JOURNAL OF MODERN SCIENCE
1/65/2026
www.jomswsge.com
DOI: 10.13166/jms/217459

IZABELA OLEKSIEWICZ
Rzeszow University of Technology, Poland
ORCID iD: 0000-0002-1622-7467

RAMY POLITYKI CYBERBEZPIECZEŃSTWA UNII EUROPEJSKIEJ – ANALIZA WYBRANYCH ZMIAN PRAWNYCH

THE EUROPEAN UNION CYBERSECURITY POLICY FRAMEWORK - AN ANALYSIS OF SELECTED LEGAL DEVELOPMENTS

Abstract

Eskalacja cyberzagrożeń wpływa na aktualną politykę Unii Europejskiej w zakresie cyberbezpieczeństwa, co stanowi istotny element zarządzania kryzysowego państw członkowskich. Od momentu wybuchu wojny w Ukrainie w centrum zainteresowania Unii Europejskiej znalazły się zagadnienia dotyczące skutecznej ochrony cyberprzestrzeni przed działaniami dezinformacyjnymi. Wyrazem tego jest przyjęcie takich aktów prawnych, jak CRA, AI Act czy DORA. Analiza zmian prawnych od strony systemowej, jakie następują w polityce cyberbezpieczeństwa UE jest głównym celem tego artykułu. Podmiotem analizy badawczej jest UE, a przedmiotem – polityka cyberbezpieczeństwa i zmiany prawne, jakie następują. Należy przyjąć założenie, że podejście do tworzenia regulacji zapewniających bezpieczeństwo w cyberprzestrzeni na szczeblu unijnym i państwowym będzie ewoluowało. Istotne jest zatem tworzenie spójnych i transparentnych mechanizmów polityki cyberbezpieczeństwa określających determinanty wzajemnej pomocy w przypadku zaistnienia tzw. incydentów oraz wprowadzenie europejskich ram prawnych w tym zakresie. Jeżeli przyjmiemy, że ewolucja polityki cyfryzacji jest reakcją na wzrost niestabilności i zagrożeń w tym obszarze oraz brak istnienia odpowiednich mechanizmów i regulacji w tym zakresie to istotne jest, zatem tworzenie spójnych i transparentnych mechanizmów polityki cyberbezpieczeństwa określających determinanty wzajemnej pomocy w przypadku zaistnienia tzw. incydentów oraz wprowadzenie europejskich ram prawnych w tym zakresie. Głównym problemem badawczym jest wykazanie, jak istotnym elementem w obecnych regulacjach prawnych jest umiejętnie prowadzona polityka na poziomie unijnym, ponieważ ma to ogromne znaczenie dla bezpieczeństwa wewnętrznego samych państw członkowskich oraz całej UE.

Keywords: *European Union, AI, cyber threat, Keywords: cyber security, CRA, DORA*

Abstrakt

Eskalacja cyberzagrożeń wpływa na aktualną politykę Unii Europejskiej w zakresie cyberbezpieczeństwa, co stanowi istotny element zarządzania kryzysowego państw członkowskich. Od momentu wybuchu wojny w Ukrainie w centrum zainteresowania Unii Europejskiej znalazły się zagadnienia dotyczące skutecznej ochrony cyberprzestrzeni przed działaniami dezinformacyjnymi. Wyrazem tego jest przyjęcie takich aktów prawnych, jak CRA, AI Act czy DORA. Analiza zmian prawnych od strony systemowej, jakie następują w polityce cyberbezpieczeństwa UE jest głównym celem tego artykułu. Podmiotem analizy badawczej jest UE, a przedmiotem – polityka cyberbezpieczeństwa i zmiany prawne, jakie następują. Należy przyjąć założenie, że podejście do tworzenia regulacji zapewniających bezpieczeństwo w cyberprzestrzeni na

szczeblu unijnym i państwowym będzie ewoluowało. Istotne jest zatem tworzenie spójnych i transparentnych mechanizmów polityki cyberbezpieczeństwa określających determinanty wzajemnej pomocy w przypadku zaistnienia tzw. incydentów oraz wprowadzenie europejskich ram prawnych w tym zakresie. Jeżeli przyjmiemy, że ewolucja polityki cyfryzacji jest reakcją na wzrost niestabilności i zagrożeń w tym obszarze oraz brak istnienia odpowiednich mechanizmów i regulacji w tym zakresie to istotne jest, zatem tworzenie spójnych i transparentnych mechanizmów polityki cyberbezpieczeństwa określających determinanty wzajemnej pomocy w przypadku zaistnienia tzw. incydentów oraz wprowadzenie europejskich ram prawnych w tym zakresie. Głównym problemem badawczym jest wykazanie, jak istotnym elementem w obecnych regulacjach prawnych jest umiejętnie prowadzona polityka na poziomie unijnym, ponieważ ma to ogromne znaczenie dla bezpieczeństwa wewnętrznego samych państw członkowskich oraz całej UE.

Słowa kluczowe: *Unia Europejska, cyberzagrożenie, AI, cyberbezpieczeństwa, CRA, DORA*

Cyberbezpieczeństwo a cyberzagrożenie

Zapewnienie odpowiedniego poziomu bezpieczeństwa w cyberprzestrzeni to coraz ważniejsze wyzwanie. We współczesnym świecie, w którym technologia odgrywa coraz większą rolę, cyberbezpieczeństwo staje się systematycznie jednym z kluczowych obszarów bezpieczeństwa państwa (Rezolucja Parlamentu Europejskiego z dnia 10 czerwca 2021 r.). Pojęcie *cyberbezpieczeństwo* w wąskim ujęciu obejmuje jedynie ochronę systemów komputerowych, sieci i danych przed atakami cyfrowymi i tak też zostało ujęte w ustawie o krajowym systemie cyberbezpieczeństwa z 2018 r. (Ustawa z dnia 5 lipca 2018 r.). W art. 2 pkt 4 tej ustawy cyberbezpieczeństwo zdefiniowano jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Ustawa wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r.), co miało się przyczynić do lepszego funkcjonowania rynku wewnętrznego. Przełomem na tamtą chwilę było

zobowiązanie państw wchodzących w skład UE do wyznaczenia właściwych organów krajowych, punktów kontaktowych oraz zespołów odpowiedzialnych za cyberbezpieczeństwo, czyli CSIRT. Jest to sieć, która została utworzona na mocy niniejszej dyrektywy w celu zapewnienia sprawnej i skutecznej współpracy operacyjnej. Dodatkowo powołano także Grupę Współpracy mającą na celu wspieranie strategicznej współpracy, wymianę informacji między państwami oraz budowanie wzajemnego zaufania (Skoczylas, 2023, s. 123).

