STYCZEŃ 2026

NOWE TECHNOLOGIE (2026) – LEGISLACJA I REGULACJA W POLSCE I UNII EUROPEJSKIEJ (OD A DO Z)

Traple
Konarski
Podrecki
& Wspólnicy

TKP

SPIS TREŚCI

Prawo nowych technologii można podzielić na dwa podstawowe obszary: **a) prawo Internetu** oraz **b) prawo przełomowych technologii** (*disruptive technologies*).

Prawo Internetu obejmuje akty prawne i wytyczne organów nadzorczych (regulatorów) dotyczące między innymi: a) zasad świadczenia usługi elektronicznych, b) handlu elektronicznego, c) marketingu elektronicznego, d) zarządzania danymi w Internecie (realizacja Europejskiej strategii danych).

Prawo przełomowych innowacji (*„disruptive technologies"*) to z kolei akty prawne i wytyczne regulatorów dotyczące między innymi: chmury obliczeniowej (CC), sztucznej inteligencji (AI), Internetu rzeczy (IoT), blockchain, kryptowalut, aut autonomicznych, dronów i robotów przemysłowych oraz *gig economy* („gospodarka na żądanie")

Większość źródeł prawa nowych technologii to akty prawa Unii Europejskiej (UE), uchwalanych przede wszystkim w formie rozporządzeń, a mniejsza tylko część w formie dyrektyw. Dla podkreślenia wagi nowo przyjmowanych Rozporządzeń często przyjmują one nazwy „Aktów" (np. Akt w sprawie usług cyfrowych, Akt w sprawie danych, Akt w sprawie sztucznej inteligencji), nie ma to jednak znaczenia prawnego.

Akty Unii Europejskiej mają zastosowanie również do podmiotów mających siedzibę poza UE, o ile tylko oferują one usługi użytkownikom znajdującym się na terytorium UE (*„The Long Arm of European Tech Regulation"*).

W wielu nowo przyjmowanych aktach prawnych z zakresu prawa nowych technologii, implementowana jest zasada proporcjonalności, zgodnie z którą zakres nakładanych obowiązków powiązany jest z wielkością i rodzajem świadczonych usług; z szeregu obowiązków zwalniani są również mikro i mali przedsiębiorcy w rozumieniu zalecenia Komisji Europejskiej nr 2003/361.

W latach 2025-2026 r. po raz pierwszy ustanawiani zostają „regulatorzy Internetu", wyposażeni w kompetencje do nakładania wysokich kar pieniężnych o wysokości maksymalnej do kilkudziesięciu milionów Euro lub nawet 20% rocznego światowego obrotu danego dostawcy usług w poprzednim roku obrotowym) istotnie zwiększa się więc ryzyko prawne prowadzenia działalności w Internecie. Nadanie nowych uprawnień regulatorom następuję poprzez poszerzenie kompetencji już istniejących organów (w Polsce m.in. UKE, UOKiK, UODO), planowane jest również utworzenie nowego organu (Komitet Rozwoju i Bezpieczeństwa Sztucznej Inteligencji).

Nowością jest również to, że nad przestrzeganiem przepisów danego aktu prawnego ma w niektórych przypadkach czuwać nie jeden, ale kilku regulatorów (ryzyko *„overlappingu"* regulacyjnego); przykładem jest Akt o usługach cyfrowych, nad przestrzeganiem którego przepisów czuwać ma dwóch regulatorów – Prezes UKE oraz Prezes UOKiK.

W poszczególnych aktach prawnych pojawiają się również możliwości składania przez osoby fizyczne indywidualnych skarg do organów na działalność podmiotów świadczących usługi w Internecie, a także wytaczania powództw cywilnoprawnych (niezależnie od ewentualnie prowadzonych spraw administracyjnych przed organami nadzorczymi).

Poniżej przedstawiony zostanie stan prawny odnośnie poszczególnych obszarów prawa nowych technologii, ze szczególnym uwzględnieniem aktów prawnych przyjętych w 2025 roku, jak również tych które mają zacząć obowiązywać w 2026 roku lub nad którymi w tym roku prowadzone będą prace legislacyjne w Unii Europejskiej i/lub w Polsce.

2. 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**, numerowanych od 0 do 5. Poziomy 0–2 traktuje się jako systemy wsparcia kierowcy (kierowca odpowiada za prowadzenie), a poziomy 3–5 jako faktyczną automatyzację jazdy (system przejmuje cały lub prawie cały *„dynamic driving task”*).

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.Urz.UE.L Nr 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. Czechy, Holandia, Niemcy, Szwecja).

W związku z powyższym, w Polsce w ramach **nowelizacji Prawa o ruchu drogowym z dnia 7 listopada 2025 r.** (Dz.U. 2025 poz. 1734) zawarto przepisy dotyczące „pojazdów autonomicznych”, w rozdziale o pracach badawczych (art. 65k–65n), wprowadzając legalną definicję pojazdu autonomicznego oraz ramy ich testów na drogach publicznych. Co do zasady nadal obowiązuje klasyczne założenie, że w ruchu musi być kierujący spełniający wymogi ustawy, a systemy wspomagania jazdy są traktowane jako wyposażenie pojazdu, a nie „kierowca”. W trakcie badań ustawodawca wymaga, aby w miejscu kierującego znajdowała się osoba z uprawnieniami, zdolna w każdej chwili przejąć kontrolę nad pojazdem, zwłaszcza w razie zagrożenia bezpieczeństwa ruchu drogowego. Prowadzenie testów na drogach publicznych jest dopuszczalne tylko po uzyskaniu zezwolenia administracyjnego, określeniu obszaru, czasu, liczby pojazdów i spełnieniu wymogów bezpieczeństwa

Nowelizacja prawa o ruchu drogowym, dotyczące testów pojazdów autonomicznych, wchodzi w życie w dnu 24 czerwca 2026 roku.

3. BLOCKCHAIN

Z uwagi na kompleksowe wykorzystanie technologii blockchain, która może być między innymi wykorzystywana w energetyce, finansach czy ochronie zdrowia, aktualnie nie planuje się w Unii Europejskiej, czy Polsce uchwalenia 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 (*Distributed Ledger Technology*, 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.Urz. UE L 150/1), zwane **Rozporządzeniem MiCA**. Część z tych przepisów zaczęła obowiązywać od dnia **30 czerwca 2024 roku (art.149 ust.1), a pozostałe od dnia 30 grudnia 2024 roku (art.149 ust.2)**. Stosowanie przepisów MiCA umożliwić mają przepisy krajowe. W Polsce ustawa kryptoktywach (zob. pkt 13 poniżej).

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 zaczęły 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, przyjęte zostały także w polskim systemie prawnym. Przykładowo, **w art. 300^{31} § 3 oraz art. 328^{1} § 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 ustawy o kryptoaktywach, której przyjęcie planowane jest w tym roku, w 2026 roku nie zaczną obowiązywać przepisy nowych aktów prawnych znajdujących zastosowanie do blockchain.

4. 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**. Prowadzone są natomiast prace legislacyjne dotyczące uregulowania korzystania z chmury obliczeniowej przez wybrane sektory (np. administrację publiczną, zob. uwagi poniżej).

