Wprowadzenie

Szanowni Państwo,

W czasach dynamicznego rozwoju technologicznego, prawo staje przed wyjątkowymi wyzwaniami, które wymagają nowatorskich rozwiązań i dogłębnej refleksji nad ochroną praw i wolności obywateli, etycznymi implikacjami nowych technologii oraz sposobami regulacji cyfrowego świata. „Kwartalnik Prawa Nowych Technologii" ma na celu dostarczenie wieloaspektowej analizy problemów prawnych, które rodzą się na styku innowacji technologicznych i tradycyjnych zasad prawa. W niniejszym numerze koncentrujemy się na zagadnieniach cyberbezpieczeństwa i regulacji prawnych z tego obszaru. Każdy z przedstawionych artykułów podejmuje kluczowe kwestie związane z adaptacją prawa do szybko zmieniającej się rzeczywistości, dostarczając solidnej podstawy teoretycznej oraz wskazując praktyczne aspekty wdrażania regulacji.

Pierwszy artykuł, napisany przez *Eleezę Agopian* (wiceprezes ds. inicjatyw strategicznych w ICANN), analizuje problematykę dostępu do danych rejestracyjnych nazw domen w kontekście współczesnych regulacji prawnych, które koncentrują się na ochronie prywatności. Autorka wskazuje na złożoność procesu wyważania interesów: z jednej strony, dostęp do danych rejestracji jest kluczowy dla zapewnienia przejrzystości i odpowiedzialności w Internecie, szczególnie dla organów ścigania, badaczy cyberbezpieczeństwa i właścicieli praw własności intelektualnej. Z drugiej strony, zasady ochrony prywatności, szczególnie te wprowadzone przez RODO, znacząco ograniczają dostęp do informacji, uznawanych za dane osobowe, co w efekcie utrudnia dostęp do pełnych danych rejestracyjnych. W artykule podkreślono istotne działania ICANN mające na celu zachowanie równowagi pomiędzy prywatnością a dostępem do danych, takie jak wdrożenie narzędzia wyszukiwania danych rejestracyjnych oraz systemów takich jak RDRS (*Registration Data Request Service*), które oferują ujednoliconą, globalną platformę wspierającą kontrolowany dostęp do danych rejestracyjnych. Artykuł zarysowuje trwające wyzwania i rozwiązania ICANN w zakresie adaptacji do nowych regulacji wskazując, że proces wypracowywania stabilnych polityk dotyczących dostępu do danych rejestracyjnych jest długotrwały i wymaga odpowiedzi na stale zmieniające się wymogi prawne.

Z kolei artykuł „Cyberbezpieczeństwo – w kierunku redefinicji odpowiedzialności w cyberprzestrzeni", autorstwa *Katarzyny Chałubińskiej-Jentkiewicz*, odnosi się do lokalnych, polskich przepisów prawa dokonując analizy rozwoju pojęcia cyberbezpieczeństwa w kontekście zmieniających się wyzwań związanych z cyfryzacją. Autorka identyfikuje ewolucję cyberbezpieczeństwa z klasycznego pojmowania bezpieczeństwa jako „stanu braku zagrożenia" do dynamicznego procesu wymagającego ochrony nie tylko systemów teleinformatycznych, ale również relacji między użytkownikami i aspektów społecznych bezpieczeństwa informacji. Cyberprzestrzeń, jak słusznie zauważa autorka, staje się kluczowym elementem bezpieczeństwa narodowego, a jej rola wzrasta wraz z postępującą automatyzacją i uzależnieniem gospodarki i życia społecznego od rozwiązań cyfrowych. Cyberprzestrzeń przyciąga jednocześnie zorganizowane grupy przestępcze oraz stanowi narzędzie politycznych i wywiadowczych działań. W związku z tym cyberbezpieczeństwo nabiera interdyscyplinarnego charakteru, wymagając współpracy specjalistów z zakresu prawa, administracji, technologii i edukacji. Wskazano również na nowe wyzwania dla cyberbezpieczeństwa, w tym problem dezinformacji oraz potrzebę ochrony prywatności i retencji danych w świetle rozwoju technologii cyfrowych. Autorka podkreśla konieczność wypracowania jasnych zasad odpowiedzialności za naruszenia w cyberprzestrzeni, zwłaszcza w kontekście e-commerce, danych osobowych i cyfrowej tożsamości. Postuluje także redefinicję cyberbezpieczeństwa, wskazując na potrzebę uwzględnienia nie tylko aspektów technicznych, ale również społecznych i prawnych. Wydaje się, że zarówno definicje zawarte w NIS2, np. cyberzagrożeń, incydentu, a także te, które znajdują się w kolejnych projektach nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (CyberbezpU) zmierzają w kierunku rozszerzenia zakresu pojęcia cyberbezpieczeństwa.