Warto podkreślić, że cyberbezpieczeństwo jest nie tylko kwestią techniczną, ale także społeczną i ekonomiczną. Cyfryzacja wszystkich obszarów życia współczesnego człowieka, powszechny dostęp do internetu, nieograniczony zasięg sieci komunikacyjnych sprzyjają bowiem powstawaniu kolejnych form zagrożeń. Są to już nie tylko zagrożenia związane ze złamaniem zabezpieczeń i nieuprawnionym dostępem do danych i informacji, ale także różne działania przestępcze, w tym przestępczość kryminalna, gospodarcza, narkotykowa, pedofilska, a także działania terrorystyczne. Bez odpowiedniej ochrony w tym zakresie, zarówno jednostki, jak i organizacje mogą ponieść poważne straty finansowe i reputacyjne. Pojmowanie cyberbezpieczeństwa jeszcze cały czas ewoluuje, stale się poszerzając. Wymaga ono niewątpliwie ciągłego zaangażowania i szczególnej uwagi ze strony wielu podmiotów (Żywucka-Kozłowska, Dziembowski, 2023, s. 125, Fehler, 2023, s. 42).

Ochronie zasobów cyfrowych i unikaniu skutków potencjalnych zagrożeń służy polityka cyberbezpieczeństwa. Definiuje ona sposoby korzystania z kont użytkowników i danych przechowywanych w systemie, zapewniając właściwą ochronę informacji instytucji. W każdej organizacji są informacje chronione, np. dane osobowe, informacje finansowe i informacje jawne, w tym informacje marketingowe (por.: Woszek, 2022, s. 208, Misiuk i in, s. 125). Dlatego też przedmiotem polityki bezpieczeństwa państwa jest również informacja znajdująca się w systemie teleinformatycznym. Celem polityki bezpieczeństwa informacyjnego jest opracowanie procedur i wymagań niezbędnych do zapewnienia właściwej ochrony informacji danego państwa bądź organizacji międzynarodowej, takiej jak Unia Europejska czy NATO. Używając pojęcia *polityka cyberbezpieczeństwa*, ustala się zbiór praw, reguł i wskazówek praktycznych, które określają takie kwestie, jak zasoby teleinformatyczne, w tym informacje wrażliwe, które są zarządzane, chronione i dystrybuowane w samej

organizacji i państwach członkowskich, w ich systemach teleinformatycznych (por.: Wyrok ETS z w sprawie C-176/03 Komisja p. Radzie).

Polityka ochrony cyberprzestrzeni państwa kierowana jest do wszystkich użytkowników cyberprzestrzeni w obrębie danego państwa i poza jego terytorium, w miejscach, gdzie funkcjonują jego przedstawiciele. Jej zadaniem jest zobowiązanie organów administracji rządowej do stworzenia systemu ochrony cyberprzestrzeni państwa, który będzie szybko reagował i zapobiegał powstaniu cyberataku, a w przypadku dojścia do tego zdarzenia potrafił sprawnie pokonać przeprowadzony atak cybernetyczny (Brzostek, 2023, s. 98–100).

Cyberbezpieczeństwo stanowi podstawowy składnik transformacji cyfrowej w ujęciu ponadnarodowym. Można powiedzieć, że zapewnienie bezpiecznej cyberprzestrzeni i bezpieczeństwa w cyberprzestrzeni stanowi wyzwanie w skali makro, jest problemem globalnym. Biorąc pod uwagę rosnącą liczbę cyberataków, należy zintensyfikować działania dotyczące tzw. współpracy transgranicznej. Koordynacja i konsolidacja działań w obszarze cyberbezpieczeństwa powinna być wprost proporcjonalna do poziomu cyberzagrożeń (Art. 2 Rozporządzenia 2019/881 w sprawie *cyberzagrożenia* oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób. Zob. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.Urz. UE L 151, s. 15) – dalej akt o cyberbezpieczeństwie).

Polityka cyberbezpieczeństwa państwa jest reakcją na zaistniałe zagrożenie, jakim jest ochrona jakiegoś wspólnego dobra (Janowski, 2012, s. 143). Dzisiaj niemal każda nielegalna działalność ma odzwierciedlenie w internecie. Globalny charakter internetu dał natomiast szansę ludziom na zmianę wymiaru komunikacji i aktywności życiowych. Cyberprzestrzeń jest obecnie postrzegana jako przestrzeń polityczno-społeczna, w której odbijają się te same problemy, co w świecie rzeczywistym. Cyberprzestępczość jest również odmianą przestępczości wykorzystującą możliwości technik cyfrowych i środowiska sieci

komputerowych (Oleksiewicz, Pomykała, 2024, s. 11). Przyczyną powstania polityki cyberbezpieczeństwa jest również brak odpowiednich mechanizmów i regulacji w tym zakresie, dlatego mamy tu do czynienia z procesem instytucjonalizacji. Cyberprzestępczość od klasycznej przestępczości odróżnia przede wszystkim element wirtualności (Malešević, 2017, s. 12–19).

