także osoby fizyczne.
2. **Dostawcy usług reklamowych** - platformy internetowe, media społecznościowe oraz inne podmioty, które umożliwiają publikowanie reklam politycznych.
3. **Sponsorzy** - podmioty, które finansują reklamy polityczne, ale nie są bezpośrednio zaangażowane w ich tworzenie.

Za nieprzestrzeganie przepisów rozporządzenia o reklamie politycznej przewidziany jest **katalog sankcj**i (np. nakaz usunięcia nieprawidłowej reklamy, zablokowanie dostępu do platformy internetowej, na której była publikowana niezgodna z prawem reklama, czy ograniczenie możliwości prowadzenia działalności w zakresie reklamy politycznej na określony czas). Przewidziane są również kary pieniężne do wysokości 6% rocznego dochodu lub budżetu sponsora lub dostawcy usług reklamy politycznej, względnie 6% rocznego światowego obrotu sponsora lub dostawcy usług reklamy politycznej w poprzednim roku finansowym.

Każde państwo członkowskie UE jest zobowiązane do wdrożenia powyższych przepisów do swojego porządku prawnego, między innymi w zakresie wyznaczenia organu bądź organów odpowiedzialnych za przestrzeganie przepisów rozporządzenia. **W chwili obecnej w Polsce nie zostało jeszcze ustalone, które organy mają pełnić tę rolę.**

20. Sztuczna inteligencja

Podstawowym aktem prawnym regulującym tworzenie i korzystanie z systemów sztucznej inteligencji jest Rozporządzenie Unii Europejskiej nr 2024/1689 pt. **Akt w sprawie sztucznej inteligencji.**

Zasadniczą datą rozpoczęcia stosowania rozporządzenia jest **2 sierpnia 2026 r.** Przyjęto przy tym regułę intertemporalną, że przepisy stosują się do systemów wprowadzonych do obrotu lub oddanych do użytku przed tą datą, chyba że po tej dacie w systemach tych „wprowadzane będą istotne zmiany w ich projekcie" (art. 111 ust. 2). Wyjątkiem od zasady rozpoczęcia stosowania rozporządzenia w dniu 2 sierpnia 2026 r. są przepisy dotyczące niedopuszczalnych praktyk w zakresie AI, które zaczną obowiązywać już **od dnia 2 lutego 2025 r.** Również niektóre przepisy dotyczące systemów wysokiego ryzyka, a także modeli ogólnego przeznaczenia zaczną obowiązywać wcześniej, tj. **od dnia 2 sierpnia 2025 r.**

Głównym celem powyższej regulacji jest bezpieczeństwo tworzenia i korzystania z systemów sztucznej inteligencji (AI). Stosuje się je zarówno do systemów przetwarzających **dane osobowe, jak i systemów przetwarzających dane nieosobowe.** W rozporządzeniu wprowadzono również wyjątki stosowania jego przepisów (cele badawczo-naukowe, cele wojskowe etc.). Akt w sprawie sztucznej inteligencji stosuje się nie tylko do dostawców, ale również do organizacji korzystających z narzędzi AI. Rozporządzenie będzie również odnosiło się do podmiotów spoza UE, „w przypadku gdy wyniki wytworzone przez system AI są wykorzystywane w Unii" (art. 2 ust. 1 pkt c).

W art. 5 Aktu w sprawie sztucznej inteligencji określono **praktyki,** które po 2 lutego 2025 roku mają być **zakazane**. Przykładem jest „wprowadzanie do obrotu, oddawanie do użytku lub wykorzystywanie systemu sztucznej inteligencji, który stosuje techniki podprogowe będące poza świadomością danej osoby w celu lub ze skutkiem istotnego zniekształcenia zachowania tej osoby w sposób, który powoduje lub może z uzasadnionym prawdopodobieństwem spowodować u niej lub u innej osoby szkodę fizyczną lub psychiczną" (art. 5 ust. 1a).

