MACIEJ ROGALSKI

# BEZPIECZEŃSTWO SIECI I USŁUG ŁĄCZNOŚCI ELEKTRONICZNEJ W PRAWIE UNII EUROPEJSKIEJ ORAZ W PRAWIE POLSKIM

WYDAWNICTWA ŁAZARSKI
WARSZAWA

# Bezpieczeństwo sieci i usług łączności elektronicznej w prawie Unii Europejskiej oraz w prawie polskim

DOI 10.26399/978-83-66723-71-9

Maciej Rogalski

# Bezpieczeństwo sieci i usług łączności elektronicznej w prawie Unii Europejskiej oraz w prawie polskim

Warszawa 2024

*Bezpieczeństwo sieci i usług łączności elektronicznej w prawie Unii Europejskiej oraz w prawie polskim*
Maciej Rogalski
(Uczelnia Łazarskiego, ORCID: 0000-0003-4366-642X)

Recenzenci:
dr hab. Andrzej Zapałowski, prof. UR
dr hab. Mariusz Wieczorek, prof. URad

Redaktor prowadząca: Aleksandra Szudrowicz
Redakcja językowa i korekta: Zuzanna Guty
Projekt okładki: Małgorzata Siwa

DOI 10.26399/978-83-66723-71-9
ISBN 978-83-66723-71-9
e-ISBN 978-83-66723-72-6




Wydanie 1
Oficyna Wydawnicza Uczelni Łazarskiego, Warszawa 2024

# Spis treści

# Wykaz skrótów

## Akty prawne

| | |
|---|---|
| dyrektywa 95/46 | dyrektywa Parlamentu Europejskiego i Rady 95/46/WE z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. L 281 z dnia 23.11.1995 r.). |
| dyrektywa 2002/21 | dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) (Dz.Urz. WE L 108 z dnia 24.04.2002 r., s. 33 ze zm.) |
| dyrektywa 2002/58 | dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. UE L 20 z dnia 31.07.2002 r.) |
| dyrektywa 2009/140 | dyrektywa Parlamentu Europejskiego i Rady 2009/140/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywy 2002/21/WE w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej 2002/19/EW w sprawie dostępu do sieci i usług łączności elektronicznej oraz wzajemnych połączeń oraz 2002/20/WE w sprawie zezwoleń na udostępnienie sieci i usług łączności Elektronicznej (Dz.Urz. UE L 337 z dnia 18.12.2009 r.) |
| dyrektywa 2011/93 | dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WSiSW (Dz.Urz. L 335 z dnia 17.12.2011 r.) |
| dyrektywa 2013/36 | dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE (Dz.Urz. UE L 176 z dnia 27.06.2013 r.) |
| dyrektywa 2013/40 | dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (Dz.Urz. L 218/8 z dnia 14.08.2013 r.) |
| dyrektywa 2022/2557 | dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów |

| | |
|---|---|
| | krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz.Urz. UE L 333/164 z dnia 27.12.2022 r.) |
| EKŁE | dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona) (Dz.Urz. UE L 321 z dnia 17.12.2018 r.) |
| EKPC | Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 z dnia 4 listopada 1950 r. (Dz.U. z 1993 r. Nr 61, poz. 284) |
| k.c. | ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz.U. z 2023 r. poz. 1610 ze zm.) |
| Konstytucja RP | Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483 ze zm.) |
| k.p.a. | ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (t.j. Dz.U. z 2023 r. poz. 775 ze zm.) |
| KPPUE | Karta praw podstawowych Unii Europejskiej (Dz.Urz. UE C 83 z dnia 30.03.2010 r.) |
| NIS | dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii z dnia 6 lipca 2016 r. (Dz.Urz. UE L Nr 194 z dnia 19.07.2016 r.) |
| NIS 2 | dyrektywa 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, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Tekst mający znaczenie dla EOG) (Dz.Urz. UE L Nr 333 z dnia 27.12.2022 r.) |
| p.k.e. | projekt ustawy – Prawo komunikacji elektronicznej, druk sejmowy nr 2861 z 9 grudnia 2022 r. |
| p.p.s.a. | ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz.U. z 2023 r. poz. 1634 ze zm.) |
| projekt z dnia 3 lipca 2023 r. | projekt z dnia 3 lipca 2023 r. ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (druk sejmowy nr 3457) |
| p.t. | ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2022 r. poz. 1648 ze zm.) |
| RODO | rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych |

| | |
|---|---|
| | w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z dnia 4.05.2016 r.) |
| rozporządzenie 910/2014 | rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (rozporządzenie eIDAS) (Dz.Urz. UE L 257 z dnia 28.08.2014 r.) |
| rozporządzenie 2019/881 | rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 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 z dnia 17.06.2019 r.) |
| rozporządzenie z 22 czerwca 2020 r. | rozporządzenie Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług (Dz.U. z 2020 r. poz. 1130) |
| rozporządzenie z 19 sierpnia 2020 r. | rozporządzenie Rady Ministrów w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń z dnia 19 sierpnia 2020 r. (Dz.U. z 2020 r. poz. 1464) |
| rozporządzenia 2022/2554 | 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.Urz. UE L 333 z dnia 27.12.2022 r.) |
| TFUE | Traktat o funkcjonowaniu Unii Europejskiej z dnia 25 marca 1957 r. (Dz.U. z 2004 r. Nr 90, poz. 864[2]) |
| u.k.s.c. | ustawa o krajowym systemie cyberbezpieczeństwa z 5 lipca 2018 r. (t.j. Dz.U. z 2023 r. poz. 913 ze zm.) |
| u.o.d.o. | ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. (t.j. Dz.U. z 2019 r. poz. 1781) |

| | |
|---|---|
| u.o.k.k. | ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz.U. z 2023 r. poz. 1689 ze zm.) |
| u.z.k. | ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r. (t.j. Dz.U. z 2007 r. Nr 89, poz. 590 ze zm.) |
| ustawa z 14 maja 2020 r. | ustawa z dnia 14 maja 2020 r. o zmianie niektórych ustaw w zakresie działań osłonowych w związku z rozprzestrzenianiem się wirusa SARS-CoV-2 (Dz.U. z 2023 r. poz. 122 ze zm.) |
| zalecenie 2003/361/WE | zalecenie Komisji z dnia 6 maja 2003 r. w sprawie definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (notyfikowane jako dokument nr C(2003) 1422) (Dz.Urz. UE L 124 z dnia 20.05.2003 r.) |
| zalecenie 2019/2335 | zalecenia Komisji Europejskiej z dnia 26 marca 2019 r. (UE) 2019/2335 w sprawie cyberbezpieczeństwa sieci 5G (Dz.Urz. UE L 88 z dnia 29.03.2019 r.) |
| z.t.p. | rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" (Dz.U. z 2002 r. Nr 100, poz. 908 ze zm.) |

## Wydawnictwa promulgacyjne

| | |
|---|---|
| CBOSA | Centrala Baza Orzeczeń Sądów Administracyjnych |
| Dz.U. | Dziennik Ustaw |
| ONSA | Orzecznictwo Naczelnego Sądu Administracyjnego |
| OTK ZU | Orzecznictwo Trybunału Konstytucyjnego Zbiór Urzędowy |

## Inne

| | |
|---|---|
| AI | Artificial Intelligence |
| ABW | Agencja Bezpieczeństwa Wewnętrznego |
| B2B | business to business |
| BBN | Biuro Bezpieczeństwa Narodowego |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| CERT | Computer Emergency Response Team |
| CERT-EU | Computer Emergency Response Team for the EU |
| CRM | Customer Relationship Management |
| CRP | Cyberprzestrzeń Rzeczypospolitej Polskiej |
| CSIRT | Zespoły Reagowania na Incydenty Związane z Bezpieczeństwem Komputerowym |