Kolejny artykuł, dotyczący wpływu dyrektywy NIS2 na procedury zamówień publicznych, przygotowany przez *Agnieszkę Wachowską* oraz *Martę Pasztaleniec*, omawia pozornie wąskie zagadnienie relacji cyberbezpieczeństwa i zamówień publicznych. Autorki wskazują jednak na niezwykle istotny aspekt bezpieczeństwa systemów informacyjnych sfery publicznej. Dyrektywa NIS2 wprowadza bowiem nowe, istotne wymagania w zakresie cyberbezpieczeństwa, które mają zastosowanie zarówno do sektora prywatnego, jak i publicznego, obejmując kluczowe jednostki administracji publicznej. W odpowiedzi na te przepisy, projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa klasyfikuje szeroko rozumianą administrację publiczną jako podmioty kluczowe, co zobowiązuje je do stosowania zaawansowanych środków ochrony, zwłaszcza w obszarze zamówień publicznych. Jak słusznie wskazują autorki, główne zmiany dotykają zamówień z udziałem dostawców wysokiego ryzyka oraz procedur weryfikacji cyberbezpieczeństwa łańcucha dostaw. Autorki

podsumowują artykuł konkluzją, że nowe regulacje wzmacniają rolę cyberbezpieczeństwa w zamówieniach publicznych, nakładając na zamawiających obowiązek stosowania środków proporcjonalnych i związanych z przedmiotem zamówienia, w celu zapewnienia odpowiedniej ochrony sieci i systemów, szczególnie w kontekście wysokiego ryzyka.

W artykule „Nowe obowiązki sektora finansowego w świetle Digital Operational Resilience Act i projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa" ponownie poruszony został temat relacji tej ustawy do innych aktów prawnych. Autorzy – *Adrian Dulczewski* i *Radosław Nożykowski* omawiają znaczenie rozporządzenia DORA (Digital Operational Resilience Act) dla poprawy bezpieczeństwa cyfrowego sektora finansowego w Unii Europejskiej. Podkreślają, że w obliczu rosnących zagrożeń cybernetycznych UE dąży do ujednolicenia wymagań bezpieczeństwa cyfrowego, co ma kluczowe znaczenie dla stabilności gospodarki. Celem DORA jest zwiększenie odporności operacyjnej podmiotów finansowych, co wymaga od instytucji skutecznego zarządzania ryzykiem ICT, zgłaszania incydentów, regularnych testów bezpieczeństwa systemów oraz zaostrzenia wymagań wobec dostawców usług IT. Artykuł wskazuje na istotne zagadnienie: otóż DORA poszerza katalog regulowanych podmiotów, obejmując instytucje kredytowe, ubezpieczeniowe i dostawców usług kryptoaktywnych. Rozporządzenie wprowadza również obowiązek współpracy i wymiany informacji z regulatorami, co ma sprzyjać budowaniu cyberodporności na poziomie UE. Autorzy zwracają uwagę, że implementacja DORA wymaga nowelizacji polskich przepisów, zwłaszcza ustawy o krajowym systemie cyberbezpieczeństwa, aby sprostać nowym wymogom raportowania incydentów i zapewnienia zgodności z europejskimi regulacjami. W Polsce oznacza to m.in. obowiązek zgłaszania poważnych incydentów ICT do Komisji Nadzoru Finansowego oraz włączenie do regulacji nowych podmiotów kluczowych. Autorzy podkreślają, że wdrożenie DORA oznacza nie tylko konieczność szybkiej adaptacji ze strony podmiotów finansowych, lecz również potencjalne zmiany w rekomendacjach regulatorów, takich jak KNF.