Zasadnicza część przepisów Aktu w sprawie sztucznej inteligencji dotyczy tworzenia i korzystania z tzw. systemów wysokiego ryzyka (Rozdział III). Są to systemy spełniające warunki określone w art. 6 ust. 1 rozporządzenia, jak również wymienione w załączniku III do rozporządzenia jako stwarzające znaczące ryzyko powstania szkody dla zdrowia, bezpieczeństwa, praw podstawowych (np. prywatności) lub środowiska. W rozporządzeniu odrębnie określono obowiązki dostawców systemów wysokiego ryzyka (przede wszystkim art. 16 i n.) oraz podmiotów stosujących tego rodzaju systemy (art. 26-27). Dostawcy systemów wysokiego ryzyka będą również musieli przejść procedurę oceny ich zgodności z wymogami rozporządzenia.

Rozporządzenie w sprawie sztucznej inteligencji **w zasadzie nie reguluje tworzenia i korzystania z systemów niskiego ryzyka. W art. 50 rozporządzenia, na zasadzie wyjątku, wprowadzono jednak pewne wymogi transparentności (przejrzystości) dla tych systemów.** Przykładowo, w przypadku systemów AI przeznaczonych do wchodzenia w bezpośrednią interakcję z osobami fizycznymi, ich dostawcy powinni zapewnić, aby zainteresowane osoby fizyczne były informowane o tym, że prowadzą interakcję z systemem AI (ust. 1), a w przypadku systemów „generujących treści w postaci syntetycznych dźwięków, obrazów, wideo lub tekstu", dostawcy powinni zapewnić, aby wyniki systemu AI zostały „oznakowane w formacie nadającym się do odczytu maszynowego i były wykrywalne jako sztucznie wygenerowane lub zmanipulowane" (ust. 2). Pewne obowiązki w tym zakresie nałożono również na podmioty stosujące „system AI, który generuje obrazy, treści audio lub wideo stanowiące treści deepfake lub który manipuluje takimi obrazami lub treściami." W takim przypadku zasadą jest obowiązek ujawnienia, że treści te zostały sztucznie wygenerowane lub zmanipulowane (ust. 4).

W rozporządzeniu wprowadzono również **szczególną regulację dla dostawców tzw. modeli ogólnego przeznaczenia** (np. GPT). Zgodnie z art. 53 nałożono na nich szczególne obowiązki związane z korzystaniem przez nich, na etapie trenowania tych modeli, z danych stanowiących przedmioty praw autorskich i praw pokrewnych.

W Akcie w sprawie sztucznej inteligencji przewidziane jest powołanie **niezależnego organu ds. nadzoru nad przepisami rozporządzenia**, a organ ten ma być wyposażony w szereg kompetencji, w tym w zakresie nakładania wysokich kar pieniężnych jako sankcji administracyjnych (w wysokości nawet do 7 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego). Novum jest możliwość nakładania kary również przez Europejskiego Inspektora Ochrony Danych, który może nakładać sankcje za nieprzestrzeganie zakazu praktyk w zakresie AI, w wysokości do 1.500.000 EUR.

W chwili obecnej w Polsce prowadzone są prace nad ustawą wdrażającą Akt w sprawie sztucznej inteligencji. Projekt ustawy o systemach sztucznej inteligencji, opracowany przez Ministerstwo Cyfryzacji i przedłożony do konsultacji, zakłada między innymi, że organem nadzoru ma być nowy organ, tj. **Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji,** na czele którego ma stać przewodniczący, powoływany przez Prezesa Rady Ministrów.

Uchwalenie ustawy o systemach sztucznej inteligencji planowane jest w 2025 roku.

