Maciej Rogalski*

POLITYKA UNII EUROPEJSKIEJ WOBEC CHIN – UREGULOWANIA W ZAKRESIE DOSTAWCÓW INFRASTRUKTURY 5G

DOI: 10.26399/meip.4(79).2023.31/m.rogalski

WPROWADZENIE

Od kilku lat na całym świecie, w tym w Europie, trwa budowa sieci służących do świadczenia usług telekomunikacyjnych w technologii 5G[1]. Technologia ta pozwala na nieporównywalnie większe przesyłanie danych niż te dotychczas stosowane. Będzie to rewolucja technologiczna w zakresie świadczenia usług telekomunikacyjnych, pozwalająca na szybszy rozwój różnych nowych usług i rozwiązań, jak pojazdy autonomiczne czy operacje chirurgiczne na odległość. Technologia ta będzie oczywiście stosowana nie tylko w różnych sektorach najnowszych dziedzin gospodarki, ale także przez struktury państwowe, wojsko czy policję. Na świecie infrastrukturę do technologii 5G dostarcza zaledwie kilku producentów: w Europie Nokia i Ericsson, a poza nią chiński Huawei i ZTE oraz koreański Samsung. W ostatnich kilku latach kwestia sprzętu do budowy infrastruktury 5G pochodzącego z Chin stała się przedmiotem bardzo ożywionej dyskusji pomiędzy USA a Chinami. Ze strony USA podnoszone są wątpliwości, czy sprzęt ten zapewnia bezpieczeństwo w korzystaniu z usług 5G przez obywateli i podmioty na świecie, w tym w Unii Europejskiej (UE), z uwagi na możliwy wpływ na ich producentów ze strony chińskiego rządu. Po raz pierwszy więc pojawiła się kwestia zapewnienia

* Uczelnia Łazarskiego, e-mail: maciej@rogalski.waw.pl, ORCID: 0000-0003-4366-642X.

1 Technologia mobilna piątej generacji obejmująca standard systemu, który musi spełniać założenia Międzynarodowego Związku Telekomunikacyjnego (ang. ITU), oznaczona jako IMT-2020.

bezpieczeństwa korzystania z usług telekomunikacyjnych w związku z tym, z jakiego kraju pochodzi producent, którego sprzęt będzie wykorzystywany do budowy infrastruktury służącej do świadczenia usług w określonej technologii, w tym przypadku 5G.

Prowadzona pomiędzy USA i Chinami dyskusja spowodowała, że w UE poza już obowiązującymi uregulowaniami ochrony sieci komunikacji elektronicznej[2] przyjęto nowe dokumenty, które odnoszą się bezpośrednio do bezpieczeństwa infrastruktury i usług świadczonych w określonej technologii, czyli 5G. 26 marca 2019 r. Komisja Europejska (KE) przyjęła Zalecenia (UE) 2019/534 w sprawie cyberbezpieczeństwa sieci 5G, C/2019/2335 (Zalecenia)[3]. Grupa Współpracy ds. Sieci i Systemów Informatycznych (NISCG)[4] przygotowała raport z 9 października 2019 r., *EU coordinated risk assessment of the cybersecurity of 5G networks*, który zawierał analizę zagrożeń dla sieci 5G. W listopadzie 2019 r. ENISA w raporcie *ENISA Threat Landscape for 5G Networks*[5] przedstawiła katalog możliwych zagrożeń dla sieci 5G. 29 stycznia 2020 r. został opublikowany przez NISCG, przygotowany we współpracy z KE i ENISA, raport zatytułowany: *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures* (5G Toolbox[6]).

W artykule przeanalizowane zostanie wdrożenie tych wymagań pod względem formy prawnej regulacji. Celem tej analizy jest udzielenie odpowiedzi na pytanie, czy uzasadnione jest na obecnym etapie przyjętych uregulowań dotyczących HRV i ich wdrażania uchwalanie jednolitych unijnych przepisów

---

[2] Zob. dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającą Europejski kodeks łączności elektronicznej (wersja przekształcona) („EKŁE"), Dz. Urz. UE L Nr 321, dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014, i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (tekst mający znaczenie dla EOG) („NIS 2"), Dz. Urz. UE L Nr 333; rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa Sieci i Informacji) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013, Dz. Urz. UE L Nr 151 („Rozporządzenie 2019/881").

[3] *Commission Recommendation on the Cybersecurity of 5G networks*, C(2019) 2335 final, Dz. U. UE L 88, 29.3.2019, s. 42–47.

[4] Network and Information System Cooperation Group.

[5] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks [dostęp: 30.09.2023].

[6] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures [dostęp: 25.08.2023].

w tym zakresie. W celu weryfikacji tezy o braku konieczności przyjmowania takich przepisów zastosowana zostanie głównie metoda formalno-dogmatyczna oraz komparatystyczna.