Artykuł autorstwa *Joanny Wziątek-Ładosz* przedstawia z kolei szczegółową analizę zmian w polskich przepisach dotyczących cyberbezpieczeństwa, które są wdrażane w ramach dyrektywy NIS2 oraz rozporządzenia DORA. Jednym z kluczowych obszarów omówionych w artykule jest zmiana klasyfikacji podmiotów objętych regulacjami. Dotychczasowy podział na operatorów usług kluczowych, dostawców usług cyfrowych oraz podmioty publiczne zostaje zastąpiony nowymi kategoriami: podmiotami kluczowymi i ważnymi. Nowe przepisy nakładają również liczne obowiązki na firmy objęte regulacjami, takie jak wdrażanie proporcjonalnych środków technicznych i operacyjnych w zakresie cyberbezpieczeństwa, obowiązkowe zgłaszanie incydentów do CSIRT lub właściwego organu, a także informowanie odbiorców usług o zagrożeniach. Podmioty zobowiązane będą do stosowania certyfikowanych produktów i procesów oraz regularnego szkolenia kadry zarządzającej w zakresie zarządzania bezpieczeństwem informacji. Autorka podkreśla, że rozporządzenie wprowadza także nowe sankcje za nieprzestrzeganie przepisów. Dodatkowo, nowe regulacje zwiększają uprawnienia organów nadzorczych, które będą mogły prowadzić nadzór prewencyjny dla podmiotów kluczowych oraz stosować różnorodne środki nadzorcze, w tym kontrole i żądania dokumentacji. Specyficzne wymagania DORA dotyczące rynku finansowego, jako przepisy szczególne względem NIS2, wskazują na szczególną potrzebę zarządzania ryzykiem ICT w instytucjach finansowych, w tym testowania odporności operacyjnej oraz monitorowania współpracy z dostawcami. Przepisy DORA przewidują też wysokie kary pieniężne za brak zgodności, co podkreśla ich rygorystyczne podejście do bezpieczeństwa w sektorze finansowym. Autorka trafnie konkluduje, że pod kątem praktycznym, wdrożenie nowych wymogów wymaga dokładnej współpracy wewnątrz firm między działami prawnymi, IT, ryzyka i audytu. Rekomendowane działania obejmują m.in. audyty wstępne, opracowanie planów zarządzania ryzykiem i procedur monitorowania incydentów, a także szkolenia kadry kierowniczej. Zarządzanie cyberbezpieczeństwem staje się więc procesem dynamicznym, wymagającym stałej adaptacji i doskonalenia w odpowiedzi na zmieniające się zagrożenia oraz pojawiające się nowe regulacje.

Artykuł „Problemy z zakresem podmiotowym dyrektywy NIS2 na przykładzie dostawców usług zarządzanych oraz dostawców usług chmurowych", autorstwa *Agnieszki Wachowskiej* i *Konrada Basaja*, powraca do dyrektywy NIS2, wskazując na istotne trudności interpretacyjne wynikające z szerokiego zakresu podmiotowego nowej dyrektywy. Autorzy skupiają się na dostawcach usług zarządzanych (MSP) oraz usług chmurowych, podkreślając, że zawarte w dyrektywie definicje mogą prowadzić do objęcia regulacjami podmiotów, których działalność jedynie marginalnie lub incydentalnie wiąże się z sektorem ICT, co będzie skutkować nadmiernymi obciążeniami regulacyjnymi. Ma to znaczenie szczególnie w stosunku do mniejszych podmiotów. Podobne problemy pojawiają się przy definicji dostawców usług chmurowych, która obejmuje m.in. IaaS, PaaS, SaaS i NaaS. W porównaniu z poprzednią dyrektywą NIS, NIS2 znacznie rozszerza zakres regulacji, obejmując nowe sektory i wprowadzając kryterium wielkości przedsiębiorstw, przez co obejmuje nie tylko kluczowe, lecz również ważne sektory gospodarki. Co więcej, dyrektywa wprowadza zasadę samookreślenia, która oznacza, że przedsiębiorstwa muszą same ocenić, czy podlegają nowym przepisom. Autorzy wskazują, że taki mechanizm może być problematyczny, ponieważ dyrektywa odnosi się do definicji zawartych w wielu innych aktach prawnych UE, co komplikuje ustalenie, które podmioty są zobowiązane do wdrożenia regulacji. W podsumowaniu autorzy słusznie postulują, aby doprecyzować zakres dyrektywy NIS2, aby uniknąć nieproporcjonalnych obciążeń dla firm jedynie marginalnie związanych z sektorem ICT.