Polityka cyberbezpieczeństwa definiuje sposoby korzystania z kont użytkowników i danych przechowywanych w systemie, zapewniając właściwą ochronę informacji instytucji (Andersson, 2017, s. 122). Jak już wcześniej wspomniano, w każdej organizacji występują informacje chronione, jak dane osobowe, informacje finansowe i informacje jawne, np. informacje marketingowe (Małecka, 2021, s. 73; zob. też: Szpor, 2021, s. 234). Polityka ochrony cyberprzestrzeni państwa kierowana jest do wszystkich użytkowników cyberprzestrzeni w obrębie danego państwa i poza jego terytorium, w miejscach, gdzie funkcjonują jego przedstawiciele. Jej zadaniem jest zobowiązanie organów administracji rządowej do stworzenia systemu ochrony cyberprzestrzeni państwa, który będzie szybko reagował i zapobiegał powstaniu cyberataku, a w przypadku dojścia do tego zdarzenia potrafił sprawnie pokonać przeprowadzony atak cybernetyczny (Skoczylas, 2024, s. 39–44).

Z uwagi na globalny trend cyfryzacji i jednoczesną intensyfikację cyberzagrożeń, nie dziwi zatem aktywność legislacyjna Unii Europejskiej przejawiająca się w zakresie tworzenia bądź nowelizacji aktów prawnych w dziedzinie cyberbezpieczeństwa (Skoczylas, 2023, s. 103). Przedmiotem wspólnego zainteresowania państw członkowskich Unii Europejskiej jest stworzenie skutecznej polityki cyberbezpieczeństwa umożliwiającej wzmocnienie odporności na cyberzagrożenia, które mogą spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku cyberataków. Cyberprzestrzeń stała się miejscem różnorodnych cyberzagrożeń, do których należą m.in. złośliwe oprogramowania typu *ransomware*, *malware cryptojacking*, ataki socjotechniczne (np. *phishing*, *smishing*), wyłudzenia finansowe, odmowa wykonania usługi czy dezinformacja. W ostatnich latach obserwuje się nasilenie cyberataków, np. *phishing* czy ataków typu DDoS. Działania dezinformacyjne z kolei stanowią domenę wojny hybrydowej ukraińsko-rosyjskiej.

NIS 2 a CRA

Kolejna dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 NIS 2 (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r.) została przyjęta w odpowiedzi na zdiagnozowane braki w dyrektywie NIS. Dyrektywa NIS 2 wprowadza podział na podmioty kluczowe i podmioty ważne większej liczby pomiotów, a także odnośnie do nowych mechanizmów nadzoru wprowadzono nadzór *ex ante i ex post*, w tym regularne audyty bezpieczeństwa, kontrole na miejscu oraz skany bezpieczeństwa. NIS 2 promuje współpracę i wymianę informacji na poziomie krajowym i unijnym poprzez grupę współpracy, sieć CSIRT, CYCLONe i europejską bazę danych (Chałubińska-Jentkiewicz, Nowikowska, 2024). Ponadto na podstawie decyzji państwa członkowskiego do podmiotów kluczowych mogą być zaliczone inne podmioty z tych sektorów lub podmioty, które opierając się na dyrektywie NIS zostały uznane za podmioty kluczowe. Należy jednak zwrócić uwagę, że art. 4 dyrektywy NIS 2 wskazuje, iż w przypadku istnienia przepisów sektorowych, które nakładają wymogi co najmniej równoważne do obowiązków, które są w niej przewidziane, pierwszeństwo w stosowaniu mają przepisy sektorowe, a dyrektywy NIS 2 nie stosuje się. Zestawienie najważniejszych zmian w dyrektywie NIS 2 opisano w tabeli 1.

Tabela 1. *Zestawienie najważniejszych zmian w NIS 2*

Podmioty kluczowe	**Podmioty ważne**
Nadzór ex ante i ex post	Nadzór ex post
Regularne i ukierunkowane audyty bezpieczeństwa	ukierunkowane audyty bezpieczeństwa
Skany bezpieczeństwa	Skany bezpieczeństwa
Wnioski o udzielenie dostępu do danych, dokumentów i informacji	Wnioski o udzielenie dostępu do danych, dokumentów i informacji
Audyty doraźne, np. po poważnym incydencie	brak

Źródło: opracowanie własne

Rozporządzenie CRA (Kolupaieva, Sheiko, Polozova, 2024, s. 89) ma stanowić *lex specialis* do NIS 2, a jego zakres podmiotowy obejmuje szeroki katalog podmiotów z elementami cyfrowymi, które zostaną wprowadzone na rynek wewnętrzny. Jego celem systemowym jest doprowadzenie do podniesienia i wzmocnienia poziomu odporności (cyberbezpieczeństwa) Unii Europejskiej na cyberzagrożenia przez nałożenie na producentów, dystrybutorów i importerów produktów z elementami cyfrowymi umieszczanych na rynku wewnętrznym, obowiązków regulacyjnych mających na celu wyeliminowanie podatności tych produktów. W art. 1 ust. 1 aktu CRA wskazano środki, które mają zwiększyć zdolności UE w obszarze wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty. W myśl art. 3 pkt 1 CRA za produkt z elementami cyfrowymi należy uznać produkt w postaci oprogramowania lub sprzętu komputerowego oraz powiązane z nim rozwiązania w zakresie zdalnego przetwarzania danych, w tym oddzielnie wprowadzone do obrotu komponenty oprogramowania lub sprzętu. Definicja produktu z elementami cyfrowymi co do zasady nie obejmie usług chmurowych, takich jak te świadczone w modelu oprogramowanie jako usługa (*SaaS*), chyba że świadczenie tej usługi będzie następowało w związku z używaniem produktu z elementami cyfrowymi, na potrzeby którego takie oprogramowanie zostało zaprojektowane i opracowane, a którego brak spowodowałby, że produkt z elementami cyfrowymi nie mógłby wykonywać jednej ze swych funkcji (motyw 12 preambuły CRA). CRA zakłada pewne wyłączenia przepisów rozporządzenia, które będą stosowane do określonych kategorii produktów, m.in. do wyrobów medycznych (zgodnie z art. 2 ust. 2 pkt a CRA, rozporządzenia nie stosuje się do produktów z elementami cyfrowymi, do których zastosowanie ma rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z 5.04.2017). W sprawie wyrobów medycznych zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG (Dz.Urz. L 117 z 5.05.2017, s. 1 ze zm.), w tym do diagnostyki *in vitro* (zgodnie z art. 2 ust. 2 pkt b CRA, rozporządzenia nie stosuje się do produktów z elementami cyfrowymi, do których zastosowanie ma rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 z 5.04.2017), pojazdów mechanicznych (zgodnie z art. 2 ust. 2 pkt c CRA, rozporządzenia