1. 5G Toolbox

5G Toolbox to opracowanie w zakresie kalkulacji ryzyk i zarządzania nimi, stosowane w korporacjach. Ma charakter techniczny i organizacyjny. Określa potencjalne obszary ryzyk oraz środki zaradcze. Środki zaradcze dzieli na środki strategiczne (*strategic measures*) i techniczne (*technical measures*). Wśród ośmiu środków zaradczych wymienia działania polegające na ocenie ryzyk związanych z konkretnym dostawcą i „zastosowanie restrykcji" w stosunku do dostawcy uznanego za „dostawcę wysokiego ryzyka" (*high risk vendor* – HRV), włączając w to „niezbędne wyłączenia" w zakresie kluczowych zasobów (*key assets*) w celu skutecznego zarządzania ryzykiem. W dalszej części 5G Toolbox podaje się przykłady *key assets*: *core network functions* czy *access network functions*. Ryzyka związane z danym dostawcą są ogólnie opisane, bez określenia jasnych i sprawdzalnych kryteriów. Wśród kilku zdań poświęconych temu ryzyku wskazuje się m.in. na możliwość „wywierania wpływu na danego dostawcę przez dane państwo, zgodnie z jego systemem prawnym, w celu uzyskania dostępu do kluczowych elementów sieci".

29 stycznia 2020 r. KE przedstawiła komunikat COM (2020)50 *Secure 5G deployment in the EU – Implementing the EU Toolbox*[7], w którym zatwierdziła wnioski wynikające z 5G Toolbox i podkreśliła znaczenie ich skutecznego i szybkiego wdrożenia oraz wezwała państwa członkowskie do podjęcia konkretnych kroków w celu ich wprowadzenia. NISCG, przy wsparciu KE oraz ENISA, przygotował w lipcu 2020 r. *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity*[8]. 10 grudnia 2020 r. ENISA opublikowała wytyczne w celu zapewnienia wspólnego podejścia do bezpieczeństwa sieci i usług łączności elektronicznej (*Guideline on Security Measures under the EECC*) (Wytyczne)[9]. Uzupełnieniem Wytycznych jest

[7] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64481 [dostęp: 22.09.2023].

[8] https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity [dostęp: 24.08.2023].

[9] https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc/ [dostęp: 20.08.2023].

5G Supplement – to the Guideline on Security Measures under the EECC (5G Supplement)[10], który koncentruje się na cyberbezpieczeństwie sieci 5G.

W grudniu 2020 r. Komisja dokonała przeglądu skutków Zalecenia z 26 marca 2019 r., a w szczególności oceniła osiągnięte etapy wdrożenia[11]. Wnioski z tego przeglądu doprowadziły do określenia kluczowych celów i konkretnych działań na potrzeby przyszłych skoordynowanych prac na poziomie UE w zakresie cyberbezpieczeństwa 5G, określonych w unijnej strategii bezpieczeństwa cybernetycznego na dekadę cyfrową. Wśród nich wskazano w szczególności na potrzebę zapewnienia zbieżnych krajowych podejść do ograniczania ryzyka w całej UE[12]. Zalecenia zostały przygotowane także przez Europejski Trybunał Obrachunkowy (the European Court of Auditors, ECA) w specjalnym raporcie ze stycznia 2022 r.[13] ECA zwrócił uwagę, że państwa członkowskie zastosowały rozbieżne podejścia do stosowania sprzętu od dostawców wysokiego ryzyka lub zakresu ograniczeń. Wskazał na potrzebę dostarczenia dalszych wskazówek lub działań wspierających dotyczących kluczowych elementów zestawu narzędzi UE w zakresie cyberbezpieczeństwa 5G, takich jak kryteria oceny dostawców 5G i klasyfikowania ich jako dostawców wysokiego ryzyka oraz monitorowanie i składanie sprawozdań z wdrażania środków bezpieczeństwa przez państwa członkowskie[14].

W swoim zaleceniu z 9 grudnia 2022 r. Rada zwróciła się do agencji NISCG o przyspieszenie trwających prac nad oceną ryzyka bezpieczeństwa cybernetycznego i odporności europejskich infrastruktur i sieci komunikacyjnych[15]. 15 czerwca 2023 r. został opublikowany przygotowany przez NISCG

---

[10] https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc/ [dostęp: 20.09.2023].

[11] *Commission Report on the impacts of the Commission Recommendation 2019/534 of 26 March 2019 on the Cybersecurity of 5G networks*, SWD(2020) 357 final, https://data.consilium.europa.eu/doc/document/ST-14354-2020-INIT/en/pdf [dostęp: 14.08.2023].

[12] *Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade*, *JOIN (2020)18*, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018 [dostęp: 14.09.2023].

[13] *Special Report. 5G roll-out in the EU: delays in deployment of networks with security issues remaining unresolved*, https://www.eca.europa.eu/lists/ecadocuments/sr22_03/sr_security-5g-networks_en.pdf [dostęp: 13.07.2023].

[14] https://data.consilium.europa.eu/doc/document/ST-9616-2022-INIT/en/pdf [dostęp: 13.07.2023].

[15] *Council Recommendation 15623/22 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, 9 December 2022*, https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity [dostęp: 26.07.2023].