Cyber Resilience Act (CRA) to unijne rozporządzenie, które ma na celu wzmocnienie cyberbezpieczeństwa w Europie poprzez wprowadzenie wielu wymogów dla producentów, importerów oraz dystrybutorów produktów z elementami cyfrowymi, takich jak oprogramowanie i sprzęt komputerowy. Ten ważny temat porusza artykuł autorstwa *Szymona Sieniewicza* oraz *Małgorzaty Czubernat*. Jak wskazują autorzy, głównym założeniem CRA jest podniesienie poziomu ochrony cyfrowej na rynku unijnym. Aby osiągnąć ten cel, rozporządzenie nakłada obowiązki związane z eliminacją podatności, zapewnianiem regularnych aktualizacji oraz informowaniem użytkowników o zagrożeniach i wymaganiach bezpieczeństwa. CRA obejmuje szeroki zakres podmiotów działających na rynku produktów

cyfrowych, w tym producentów, importerów i dystrybutorów. Istnieją jednak pewne wyłączenia, np. dla produktów z sektorów takich jak medycyna, motoryzacja, lotnictwo, a także dla niektórych produktów *open-source*. Rozporządzenie przewiduje również specjalne zasady dla produktów krytycznych. Autorzy podkreślają, że rozporządzenie CRA jest także ściśle powiązane z regulacjami dotyczącymi sztucznej inteligencji (AI Act). Produkty cyfrowe uznane za systemy AI wysokiego ryzyka, które spełniają wymogi CRA, będą automatycznie uznawane za zgodne z wymogami cyberbezpieczeństwa przewidzianymi w AI Act. Organy nadzoru rynku będą odpowiedzialne za kontrolę zgodności produktów z nowymi wymogami, a także za nakładanie sankcji w przypadkach naruszeń. Rozporządzenie wejdzie w życie w 2026 r., obejmując początkowo obowiązki notyfikacyjne, a pełne wymagania zaczną obowiązywać około 2027–2028 r. Należy zgodzić się z autorami, że CRA będzie wymagało wprowadzenia nowych procedur i dostosowania produktów cyfrowych do wysokich standardów cyberbezpieczeństwa w UE.

Artykuł zamykający wydanie Kwartalnika, zatytułowany „Regulacyjne ramy operacyjnej odporności cyfrowej w sektorze finansowym – zagadnienia wybrane", autorstwa *Doroty Echaust-Przybytniak*, ponownie zwraca się w kierunku DORA (rozporządzenia UE 2022/2554). Koncentruje się na rosnącej liczbie cyberzagrożeń, jak ransomware i ataków socjotechnicznych, oraz na wpływie tych zjawisk na polski sektor finansowy, który mierzy się z ich coraz większą skalą. W artykule omówione są kluczowe wymogi DORA, które dotyczą zarządzania ryzykiem ICT, zarządzania incydentami oraz testowania odporności operacyjnej, w tym współpracy z zewnętrznymi dostawcami ICT. DORA nakłada na instytucje obowiązek wdrożenia szczegółowych procedur, takich jak regularne audyty, zarządzanie dostawcami ICT oraz opracowywanie planów ciągłości działania. Wnioski autorki wskazują, że wdrożenie DORA w Polsce będzie ewolucyjnym procesem, który zwiększy cyfrową odporność instytucji finansowych bez radykalnych zmian strukturalnych, co stanowi dobre podsumowanie skutków regulacji opisanych w bieżącym numerze Kwartalnika.

Zapraszam do lektury, która z pewnością wzbogaci wiedzę zarówno praktyków prawa, jak i badaczy zajmujących się technologiami cyfrowymi.

r.pr. *Artur Piechocki*