| | |
|---|---|
| DNS | Domain Name System |
| ECA | European Court of Auditors |
| EFTA | Europejskie Stowarzyszenie Wolnego Handlu |
| ENISA | Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji |
| ETSI | Europejski Instytut Norm Telekomunikacyjnych |
| GPS | Global Positioning System |
| GSMA | Groupe Speciale Mobile Association |
| HPC | High Performance Computing |
| ICT | Information and Communication Technology |
| IEC | International Electrotechnical Commission |
| IETF | Internet Engineering Task Force |
| IoV | Internet of Vehicles |
| IP | Internet Protocol |
| ISO | International Organization for Standardization |
| IŁ | Instytut Łączności |
| IoT | Internet of Things |
| IXP | Internet Exchange Point |
| IT | Information Technology |
| ITIL | Information Technology Infrastructure Library |
| ITU | International Telecommunication Union |
| KE | Komisja Europejska |
| KSO3C | Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria |
| M2M | machine to machine |
| MC | Ministerstwo Cyfryzacji |
| MON | Ministerstwo Obrony Narodowej |
| NASK | Naukowa i Akademicka Sieć Komputerowa |
| NCBiR | Narodowe Centrum Badań i Rozwoju |
| NFV | Network Function Virtualization |
| NISCG | Network and Information System Cooperation Group |
| NIST | National Institute of Standards and Technology |
| NPS | Narodowy Plan Szerokopasmowy |
| NSA | Naczelny Sąd Administracyjny |
| ONF | Open Network Foundation |
| OSS | One Stop Shop |
| OT | Operational Technologies |
| PIB | Państwowy Instytut Badawczy |
| POPC | Program Operacyjny Polska Cyfrowa |
| RM | Rada Ministrów |

| | |
|---|---|
| SOC | Security Operations Center |
| TK | Trybunał Konstytucyjny |
| TLD | Top Level Domain |
| TLS | Transport Layer Security |
| UE | Unia Europejska |
| UKE | Urząd Komunikacji Elektronicznej |
| UODO | Urząd Ochrony Danych Osobowych |
| UOKiK | Urząd Ochrony Konkurencji i Konsumentów |
| WSA | Wojewódzki Sąd Administracyjny |
| WTSA | World Telecommunication Standardization Assembly |
| 3 GPP | 3rd Generation Partnership Project |
| 5G | technologia mobilna piątej generacji |
| 5G Toolbox | Cybersecurity of 5G networks EU Toolbox of risk mitigating measures |

# Wstęp

W związku z bardzo dynamicznym postępem technologicznym oraz tworzącymi się nowymi dziedzinami gospodarki opartymi na wiedzy, gromadzeniu danych i wymianie informacji kluczową rolę odgrywa infrastruktura, która zapewnia funkcjonowanie nowoczesnej gospodarki i dostęp do informacji dla podmiotów gospodarczych oraz obywateli. W obszarze komunikacji najistotniejszym elementem infrastruktury są sieci łączności elektronicznej. Sieci łączności elektronicznej oznaczają systemy transmisyjne, niezależnie do tego, czy opierają się na stałej infrastrukturze czy scentralizowanym zarządzaniu zasobami, oraz – w stosownych przypadkach – urządzenia przełączające lub routingowe, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają przekazywanie sygnałów przewodowo, za pomocą radia, środków optycznych lub innych rozwiązań wykorzystujących fale, w tym sieci satelitarnych, stacjonarnych (komutowanych i pakietowych, włącznie z internetem), wreszcie sieci ruchomych, elektroenergetycznych systemów kablowych, w zakresie, w jakim są one wykorzystywane do przekazywania sygnałów, w sieciach nadawania radiowego i telewizyjnego oraz sieciach telewizji kablowej, niezależnie od rodzaju przekazywanej informacji (art. 2 pkt 1 EKŁE). Z pomocą sieci łączności elektronicznej możliwe jest świadczenie usług łączności elektronicznej, które oznaczają usługi zazwyczaj świadczone za wynagrodzeniem za pośrednictwem sieci łączności elektronicznej, które obejmują, z wyjątkiem usług związanych z zapewnianiem albo wykonywaniem kontroli treści przekazywanych przy wykorzystaniu sieci lub usług łączności elektronicznej, następujące rodzaje usług: usługę dostępu do internetu, usługę łączności interpersonalnej oraz usługi polegające całkowicie lub częściowo na przekazywaniu sygnałów, takie jak usługi transmisyjne stosowane na potrzeby świadczenia usług łączności maszyna–maszyna oraz na potrzeby nadawania (art. 2 pkt 4 EKŁE).