Second report on Member States' Progress in implementing the EU Toolbox on 5G Cybersecurity (raport z 15 czerwca 2023 r.)[16]. Przedstawiono w nim stan wdrażania różnych środków z zestawu narzędzi UE, w tym środków z 5G Toolbox, na szczeblu krajowym i unijnym od pierwszego sprawozdania z postępów z lipca 2020 r. Zgodnie ze środkami strategicznymi wyznaczonymi jako SM03 w 5G Toolbox państwa członkowskie powinny wyznaczać ramy prawne, aby władze krajowe mogły oceniać profil ryzyka dostawców i na tej podstawie stosować ograniczenia (wyłączenia). Zaleca dokonanie oceny profilu ryzyka dostawców i zastosowanie ograniczeń, w tym niezbędnych wyłączeń, aby skutecznie ograniczać ryzyko dla wrażliwych i krytycznych aktywów. Według tego raportu odpowiednie uregulowania prawne, które dają władzom krajowym uprawnienia do wprowadzania ograniczeń dla dostawców wysokiego ryzyka, wprowadziła większość krajów. Trzy kraje są w trakcie wdrażania lub przygotowania, a trzy pozostałe nie podjęły w tym zakresie działań. W obszarze wprowadzania ograniczeń na HRV spośród tych krajów 10 krajów wdrożyło restrykcje na HRV, trzy pracują nad wdrażaniem do ustawodawstwa krajowego, a 14 nie wdrożyło żadnych restrykcji. W raporcie wskazano, że w przypadku braku działań ze strony państw członkowskich co do wdrażania zestawu narzędzi w UE KE rozważy dalsze działania mające na celu zwiększenie odporności rynku wewnętrznego, w tym zbadanie możliwych ścieżek legislacyjnych, bez uszczerbku dla istniejącego prawodawstwa w krajach, które wdrożyły już ograniczenia zgodnie z 5G Toolbox lub w oparciu o niego, przy poszanowaniu kompetencji praw państw członkowskich w zakresie bezpieczeństwa narodowego. W tym zakresie uwzględnione zostaną również wyniki bieżącej oceny ryzyka cyberbezpieczeństwa infrastruktur i sieci komunikacyjnych[17].

2. Stan regulacji dotyczących HRV w krajach członkowskich UE

5G Toolbox przewiduje środki strategiczne, techniczne i działania wspierające. W ramach środków strategicznych przewidziany jest środek oznaczony jako SM03, polegający na ocenie ryzyka dostawców sprzętu telekomunikacyjnego, a w przypadku uznania ich za HRV na zastosowaniu odpowiednich ograni-

16 https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity [dostęp: 28.08.2023].

17 Ibidem.

czeń dla nich. Poszczególne kraje członkowskie UE przyjęły różne sposoby wdrożenia tego środka. W większości przyjęły na poziomie krajowym odpowiednie regulacje prawne, które przewidują wdrożenie w całości 5G Toolbox lub tylko jego pewnych założeń albo też innych rozwiązań w omawianym zakresie. W celu udzielenia odpowiedzi na pytanie o potrzebę wprowadzenia ewentualnie jednolitych regulacji na poziomie UE dotyczących HRV niezbędne jest dokonanie analizy dotychczasowego prawnego sposobu wdrożenia 5G Toolbox w poszczególnych krajach członkowskich. Chodzi o ustalenie, czy w ogóle zostały uchwalone w poszczególnych krajach przepisy i jaką mają formę. Odnośnie do formy prawnej istotne jest w szczególności ustalenie, czy regulacje miały charakter przepisów rangi ustawowej lub dekretów. Przepisy tej rangi są bowiem przepisami powszechnie obowiązującymi w danym kraju. Nie chodzi więc o wytyczne, zalecenia czy opracowania pochodzące od podmiotów, które nie mają kompetencji do uchwalania (wydawania) przepisów rangi ustawowej czy dekretów, np. zalecenia wydawane przez organ regulacyjny w danym kraju.

W raporcie z 15 czerwca 2023 r. jest mowa o przyjęciu przez większość krajów UE „legislative measures giving national authorities the powers to perform an assessment of suppliers and issue restrictions”[18]. W raporcie tym nie ma definicji określenia *legislative measures*. Wynika jednak z niego, że przyjęto szerokie rozumienie *legislative measures*, a więc jakichkolwiek regulacji prawnych, które umożliwiłyby wdrożenie 5G Toolbox. W tym szerokim ujęciu są to więc nie tylko ustawy czy dekrety z mocą ustaw, ale także akty wykonawcze do ustaw, a ponadto wszelkie regulacje wydawane podczas rozdysponowywania w trybie aukcyjnym częstotliwości 5G, zalecenia i wytyczne organów regulacyjnych czy rekomendacje innych organów lub zespołów doradczych.

Zgodnie jednak z art. 288 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE)[19] do aktów prawnych UE zalicza się: rozporządzenia, dyrektywy, decyzje, zalecenia i opinie. Rozporządzenie ma zasięg ogólny. Wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich. Dyrektywa wiąże każde państwo członkowskie, do którego jest kierowana, w odniesieniu do rezultatu, który ma być osiągnięty, pozostawia jednak organom krajowym swobodę wyboru formy i środków. Decyzja wiąże w całości,

[18] Zob. *Second report on Member States' Progress in implementing the EU Toolbox on 5G Cybersecurity*, https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity, s. 22 [dostęp: 26.07.2023].