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

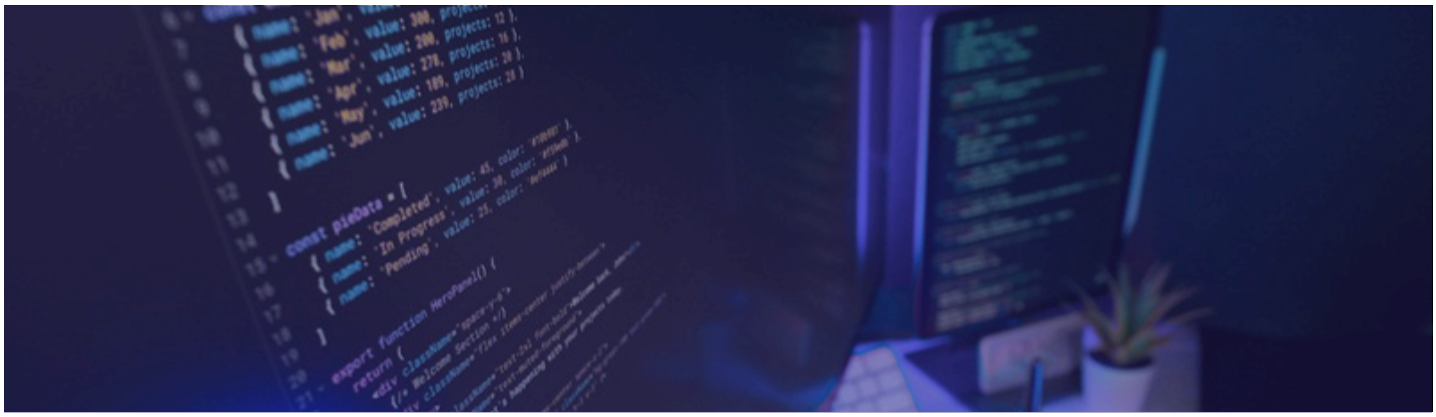
1. przepisy ustawy o krajowym systemie cyberbezpieczeństwa (KSC),
2. przepisy o ochronie danych osobowych (RODO),
3. przepisy sektorowe (m.in. usługi finansowe, life science, public),
4. przepisy dotyczące praw własności intelektualnej (prawo autorskie, ustawa o ochronie baz danych),
5. przepisy prawa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

Jeżeli chodzi o **nowe akty i regulacje prawne dotyczące chmury obliczeniowej, a które mają zacząć obowiązywać lub nad którymi prace mają być kontynuowane w 2026 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 przetwarzania danych, w tym usług chmurowej obliczeniowej (zob. pkt 6 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 organ nadzorczy (zob. pkt 15 poniżej).

Istotne znaczenie odgrywają również **wytyczne organów nadzorczych** 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 z 2024 r, poz.908).** Zmieniona uchwała Rady Ministrów **obowiązuję od dnia 29 października 2024 r.** i ma kluczowe znaczenie dla realizacji projektów chmury obliczeniowej realizowanych w sektorze publicznym. Z inicjatywą „Wspólna Infrastruktura Informatyczna Państwa" i rządową chmurą obliczeniową, powiązane są wydawane przez Ministerstwo Cyfryzacji Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO), które określają wymagania prawne, organizacyjne i techniczne dla korzystania z chmury przez administrację rządową, wyznaczając minimalne poziomy zabezpieczeń, zależnie od kategorii systemu i rodzaju modelu chmurowego. Są one publikowane jako osobny dokument na portalu *chmura.gov.pl*.

W chwili obecnej, Ministerstwo Cyfryzacji przygotowuje również **projekt ustawy o usługach przetwarzania w chmurze obliczeniowej dla administracji publicznej** (tzw. ustawa chmurowa), która ma uregulować między innymi funkcjonowanie Rządowej Chmury Obliczeniowej, korzystanie z publicznych chmur obliczeniowych przez administrację oraz system zapewnienia usług chmurowych (ZUCH). Ustawa ma objąć wszystkie podmioty administracji publicznej, zarówno na szczeblu rządowym, jak i samorządowym, jako użytkowników usług chmurowych. Ma ona uregulować funkcjonowanie Rządowej Chmury Obliczeniowej (RChO) jako wspólnotowej chmury dla administracji, zasady korzystania z publicznych chmur obliczeniowych (PChO) przez administrację oraz funkcjonowanie Systemu Zapewniania Usług Chmurowych (ZUCH) jako platformy nabywania usług. Celem ustawy ma być zapewnienie administracji łatwego, ustandaryzowanego dostępu do skalowalnych usług chmurowych w różnych modelach (IaaS, PaaS, SaaS), przy jednoczesnym zapewnieniu wysokiego poziomu bezpieczeństwa i zgodności z SCCO 2025 i Krajowych Ram Oepracyjności (KRI). Projekt ma więc w dużej mierze skodyfikować i wynieść treści dziś rozproszone w WIIP i SCCO na poziom ustawowy.



Na koniec, warto jeszcze odnotować, że w 2025 roku Komisja Europejska zapowiedziała przygotowanie **Cloud and AI Development Act,** którego celem ma być co najmniej potrojenie unijnej mocy centrów danych w horyzoncie 5–7 lat oraz pełne zaspokojenie potrzeb gospodarki i administracji do 2035 r. Projekt ten ma być przedstawiony **w I kwartale 2026 r.**,

Komisja rozwija również tzw. **EU Cloud Rulebook**, czyli zbiór wspólnych wymogów dla usług chmurowych na rynku UE, obejmujących między innymi. bezpieczeństwo, interoperacyjność, przenoszalność danych i odwracalność umów. Działania te są częścią „*Rolling Plan for ICT Standardisation*" i mają prowadzić m.in. do paneuropejnych rynków (*marketplaces*) usług chmurowych spełniających unijne standardy i reguły.

5. CYBERBEZPIECZEŃSTWO

Podstawowym aktem prawnym w zakresie cyberbezpieczeństwa jest ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 roku (tj. z dnia 10 lipca 2024 r., Dz.U. z 2024 r., poz.1077). Wzorowana jest ona na Dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. dyrektywa NIS-1). Została ona zastąpiona przepisami tzw. dyrektywy NIS-2 (Dyrektywa Parlamentu i Rady UE nr 2022/2555), której implementacja do systemów prawnych poszczególnych państw Unii Europejskiej miała nastąpić do dnia 17 października 2024 roku. Polski ustawodawca nie dotrzymał jednak tego terminu.

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. Przewidziano również włączenie do systemu cyberbezpieczeństwa dodatkowych branż, które do tej pory nie były nim objęte (np. zarządzanie usługami ICT, produkcja, przetwarzanie i dystrybucja żywności).

Postanowienia dyrektywy NIS-2 mają zostać przejęte do polskiego porządku prawnego w ramach **nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa**, która uwzględnia również zalecenia tzw. EU 5G Toolbox. Prace legislacyjne są obecnie na ukończeniu i przyjmuję się, że nowelizacja zostanie uchwalona **na początku 2026 roku.** Szacuje się, że po uchwaleniu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, liczba podmiotów objętych tą regulacją wzrośnie z kilkuset do około 40.000.

Nowelizacja UKSC nie jest jedynym aktem prawnym z zakresu cyberbezpieczeństwa, który zaczął obowiązywać w 2025 r. lub ma obowiązywać w 2026 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 z tym 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, *Cyberislence Act, CRA*)**.

Cyber Resilience Act (CRA) ustanawia horyzontalne wymagania cyberbezpieczeństwa dla „produktów z elementami cyfrowymi" (sprzętu i oprogramowania) wprowadzanych do obrotu w Unii Europejskiej. Jego podstawowym celem jest, aby produkty trafiały na rynek z mniejszą liczbą tzw. podatności oraz aby producenci zapewniali bezpieczeństwo w całym cyklu życia produktu. Chodzi w szczególności o ochronę konsumentów i przedsiębiorstw kupujących oprogramowanie lub sprzęt komputerowy z elementami cyfrowymi.

CRA obejmuje produkty, których przeznaczenie lub racjonalnie przewidywalne użycie zakłada bezpośrednie lub pośrednie logiczne albo fizyczne połączenie danych z urządzeniem lub siecią. Produkty mają spełniać tzw. zasadnicze wymagania w zakresie cyberbezpieczeństwa, określone w załączniku I do Rozporządzenia.