Niezwykle ważne jest bezpieczeństwo sieci i świadczonych usług, które oznacza zdolność sieci i usług łączności elektronicznej do odpierania na danym poziomie pewności wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność tych sieci i usług, przechowywanych, przekazywanych lub przetwarzanych danych lub związanych z nimi usług oferowanych przez te sieci lub usługi łączności elektronicznej lub dostępnych za ich pośrednictwem (art. 2 pkt 21 EKŁE). Bezpieczeństwo sieci i świadczonych usług może być rozpatrywane na różnych płaszczyznach. W płaszczyźnie technologicznej, rozumiane jako zapewnienie odpowiednich rozwiązań technicznych, chroniących użytkowników

usług w zakresie korzystania z tych usług, przed utratą danych czy popełnieniem na ich szkodę przestępstw lub innego rodzaju nadużyć. Może być rozpatrywane w sensie politycznym, co nabiera szczególnego znaczenia w obecnym czasie z uwagi na wojny, konflikty międzynarodowe i podziały polityczne. Chodzi tu głównie o ochronę przed cyberatakami, pozyskiwaniem wrażliwych danych jednego państwa przez służby innego państwa itp. Wreszcie może być rozpatrywane i analizowane bezpieczeństwo sieci i usług w aspekcie prawnym, czyli w obszarze przepisów, które regulują kwestie dotyczące bezpieczeństwa sieci i usług. Niniejsze opracowanie jest poświęcone temu obszarowi, czyli uregulowaniom prawnym dotyczącym bezpieczeństwa sieci i usług łączności elektronicznej.

W książce omówione są uregulowania unijne oraz krajowe w zakresie bezpieczeństwa sieci i usług łączności elektronicznej. Przedstawienie regulacji UE jest niezbędne, gdyż regulacje krajowe opierają się na dyrektywach UE w zakresie bezpieczeństwa oraz łączności elektronicznej. W zakresie bezpieczeństwa do niedawna obowiązywała dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii z dnia 6 lipca 2016 r. (dyrektywa NIS). Obecnie natomiast obowiązuje dyrektywa 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, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2). Z kolei jeśli chodzi o regulacje sektorowe w zakresie łączności elektronicznej, obowiązuje dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej. Aktem obowiązującym natomiast bezpośrednio wszystkie kraje UE jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 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), które odgrywa istotną rolę w zakresie wprowadzania w krajach członkowskich certyfikacji cyberbezpieczeństwa. Wreszcie dokumentem, który nie ma charakteru przepisów unijnych, ale ma duże znaczenie w zakresie cyberbezpieczeństwa, gdyż jest dedykowany najnowszym technologiom telekomunikacyjnym, tj. standardowi 5G, jest dokument zatytułowany *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures* („5G Toolbox"). Dokument ten został przygotowany przez Grupę Współpracy ds. Sieci i Systemów Informatycznych (NISCG) we współpracy z Komisją Europejską (KE) i Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA).

W rozdziale II książki są przedstawione obecnie obowiązujące regulacje w zakresie bezpieczeństwa sieci i usług telekomunikacyjnych. Podstawowe regulacje znajdują się w ustawie – Prawo telekomunikacyjne oraz w rozporządzeniu Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług. Ważnym elementem zapewnienia bezpieczeństwa sieci i usług telekomunikacyjnych są przygotowywane przez największych przedsiębiorców telekomunikacyjnych plany działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń. Z przedstawianymi zagadnieniami wiążą się także niektóre regulacje ustawy o zarządzaniu kryzysowym. Omówiony zostanie także dokument w postaci Strategii Cyberbezpieczeństwa Polski, który pokazuje kierunki przygotowywanych regulacji w aspekcie istniejących i spodziewanych zagrożeń. Krótko zostaną wreszcie scharakteryzowane wybrane postanowienia ustawy o krajowym systemie cyberbezpieczeństwa jako aktu podstawowego dla cyberbezpieczeństwa i implementującego dyrektywę NIS, a z drugiej strony nieodnoszącego się bezpośrednio do przedsiębiorców telekomunikacyjnych w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów, z uwagi na wyraźne wyłączenie sformułowane w art. 1 ust. 2 pkt 1 u.k.s.c.