[19] Dz. Urz. UE 2012 C 326/47.

ale gdy wskazuje adresatów, wiąże tylko tych adresatów. Zalecenia i opinie nie mają mocy wiążącej. Akt prawny UE powinien więc być rozporządzeniem lub dyrektywą. Nie może być zaleceniem lub opinią, gdyż są one niewiążące. Z kolei decyzje wiążą tylko ich adresatów.

W związku z tym, w aspekcie zapowiedzi możliwych dalszych działań legislacyjnych, polegających na przyjęciu w UE przepisów, które zobowiązywały wszystkie państwa członkowskie do wykluczenia sprzętu HRV z możliwości zakupu oraz jego osunięcia z infrastruktury operatorów[20], należy założyć, że tego typu regulacje nie mogłyby mieć formy 5G Toolbox, czyli pewnych zaleceń (rekomendacji), ale musiałby posiadać formę odpowiedniego unijnego aktu prawnego, który jest wiążący dla państw członkowskich. Zakładając więc, że ewentualne regulacje unijne musiałyby mieć postać rozporządzenia lub dyrektywy, należałoby przeanalizować, w ilu obecnie krajach członkowskich UE znajdują się regulacje podobnej rangi legislacyjnej, jak rozporządzenia czy dyrektywy, a więc odpowiednio ustawy, dekrety i akty wykonawcze do ustaw lub dekretów. W Raporcie z 15 czerwca 2023 r. wskazano bowiem, że ewentualne rozwiązania legislacyjne będą wdrażane „bez uszczerbku dla obowiązującego prawodawstwa, które wprowadziło już ograniczenia zgodnie z 5G Toolbox lub na jego podstawie oraz przy jednoczesnym poszanowaniu kompetencji państw członkowskich w zakresie regulacji bezpieczeństwa”[21].

Analiza w zakresie formy prawnej regulacji pokazuje, że uregulowania dotyczące HRV zostały wprowadzone w formie ustaw, dekretów lub aktów wykonawczych w 16 krajach (Austria[22], Cypr[23], Czechy[24], Dania[25], Estonia[26], Finlandia[27],

20 *Second report on Member States' Progress…*, s. 6, 22, 24.

21 Ibidem, s. 24.

22 Telekommunikationsgesetz 2021, StF: Bundesgesetzblatt („BGBI”) I Nr 190/2021.

23 Ο περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών Νόμος, 12 Αυγούστου 2020, Αριθμός 4770.

24 Dekret o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, hlášení kybernetické bezpečnosti požadavky a likvidace dat, dne 21. května 2018, č. 82/2018 Sb.

25 Lov om leverandørsikkerhed i den kritiske teleinfrastruktur, LOV nr 1156 af 08/06/2021.

26 Elektroonilise side seadus, RT I 2004, 87, 593.

27 Laki sähköisistä viestintäpalveluista, 7.11.2014/917. Viestintäverkon kriittisiä osia koskeva asetus, TRAFICOM/161584/03.04.05.00/2020.

Francja[28], Niemcy[29], Irlandia[30], Włochy[31], Łotwa[32], Litwa[33], Luksemburg[34], Niderlandy[35], Rumunia[36], Szwecja[37]), a więc w większości krajów UE. Spośród tych 16 krajów w 10 były to ustawy, w dwóch dekrety, a w czterech regulacje znalazły się zarówno w ustawie, jak i w aktach wykonawczych do nich. Pod względem przedmiotowym, czyli w jakiego rodzaju aktach prawnych (jaką pro-

[28] Loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, LOI n° 2019-810 du 1er août 2019. Code des postes et des communications électroniques.

[29] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021 (BGBI. Teil I Nr 25). Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG), vom 14. August 2009 (BGBl. I S. 2821). Das Telekommunikationsgesetz vom 23. Juni 2021 (BGBl. I S. 1858). Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG) Version 2.0. Herausgeber: Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn.

[30] Electronic Communications Security Measures.

[31] Decreto-Legge 15 marzo 2012, n. 21. Norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonche' per le attivita' di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni (12G0040). Decreto-Legge 21 settembre 2019, n. 105. Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica ((e di disciplina dei poteri speciali nei settori di rilevanza strategica)) (19G00111). Decree-Law 21 September 2019, n. 105. Urgent provisions on the perimeter of national cyber security ((and on the regulation of special powers in sectors of strategic importance)) (19G00111).

[32] Informācijas tehnoloģiju drošības likums,Latvijas Vēstnesis, 178, 10.11.2010. MK noteikumi Nr.100 Pieņemti 2011.gada 1.februārī Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība, Latvijas Vēstnesis, 25, 15.02.2011. MK noteikumi Nr.442 Pieņemti 2015.gada 28.jūlijā, Kārtība, kādā nodrošina informācijas un komunikācijas tehnoloģiju sistēmu atbilstību minimālajām drošības prasībām, Latvijas Vēstnesis, 149, 03.08.2015.