Przepisy Rozporządzenia mają zacząć obowiązywać sukcesywnie w latach 2026-2027, warto w związku z tym odnotować, że od **11 września 2026 r.** zaczną obowiązywać tzw. obowiązki raportowe (art.14), polegające na obowiązku zgłaszania, odpowiedniemu CSIRT-owi oraz ENISA „aktywnego wykorzystywane podatności zawarte w produkcie z elementami cyfrowymi". Mimo, że pozostałe, główne obowiązki określone w CRA zaczną obowiązywać dopiero od dnia 11 grudnia 2027 r., to warto już w tym roku przygotować się do ich wdrożenia.

6. DATA ACT

Akt w sprawie danych (Data Act) to unijne rozporządzenie mające stworzyć jednolity rynek danych w Europie. **Jego pełna nazwa to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. w sprawie harmonijnych zasad dotyczących sprawiedliwego dostępu do danych i korzystania z nich.**

Rozporządzenie obejmuje zarówno dane osobowe, jak i nieosobowe. Data Act ma charakter horyzontalny i reguluje wymianę danych w relacjach B2B, B2C oraz B2G.

W Akcie w sprawie danych doszło do wzmocnienia uprawnień użytkowników (zarówno konsumentów, jak i przedsiębiorców) w zakresie dostępu i wykorzystania danych generowanych przez urządzenia tzw. Internetu rzeczy (IoT). Rozporządzenie przyznaje w szczególności użytkownikom większą kontrolę nad danymi generowanymi przez produkty, które posiadają. Oznacza to, że użytkownicy powinni mieć zapewnioną możliwość łatwiejszego przenoszenie swoich danych do innych usługodawców oraz decydować, kto może mieć do nich dostęp. Wcześniej dostęp do takich danych mieli często wyłącznie producenci urządzeń, co uniemożliwiało użytkownikom korzystanie z konkurencyjnych usług posprzedażowych lub naprawczych (np. serwis prowadzony przez inny podmiot niż producent). W związku z tym, 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.

W obszarze B2B przewiduje również katalog nieuczciwych postanowień umownych dotyczących dostępu i wykorzystania danych, szczególnie chroniąc MŚP.

Niezależnie od powyższego, Data Act wprowadza także ułatwienia w zmianie dostawcy usług chmurowych (również spoza UE, jeśli świadczą usługi w UE), w tym obowiązek jasnych zapisów umownych, standardy interoperacyjności oraz docelowo brak opłat w przypadku zmiany dostawcy od 12 stycznia 2027 r.

Odrębne przepisy umożliwiają także organom publicznym dostęp do danych sektora prywatnego wyłącznie w nadzwyczajnych sytuacjach, np. dla reagowania na klęski żywiołowe, gdy nie da się pozyskać danych inaczej na czas.

Większość przepisów Data Act zaczęła obowiązywać w dniu 12 września 2025 r., natomiast **od dnia 12 września 2026 r.** zacznie obowiązywać wymóg *„access by design”* dla nowych produktów i usług IoT, które muszą być zaprojektowane tak, aby umożliwiać użytkownikowi bezpośredni dostęp do danych. W praktyce oznacza to konieczność uwzględnienia mechanizmów dostępu do danych (interfejsy, AP etc.) dla produktów wprowadzanych na rynek po tej dacie.

W pierwszej połowie 2026 r. planowane jest również uchwalenie ustawy wdrażającej Data Act tj. ustawy o sprawiedliwym dostępie do danych. Ustawa ta będzie między innymi określać mechanizmy nadzoru i egzekwowania przepisów Aktu w sprawie danych, w tym organ nadzorczy za nie odpowiedzialny (ma nim być Prezes Urzędu Komunikacji Elektronicznej) oraz sankcje za naruszenie tych przepisów. Uchwalenie tej ustawy z pewnością przyczyni się do bardziej efektywnego stosowania wymogów Data Act.

7. E-DORĘCZENIA

Istota e-Doręczeń polega na tym, że są to rejestrowane doręczenia elektroniczne – przesyłanie pism i dokumentów online w sposób, który daje dowód nadania i odebrania oraz chroni treść przed nieuprawnioną zmianą, a więc ma „walor dowodowy” podobny do listu poleconego z potwierdzeniem odbioru. W praktyce e-Doręczenia opierają się na posługiwaniu się adresem do doręczeń elektronicznych (ADE) i skrzynką doręczeń, przez którą urząd komunikuje się z obywatelem lub przedsiębiorcą w sprawach urzędowych.

Aktem prawnym, które je reguluję jest przede wszystkim **ustawa z 18 listopada 2020 r. o doręczeniach elektronicznych** (tj. z dnia 21 czerwca 2024 r., Dz.U. z 2024 r., poz.1045). Zgodnie z tymi przepisami, **od 1 stycznia 2026 roku e-Doręczenia stają się podstawowym kanałem elektronicznego doręczania pism** w relacji podmiot publiczny – obywatel lub przedsiębiorca (podmiot niepubliczny), o ile przepisy szczególne nie przewidują innej formy. W praktyce oznacza to odejście od ePUAP jako standardu, a jego użycie zostaje ograniczone do przypadków wskazanych w przepisach.

Doręczenia w systemie e-Doręczeń mają moc prawną równoważną listowi poleconemu za potwierdzeniem odbioru, wraz z dowodami nadania i otrzymania. W obrocie profesjonalnym aktywacja i bieżące monitorowanie ADE stają się elementem należytej staranności, bo nieodebranie korespondencji może skutkować doręczeniem po upływie ustawowego terminu i ryzykiem uchybienia terminom. Dotyczy to np. przedsiębiorców, adwokatów czy radców prawnych.

8. FREEDOM MEDIA ACT (AKT O WOLNOŚCI MEDIÓW)

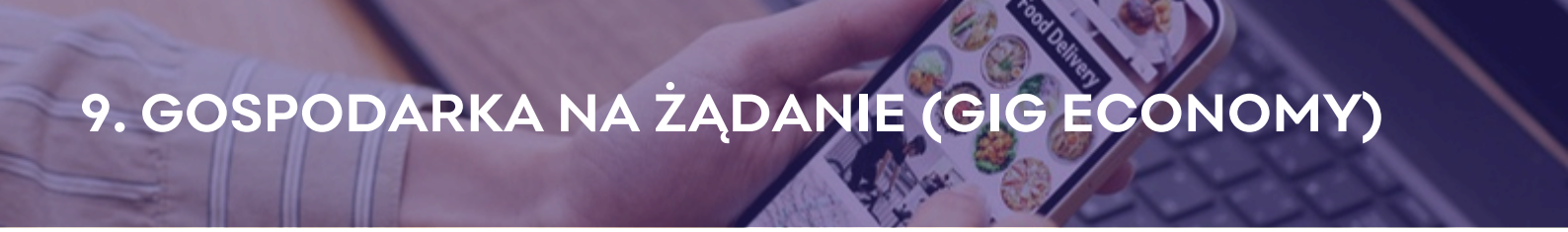
W dniu 17 kwietnia 2024 r. opublikowane zostało rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2024/1083 z dnia 11 kwietnia 2024 r. w sprawie ustanowienia wspólnych ram dla usług medialnych na rynku wewnętrznym i zmiany dyrektywy 2010/13/UE (**Europejski Akt o Wolności Mediów**). **Większość przepisów Rozporządzenia zaczęła 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 zarówno 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 nie dyskryminujący. 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 2026 roku.