nie stosuje się do produktów z elementami cyfrowymi, do których zastosowanie ma rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/2144 z 27.11.2019). W sprawie wymogów dotyczących homologacji typu pojazdów silnikowych i ich przyczep oraz układów, komponentów i oddzielnych zespołów technicznych przeznaczonych do tych pojazdów, w odniesieniu do ich ogólnego bezpieczeństwa oraz ochrony osób znajdujących się w pojeździe i niechronionych uczestników ruchu drogowego, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/858 oraz uchylające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 78/2009, (WE) nr 79/2009 i (WE) nr 661/2009 oraz rozporządzenia Komisji (WE) nr 631/2009, (UE) nr 406/2010, (UE) nr 672/2010, (UE) nr 1003/2010, (UE) nr 1005/2010, (UE) nr 1008/2010, (UE) nr 1009/2010, (UE) nr 19/2011, (UE) nr 109/2011, (UE) nr 458/2011, (UE) nr 65/2012, (UE) nr 130/2012, (UE) nr 347/2012, (UE) nr 351/2012, (UE) nr 1230/2012 i (UE) 2015/166 (Dz.Urz. L 325 z 16.12.2019, s. 1 ze zm.), certyfikowanych produktów lotniczych (zgodnie z art. 2 ust. 3 CRA, przepisów rozporządzenia nie stosuje się do produktów z elementami cyfrowymi, które uzyskały certyfikację zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1139 z 4.07.2018). W sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i utworzenia Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego oraz zmieniającym rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 2111/2005, (WE) nr 1008/2008, (UE) nr 996/2010, (UE) nr 376/2014 i dyrektywy Parlamentu Europejskiego i Rady 2014/30/UE i 2014/53/UE, a także uchylającym rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 552/2004 i (WE) nr 216/2008 i rozporządzenie Rady (EWG) nr 3922/91 (Dz.Urz. L 212 z 22.08.2018, s. 1 ze zm.) oraz wyposażenia morskiego (zgodnie z art. 2 ust. 4 CRA, rozporządzenie nie ma zastosowania do urządzeń objętych zakresem dyrektywy Parlamentu Europejskiego i Rady 2014/90/UE z 23.07.2014. W sprawie wyposażenia morskiego i uchylającej dyrektywę Rady 96/98/WE (Dz.Urz. L 257 z 28.08.2014, s. 146 ze zm.), dla których Unia Europejska ustanowiła odrębne wymagania w zakresie cyberbezpieczeństwa w odpowiednich przepisach sektorowych. Przepisy CRA nie znajdą również zastosowania do produktów z elementami cyfrowymi, opracowanych wyłącznie na potrzeby bezpieczeństwa narodowego lub obronności ani do produktów specjalnie zaprojektowanych w celu przetwarzania informacji

niejawnych (Art. 2 ust. 7 CRA). CRA nie będzie miało również zastosowania do części zamiennych, jeśli są one identyczne z komponentami oryginalnego produktu z elementami cyfrowymi i wyprodukowane zgodnie ze specyfikacją tych komponentów, które mają zastąpić (Art. 2 ust. 6 CRA).

Warto zauważyć, że CRA jest kolejnym etapem harmonizacji przepisów prawa unijnego po NIS 2, gdzie to właśnie producenci są zobowiązani do zapewnienia zgodności produktów z unijnymi normami cyberbezpieczeństwa na każdym etapie cyklu życia produktu, co oznacza konieczność wdrożenia nowych procedur i standardów. Będzie istniała konieczność długoterminowego wsparcia i aktualizacji przez co najmniej pięć lat od wprowadzenia produktu na rynek.

Na chwilę obecną w przyjętych aktach prawa wtórnego jest identyczne rozumienie dwóch pojęć *incydentu* oraz *incydent w cyberbezpieczeństwie na dużą skalę*. Ponadto w istniejących aktach prawnych funkcjonuje termin *poważny incydent*, który jest definiowany w zależności od zakresu legislacyjnego i przedmiotu regulacyjnego na dwa różne sposoby. To, co jest wspólne dla tych definicji, to sposób ich ujęcia (przyczynowo-skutkowy) oraz podkreślenie, że istotą jest nieprawidłowe działanie systemu. Ewolucję pojęcia *incydent* w wybranych aktach UE zaprezentowano w tabeli 2. Z kolei warto zauważyć, że rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Rozporządzenie DORA), którego celem jest zwiększenie operacyjnej odporności cyfrowej podmiotów finansowych oraz uregulowanie świadczenia usług ICT na rynku finansowym (Dz.Urz. L 333 z 27.12.2022) nie posługuje się pojęciem *incydent* czy *poważny incydent*, lecz legislator ze względu na specyfikę zagrożeń w obszarze finansowym zdefiniował w tym akcie prawnym pojęcia *incydent związany z ICT* czy *poważny incydent związany z ICT*, co wynika po pierwsze z samej specyfiki usług finansowych i kontroli Europejskiego Systemu Nadzoru Finansowego. Po drugie, istnieje potrzeba powiązania elementu przyczynowo-skutkowego, jak to zostało dotyczas ujęte w NIS 2 czy CRA, z elementem zarządzania ryzykiem ICT w sektorze finansowym, mająca na celu ochronę integralności i efektywności rynku wewnętrznego. Warto zauważyć, że oprócz części wspólnej definicji mamy tutaj do czynienia z dodatkową przesłanką zdefiniowaną jako *zdarzenie lub*

seria powiązanych ze sobą zdarzeń nieplanowanych. Najprościej rzecz ujmując, w tak szeroką definicję ustawodawcy będą wpisywać się nie tylko cyberataki, ale również awarie systemów i inne zakłócenia technologiczne.