[33] Lietuvos Respublikos elektroninių ryšių įstatymas, 2004 m. balandžio 15 d. Nr. IX-2135.

[34] Loi du 17 décembre 2021 portant transposition de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen et portant modification de la loi modifiée du 30 mai 2005 portant: 1) organisation de l'Institut Luxembourgeois de Régulation; 2) modification de la loi modifiée du 22 juin 1963 fixant le régime des traitements des fonctionnaires de l'État.

[35] Besluit veiligheid en integriteit telecommunicatie, Geldend van 01-03-2020.

[36] Legea nr. 163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice şi de comunicaţii de interes naţional şi condiţiile implementării reţelelor 5G, Monitorul Oficial, Partea I nr. 590 din 11 iunie 2021.

[37] Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, v znení účinnom k Lag om elektronisk kommunikation (2022-482).

blematykę regulujących) znajdowały się postanowienia dotyczące HRV, były to w większości krajowe regulacje dotyczące sfery prawa komunikacji elektronicznej, wprowadzane przeważnie z związku z implementacją EKŁE. Drugim miejscem zamieszczania tych regulacji były odpowiednie regulacje krajowe poświęcone cyberbezpieczeństwu, a trzecim specjalnie przyjęte, poświęcone HRV, akty prawne.

3. Potrzeba wprowadzenia jednolitych regulacji unijnych

W raporcie z 15 czerwca 2023 r.[38] wskazano, że KE rozważa wprowadzenie jednolitych regulacji unijnych dla HRV. W związku z tym należy uwzględnić kilka istotnych elementów. Przede wszystkim, jak już to zostało zastrzeżone we wspomnianym raporcie, należy uwzględnić, że część krajów wprowadziła już do swoich przepisów regulacje dotyczące HRV, oparte na postanowieniach 5G Toolbox. W przypadku przyjęcia jednolitych regulacji unijnych musiałyby one m.in. spełniać wymagania UE w zakresie zagwarantowania uczestnikom tych postępowań ochrony ich podstawowych praw w tym postępowaniu, w szczególności prawa do sądu poprzez możliwość zaskarżenia wydanych decyzji w takim postępowaniu[39], w tym także tymczasowego, do czasu rozpoznania sprawy przez sąd wstrzymania ich wykonalności[40].

Według raportu z 15 czerwca 2023 r. spośród państw członkowskich, w których obowiązują lub przygotowywane są ramy regulacyjne, 17 państw członkowskich wprowadziło lub wprowadzi podejście *ex ante*, umożliwiające zakazanie wdrażania sprzętu 5G[41], a 10 państw członkowskich skorzystało z tych uprawnień, aby nałożyć na MNO obowiązek ograniczenia lub wykluczenia dostawców uznanych za HRV z ich sieci 5G, np. Dania, Szwecja, Estonia, Łotwa i Litwa. W trzech państwach członkowskich decyzje dotyczące dostawców lub sprzętu wysokiego ryzyka są podejmowane na podstawie wniosków MNO[42] o wdrożenie sprzętu 5G. Ograniczenia dotyczą krytycznego sprzętu sieciowego w co najmniej sześciu państwach członkowskich. W pozostałych

---

38 https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity, s. 24 [dostęp: 28.08.2023].

39 Por. P. Hofmański, A. Wróbel, *Artykuł 6* [w:] *Konwencja o ochronie praw człowieka i podstawowych wolności. Tom I. Komentarz do artykułów 1–18*, red. L. Garlicki, CH Beck, Warszawa 2010, SIP Legalis, pkt 36–37.

40 Por. P Daniel, *Ochrona tymczasowa w przepisach p.p.s.a. w świetle prawa unijnego*, „Zeszyty Naukowe Sądownictwa Administracyjnego" 2011, nr 5, s. 36 i n.

41 *Second report on Member States' Progress…*, s. 7–8.

42 Mobile Network Operator.

czterech państwach członkowskich treść decyzji jest poufna, a ich dokładny zakres nie jest znany[43]. W co najmniej ośmiu państwach członkowskich jeden lub kilku operatorów przeszło od jednego z dwóch dostawców nieposiadających siedziby w UE (Huawei lub ZTE) do dostawców z siedzibami w UE (Ericsson lub Nokia). W niektórych przypadkach zmiany te zostały wprowadzone przed podjęciem decyzji o ograniczeniach dla HRV lub w państwach członkowskich, w których nie podjęto jeszcze takich decyzji. Z drugiej strony, w co najmniej dwóch państwach członkowskich jeden operator zmienił dostawcę z pochodzącego z UE na dostawcę spoza UE. W pozostałych przypadkach operatorzy nie wybrali jeszcze swoich dostawców sprzętu do budowy sieci niezbędnej do świadczenia usług 5G[44]. W przypadku przyjęcia jednolitych regulacji unijnych powstanie kwestia relacji przyjętych regulacji unijnych do przepisów obowiązujących już w krajach członkowskich UE. Spowodować to może szereg niejasności i wątpliwości wynikających z tego, że w tym samym zakresie przedmiotowym występują zarówno regulacje unijne, jak i krajowe. Rozwiązaniem tego problemu mogłoby być przyjęcie zasady, że regulacje unijne obowiązują tylko w tym zakresie, który nie jest uregulowany przez prawo krajowe, ale z kolei mogłoby to być sprzeczne z zasadą pierwszeństwa prawa unijnego przed krajowym[45].