9. GOSPODARKA NA ŻĄDANIE (GIG ECONOMY)

Gig economy (ekonomia pracy dorywczej) to model gospodarczy i rynku pracy oparty na krótkoterminowych zleceniach („*gigach*"), projektach i pracy na żądanie zamiast stałego etatu u jednego pracodawcy. Najczęściej łączy się z platformami cyfrowymi (np. aplikacje do przewozu osób, dostaw czy platformy freelancerskie), które kojarzą zleceniodawców z wykonawcami.

Dla gig economy szczególne znaczenie ma **Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/2831 z dnia 13 września 2024 r. w sprawie poprawy warunków pracy za pośrednictwem platform cyfrowych oraz zmiany dyrektywy 2019/1152 i 2019/1158 (tzw. dyrektywa o platformach).**

Dyrektywa platformowa ma zwiększyć ochronę osób pracujących za pośrednictwem platform cyfrowych, głównie poprzez ułatwienie ustalenia prawidłowego statusu zatrudnienia oraz uregulowanie algorytmicznego zarządzania pracą. Jej celem jest poprawa warunków pracy przy zachowaniu elastyczności związanej z modelem platformowym. Istotnym rozwiązaniem jest wprowadzenie wzruszalnego domniemania istnienia stosunku pracy między platformą a osobą wykonującą pracę, gdy występują fakty wskazujące na „kierownictwo i kontrolę" po stronie platformy.

Celem jest odwrócenie ciężaru dowodu: to platforma musi wykazać, że dana osoba nie jest pracownikiem, jeśli chce utrzymać model „niezależnego wykonawcy". Ważne jest także ograniczenie wykorzystania automatycznego monitoringu i podejmowania decyzji w sposób wywierający nadmierną presję lub zagrażający zdrowiu psychicznemu i fizycznemu pracowników platformowych.

W Dyrektywie wzmocniono także ochronę danych osobowych osób pracujących na platformach, w szczególności w zakresie monitoringu, profilowania i wykorzystywania danych do zarządzania pracą.

Dyrektywa 2024/2831 **obowiązuje w Unii Europejskiej od 1 grudnia 2024 r.,** a państwa członkowskie muszą **dokonać transpozycji do prawa krajowego najpóźniej do 2 grudnia 2026 r.**

W chwili obecnej, Ministerstwo Rodziny, Pracy i Polityki Społecznej prowadzi prace **nad projektem ustawy o pracy platformowej.**

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)**
5. **szczególne przepisy dotyczące świadczenia usług handlu elektronicznego określonym kategoriom osób. Chodzi w szczególności o ustawę z dnia 26 kwietnia 2024 r. o zapewnieniu spełniania wymagań dostępności niektórych produktów i usług przed podmioty gospodarcze (Dz.U. z 2024 r. poz. 731).** Ustawa ta ma na celu usunięcie barier, które uniemożliwiają lub utrudniają osobom z niepełnosprawnościami korzystanie z produktów i usług dostępnych na rynku. Przepisy ustawy stosuję 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 zapewnić alternatywne sposoby komunikacji, takie jak opisane w ustawie (np. kontakt tekstowy). Regulatorem w zakresie handlu elektronicznego i usług cyfrowych jest Minister Cyfryzacji.

W 2026 roku ma dojść do implementacji do prawa polskiego dwóch ważnych, również z punktu widzenia handlu elektronicznego, dyrektyw unijnych tj. tzw. dyrektywy UE o prawie do naprawy oraz nowej dyrektywy o odpowiedzialności za produkty wadliwe.

Dyrektywa Parlamentu Europejskiego i Rady (UE) nr 2024/1799 z dnia 13 czerwca 2024 r. w sprawie wspólnych zasad promujących naprawę towarów (tzw. *Dyrektywa Right to Repair*) to akt prawny, który ma kluczowe znaczenie dla sektora e-commerce, produkcji elektroniki oraz ochrony konsumentów.

Celem Dyrektywy jest ustanowienie wspólnych zasad promujących naprawę towarów dla konsumentów, aby ograniczać wymianę na nowe, wspierając tym samym cele ochrony środowiska. Obejmuje ona zarówno środki działające w ramach ustawowej odpowiedzialności sprzedawcy za brak zgodności towaru, jak i poza tym reżimem.

W okresie odpowiedzialności z tytułu niezgodności towaru z umową, dyrektywa o prawie do naprawy ingeruje w wybór środka ochrony - jeżeli konsument decyduje się na naprawę zamiast wymiany, sprzedawca jest zobowiązany do naprawy, a okres odpowiedzialności zostaje wydłużony co najmniej o dodatkowe 12 miesięcy. „Prawo do naprawy" ma w tej fazie charakter zachęty regulacyjnej.

Istotnym *novum* jest wprowadzenie rozwiązania, zgodnie z którym po upływie okresu odpowiedzialności sprzedawcy, konsument uzyskuje bezpośrednie uprawnienie do żądania naprawy od producenta towaru objętego załącznikiem II do dyrektywy. Chodzi w szczególności o kategorie towarów „technicznie naprawialnych", wymienionych w tym załączniku II (np. smartfony, tablety, produkty do przechowywania danych). W takich przypadkach producent musi oferować naprawę w rozsądnym terminie i za rozsądną cenę lub nieodpłatnie (chyba że naprawa jest „niemożliwa"), przy czym nie wolno odmówić naprawy wyłącznie z powodu wcześniejszej naprawy przez podmiot trzeci.

Dyrektywa powinna zostać implementowana do ustawodawstw krajowych państw członkowskich Unii Europejskiej **do dnia 31 lipca 2026 r**. Prace w tym zakresie prowadzi Prezes Urzędu Ochrony Konkurencji i Konsumentów (UOKiK), który na zlecenie Kancelarii Prezesa Rady Ministrów, prowadzi analizy i prekonsultacje z rynkiem. Do transpozycji przepisów Dyrektywy prawdopodobnie dojdzie w ramach nowelizacji ustawy o prawach konsumenta oraz Kodeksu cywilnego.

Nowa Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/2853 o odpowiedzialności za produkty wadliwe zastąpiła dotychczasową dyrektywę 85/374/EWG, dostosowując postanowienia tego ostatniego aktu prawnego do realiów gospodarki cyfrowej i AI. Ustanawia ona w pełni zharmonizowane zasady odpowiedzialności na zasadzie ryzyka (bez winy) „podmiotów gospodarczych" za szkodę poniesioną przez osoby fizyczne wskutek produktu wadliwego. Najważniejszą zmiana z perspektywy prawa nowych technologii jest poszerzenie pojęcia produktu, którym w rozumieniu Dyrektywy przestaje być tylko przedmiot materialny, a staje się nim również oprogramowanie, systemy AI, czy usługi cyfrowe. W tym ostatnim przypadku chodzi o sytuacje, gdy usługa cyfrowa jest zintegrowana z produktem w taki sposób, że jej brak uniemożliwia jego działanie (np. nawigacja w aucie autonomicznym), traktuje się ją jako element produktu.

Produkt jest „wadliwy", gdy nie zapewnia bezpieczeństwa, którego można zasadnie oczekiwać lub które wynika z przepisów prawa, a ryzyka mogą dotyczyć również elementów cyfrowych i „posprzedażowych" (np. aktualizacje oprogramowania). Krąg potencjalnie odpowiedzialnych podmiotów obejmuje nie tylko producenta, lecz także producenta komponentu, dostawcę powiązanej usługi cyfrowej, a w określonych sytuacjach również dystrybutora.