Tabela. 2. *Ewolucja pojęcia „incydent" w wybranych aktach UE*

NIS 2	CRA	Akt o cybersolidarności	DORA	AI
Incydent oznacza zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem;	**incydent** zgodnie z definicją zawartą w NIS II;	incydent zgodnie z definicją zawartą w NIS II	**incydent związany z ICT** oznacza pojedyncze, nieplanowane zdarzenie lub serię powiązanych ze sobą zdarzeń przez dany podmiot finansowy które naruszają bezpieczeństwo sieci i systemów informatycznych i mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych lub na usługi świadczone przez ten podmiot finansowy;	
	Incydent wywierający wpływ na bezpieczeństwo produktu z elementami cyfrowymi" oznacza incydent, który negatywnie wpływa lub może mieć negatywny wpływ na zdolność produktu z elementami cyfrowymi do ochrony dostępności, autentyczności, integralności lub poufności danych lub funkcji	**Poważny incydent** oznacza poważny incydent oznacza incydent, który powoduje zakłócenie o stopniu przekraczającym zdolność reagowania podmiotu Unii i CERT-UE lub który ma znaczący wpływ na co najmniej dwa podmioty Unii;	**poważny incydent związany z ICT** oznacza incydent związany z ICT o dużym negatywnym wpływie na sieci i systemy informatyczne, które wspierają krytyczne lub istotne funkcje podmiotu finansowego;	**Poważny incydent** oznacza nieprawidłowe działanie systemu AI, które prowadzą bezpośrednio lub pośrednio do któregokolwiek ze zdarzeń np.: a) śmierć osoby lub poważny uszczerbek na zdrowiu, b) poważne i nieodwracalne zakłócenia w zarządzaniu infrastrukturą krytyczną
„incydent w cyberbezpieczeństwie na dużą skalę" oznacza incydent, który powoduje zakłócenia na poziomie przekraczającym zdolność państwa członkowskiego do reagowania na ten incydent lub który wywiera znaczące skutki w co najmniej 2 państwach członkowskich;		**„incydent w cyberbezpieczeństwie na dużą skalę" oznacza incydent w cyberbezpieczeństwie na dużą skalę** zgodnie z definicją zawartą w NIS II;		
		„poważny incydent w cyberbezpieczeństwie" a) spowodował lub może spowodować dotkliwe zakłócenia operacyjne usług lub straty finansowe dla danego podmiotu; b) wpłynął lub jest w stanie wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe i niemajątkowe.	**incydent operacyjny lub incydent w zakresie bezpieczeństwa** związany z płatnościami oznacza nieplanowane zdarzenie lub serię powiązanych ze sobą zdarzeń przez podmioty finansowe, o których mowa w art. 2 ust. 1 lit. a)-d), związanych z ICT lub nie, **które mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych związanych** z płatnościami lub na świadczone przez dany podmiot finansowy usługi związane z płatnościami;	

Źródło: opracowanie własne

Rzeczą zupełnie odrębną jest stworzenie definicji *poważnego incydentu w cyberbezpieczeństwie* przez akt o cybersolidarności, *incydentu wywierającego wpływ na bezpieczeństwo produktu z elementami cyfrowymi*, a także *incydentu operacyjnego lub incydentu w zakresie bezpieczeństw* w rozporządzeniu DORA. Są to różne definicje, chociaż ze sobą powiązane ze względu na sam trzon, jakim jest słowo *incydent*. Pierwsza z nich dotyczy wirtualnej przestrzeni oraz możliwości poniesienia szkód oraz strat na skutek działań innego podmiotu czy osoby fizycznej. Druga dotyczy sytuacji, kiedy zmniejsza się wiarygodność produktu z elementami cyfrowymi na skutek zaistniałego zdarzenia. Trzecia z kolei związana jest z rynkiem finansowym i usługami świadczonymi przez podmioty finansowe, które mogą mieć negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych związanych z tymi usługami. Rozwój technologiczny generuje w UE i państwach członkowskich potrzebę dostosowania definicji i terminów prawnych odpowiadających różnym cyberzagrożeniom, które są spójne odnośnie do pojęcia *incydent* z terminologią przyjętą przez NIS. Jeżeli natomiast przyjrzymy się temu bardziej szczegółowo, to każdy akt prawny tworzy zgodnie z zasadą *lex specialis* szczegółowe normy prawne względem NIS 2, a tym samym konstruuje własne rozwiązania definicyjne.

CRA a rozporządzenie AI ACT

Artykuł 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13 czerwca 2024 r.) definiuje sztuczną inteligencję jako system maszynowy, który – aby osiągnąć cele wyraźne lub ukryte – wnioskuje na podstawie otrzymanych danych wejściowych, w jaki sposób generować wyniki, takie jak przewidywania, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne. Warto już tu podkreślić, że w założeniu legislatora różne systemy sztucznej inteligencji różnią się poziomem autonomii i adaptacyjności po wdrożeniu. Zgodnie z art. 2 ust. 3 CRA, przepisów rozporządzenia nie stosuje się do produktów z elementami cyfrowymi, które uzyskały certyfikację zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1139 z 4 lipca 2018 r. w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i utworzenia Agencji Unii Europejskiej ds. Bezpieczeństwa

Lotniczego oraz zmieniającym rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 2111/2005, (WE) nr 1008/2008, (UE) nr 996/2010, (UE) nr 376/2014 i dyrektywy Parlamentu Europejskiego i Rady 2014/30/UE i 2014/53/UE, a także uchylającym rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 552/2004 i (WE) nr 216/2008 i rozporządzenie Rady (EWG) nr 3922/91 (Dz.Urz. L 212 z 22.08.2018, s. 1 ze zm.).