Znacząca część monografii jest poświęcona projektowanym regulacjom prawnym. Dotychczas nie wprowadzono bowiem nowej ustawy – Prawo komunikacji elektronicznej, która miała implementować dyrektywę z dnia 11 grudnia 2018 r. ustanawiającą Europejski kodeks łączności elektronicznej. Implementacja EKŁE do krajowego porządku prawnego miała nastąpić do 21 grudnia 2020 r. Także od 2020 r. toczyły się prace nad nowelą ustawy o krajowym systemie cyberbezpieczeństwa. Ostatnia wersja tej noweli z dnia 3 lipca 2023 r. (druk sejmowy nr 3457) została jednak wycofana przez rząd z dalszych prac sejmowych w dniu 11 września 2023 r. W międzyczasie została przyjęta nowa dyrektywa w sprawie cyberbezpieczeństwa – dyrektywa NIS 2, która powinna być implementowana do polskiego porządku prawnego do 17 października 2024 r. W grudniu 2023 r. zakończyła się także aukcja na rozdysponowanie częstotliwości niezbędnych do świadczenia usług w technologii 5G. W związku z nią pojawiła się po raz pierwszy kwestia wprowadzenia wymagań dla dostawców sprzętu telekomunikacyjnego niezbędnego do budowy infrastruktury 5G, wynikających z przyjętego w UE dokumentu zawierającego takie wymagania, wspomnianego wcześniej 5G Toolbox. Z tymi zagadnieniami wiąże się także kwestia certyfikacji cyberbezpieczeństwa sprzętu do świadczenia usług komunikacji elektronicznej. Wymienione zagadnienia zostały przedstawione w rozdziale III monografii.

Powinny one stanowić użyteczny materiał, zbierający dotychczasowe doświadczenia z prac nad wspomnianymi projektami aktów prawnych. Zawiera opis dotychczas proponowanych rozwiązań w zakresie bezpieczeństwa sieci i usług telekomunikacyjnych wraz z uwagami krytycznymi, obejmującymi także propozycje konkretnych zmian czy modyfikacji projektowanych przepisów. Zebrany materiał, gromadzący dotychczasowe doświadczenia w prowadzonych pracach, powinien być pomocny w dalszych pracach nad nowymi aktami prawnymi, czyli nową ustawą – Prawo komunikacji elektronicznej oraz nową ustawą o krajowym systemie cyberbezpieczeństwa.

# Rozdział I
# Regulacje Unii Europejskiej

W UE obowiązują ogólne regulacje, które odnoszą się do ochrony sieci komunikacji elektronicznej (ang. *electronic communication networks*). W szczególności wskazać należy dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającą Europejski kodeks łączności elektronicznej (wersja przekształcona) oraz 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). Obowiązuje także 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. W UE przyjęte zostały także regulacje, które odnoszą się bezpośrednio do bezpieczeństwa infrastruktury i usług świadczonych w określonej technologii, czyli 5G. W szczególności należy wskazać na opublikowany w dniu 29 stycznia 2020 r. raport NISCG, przygotowany we współpracy z KE i ENISA *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*[1].

## 1. Europejski Kodeks Łączności Elektronicznej

Zagadnienia dotyczące bezpieczeństwa sieci i usług telekomunikacyjnych są zawarte w najważniejszym dla rynku łączności elektronicznej akcie prawnym – dyrektywie Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej. Zgodnie z pkt 5 preambuły EKŁE celem tej dyrektywy jest stworzenie ram prawnych dla zapewnienia swobody w zakresie dostarczania sieci i usług łączności elektronicznej, podlegających wyłącznie warunkom określonym w niniejszej dyrektywie oraz ograniczeniom zgodnie z art. 52 ust. 1 TFUE, a w szczególności środkom podejmowanym w związku z polityką państwową, bezpieczeństwem publicznym oraz zdrowiem publicznym, oraz spójnych z art. 52 ust. 1 KPPUE.

---

[1] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures [dostęp: 25.02.2023 r.].

W preambule EKŁE znajdują się postanowienia, które wyjaśniają uregulowania dotyczące bezpieczeństwa sieci i usług, a znajdujące się w EKŁE. Problematyka związana z bezpieczeństwem sieci i usług jest uregulowana w EKŁE, jednak w ograniczonym zakresie. Zgodnie bowiem z art. 1 ust. 3 lit. c EKŁE postanowienia niniejszej dyrektywy nie ograniczają działań podejmowanych przez państwa członkowskie dla zachowania porządku publicznego i bezpieczeństwa publicznego oraz obronności. W pkt 6 preambuły EKŁE wyjaśniono, że dyrektywa ta pozostaje bez uszczerbku dla uprawnień każdego z państw członkowskich do podejmowania środków mających na celu zapewnienie ochrony jego podstawowych interesów w zakresie bezpieczeństwa, zapewnienie porządku publicznego i bezpieczeństwa publicznego oraz umożliwienie wykrywania lub ścigania przestępstw i prowadzenia dochodzeń w ich sprawie, mając na uwadze, że wszelkie ograniczenia korzystania z praw i wolności uznanych w KPPUE, w szczególności jej art. 7, 8 i 11, takie jak ograniczenia dotyczące przetwarzania danych, muszą być przewidziane prawem, przestrzegać istoty praw i wolności oraz podlegać zasadzie proporcjonalności zgodnie z art. 52 ust. 1 KPPUE. Kwestie dotyczące bezpieczeństwa sieci i usług powinny znajdować się więc w przepisach krajowych, jednakże przepisy te powinny być zgodne z regulacjami UE, a w szczególności z EKŁE oraz KPPUE.