Akt w sprawie sztucznej inteligencji stanowi podstawową regulację dotyczącą stosowania systemów AI. Należy jednak podkreślić, że do tworzenia i korzystania z AI zastosowanie znajdą **również przepisy innych aktów prawnych**, w szczególności:

1. prawa autorskiego, np. w zakresie przesłanek dopuszczalności wykorzystywania utworów jako danych treningowych na etapie tworzenia modeli AI (art. 263 i wyjątek dotyczący tzw. eksploracji tekstu i danych),
2. **RODO**, np. w zakresie dopuszczalności podejmowania automatycznych decyzji dotyczących podmiotów danych, przy wykorzystaniu narzędzi AI,
3. **prawa cywilnego**, np. w zakresie określenia odpowiedzialności za szkody związane z korzystaniem z AI,
4. **nieuczciwej konkurencji**, np. w sytuacji ujawnienia informacji objętych tajemnicą przedsiębiorstwa poprzez wprowadzenie do systemu AI informacji objętych tą tajemnicą, a które to informacje są następnie traktowane przez operatora systemu AI jako dane treningowe (art.11 uznk),
5. **prawa konsumenckiego**, np. w zakresie obowiązku podania konsumentowi informacji o indywidualnym dostosowaniu ceny w oparciu o zautomatyzowane podejmowanie decyzji (art. 12 ust. 1 pkt. 5a ustawy o prawach konsumenta).

21. Usługi zaufania w transakcjach elektronicznych (rozporządzenie eIDAS)

Dotychczas obowiązujące Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającym dyrektywę 1999/93/WE **(rozporządzenie eIDAS)** zapewniało podstawy prawnej dla podpisów elektronicznych i innych usług zaufania, dostarczanych przez uprawnionych do tego dostawców. Ustanowiono w nim standardy dla podpisów elektronicznych, pieczęci, znaczników czasu oraz usług doręczenia elektronicznego, aby zwiększyć bezpieczeństwo i pewność prawną transakcji elektronicznych na terenie Unii Europejskiej. Zapewniono również, że środki identyfikacji elektronicznej (eID) oraz certyfikaty (np. podpisów elektronicznych) wydane przez jedno z państw członkowskich były uznawane i akceptowane w innych krajach. Dzięki temu obywatele, przedsiębiorstwa i administracja publiczna mogą korzystać z usług elektronicznych bez ograniczeń geograficznych – kraje członkowskie Unii Europejskiej wzajemnie uznają swoje identyfikatory elektroniczne, oczywiście pod warunkiem spełnienia określonych kryteriów.

W dniu 11 kwietnia 2024 r. uchwalona została zmiana rozporządzenia eIDAS poprzez przyjęcie Rozporządzenia Parlamentu Europejskiego i Rady nr 2024/1183 w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (tzw. rozporządzenie **eIDAS 2.0**). Celem eIDAS 2.0 jest usprawnienie mechanizmów uwierzytelniania i autoryzacji, zapewnienie większej spójności i interoperacyjności pomiędzy systemami identyfikacji cyfrowej w różnych krajach członkowskich UE oraz wzmocnienie ram bezpieczeństwa transakcji elektronicznych w państwach członkowskich UE. Należy przy tym podkreślić, że na mocy art. 51 eIDAS 2.0. bezpieczne urządzenia do składania podpisu, których zgodność ustalono zgodnie z art. 3 ust. 4 dyrektywy 1999/93/WE, **w dalszym ciągu uznaje się za kwalifikowane urządzenia do składania podpisu elektronicznego na podstawie niniejszego rozporządzenia do dnia 21 maja 2027 r.**, a kwalifikowane certyfikaty wydane osobom fizycznym na podstawie dyrektywy 1999/93/WE w dalszym ciągu uznaje się za **kwalifikowane certyfikaty podpisów elektronicznych na podstawie niniejszego rozporządzenia do dnia 21 maja 2026 r.** W praktyce nadal więc można korzystać z wydanych już przez dostawców usług zaufania podpisów kwalifikowanych oraz certyfikatów kwalifikowanych. Listę kwalifikowanych dostawców usług zaufania w Polsce można znaleźć na stronie internetowej Narodowego Centrum Certyfikacji.