Uczenie maszynowe może pomóc w wykrywaniu i identyfikowaniu zagrożeń w sieciach informatycznych, jednak jego wykorzystanie w dziedzinie cyberbezpieczeństwa niesie ze sobą pewne zagrożenia, ponieważ istnieje ryzyko ataku na system z wykorzystaniem wiedzy o działaniu wytrenowanego algorytmu (Bar, 2021, 10–13). Jest to kolejny przykład rozwiązania systemowego w UE, który ustanawia zharmonizowane przepisy dotyczące sztucznej inteligencji, a zarazem stanowi pierwszy na świecie kompleksowy system prawny dotyczący tej kwestii. Celem niniejszego aktu prawnego jest wspieranie innowacji, poprawa funkcjonowania rynku wewnętrznego (podobnie jak w CRA) przy jednoczesnym zapewnieniu wysokiego poziomu ochrony zdrowia, bezpieczeństwa oraz praw podstawowych. Jak widać, przepisy AI Act dotyczą bezpieczeństwa i ustanawiają zasady mające zapewnić bezpieczeństwo produktów i ograniczenie ryzyka związanego ze stosowaniem AI. Dlatego rozporządzenie o AI definiuje ramy umożliwiające zrozumienie ryzyka związanego z AI. Klasyfikuje systemy AI na podstawie ich potencjalnych ryzyk i dzieli je na różne kategorie w zależności od gromadzonych przez nie danych oraz decyzji lub działań podejmowanych na podstawie tych danych. Zobowiązania UE będą się różnić w zależności od kategorii wykorzystywanej AI. Twórcy aktu zmierzają do zrozumienia, jakie czynniki wpływają na podjęcie decyzji systemu AI, co pozwoli na bardziej skuteczną reakcję na potencjalne zagrożenia.

Jak wynika z CRA i AI Act, produkty z elementami cyfrowymi sklasyfikowane jako systemy sztucznej inteligencji wysokiego ryzyka, które spełnią zasadnicze wymogi nałożone przez CRA, będą uznawane za spełniające wymogi dotyczące cyberbezpieczeństwa określone w art. 15 AI Act, bez uszczerbku dla innych wymogów wskazanych w tym artykule i w zakresie, w jakim osiągnięcie poziomu ochrony określonego w tych wymogach wykazano w deklaracji zgodności UE wydanego na podstawie CRA (Art. 12 ust. 1 CRA).

Do produktów tych stosuje się odpowiednią procedurę oceny zgodności przewidzianą w art. 43 AI Act. Na zasadzie odstępstwa ważne produkty z elementami cyfrowymi, które podlegają procedurom oceny zgodności oraz produkty krytyczne z elementami cyfrowymi, które muszą uzyskać europejski certyfikat cyberbezpieczeństwa lub które w przypadku jego braku podlegają procedurom oceny zgodności i które są również sklasyfikowane jako systemy sztucznej inteligencji wysokiego ryzyka, zgodnie z art. 6 AI Act będą podlegać procedurom oceny zgodności przewidzianym w CRA (Art. 12 ust. 3 CRA) Organami nadzoru rynku w rozumieniu CRA dla produktów z elementami cyfrowymi sklasyfikowanych także jako systemy sztucznej inteligencji wysokiego ryzyka będą organy wyznaczone do celów AI Act (Art. 52 ust. 14 CRA).

Zgodnie z CRA każde państwo członkowskie będzie musiało wyznaczyć co najmniej jeden organ nadzoru rynku w celu zapewnienia skutecznego wdrażania rozporządzenia (Art. 52 ust. 2 CRA). Organy te będą odpowiadać za weryfikację, czy produkty z elementami cyfrowymi spełniają wymagania określone w rozporządzeniu. Będą miały także prawo nakazywania podjęcia działań naprawczych lub wycofywania produktów z rynku, zależnie od poziomu ryzyka (Wysokińska, 2021, s. 81). Dodatkowo organ nadzoru może wymagać od producentów usunięcia niezgodności związanych z umieszczeniem oznakowania CE, sporządzeniem lub brakiem deklaracji zgodności UE, kompletnością i dostępnością dokumentacji technicznej i umieszczeniem numeru identyfikacyjnego jednostki notyfikowanej zaangażowanej w procedurę zgodności, jeśli jest to wymagane (Banasiński, Rojszczak, 2020, s. 323–325; Nowak, 2020, s. 103–113).

Akt o cybersolidarności

Unijny akt o cybersolidarności (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/38 z dnia 19 grudnia 2024 r.), który wszedł w życie 4 lutego 2025 r. zyskuje na znaczeniu w kontekście pogłębiających się konfliktów cybernetycznych, przyjmujących postać wojny cyfrowej, tzw. cyberwojny. Celem tego rozporządzenia jest zwiększenie zdolności UE w zakresie wykrywania cyberzagrożeń i incydentów oraz przygotowywania się i reagowania na tego typu zagrożenia, m.in. Europejskiego Systemu Cyberostrzeżeń.

Jednocześnie cybersolidarność (Radzińska, 2014, s. 58–68) ma złagodzić skutki innych cyberzagrożeń będących następstwem napięć geopolitycznych (Art. 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/694 z 29 kwietnia 2021 r.). Niemniej jednak kluczową rolę odgrywają dwie zasadnicze kwestie, tj. stworzenie europejskiej tarczy cyberbezpieczeństwa i mechanizmu cyberkryzysowego. Europejska tarcza cyberbezpieczeństwa to wzajemnie połączona ogólnoeuropejska infrastruktura centrów monitorowania bezpieczeństwa, w skład której wchodzą krajowe centra monitorowania bezpieczeństwa oraz transgraniczne centra monitorowania bezpieczeństwa. Głównym celem wdrożenia europejskiej tarczy cyberbezpieczeństwa jest przetwarzanie danych o cyberzagrożeniach i cyberincydentach. W akcie o cybersolidarności ustanawia system oceny i przeglądu cyberincydentów, który proceduralnie jest zbliżony do NIS 2. Można zauważyć, że zamierzeniem twórców było osiągnięcie kolejnego poziom cyberbezpieczeństwa produktów (tym razem z elementami cyfrowymi). W założeniu ma to ułatwić funkcjonowanie i spójność z dyrektywą NIS 2 oraz wzmocnić bezpieczeństwo całego łańcucha dostaw.