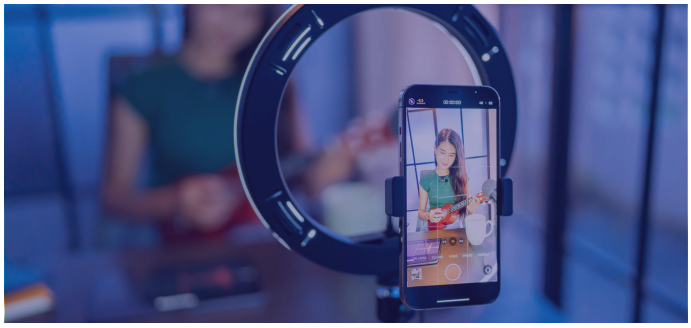
W modelach sprzedaży online Dyrektywa przewiduje możliwość pociągnięcia do odpowiedzialności także niektórych platform internetowych. Wprowadzono również ułatwienia dowodowe, w tym mechanizmy ujawniania dowodów oraz domniemania wadliwości i/lub związku przyczynowego w typowych sytuacjach.

Termin na implementację postanowień Dyrektywy do krajowych systemów prawnych upływa **w dniu 9 grudnia 2026 r.**

11. INFLUENCER MARKETING

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

W praktyce stosuję się przepisy ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym, ustawy o zwalczaniu nieuczciwej konkurencji oraz ustawy ochronie konkurencji i zbiorowych interesów konsumentów (kompetencje Prezesa UOKiK).



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

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 2026 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, to w **2025 roku zaczęły obowiązywać lub zaczną obowiązywać w latach 2026-2027 przepisy następujących aktów prawnych, które będą miały istotny wpływ na rynek Internetu rzeczy**:

1. Rozporządzenie Unii Europejskiej pt. **Akt w sprawie danych**, w szczególności w zakresie zwiększenia uprawnień użytkowników urządzeń IoT (zob. pkt 6 powyżej),
2. Rozporządzenie Unii Europejskiej pt. **Akt w sprawie sztucznej inteligencji** (zob. pkt 20 poniżej)
3. Rozporządzenie Unii Europejskiej pt. **Akt o cyberodporności** (zob. pkt 5 powyżej).

13. KRYPTOAKTYWA

MiCA tj. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 to akt prawny, który tworzy pierwszy kompleksowy reżim prawny dla emisji kryptoaktywów i świadczenia usług na nich opartych w całej UE. Jego celem jest jednocześnie ujednolicenie rynku, podniesienie ochrony inwestorów i ograniczenie ryzyk systemowych związanych z kryptoaktywami.

Stosowanie MiCA mają zapewnić ustawy krajowe, w szczególności przez wskazanie organu właściwego, uregulowanie procedur licencyjnych, trybów nadzorczych i katalogu sankcji administracyjnych i karnych. W Polsce projekt ustawy przygotowany przez Ministerstwo Finansów we współpracy z KNF i uchwalony następnie przez Parlament, jako akt zapewniający stosowanie MiCA oraz rozporządzenia w sprawie transferu środków w kryptoaktywach został zawetowany przez Prezydenta RP w dniu 1 grudnia 2025 r. Rządowy **projekt ustawy o kryptoaktywach** (w wersji „2.0") został ponownie przyjęty przez Radę Ministrów w grudniu 2025 r. i obecnie trwają nad nim prace w Parlamencie. Jego uchwalenie jest planowane **na początku 2026 r.**

Ustawa wskazuje Komisję Nadzoru Finansowego jako organ właściwy do między innymi licencjonowania dostawców usług w zakresie kryptoaktywów (CASP), a także prowadzenia kontroli oraz nakładania sankcji administracyjnych. Przewiduje również rejestr domen i adresów IP podmiotów nielegalnie oferujących usługi krypto, możliwość blokowania rachunków i portfeli, a także szeroki katalog kar pieniężnych i karnych.

Ustawa o kryptoaktywach ma istotne znaczenie przede wszystkim dla podmiotów z „branży krypto" (np. giełdy, kantory krypto, brokerzy, emitenci tokenów etc.), ale również instytucji finansowych i płatniczych (np. banki, domy maklerskie), a także podmiotów spoza branży „krypto" (np. firmy e-commerce akceptujące płatności w krypto).

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.

W związku z powyższym, w Polsce **uchwalono nowelizację Prawa lotniczego z dnia 24 stycznia 2025 r. (Dz.U. 2025 poz. 179). Ta nowelizacja w sposób kompleksowy „domyka" wdrożenie unijnych regulacji EASA dla BSP i wprowadza nowe obowiązki dla operatorów**.

W nowelizacji dokonano wyszczególnienia trzech kategorii operacji bezzałogowymi statkami powietrznymi (BSP):

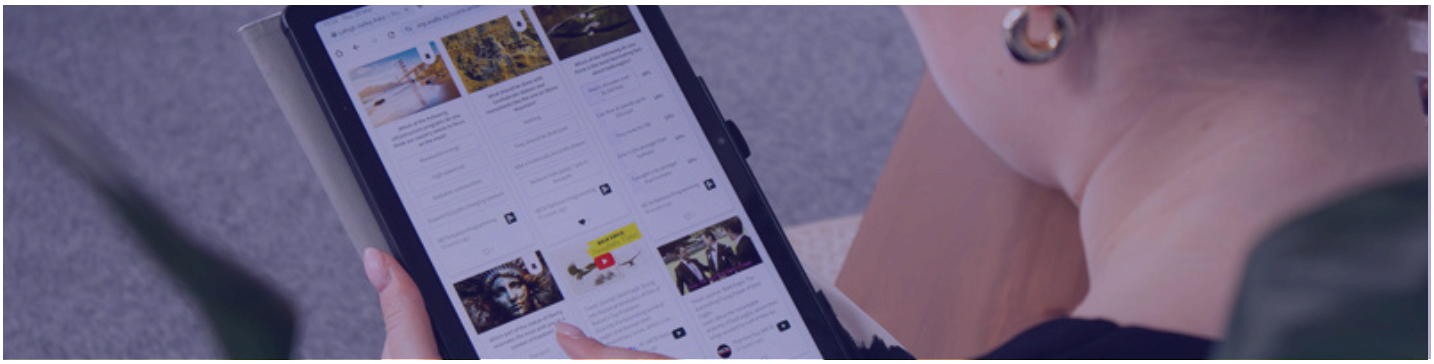
1. operacja „otwarta",
2. operacja „szczególna",
3. operacja „certyfikowana".

Istotne znaczenie odgrywają również Wytyczne Prezesa Urzędu Lotnictwa Cywilnego wydawane między innymi na podstawie art. 23 ust. 2 pkt 2 Prawa lotniczego jako sposób implementacji i doprecyzowania przepisów unijnych (np. rozporządzenia 2019/947).

15. MEDIA CYFROWE

W 2026 roku uchwalone mają być dwa akty prawne dotyczące mediów cyfrowych:

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



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 do uregulowania na poziomie krajowym przekazano wyznaczenie 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.

Zgodnie z rządowym **projektem nowelizacji ustawy o świadczeniu usług drogą elektroniczną wniesionym do Sejmu w dniu 29 września 2025 r. (druk sejmowy nr 1757), 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). Powołana ma zostać przy Prezesie UKE, 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 było na początku 2026, jednak z uwagi na weto Prezydenta RP w dniu 9.01.2026 r., termin ten nie będzie utrzymany. Należy się w związku z tym spodziewać, podobnie jak w przypadku zawetowanej ustawy o kryptoaktywach, że rząd w I kwartale 2026 r, przygotuje wersję 2.0 nowelizacji uśude.

W 2026 roku Komisja Europejska zamierza również ogłosić propozycję zmian do Dyrektywy UE o audiowizualnych usługach medialnych (AVMSD), na której wzorowana jest polska ustawa o radiofonii i telewizji.