Bazując na podstawowych założeniach rozporządzenia eIDAS 1.0, eIDAS 2.0 wprowadza nowe postanowienia, aby sprostać wyzwaniom i możliwościom w cyfrowym świecie. eIDAS 2.0 ustanawia w szczególności wymagania nie tylko dla kwalifikowanych, ale także wobec niekwalifikowanych dostawców usług zaufania. Dzięki temu uznanie niekwalifikowanych usług zaufania będzie jeszcze wyższe. eIDAS 2.0 wprowadza także bardziej rygorystyczne wymagania bezpieczeństwa i programy certyfikacyjne, aby zwiększyć odporność identyfikacji elektronicznej i usług zaufania.

Szczególne znaczenie mają nowe usługi zaufania, w tym przede wszystkim Europejski Portfel Tożsamości Cyfrowej (EU Digital ID Wallet), którym będzie można posługiwać się na terenie całej Unii. Portfel ma być dostępny jako aplikacja w smartfonie, na której mają być przechowywane różne dokumenty w formie cyfrowej (np. dowód osobisty, prawo jazdy).

Nowelizacja rozporządzenia eIDAS weszła w życie 20 maja 2024 r., jednak zawarte są w nim również okresy przejściowe lub terminy, w których Komisja Europejska ma opracować akty wykonawcze dla określonych usług zaufania. Na przykład, artykuł 5a rozporządzenia eIDAS zobowiązuje państwa członkowskie UE **do zapewnienia co najmniej jednego Europejskiego Portfela Tożsamości w ciągu 24 miesięcy od wejścia w życie aktów wykonawczych określających normy oraz wymagania dla usługi.**

W Polsce za wdrożenie eIDAS 2.0 odpowiada Ministerstwo Cyfryzacji, które między innymi będzie musiało dostosować aplikację mObywatel do wymogów Europejskiego Portfela Tożsamości Cyfrowej.

22. Własność intelektualna w Internecie (prawa autorskie)

Z punktu widzenia praw własności intelektualnej i prowadzenia działalności w Internecie w 2025 roku największe znaczenie prawne mają, uchwalone w 2024 r., przepisy **nowelizacji ustawy o prawie autorskim i pokrewnych.** Niezależnie od tego, wraz z coraz szerszym zastosowaniem generatywnej sztucznej inteligencji, coraz aktualniejsze stają się problemy związane ze stosowaniem dotychczasowych paradygmatów praw własności intelektualnej do nowego sposobu tworzenia i eksploatacji treści.

W ramach **nowelizacji ustawy o prawie autorskim i prawach pokrewnych z dnia 26 lipca 2024 r.** dokonano implementacji przepisów Dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/790 z 17.4.2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz.U. UE L. 130). Większość tych przepisów zaczęła obowiązywać **w dniu 20 września 2024 roku.** Art. 861 Prawa autorskiego w drodze wyjątku wejdzie w życie **z dniem 20 lutego 2025 roku.**

Z punktu widzenia działalności w Internecie najważniejsze z regulacji zawartych w nowelizacji prawa autorskiego obejmują:

1) dozwolony użytek w zakresie eksploracji tekstów i danych (text data mining, TDM)
Eksploracją tekstów i danych jest ich analiza wyłącznie przy zastosowaniu zautomatyzowanej techniki służącej do analizowania tekstów i danych w postaci cyfrowej w celu wygenerowania określonych informacji, obejmujących w szczególności wzorce, tendencje i korelacje **(art. 6 ust. 1 pkt 22 pr. aut.**). Tego rodzaju działania wykonywane są między innymi **przez systemy sztucznej inteligencji**, które korzystają z różnego rodzaju treści dostępnych w Internecie jako danych treningowych do „uczenia" tworzonych modeli. W nowelizacji prawa autorskiego wprowadzono w związku z tym nową postać dozwolonego użytku, pozwalającą na eksplorację tekstu i danych, chyba że uprawniony zastrzegł inaczej **(art. 263). Nie opracowano jeszcze standardu takiego zastrzeżenia, polska ustawa stanowi jedynie, że** dokonuje się wyraźnie i odpowiednio do sposobu, w jaki utwór został udostępniony, a w przypadku utworów publicznie udostępnionych w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i czasie przez siebie wybranym, tj. w Internecie, zastrzeżenia dokonuje się w formacie przeznaczonym do odczytu maszynowego w rozumieniu art. 2 pkt 7 ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz.U. z 2023 r. poz. 1524) wraz z metadanymi. **(art. 263 ust. 2).**