Warto zwrócić uwagę na samo rozwiązanie systemowe, które ma polegać na wzmocnieniu odporności UE na poważne zagrożenia cyberbezpieczeństwa oraz przygotowaniu się na krótkoterminowe skutki poważnych incydentów w cyberbezpieczeństwie oraz na dużą skalę, aby złagodzić je w myśl art. 222 TL (Oleksiewicz, 2021, s. 173). Ponadto mechanizm ma charakter transgranicznej ochrony zarządzania przed cyberzagrożeniami i ma to stanowić *zwiększenie wspólnego cyberbezpieczeństwa i cyberobrony przed szkodliwymi szachowaniami i aktami agresji w cyberprzestrzeni* (Miszczak, 2024, s. 152–153). W art. 13 Aktu o solidarności cybernetycznej wprowadzono warunki ubiegania się o wsparcie w reagowaniu na incydenty i w natychmiastowym usuwaniu skutków incydentów. Ustalono, że właściwy w tym zakresie będzie tryb wnioskowy, a w przypadku istnienia równocześnie wielu wniosków pod uwagę wzięta zostanie hierarchia ważności wniosków, zgodnie z kryteriami określonymi w art. 14 ust. 2 Aktu o solidarności cybernetycznej. Mając to na uwadze, należy przyznać, że cybersolidarność stanowi podstawę wspólnych unijnych ram cyberbezpieczeństwa, a usługi reagowania na incydenty mają świadczyć zaufani dostawcy uczestniczący w unijnej rezerwie cyberbezpieczeństwa (dostawcy z sektora prywatnego).

Wnioski

Cyberincydenty są trudne do przewidzenia, gdyż ich cechą jest transgraniczność i fluktuacja, w związku z tym jest więc konieczna bliska współpraca pomiędzy sektorami publicznym i prywatnym. Tego rodzaju incydenty mogą również wpływać negatywnie na działalność gospodarczą, prowadząc do znacznych strat finansowych, podważając zaufanie użytkowników czy wyrządzając poważne szkody gospodarce.

Rozporządzenie CRA ma ułatwić dostawcom infrastruktury cyfrowej spełnienie wymogów dotyczących łańcucha dostaw określonych w NIS 2 przez zapewnienie, aby produkty z elementami cyfrowymi wykorzystywane przez tych dostawców do świadczenia usług były opracowywane w sposób bezpieczny oraz aby dostawcy w odpowiednim czasie otrzymywali aktualizacje zabezpieczeń tych produktów. Akt o cyberbezpieczeństwie ma zwiększyć bezpieczeństwo produktów, usług i procesów ICT przez wprowadzenie dobrowolnych europejskich ram certyfikacji cyberbezpieczeństwa. Jego oddziaływanie na podmioty z branży będzie pośrednie, w sytuacji gdy zostaną wydane ramy odnoszące się do przedmiotu działania przedsiębiorstwa (Dygnatowski, 2020, s. 309–320). Akt ten nie zawiera natomiast przepisów nakładających obowiązki bezpośrednio na podmioty prywatne.

DORA, podobnie jak i CRA, ma więc służyć wzmocnieniu odporności cyfrowej podmiotów sektora finansowego, poprzez wprowadzenie zunifikowanych zasad zarządzania różnymi rodzajami zewnętrznych dostawców usług ICT, w tym dostawcami usług chmurowych, oprogramowania, usług analizy danych i dostawców usług przetwarzania danych. Jest instrumentem, który skupia się na poprawie standardów w sektorze usług finansowych odnośnie do zarządzania ryzykiem związanym z cyberbezpieczeństwem. Jego celem jest wprowadzenie spójnych regulacji obejmujących wszystkie instytucje finansowe i zabezpieczenie przed poważnymi zakłóceniami operacyjnymi (Por. Bryski, Kurek-Sobieraj, 2025, s. 50–53).

Obecnie za kluczową determinantę cyberbezpieczeństwa uznaje się solidarność cybernetyczną, która ma się stać skutecznym narzędziem cyberobrony i wzmocnić wspólne unijne zdolności w kwestii cyberbezpieczeństwa. Cybersolidarność powinno się rozpatrywać przez pryzmat działań faktycznych,

jak np. współdziałanie w materii wykrywania i monitorowania zagrożeń cyberbezpieczeństwa, wypracowanie wspólnych mechanizmów reagowania na cyberzagrożenia czy udzielanie wzajemnej pomocy finansowej. W obrębie solidarności cybernetycznej nowe zmiany obejmują zarówno poziom normatywny, wynikający z obowiązujących regulacji prawnych, jak i faktyczny – urzeczywistniający się w przypadku faktycznego zaistnienia zagrożenia. Państwa członkowskie będą zatem zobowiązane nie tylko do solidarności deklarowanej, ale przede wszystkim praktycznej (Radzińska, 2014, s. 63–64). Nie sposób nie zgodzić się z B. Krzanem, który wskazuje, że solidarność może stanowić wyraźny sygnał akcentujący wspólne, spójne podejście w ramach Unii Europejskiej (Krzan, 2022, s. 645). Zważywszy na aktualne cyberzagrożenia, takie jak m.in. dezinformacja czy cyberwojna, *globalna cyberprzestrzeń może ulec fragmentacji*, a to może mieć negatywne skutki dla bezpieczeństwa europejskiego w postaci ograniczenia zdolności wywiadowczych państw członkowskich UE. Cybersolidarność jest zatem warunkiem *sine qua non* bezpieczeństwa całej Unii Europejskiej.

References

Andersson, J. i in. (2017). Envisioning European Defence: Five Futures. *Chaillot Paper*, 137.

Banasiński, C., Rojszczak, M. (red.), (2020). *Cyberbezpieczeństwo.* Wydawnictwo Wolters Kluwer Polska, s. 323–325.

Bar, G. (2021). Zakazane użycie sztucznej inteligencji., *ABI Expert*, s. 10–13.

Bryski, J., Kurek-Sobieraj, J. (2025). *Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz.* Wydawnictwo C.H. Beck.

Brzostek, A. (2023). Cyberbezpieczeństwo w administracji publicznej – aspekty prawne. *Zeszyty Prawnicze*, 23, s. 98–100.