16. NOWELIZACJA REGULACJI CYFROWYCH W UE (DIGITAL OMNIBUS)

W dniu 19 listopada 2025 roku Komisja Europejska ogłosiła inicjatywę określaną jako Digital Omnibus (COM(2025) 837 final). Jej podstawowym celem jest uproszczenie przyjętych już regulacji cyfrowych oraz obniżenie kosztów zapewnienia zgodności z nimi. Zgodnie z przyjętym rozwiązaniem, w ramach jednego aktu prawnego – o charakterze unijnego rozporządzenia – planuje się wprowadzenie zmian w szeregu aktach prawnych – m.in. RODO, Dyrektywy e-Privacy, Dyrektywy NIS-2, Rozporządzenia Data Act oraz Rozporządzenia Data Governance Act. Część pakietu stanowi propozycja, wyrodrębnionego od ogólnego rozporządzenia Digital Omnibus, rozporządzenia Digital Omnibus on AI, które ma zmienić niektóre postanowienia AI Act COM(2025) 836 final). Ta ostatnia regulacja będzie miała między innymi kluczowe znaczenie dla ustalenia obowiązywania przepisów AI Act dotyczących tzw. systemów wysokiego ryzyka (zob. pkt 20 poniżej).

Przyjęcie pakietu Digital Omnibus będzie miało ogromne znaczenie dla rynku cyfrowego. Przyjmuję się, że **jego uchwalenie powinno nastąpić do końca 2026 r., z tym, że szybciej powinno być procedowane rozporządzenie Digital Omnibus on AI.**

17. OCHRONA MAŁOLETNICH W INTERNECIE

Ministerstwo Cyfryzacji pracuje obecnie nad **projektem ustawy o ochronie małoletnich przed dostępem do treści pornograficznych w Internecie (UD179)**.

Obecnie projekt ustawy jest na etapie rządowym i sejmowym w wersji istotnie zmienionej w stosunku do pierwotnych założeń – zakres został zawężony z „treści szkodliwych" do treści pornograficznych.

Projekt przewiduje m.in. obowiązki usługodawców w zakresie stosowania skutecznej weryfikacji wieku oraz odpowiednich postanowień w regulaminach usług online. Główne założenia projektu to ograniczenie dostępu małoletnich do treści pornograficznych w Internecie poprzez obowiązkową weryfikację wieku, rejestr stron ignorujących te wymogi oraz blokowanie takich domen przez dostawców Internetu.

Ustawa ma objąć ochroną wszystkie osoby małoletnie (poniżej 18 lat) i skoncentrować się na utrudnieniu dostępu do treści pornograficznych oraz zapobieganiu przypadkowemu zetknięciu się dzieci z takimi materiałami.

Dostawcy usług, w ramach których udostępniane są treści pornograficzne (serwisy WWW, platformy), mają obowiązek wdrożyć skuteczne mechanizmy weryfikacji wieku użytkownika przed dopuszczeniem do takich treści. Jeżeli dostawca nie wdroży weryfikacji wieku, Prezes UKE będzie mógł wpisać domenę do specjalnego rejestru prowadzonego przez NASK, co obliguje operatorów telekomunikacyjnych do jej zablokowania dla użytkowników w Polsce.

NASK ma prowadzić rejestr domen, które nie spełniają wymogów dotyczących weryfikacji wieku albo omijają system ochrony małoletnich a Prezes UKE na otrzymać kompetencje do wydawania decyzji o wpisie domen do rejestru oraz nadzorowania wykonania obowiązków blokowania przez dostawców dostępu do Internetu, z możliwością nakładania sankcji.

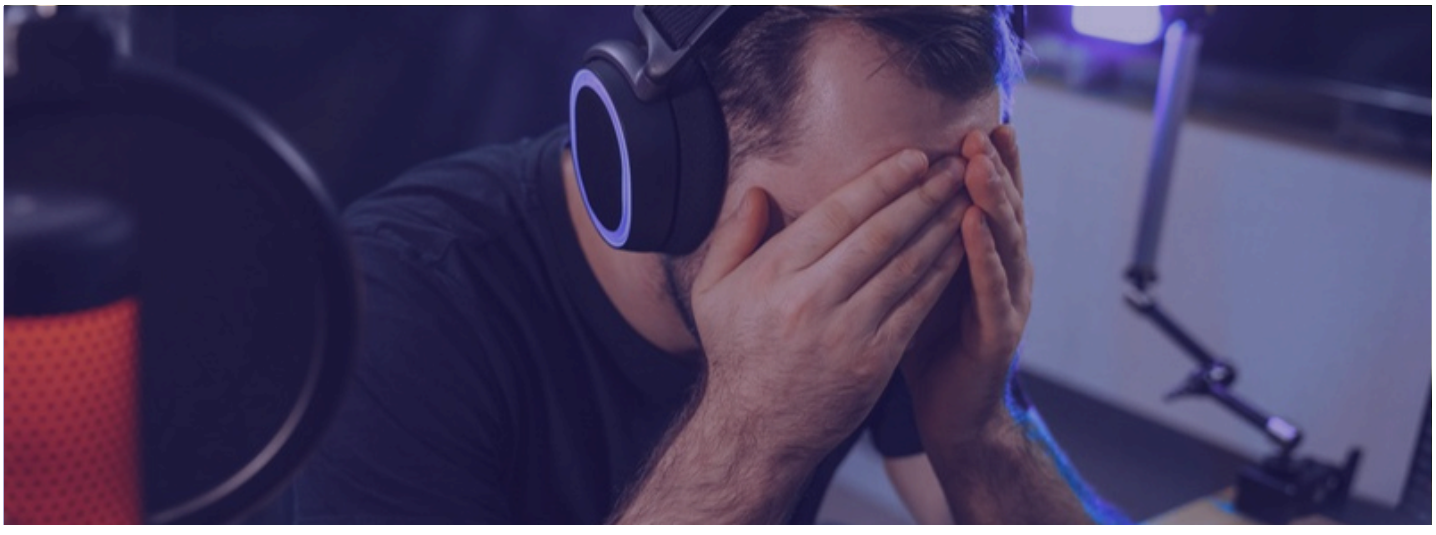
Planowany termin przyjęcia projektu przez Radę Ministrów to drugi kwartał 2026 r. a uchwalenie ustawy przewidywane jest w IV kwartale 2026 r.

18. PATOSTREAMING

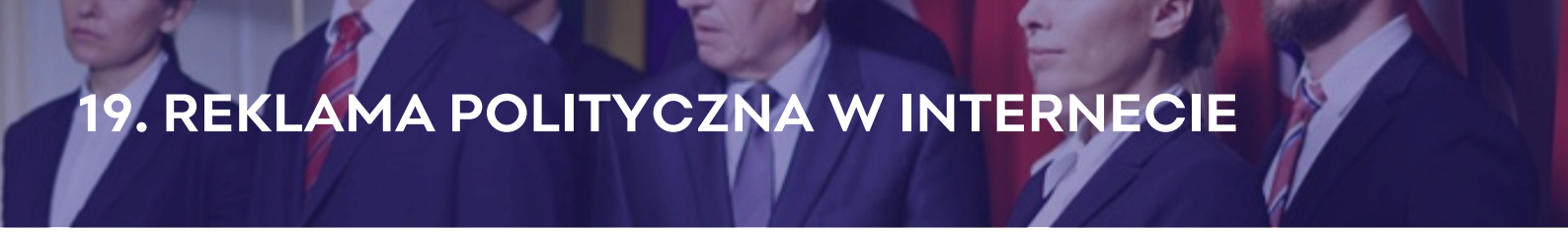
W 2025 roku dużo się w Polsce mówiło o sprawach zaliczanych do kategorii **patostreamingu**, a więc publicznego transmitowania i rozpowszechniania w Internecie treści audiowizualnych prezentujących przemoc, agresję i zachowania patologiczne, rodzi poważne zagrożenie społeczne oraz moralne.

