Wprowadzenie

Szanowni Państwo,

w Państwa ręce oddajemy numer 3–4/2025 Kwartalnika „Prawo Nowych Technologii", poświęcony przede wszystkim problematyce prawnej danych osobowych i prywatności, innowacji, Internetu i mediów oraz prawu IT.

W pierwszym z artykułów, Autorka omówiła niezmiennie aktualną problematykę zasad oraz narzędzi niezbędnych do zapewnienia bezpieczeństwa danych osobowych w przestrzeni chmurowej oraz zapewniania zgodności przetwarzania z obowiązującymi regulacjami prawnymi. Bezpieczeństwo danych w chmurze zależy zarówno od zastosowanych środków, jak i od właściwie skonstruowanych umów z dostawcami usług cyfrowych. Istotną rolę w tym zakresie odgrywają normy ISO 27017 oraz ISO 27018, które wyznaczają standardy zarządzania bezpieczeństwem informacji i ochrony danych osobowych w przestrzeni chmurowej. Powiązana z wymogami RODO, norma ISO 27018, koncentruje się na ochronie prywatności, zgodzie na przetwarzanie oraz zasadach minimalizacji i celowości przetwarzania danych. Zastosowanie tych norm oraz zasad wynikających z RODO odgrywa kluczową rolę w procesie umieszczania w chmurze danych i projektowania im w jej przestrzeni bezpiecznych rozwiązań prawnych.

Dnia 30.12.2025 r. upłynął rok od terminu, w którym rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 w sprawie rynku kryptoaktywów (MiCA) zaczęło obowiązywać w obrębie regulacji działalności m.in. tzw. dostawców usług w zakresie krytpoaktywów (CASP). Szczególnie istotnym przepisem MiCA jest w tym obszarze zakaz prowadzenia działalności jako CASP, chyba że podmiot zainteresowany uzyska zezwolenie od organu wyznaczonego przez państwo, w którym ma on swoją siedzibę statutową. Niewyznaczenie organu przez dane państwo członkowskie, tak jak to się stało w Polsce, faktycznie uniemożliwia podjęcie działalności jako CASP przedsiębiorcom mającym siedzibę statutową w tym państwie. Komplikacje prawne z tym związane są przedmiotem analizy dokonanej przez Autorów w drugim z artykułów, zawartych w tym numerze.

Rozporządzenia MICA dotyczy również kolejny tekst, w którym Autor dowodzi, że MiCA – pomimo deklarowanego celu integracji rynku wewnętrznego – nie znosi kluczowych barier dla sektora bankowego, lecz ujawnia strukturalne napięcie pomiędzy logiką harmonizacji rynku finansowego a logiką regulacji ostrożnościowej. W artykule dokonano wyodrębnienia granic normatywnych, funkcjonalnych i strategicznych aktywności banków w obszarze kryptoaktywów, a wynikających z kumulatywnego oddziaływania MiCA, reżimów CRR/CRD, regulacji AML/CFT oraz DORA, a także z praktyki nadzorczej.

Interesującym i aktualnym problemem prawnym jest dopuszczalność tokenizacji papierów wartościowych. W jednym z tekstów Autor dowodzi, że brak jest powodów, aby odmawiać możliwości tokenizacji papierów wartościowych. Stokenizowane papiery wartościowe nie stanowią kategorii materialnoprawnie odrębnej od opisanych i unormowanych papierów wartościowych w tzw. części ogólnej prawa papierów wartościowych. Ponadto, brak jest jakichkolwiek powodów, aby wyznaczać technologicznie nieneutralną linię demarkacyjną pomiędzy papierami wartościowymi związanymi z fizycznym nośnikiem dokumentu dłużnego i klauzul dokumentowych, a zdematerializowanym nośnikiem, który przybiera postać tokenu. Pojęcie „dokumentu" w polskim porządku prawnym zostało, w sposób celowy, wykreowane przez prawodawcę w sposób neutralny technologicznie. O ile we wcześniejszym stanie prawnym, który nie zawierał definicji znajdującej się *de lege lata* w art. 77^3 KC, mogły istnieć jakieś wątpliwości w tym zakresie, tak obecnie token może być dokumentem, o ile spełnia on wymóg z art. 77^2 KC w postaci możliwości ustalenia osoby składającej oświadczenie woli.

Jednym z aspektów cyfryzacji różnych sposobów rozliczeń jest koncepcja pieniądza cyfrowego banku centralnego (*Central Bank Digital Currencym* – CBDC) oparta na założeniu wprowadzenia do obiegu pieniądza, który odbiegałby w pewnym sensie od tradycyjnej jego formy (pieniądza gotówkowego), ale pozostając w powiązaniu z dotychczasowym emitentem (bankiem centralnym) miałby charakter prawnego środka płatniczego i stanowiłby alternatywę dla kryptowalut. Analizie różnych skutków związanych z ewentualną emisją pieniądza cyfrowego przez bank centralny (w tym Narodowy Bank Polski) poświęcony jest jeden z tekstów, zawarty w niniejszym numerze.