2) przyznanie twórcom oraz artystom wykonawcom prawa do wynagrodzenia za dzieła udostępniane w Internecie
W dodanych w ramach nowelizacji **przepisom art. 214 oraz art. 861 Prawa autorskiego** zapewniono twórcom oraz artystom wykonawcom utworu literackiego, publicystycznego, naukowego, muzycznego lub słowno-muzycznego, w tym twórcom lub artystom wykonawcom opracowania takiego utworu, prawo do wynagrodzenia z tytułu publicznego udostępnienia utrwalenia artystycznego wykonania w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i czasie przez siebie wybranym (internetowe pole eksploatacji). W ten sposób przesądzono, że twórcom i wykonawcom przysługuje niezbywalne **prawo do wynagrodzenia za udostępnianie ich utworów w Internecie, szczególnie na platformach takich jak serwisy streamingowe czy VOD.**

3) przyznanie współtwórcom i artystom wykonawcom utworów audiowizualnych prawa do wynagrodzenia za wykorzystywanie dzieł w Internecie
Nowy art. 70 ust. 21 pkt 5) ustawy wprowadza prawo do otrzymywania tantiem za wykorzystywanie utworów audiowizualnych w Internecie (np. przez platformy streaminigowe).

4) nowe prawo pokrewne dla wydawców prasy w przypadku eksploatacji ich publikacji w Internecie
W nowelizacji prawa autorskiego wprowadzono również **nowe prawo pokrewne dla wydawców prasy**, mające na celu wzmocnienie profesjonalnych wydawnictw i redakcji w dobie ery cyfrowej, w ramach której ich publikacje są często wykorzystywane przez różnego rodzaju agregatorów treści. W świetle nowych przepisów wydawcom publikacji prasowej przysługuje – bez uszczerbku dla praw twórców i pozostałych uprawnionych – wyłączne prawo do rozporządzania publikacją prasową i korzystania z niej, między innymi w zakresie publicznego udostępniania publikacji prasowej w taki sposób, aby każdy mógł mieć do niej dostęp w miejscu i czasie przez siebie wybranym (Internet) - **art. 997 ust. 2 pkt 2**. Dzięki temu wydawcom prasowym przysługuje prawo do dodatkowego wynagrodzenia za korzystanie z ich utworów przez dostawców usług świadczonych drogą elektroniczną (np. platformy internetowe).

W ramach nowelizacji uregulowano także kwestię wynagrodzenia twórców utworów zamieszczonych w publikacji prasowej. Twórcy ci mają prawo do 50% wynagrodzenia należnego wydawcy z tytułu korzystania z prawa do rozporządzania publikacją prasową i korzystania z niej **(art. 999 ust. 1).**

5) nowe zasady odpowiedzialności platform internetowych
W świetle nowo dodanego art. 222 Prawa autorskiego, zasadą jest ponoszenie przez dostawcę usług udostępniania treści online – który bez wymaganej zgody uprawnionego dokonał publicznego udostępnienia utworu zamieszczonego przez usługobiorcę – odpowiedzialności z tytułu naruszenia prawa autorskiego. Dostawcy usług udostępniania treści online (platformy internetowe) mogą się z powyższej odpowiedzialności zwolnić wówczas, gdy wykażą spełnienie wskazanych w tym przepisie przesłanek, np. dołożenia należytej staranności, aby uzyskać zgodę uprawnionego z tytułu praw autorskich uzyskać (pkt 1).