Obecnie w Polsce brak jest odrębnego przepisu, który wprost typizowałby „patostreaming" jako samodzielne przestępstwo, ale trwają zaawansowane prace nad jego penalizacją. W konsekwencji, aktualnie patostreaming ścigany jest na podstawie istniejących przepisów kodeksu karnego, dotyczących między innymi przestępstwa przeciwko życiu i zdrowiu, czy znieważenia, zniesławienia, gróźb karalnych, nawoływanie do nienawiści, publicznego pochwalania przestępstwa.

Równocześnie prowadzone są konsultacje na wprowadzenie **nowego przepisu kodeksu karnego (nowy art. 255b § 1 kodeksu karnego)**, zwalczającego to zjawisko. Projektowane przepisy definiują patostreaming jako rozpowszechnianie w Internecie treści przedstawiających popełnienie czynu zabronionego albo jego pozorowanie (tak, by wyglądał na rzeczywiście popełniony), często z kwalifikacją, gdy sprawca działa w celu osiągnięcia korzyści majątkowej.



Należy się spodziewać, **że w 2026 r. prowadzone będą dalsze konsultacje nad wprowadzeniem odrębnego przepisu kodeksu karnego, penalizującego patostreaming.**



19. REKLAMA POLITYCZNA W INTERNECIE

W dniu 10 października 2025 r. zaczęła 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 sposobów, w jakie Rozporządzenie realizuję w/w cel:

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 jako takie, 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.

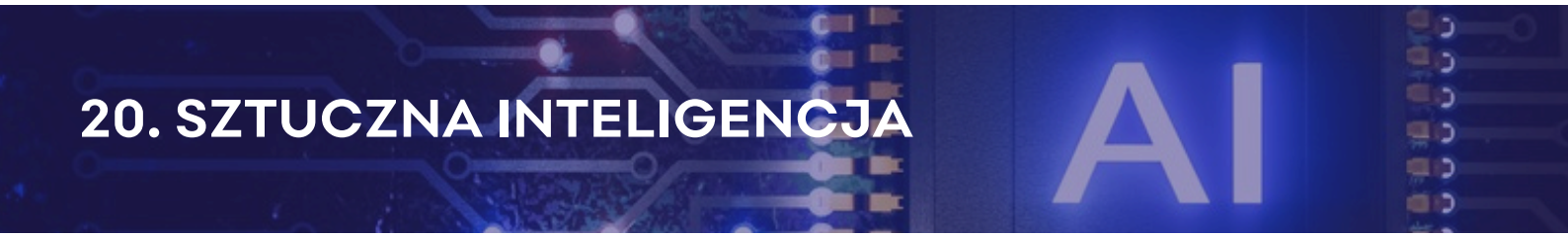
Adresatami obowiązków określonych w rozporządzeniu o reklamie politycznej są:

1. reklamodawcy polityczni, a więc 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 sankcji** (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 Unii Europejskiej jest zobowiązane do wdrożenia powyższych przepisów do swojego porządku prawnego, między innymi w zakres wyznaczenie organu/organów odpowiedzialnych za przestrzeganie przepisów rozporządzenia. W Polsce organem właściwym do nadzorowania przestrzegania zasad targetowania i przetwarzania danych w reklamie politycznej online jest **Prezes Urzędu Ochrony Danych Osobowych (PUODO)**. Kompetencja ta wynika z art.22 Rozporządzenia. Pozostałe aspekty – takie jak oznaczanie reklam czy obowiązki wydawców – mają zostać **powierzone innemu organowi właściwemu**, jak dotąd nie przyjęto jeszcze przepisów krajowych kompleksowo regulujących ten nadzór, a Ministerstwo Cyfryzacji pracuje nad tym projektem.

Uchwalenie **ustawy uzupełniającej (wdrażającej) Rozporządzenie o reklamie politycznej planowane jest w 2026 r.**



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.

Zasadnicza datą rozpoczęcia stosowania Rozporządzenia jest **2 sierpnia 2026 r.** Przyjęto przy tym regułę intertemporalną, że jego 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.**

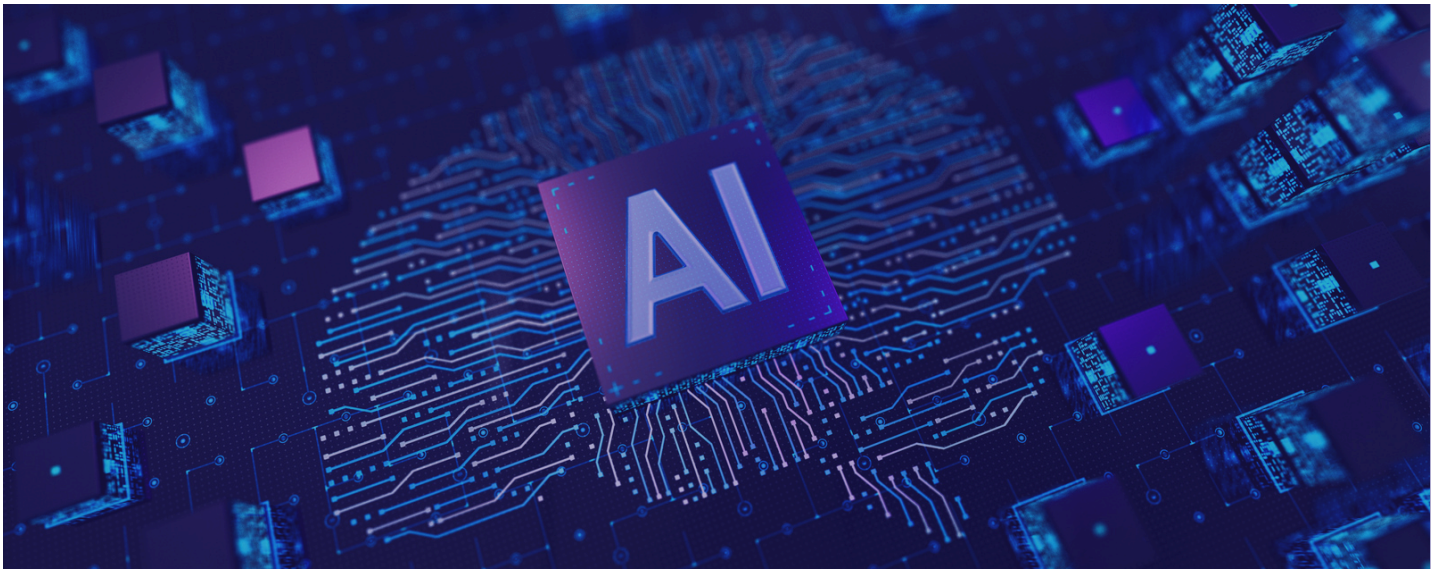
Głównym celem powyższej regulacji jest bezpieczeństwo tworzenia i korzystania z systemów sztucznej inteligencji (AI). Regulację stosuję się zarówno do systemów przetwarzających dane osobowe, jak i systemów przetwarzających dane nieosobowe. W Rozporządzeniu wprowadzono również wyjątki stosowania się jego przepisów (cele badawczo-naukowe, cele wojskowe etc.). Akt w sprawie sztucznej inteligencji stosuję się nie tylko do dostawców, ale również do organizacji stosujących AI. Rozporządzenie będzie się stosowało również 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.1 a).

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 reguluję 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).