Nawet w przypadku niektórych krajów, gdzie nie wprowadzono przepisów ustawowych, w praktyce jednak zastosowano ograniczenia dla HRV. Przykładem może być Grecja, gdzie operatorzy (COSMOTE, Wind Hellas) wybrali do budowy infrastruktury 5G dostawcę europejskiego[46]. Podobnie w Belgii, gdzie Rada Bezpieczeństwa Narodowego Belgii stwierdziła, że HRV nie powinni być częścią „rdzenia" przyszłej sieci telekomunikacyjnej 5G i mogą stanowić maksymalnie 35% całej sieci. Ich obecność nie powinna być również dozwolona w niektórych wrażliwych obszarach, np. w pobliżu terenów

---

43 *Second report on Member States' Progress…*, s. 8.

44 European Court of Auditors, Special Report 03/2022, p. 16–40, https://www.eca.europa.eu/en/publications?did=60614 [dostęp: 20.08.2023].

45 Zob. K. Wójtowicz, *Zasady stosowania prawa wspólnotowego w państwach członkowskich Unii Europejskiej*, Warszawa 2003, s. 120; D. Kornobis-Romanowska, *Kompetencje wspólnotowe sądów krajowych – przegląd zagadnień*, [w:] *Stosowanie prawa wspólnotowego w prawie wewnętrznym z uwzględnieniem prawa polskiego*, red. D. Kornobis-Romanowska, Warszawa 2004, s. 23; T. Wasilewski, *Stosunek wzajemny. Porządek międzynarodowy, prawo międzynarodowe, europejskie prawo wspólnotowe, prawo krajowe*, Toruń 2009, s. 172–174.

46 https://www.ericsson.com/en/press-releases/2020/12/ericsson-brings-5g-to-greece-with-wind-hellas; https://www.cosmote.gr/cs/otegroup/en/nea_ependysh_yphresion5g.html [dostęp: 24.09.2023].

wojskowych[47]. Działający w Belgii operatorzy (Orange, Proximus) wybrali dostawcę europejskiego do budowy sieci 5G w Belgii[48]. Podobnie w Portugalii, gdzie funkcjonuje Rada ds. Bezpieczeństwa, utworzona w ramach the Cross-sector Safety and Security Communications (CSSC), która jest organem doradczym premiera. W maju 2023 r. Rada ta wskazała na ryzyka ze strony dostawców sprzętu do budowy sieci 5G pochodzących z krajów, które nie są członkiem UE, NATO[49] lub OECD[50] i w których rządy mogą wpływać na przedsiębiorstwa z siedzibą w tych krajach, a które to przedsiębiorstwa prowadzą działalność w krajach trzecich. Rada ds. Bezpieczeństwa w Portugalii przedstawiła plan wykluczenia lub zastosowania ograniczeń w korzystaniu ze sprzętu uznanego za wysoce ryzykowny w sieci 5G. Portugalski regulator rynku telekomunikacyjnego ANACOM[51] będzie odpowiedzialny za realizację postanowień Rady, a terminy będą ustalane indywidualnie dla każdego przypadku. Z kolei w październiku 2020 r. Bułgaria podpisała porozumienie z USA w sprawie bezpieczeństwa szybkich sieci szerokopasmowych, które także może być wykorzystywane dla wprowadzenia ograniczeń dla HRV[52].

Zauważyć również należy, że dalsze zaostrzanie wymagań w stosunku do przedsiębiorców komunikacji elektronicznej będzie miało także miejsce w ramach wdrażania dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148, Dz. Urz. UE. L Nr 333 (dyrektywa NIS 2). Dyrektywa ta zapewnia NISCG we współpracy z Komisją i ENISA możliwość przeprowadzania w obszarze ICT[53] skoordynowanych ocen ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw[54]. W następstwie wezwania unijnych ministrów ds. telekomunikacji do wzmocnienia zdolności UE w zakresie

47 https://www.hln.be/ihln/belgie-zet-huawei-niet-aan-de-deur~abb1615c/?referer=https%3A%2F%2Fwww.brusselstimes.com%2F [dostęp: 24.09.2023].

48 https://www.reuters.com/article/us-orange-nokia-security-5g-idUSKBN26U0YY?taid=5f804d3d8911f900016cdeea&utm_campaign=trueAnthem:+Trending+Content&utm_medium=trueAnthem&utm_source=twitter [dostęp: 24.09.2023].

49 North Atlantic Treaty Organisation.

50 Organisation for Economic Cooperation and Development.

51 Autoridade Nacional de Comunicações.

52 https://www.dw.com/en/us-signs-5g-security-deal-with-bulgaria-north-macedonia-and-kosovo/a-55381594 [dostęp: 24.09.2023].