Chałubińska-Jentkiewicz, K., Nowikowska, M. (2024). Podmioty zaangażowane w politykę zapewnienia bezpieczeństwa sieci i systemów informatycznych w świetle dyrektywy NIS 2 (cz. 2). *Cybersecurity and Law*, s. 5–24.

Dygnatowski, S. (2020). Cyberbezpieczeństwo jako fundament bezpieczeństwa infrastruktury krytycznej w kontekście współczesnych zagrożeń. *Journal of KONBiN*, 50(4), s. 309–320.

Fehler, W. (2023). *Leksykon bezpieczeństwa informacyjnego*, Warszawa: Wydawnictwo UPH.

Kolupaieva, I., Sheiko, I., Polozova, T. (2024). Digital Transformation in the Context of Sustainable Development of European Countries. *Problems of Sustainable Development*, 19(1), s. 89–102.

Krzan, B. (2022). *Zasada solidarności w prawie Unii Europejskiej*. W: A. Kozłowski (red.), *Rządy prawa jako wartość uniwersalna. Księga jubileuszowa Profesora Krzysztofa Wójtowicza* (s. 633–645), Wrocław: E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

Janowski, J. (2012). *Cybernetyzacja prawa*. W: E. Galewska, S. Kotecka (red.), *X-lecie CBKE. Księga pamiątkowa z okazji 10-lecia Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego* (s. 143–156). Wydawnictwo: OFICYNA PRAWNICZA.

Małecka, A. (2021). Polityka cyberbezpieczeństwa Unii Europejskiej na początku trzeciej dekady XXI wieku. *Rocznik Bezpieczeństwa Międzynarodowego*, s. 73–89.

Malešević, S. (2017). *Terrorism. In The Rise of Organised Brutality: A Historical Sociology of Violence*. Cambridge University Press.

Misiuk, A. i in. (2021), *Encyklopedia bezpieczeństwa wewnętrznego*. Warszawa.

Miszczak, K. (2024). Strategiczny Kompas Unii Europejskiej. Większe bezpieczeństwo i skuteczniejsza obrona UE – plan działań do 2030 r. *Politeja*, 1(88/1), s. 152–153.

Nowak, W. (2020). *Specyfika zagrożeń w cyberprzestrzeni*. W: C. Banasiński, M. Rojszczak (red.), *Cyberbezpieczeństwo* (s. 103–113),.Wydawnictwo: Wolters Kluwer Polska.

Oleksiewicz, I., Pomykała, M. (2024). *Cyberbezpieczeństwo jako nowy wymiar współczesnego bezpieczeństwa państwa*. W: Oleksiewicz, I., Pomykała, M. (red.), *Zagrożenia i wyzwania bezpieczeństwa w cyberprzestrzeni*, Rzeszów: Oficyna Wydawnicza Politechniki Rzeszowskiej.

Oleksiewicz, I. (2021). *Ochrony cyberprzestrzeni. Polityka – strategia – prawo*. Warszawa: Wydawnictwo Naukowe PWN.

Radzińska, J. (2014). Solidarność: definicja i konteksty. *Etyka*, 48, s. 58–68.

Skoczylas, D. (2023). Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe. *Prawo w Działaniu. Sprawy Karne*, 53, s. 97–113.

Skoczylas, D. (2023). *Krajowy System Cyberbezpieczeństwa*. Wydawnictwo C.H. Beck Sp. z o.o.

Skoczylas, D. (2024). Wzmocnienie zdolności Unii Europejskiej w zakresie cyberbezpieczeństwa – cybersolidarność w kontekście cyberzagrożeń, *Europejski Przegląd Sądowy*, 12, s. 39–44.

Szpor, G. (2021). The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland. *Review of European and Comparative Law*, 46(3), s. 219–235. Woszek, S. (2022). Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej. *Przegląd Bezpieczeństwa Wewnętrznego*, 14(27), s. 198–217.

Wysokińska, Z. (2021). A Review of the Impact of the Digital Transformation on the Global and European Economy. *Comparative Economic Research. Central and Eastern Europe*, 24(3), s. 75–91.

Żywucka-Kozłowska, E., Dziembowski, R. (2023). Wokół definicji cyberbezpieczeństwa. *Cybersecurity and Law*, 2(10), s. 123–132.

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L z 2016 r., nr 194, s. 1).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.Urz. UE L 333, s. 80).

Orzeczenie Sądu Okręgowego w Paryżu z 20 października 2000 r. w sprawie Anit-Semitism LICRA v. Yahoo Inc., sygn. akt RG 00/05308.

Rezolucja Parlamentu Europejskiego z dnia 10 czerwca 2021 r. w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę (2021/2568(RSP)) (Dz.U.UE. C 67. 81, 8.02.2022).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG (Dz.Urz. L 117 z 5.05.2017, s. 1 ze zm.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z 29 kwietnia 2021 r. ustanawiające program *Cyfrowa Europa* oraz uchylającego decyzję (UE) 2015/2240 (Dz.Urz. UE L 166, s. 1).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U.UE. L 333 z 27.12.2022).

Rozporządzenie 2019/881 w sprawie *cyberzagrożenie* oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób.

Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.Urz. UE L 151, s. 15).

Rozporządzenie nie ma zastosowania do urządzeń objętych zakresem dyrektywy Parlamentu Europejskiego i Rady 2014/90/UE z 23 lipca 2014 r. w sprawie wyposażenia morskiego i uchylającej dyrektywę Rady 96/98/WE (Dz.Urz. L 257 z 28.08.2014, s. 146 ze zm.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/38 z dnia 19 grudnia 2024 r. ustanawiające środki służące wzmocnieniu solidarności i zdolności Unii do wykrywania zagrożeń i incydentów cybernetycznych, przygotowywania się na nie i reagowania na nie oraz zmieniające rozporządzenie (UE) 2021/694 (Akt o solidarności cybernetycznej) (Dz.U. L 2025.38 z 15.01.2025).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (Akt w sprawie sztucznej inteligencji), Dz.Urz. L z 12.07.2024, s. 1689.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, (t.j. Dz.U. z 2023 r., poz. 913 ze zm.).

Wyrok ETS z w sprawie C-176/03 Komisja p. Radzie.