Jest jeszcze kilka uwag dodatkowych **dotyczących prawa autorskiego i sztucznej inteligencji, w szczególności związane z tym ryzyka prawne.**

Po pierwsze, **ryzyko uznania, że wytwór działania AI nie jest utworem w rozumieniu prawa autorskiego.** Generalnie przyjmuje się, że korzystanie przez człowieka z narzędzi AI nie stoi na przeszkodzie uznaniu, że stworzony został utwór. Z drugiej strony, dla uznania prawnoautorskiego statusu dzieła musi ono powstać w wyniku ludzkiej działalności twórczej. Istotne wątpliwości budzi zatem ocena sytuacji, gdy dane dzieło w całości zostało „wygenerowane" przez AI, bez udziału człowieka choćby na etapie dalszej modyfikacji outputu AI.

Po drugie, **ryzyko ustalenia, kto jest podmiotem praw do wyników generowanych przez systemy AI.** W szczególności powstaje pytanie, czy podmiotem praw jest dostawca narzędzia AI, który przenosi prawa na użytkownika, czy też jego użytkownik.

Po trzecie, **ryzyko naruszenia praw autorskich poprzez rozpowszechnianie wyników prac AI** (output). Chodzi w szczególności o ryzyko wykorzystania cudzych utworów/elementów utworów w ramach generowania outputu.

23. Wolność słowa w Internecie (dyrektywa ant-SLAPP)

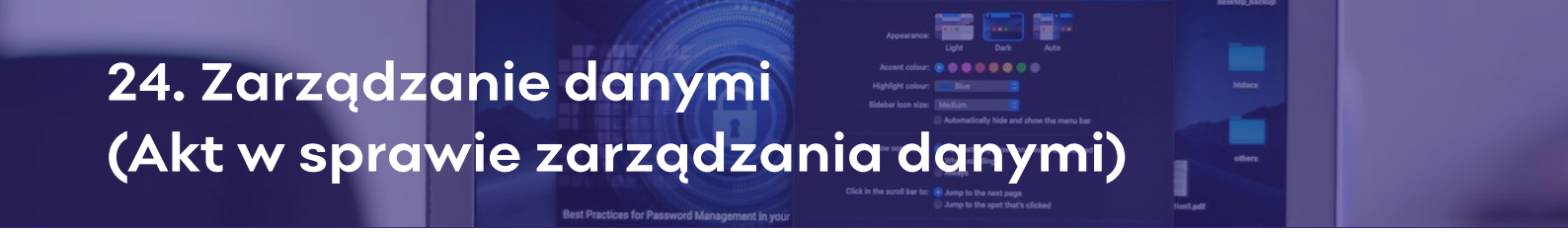
W dniu 11 kwietnia 2024 r. uchwalona została dyrektywa Parlamentu Europejskiego i Rady nr 2024/1069 w sprawie ochrony osób, które angażują się w debatę publiczną, przed oczywiście bezzasadnymi roszczeniami lub stanowiącymi nadużycie postępowaniami sądowymi („strategiczne powództwa zmierzające do stłumienia debaty publicznej"), określana również jako **dyrektywa anty-SLAPP.**

Głównym powodem uchwalenia dyrektywy jest zwalczanie zjawiska określanego jako „Strategic lawsuit against public participation" (SLAPP), **a więc wytaczanie pozwów mających na celu wywołanie efektu mrożącego (chilling efect) i zastraszanie osób, które wypowiadają się na ważne społecznie tematy.** Tego rodzaju działania są podejmowane zarówno przez rządzących, jak i korporacje. Chodzi tu nie tylko o koszty i ryzyka finansowe związane z tego rodzaju procesami, ale również o uciążliwości związane np. z koniecznością stawiania się na rozprawy etc. Istnieje w związku z tym obawa, że tego rodzaju „zniechęcające" działania mogą doprowadzić do sytuacji, gdy opinia publiczna nie dowie się o nieprawidłowościach, wykrytych przez aktywistów czy dziennikarzy.