53 Information and Communication Technologies.

54 *Council conclusions on ICT supply chain security, 13664/22, 17 October 2022*, https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/en/pdf [dostęp: 2.09.2023].

cyberbezpieczeństwa[55] państwa członkowskie w ramach grupy współpracy ds. bezpieczeństwa sieci i informacji prowadzą obecnie wraz z KE i ENISA oraz w ścisłej współpracy z Organem Europejskich Regulatorów Łączności Elektronicznej (BEREC)[56] ocenę ryzyka dotyczącą bezpieczeństwa cybernetycznego i odporności europejskich infrastruktur i sieci komunikacyjnych. Wynikiem tych prac będzie sformułowanie zaleceń potencjalnie obejmujących wszystkie części sieci 5G i wszystkie rodzaje sieci (stacjonarne i mobilne). Warto także wskazać, że w Unijnej Strategii Cyberbezpieczeństwa na Dekadę Cyfrową[57] w zakresie cyberbezpieczeństwa 5G jako jeden z podstawowych celów wskazuje się „zapewnienie zbieżnych podejść krajowych w celu skutecznego ograniczania ryzyka w całej UE". Chodzi więc o zapewnienie nie tyle dokładnie takich samych (poprzez prowadzenie jednolitych regulacji na poziomie UE), ale zapewnienie zbieżnych podejść na poziomie poszczególnych krajów członkowskich UE do skutecznego ograniczania ryzyka w całej UE.

Podsumowanie

Analiza stanu regulacji w poszczególnych krajach członkowskich UE wskazuje, że w szeregu z nich wprowadzono już regulacje dotyczące HRV oparte na postanowieniach 5G Toolbox. Z kolei w niektórych krajach, gdzie nie wprowadzono w wewnętrznych regulacjach prawnych przepisów ustawowych dotyczących HRV, w praktyce zastosowano wobec nich ograniczenia. Wymagania prawne dla HRV przewidziane są także w dyrektywie NIS 2 i dotyczą bezpieczeństwa łańcucha dostaw. Nie wydaje się więc konieczne, na obecnym etapie regulacji w poszczególnych krajach członkowskich faktycznego wdrażania ograniczeń dla HRV oraz stanu świadczenia usług telekomunikacyjnych w oparciu o technologie 5G, przyjmowanie jeszcze nowych, jednolitych unijnych regulacji w zakresie dostawców wysokiego ryzyka.

---

55 *Informal meeting of the Telecommunications Ministers, Nevers Call to Reinforce the EU's Cybersecurity Capabilities*, *9 March 2022*, https://www.consilium.europa.eu/en/meetings/tte/2022/03/08-09/ [dostęp: 1.08.2023].

56 Body of European Regulators for Electronic Communications.

57 *Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020)18*, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018 [dostęp: 11.10.2023].

Bibliografia

Daniel P., *Ochrona tymczasowa w przepisach p.p.s.a. w świetle prawa unijnego*, „Zeszyty Naukowe Sądownictwa Administracyjnego" 2011, nr 5.

Hofmański P., Wróbel A., *Artykuł 6*, [w:] *Konwencja o ochronie praw człowieka i podstawowych wolności. Tom I. Komentarz do artykułów 1–18*, red. L. Garlicki, Warszawa 2010.

Kornobis-Romanowska D., *Kompetencje wspólnotowe sądów krajowych – przegląd zagadnień*, [w:] *Stosowanie prawa wspólnotowego w prawie wewnętrznym z uwzględnieniem prawa polskiego*, red. D. Kornobis-Romanowska, Warszawa 2004.

Wasilewski T., *Stosunek wzajemny. Porządek międzynarodowy, prawo międzynarodowe, europejskie prawo wspólnotowe, prawo krajowe*, Toruń 2009.

Wójtowicz K., *Zasady stosowania prawa wspólnotowego w państwach członkowskich Unii Europejskiej*, Warszawa 2003.

Źródła internetowe [dostęp: październik–grudzień 2023]

Commission Recommendation on the Cybersecurity of 5G networks, C(2019) 2335 final, Dz. U. UE L 88, 29.3.2019

https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64481

https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

https://www.enisa.europa.eu/publications/guideline-on-security-measures--under-the-eecc/

https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc/

Commission Report on the impacts of the Commission Recommendation 2019/534 of 26 March 2019 on the Cybersecurity of 5G networks, SWD(2020) 357 final, https://data.consilium.europa.eu/doc/document/ST-14354-2020-INIT/en/pdf

Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, *JOIN (2020)18*, https://eur--lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018