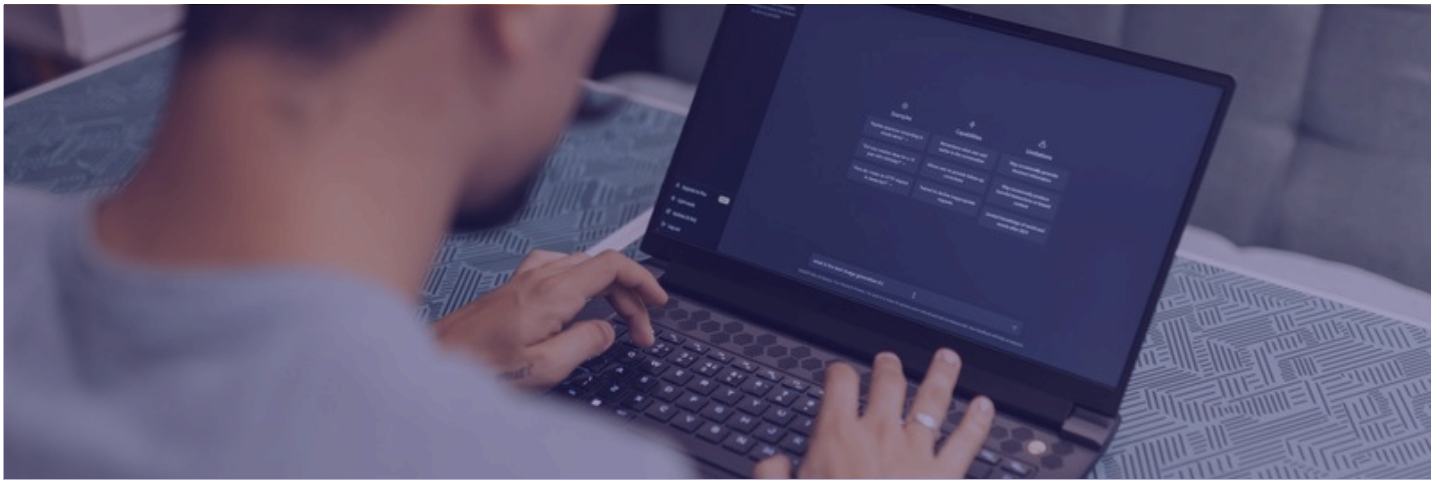
W Rozporządzeniu wprowadzono również szczególną regulację dla dostawców tzw. modeli ogólnego przeznaczenia (np. GPT). Zgodnie z art.53 nałożono na nich szczególne obowiązki związane z korzystaniem przez nich, na etapie trenowania tych modeli, z danych stanowiących przedmioty praw autorskich i praw pokrewnych.



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 kary za nieprzestrzeganie zakazu praktyk w zakresie AI, w wysokości do 1 500 000 EUR.

Data 2 sierpnia 2026 r. jako termin obowiązywania przepisów o systemach wysokiego ryzyka może zostać przesunięty, taką propozycję zgłosiła bowiem Komisja Europejska w dniu 19 listopada 2025 r. w projekcie aktu prawnego pt. AI Omnibus (COM(2025) 836 final), stanowiącego część pakietu pt. Digital Omnibus (zob. pkt 10 poniżej). Zgodnie z tą propozycją, obowiązywanie przepisów dotyczących systemów wysokiego ryzyka (art.6 ust.2) oraz systemów generujących tzw. syntetyczne treści (art.50 ust.2), ma zostać przesunięte na 2027 rok. Zmiana ta spowodowana jest między innymi opóźnieniami w większości państw Unii Europejskiej, w tym w Polsce, w wyznaczeniu krajowych organów nadzorczych, organów weryfikujących zgodność systemów wysokiego ryzyka z wymogami AI Act, a także brakiem wydania przez organy nadzorcze wytycznych dotyczących systemów wysokiego ryzyka.

W chwili obecnej w Polsce prowadzone są również prace nad **ustawą wdrażającą Akt w sprawie sztucznej inteligencji**. Projekt ustawy o systemach sztucznej inteligencji opracowany przez Ministerstwo Cyfryzacji i przedłożony do konsultacji, między innymi zakłada, że organem nadzoru ma być nowy organ nadzorczy - **Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji**, na którego czele ma stać przewodniczący powoływany przez Prezesa Rady Ministrów. **Uchwalenie ustawy o systemach sztucznej inteligencji planowane jest w 2026 roku.**



Akt w sprawie sztucznej inteligencji niewątpliwie stanowi podstawową regulację dotycząca stosowania systemów AI. Należy jednak podkreślić, że do tworzenia i korzystania z AI, w szczególności generatywnej sztucznej inteligencji (*GenAI*), 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.26[3] 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.

Polska wdraża eIDAS 2.0 przede wszystkim przez nowelizację ustawy o usługach zaufania oraz identyfikacji elektronicznej (projekt UC122) oraz powiązane zmiany między innymi w ustawie o informatyzacji i ustawie o aplikacji mObywatel. Uchwalenie tych przepisów planowane jest w 2026 r.

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 tego 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.Urz. UE L, Nr 130). Większość tych przepisów zaczęła obowiązywać **w dniu 20 września 2024 roku**, natomiast art. 86^1 Prawa autorskiego w drodze wyjątku wszedł w życie **z dniem 20 lutego 2025 roku.**

Z punktu widzenia działalności w Internecie najważniejsze z regulacji zawartych w nowelizacji dotyczą:

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 z różnego rodzaju treści dostępne w Internecie korzystają 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. 26[3]**).

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. 26[3] ust.2).

2) przyznanie twórcom oraz artystom wykonawcom prawa do wynagrodzenia za dzieła udostępniane w Internecie

Dodanym w ramach nowelizacji **przepisom art. 21[4] oraz art. 86[1] 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

Nowo wprowadzony **art. 70 ust. 2[1] 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. 99[7] ust.2 pkt 2**. Dzięki temu wydawcom prasowym 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. Art. 99^{9} ust.1)

5) nowe zasady odpowiedzialności platform internetowych

W świetle nowo dodanego **art. 22^{2} 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 (pkt 1).

W 2026 r. nie jest planowane uchwalenie zmian w przepisach ustawy o prawie autorskim i prawach pokrewnych.

23. WOLNOŚĆ SŁOWA W INTERNECIE (DYREKTYWA ANT-SLAPP)

W dniu 11 kwietnia 2024 r. uchwalona 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 effect*) i zastraszanie osób, które wypowiadają się na ważne społecznie tematy**. Tego rodzaju działania są podejmowane zarówno przez rządzących, jak i korporacje. Chodzi tu przy tym nie tylko o koszty i ryzyka finansowe związane z tego rodzaju procesami, ale również i uciążliwości związane np. z koniecznością stawiania się na rozprawy etc. Istnieje w związku z tym obawa, że tego rodzaju działania „zniechęcające" mogą doprowadzić do sytuacji, gdy opinia publiczna nie dowie się o wykrytych, przez aktywistów czy dziennikarzy, nieprawidłowościach.

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 sprawa 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.**

W Polsce projekt ustawy wdrażającej dyrektywę anty-SLAPP ma zostać przyjęty przez **Radę Ministrów na początku 2026 r. i następnie być procedowany w Sejmie**. Ma on przybrać postać odrębnej ustawy.

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 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 ma Prezes UODO, a górna granica kar to 500.000 EURO.

Projekt ustawy o zarządzaniu danymi został przyjęty przez Radę Ministrów w dniu 21 października 2025 r. i skierowany do prac parlamentarnych. Nie wiadomo jednak, jakie będą jego dalsze losy, zgodnie bowiem z projektem rozporządzenia UE Digital Omnibus planowane jest bowiem jego uchylenie i wchłonięcie treści Aktu w sprawie zarządzania danymi (*Data Governace Act*) do znowelizowanego Data Act.

Masz pytania?
Skontaktuj się z naszym ekspertem:

Xawery Konarski
Adwokat, Senior Partner,
Co-Managing Partner
xawery.konarski@traple.pl
linkedin.com/in/xawerykonarski/

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