Zgodnie z regulacją unijną, pozwani, przeciwko którym wytoczono powództwa SLAPP, będą mogli wnioskować o oddalenie ich sprawy wcześniej jako ewidentnie bezzasadnej, a obowiązek udowodnienia, że jest inaczej, ciąży na skarżącym.

Dodatkowo w razie umorzenia sprawy sąd może domagać się od powoda zapłaty kosztów postępowania i nałożyć na niego grzywnę, jeśli sprawa zostanie uznana za nadużycie. Pewną słabością omawianej regulacji jest jednak to, że dotyczy ona wyłącznie spraw cywilnych o charakterze transgranicznym, a więc gdy pozew wytoczony jest w innym państwie, niż znajduje się pozwany. Nie dotyczy więc ona spraw administracyjnych, karnych czy arbitrażowych. Z uwagi na minimalny charakter harmonizacji w dyrektywie, możliwe jest przyjęcie przez ustawodawców krajowych dalej idących rozwiązań.

Zgodnie z art. 22 ust. 1 dyrektywy, państwa członkowskie mają obowiązek implementacji przepisów dyrektywy do krajowych systemów prawnych **do dnia 7 maja 2026 r.**



24. Zarządzanie danymi (Akt w sprawie zarządzania danymi)

Od dnia 24 września 2023 r. stosują się przepisy Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi **(Akt w sprawie zarządzania danymi).**

Akt w sprawie zarządzania danymi ma zostać uzupełniony **ustawą wdrażającą**, nad którą obecnie w Polsce nadal trwają prace legislacyjne.

Istotą Aktu o zarządzaniu danymi jest ustanowienie ram prawnych, procesów i struktur zwiększających zaufanie i wspierających wymianę danych („dzielenie się danymi").

Dotyczy to:

1. **poszerzenia możliwości ponownego wykorzystywania informacji sektora publicznego przez podmioty prywatne (np. zasoby rejestrów publicznych, instytucji kultury etc.),**
2. określenia zasad świadczenia **usług pośrednictwa danych** pomiędzy podmiotami prywatnymi.
3. określenia reguł dobrowolnego udostępniania danych przez osoby fizyczne lub przedsiębiorstwa dla wspólnego dobra (interesu ogólnego) – tzw. **altruistyczne podejście do danych** (np. w zakresie badań naukowych).

Adresatami obowiązków określonych w Akcie w sprawie zarządzania danymi są zarówno **podmioty publiczne**, jak i **podmioty prywatne**.

W każdym państwie UE ma zostać powołany niezależny organ nadzorczy nad przestrzeganiem przepisów Aktu w sprawie zarządzania danymi. Zgodnie z projektem polskiej ustawy o zarządzaniu danymi, opracowanym 2024 roku przez Ministerstwo Cyfryzacji, organem tym ma być **Prezes UODO**. W projekcie przewidziano również realizację pewnych zadań, określonych w Akcie w sprawie zarządzania danymi, przez **Prezesa GUS**. W projekcie ustawy wdrażającej został również ustanowiony system sankcji, w tym kar pieniężnych, za nieprzestrzegania przepisów rozporządzenia. Kompetencje w tym zakresie otrzyma Prezes UODO, a górna granica kar to 500.000 EURO.

Uchwalenie ustawy o zarządzaniu danymi planowane jest w pierwszej połowie 2025 roku.

Masz pytania?
Skontaktuj się z naszym ekspertem:

Xawery Konarski

Adwokat, Senior Partner, Co-Managing Partner

xawery.konarski@traple.pl

www.traple.pl/team/xawery-konarski/

Traple Konarski Podrecki i Wspólnicy Sp.j.

Biuro w Krakowie:
ul. Królowej Jadwigi 170
30-212 Kraków
tel.: +48 12 426 05 30

e-mail: office@traple.pl
www.traple.pl

Biuro w Warszawie:
ul. Twarda 4
00-105 Warszawa
tel.: +48 22 850 10 10

Traple Konarski Podrecki & Partners

Zapisz się do newslettera TKP

the law TKP