Special Report. 5G roll-out in the EU: delays in deployment of networks with security issues remaining unresolved, https://www.eca.europa.eu/lists/ecadocuments/sr22_03/sr_security-5g-networks_en.pdf

https://data.consilium.europa.eu/doc/document/ST-9616-2022-INIT/en/pdf
Council Recommendation 15623/22 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, 9 December 2022; https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity
https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity
Second report on Member States' Progress in implementing the EU Toolbox on 5G Cybersecurity, https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity
https://www.ericsson.com/en/press-releases/2020/12/ericsson-brings-5g-to-greece-with-wind-hellas https://www.cosmote.gr/cs/otegroup/en/nea_ependysh_yphresion5g.html
https://www.hln.be/ihln/belgie-zet-huawei-niet-aan-de-deur~abb1615c/?referer=https%3A%2F%2Fwww.brusselstimes.com%2F
https://www.reuters.com/article/us-orange-nokia-security-5g-idUSKBN26U0YY?taid=5f804d3d8911f900016cdeea&utm_campaign=trueAnthem:+Trending+Content&utm_medium=trueAnthem&utm_source=twitter
https://www.dw.com/en/us-signs-5g-security-deal-with-bulgaria-north-macedonia-and-kosovo/a-55381594
Council conclusions on ICT supply chain security, 13664/22, 17 October 2022, https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/en/pdf
Informal meeting of the Telecommunications Ministers, Nevers Call to Reinforce the EU's Cybersecurity Capabilities, *9 March 2022*, https://www.consilium.europa.eu/en/meetings/tte/2022/03/08-09/
Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN (2020)18, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018

Polityka Unii Europejskiej wobec Chin – uregulowania w zakresie dostawców infrastruktury 5G

Streszczenie

Od kilku lat trwa proces budowy sieci służących do świadczenia usług telekomunikacyjnych w technologii 5G, która będzie wykorzystywana w różnych sektorach najnowszych dziedzin gospodarki, a także stosowana przez struktury państwowe. Na świecie infrastrukturę do technologii 5G dostarcza zale-

dwie kliku producentów: w Europie Nokia i Ericsson, a poza Europą chiński Huawei i ZTE oraz koreański Samsung. W ostatnich kilku latach kwestia dostarczania sprzętu do budowy infrastruktury 5G pochodzącego z Chin stała się przedmiotem ożywionej dyskusji pomiędzy USA a Chinami. Ze strony USA podnoszone są wątpliwości, czy sprzęt ten zapewnia bezpieczeństwo w korzystaniu z usług 5G przez obywateli i podmioty na świecie, w tym w Unii Europejskiej (UE), z uwagi na możliwy wpływ na ich producentów ze strony chińskiego rządu. Prowadzona między USA i Chinami dyskusja spowodowała, że w UE przyjęto szereg zaleceń w zakresie cyberbezpieczeństwa 5G, w tym *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures* (5G Toolbox). Sformułowano w nich określone zalecenia dotyczące tzw. dostawców wysokiego ryzyka (HRV). W oparciu o te zalecenia część krajów UE wprowadziła regulacje krajowe dotyczące HRV. Z uwagi na różne tempo przyjmowania tych regulacji w poszczególnych krajach UE i odmienny sposób ich wdrażania i egzekwowania wdrożonych już przepisów formułowane są postulaty przyjęcia jednolitej regulacji w UE w zakresie HRV, która obowiązywałaby wszystkie kraje UE. Artykuł analizuje, czy uzasadnione jest na obecnym etapie przyjętych uregulowań dotyczących HRV uchwalanie jednolitych unijnych przepisów w tym zakresie.

Słowa kluczowe: dostawcy wysokiego ryzyka, 5G Toolbox, cyberbezpieczeństwo, infrastruktura telekomunikacyjna

EU Policy Towards China: Regulations for 5G Infrastructure Vendors

Abstract

The process of building networks for the provision of telecommunications services using 5G technology has been ongoing for several years, and will be used in various sectors of the newest industries, as well as in state structures. In the world, infrastructure for 5G technology is provided by only a few manufacturers. In Europe, Nokia and Ericsson, and outside Europe, Chinese Huawei and ZTE and Korean Samsung. In the last few years, the issue of supplying equipment for the construction of 5G infrastructure from China has become the subject of a heated discussion between the US and China. From the US side, doubts are raised as to whether this equipment ensures the security of use of 5G services by citizens and entities around the world,

including those in the European Union ("EU"), due to the possible influence on their manufacturers by the Chinese government. The discussion between the US and China resulted in the adoption of a number of recommendations in the EU in the field of 5G cybersecurity, including *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures* ("5G Toolbox"). Specific recommendations have been formulated in the 5G Toolbox regarding the so-called High Risk Vendors ("HRV"). Based on these recommendations, some EU countries have introduced national regulations regarding HRV. Due to the different pace of adoption of these regulations in individual EU countries and the different ways of implementing these regulations and enforcing already implemented provisions, demands are being made to adopt a uniform regulation in the EU in the field of HRV, which would apply to all EU countries. The article analyzes whether it is justified to adopt uniform EU regulations in this regard at the current stage of the adopted regulations regarding HRV.

Keywords: high risk vendors, 5G Toolbox, cybersecurity, telecommunications infrastructure

Cytuj jako: Rogalski M., *Polityka Unii Europejskiej wobec Chin – uregulowania w zakresie dostawców infrastruktury 5G*, „Myśl Ekonomiczna i Polityczna" 2023, nr 4(79), s. 150–165. DOI: 10.26399/meip.4(79).2023.31/m.rogalski

Cite as: Rogalski M. (2023). 'EU Policy Towards China: Regulations for 5G Infrastructure Vendors'. Myśl Ekonomiczna i Polityczna 4(79), 150–165. DOI: 10.26399/meip.4(79).2023.31/m.rogalski