Kolejny z tekstów stanowi analizę instrumentów, które posiadają polskie organy regulacyjne, aby szybko i efektywnie chronić konsumentów przed nielegalnymi treściami, produktami i usługami w Internecie. Polski ustawodawca, w ślad za legislatorem unijnym, dopuszcza współistnienie różnych regulacji, które mogą chronić konsumentów w Internecie, w tym: horyzontalne regulacje przewidziane w ustawie o ochronie konkurencji i konsumentów, ustawie o prawach konsumenta, ustawie o bezpieczeństwie produktów, ustawie o zwalczaniu nadużyć w komunikacji elektronicznej czy w przepisach. Kodeksu karnego. Zdaniem Autorki, tylko jednak pełna implementacja

rozporządzenie pt. Akt o usługach cyfrowych (AUC) zapewni pełną możliwość ochrony praw użytkowników funkcjonujących w środowisku cyfrowym. Tym bardziej więc szkoda, że w Polsce nadal nie doszło do uchwalenia nowelizacji ustawy o świadczeniu usług drogą elektroniczną, która miała zapewnić funkcjonowanie przepisów AUC w polskim systemie prawnym.

Wraz z rozpoczęciem stosowania Rozporządzenia UE nr 2024/900 w sprawie przejrzystości i targetowania reklamy politycznej w porządku prawnym Unii Europejskiej istnieją dwa reżimy transparentności reklamy online. Jeden wynika z horyzontalnego reżimu Aktu o usługach cyfrowych, a drugi właśnie z – wertykalnej – regulacji nr 2024/900, która ogranicza się wyłącznie do sektora reklamy politycznej. W praktyce, w szczególności z perspektywy dostawcy usług *hostingu*, mogą powstawać wątpliwości oraz problemy dotyczące wykładni i stosowania obu regulacji. Problematyce tej poświęcony jest kolejny z artykułów.

Po rozpoczęciu pełnego stosowania rozporządzenia nr 2022/2065 (Akt o usługach cyfrowych, AUC) w porządku prawnym Unii Europejskiej pojawił się nowy katalog obowiązków po stronie dostawców usług pośrednich, w tym dostawców usług hostingu. Jednym z nich jest obowiązek niezwłocznego informowania właściwych organów o podejrzeniu popełnienia przestępstwa zagrażającego życiu lub bezpieczeństwu osób, przewidziany w art. 18 ust. 1 AUC. Na szczególną uwagę zasługuje użycie przez prawodawcę unijnego sformułowania „może dojść do popełnienia przestępstwa", które wykracza poza dotychczasowe ujęcie obowiązku zawiadomienia znane prawu polskiemu, w szczególności art. 304 § 1 KPK. Rodzi to pytania o zakres nowego obowiązku oraz granice odpowiedzialności dostawców hostingu, zobowiązanych do podejmowania decyzji w warunkach niepewności co do kwalifikacji prawnej ujawnianych treści. Analizie poddano w związku z tym genezę tej regulacji, jej relację do krajowych przepisów procesowych oraz wybrane rozwiązania przyjęte w państwach członkowskich, a także oceniono, czy art. 18 ust. 1 AUC wprowadza jakościowo nowy standard prawny, czy też modyfikuje dotychczasowe mechanizmy zawiadamiania o przestępstwach.

W ostatnim z artykułów, Autor wyjaśnia kim jest legalny użytkownik bazy danych i jakie znaczenie ma ten status w praktyce – zwłaszcza gdy pojawia się pytanie, czy do korzystania z bazy danych zawsze potrzebna jest licencja. Autor opisuje dwa niezależne reżimy ochrony baz danych: prawo *sui generis*, które chroni przede wszystkim istotną część zawartości bazy danych oraz ochronę prawnoautorską, obejmującą sam twórczy dobór lub układ (strukturę) danych. Tekst porządkuje też konsekwencje tego podziału z perspektywy użytkownika – jak odrębne reżimy ochrony wpływają na prawne aspekty korzystania z baz danych oraz kiedy (i komu) przepisy ustawowe zezwalają na korzystanie z określonych elementów bazy danych, nawet w przypadku braku odpowiednich postanowień licencyjnych.

W niniejszym numerze Kwartalnika tradycyjnie już również przedstawiono aktualności legislacyjne, regulacyjne i orzecznicze dotyczące różnych obszarów prawa nowych technologii.

Życząc Państwu dobrej lektury, mam nadzieję, że zawarte w niniejszym numerze artykuły przyczynią się do lepszego zrozumienia problematyki prawnej w nich opisanej.

adw. *Xawery Konarski*
Redaktor Naczelny