EKŁE wyjaśnia, co należy rozumieć przez termin „bezpieczeństwo sieci i usług". Oznacza on zdolność sieci i usług łączności elektronicznej do odpierania, na danym poziomie pewności, wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność tych sieci i usług, przechowywanych, przekazywanych lub przetwarzanych danych albo związanych z nimi usług oferowanych przez te sieci lub usługi łączności elektronicznej bądź dostępnych za ich pośrednictwem (art. 2 pkt 21 EKŁE).

EKŁE wśród celów dyrektywy wymienia m.in. wspieranie interesów obywateli Unii poprzez zapewnianie łączności i powszechnej dostępności oraz korzystania z sieci o bardzo wysokiej przepustowości, w tym sieci stacjonarnych, ruchomych i bezprzewodowych, a także usług łączności elektronicznej, poprzez dbanie o bezpieczeństwo sieci i usług oraz zapewnianie wysokiego i powszechnego poziomu ochrony użytkowników końcowych dzięki niezbędnym przepisom sektorowym (art. 3 ust. 2 lit. d EKŁE).

Kwestiom bezpieczeństwa sieci i usług został poświęcony tytuł V EKŁE – *Bezpieczeństwo*. W tytule tym znajdują się m.in. art. 40–41. Zgodnie z art. 40 ust. 1 EKŁE państwa UE są zobowiązane zapewnić, by dostawcy udostępniający publiczne sieci łączności elektronicznej lub świadczący publicznie dostępne usługi łączności elektronicznej podejmowali właściwe i proporcjonalne środki techniczne i organizacyjne w razie wystąpienia zagrożenia dla bezpieczeństwa

sieci lub usług. Środki te muszą zapewniać poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka z uwzględnieniem aktualnego stanu wiedzy i technologii. W szczególności w celu zagwarantowania bezpieczeństwa sieci i usług, a także bez uszczerbku dla uprawnień państw członkowskich w zakresie zapewniania ochrony ich podstawowych interesów bezpieczeństwa i bezpieczeństwa publicznego oraz w celu umożliwienia wykrywania lub ścigania przestępstw i prowadzenia dochodzeń w ich sprawie, należy promować korzystanie np. z szyfrowania – w stosownych przypadkach pełnego szyfrowania transmisji – a w razie konieczności szyfrowanie powinno być obowiązkowe zgodnie z zasadami bezpieczeństwa i prywatności domyślnie i już w fazie projektowania (pkt 97 preambuły EKŁE). Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji powinna natomiast ułatwić, zgodnie z rozporządzeniem, koordynację państw członkowskich, aby uniknąć powstawania rozbieżnych krajowych wymogów, które mogą tworzyć ryzyko dla bezpieczeństwa i bariery dla rynku wewnętrznego.

Według art. 40 ust. 2 EKŁE państwa UE są zobowiązane zapewnić, by podmioty udostępniające publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej powiadamiały bez zbędnej zwłoki właściwy organ o incydentach związanych z bezpieczeństwem, które miały znaczący wpływ na funkcjonowanie sieci lub usług. Aby określić istotność wpływu danego incydentu związanego z bezpieczeństwem, należy w szczególności uwzględniać następujące parametry, o ile są dostępne:

a) liczbę użytkowników, których dotyczy incydent związany z bezpieczeństwem;
b) czas trwania incydentu związanego z bezpieczeństwem;
c) geograficzny zasięg obszaru dotkniętego incydentem związanym z bezpieczeństwem;
d) zakres wpływu na funkcjonowanie sieci lub usługi;
e) zakres wpływu na działalność ekonomiczną i społeczną.

W stosownych przypadkach właściwy organ informuje odpowiednie organy innych państw członkowskich oraz ENISA. W przypadku gdy właściwy organ uzna, że ujawnienie incydentu związanego z bezpieczeństwem leży w interesie publicznym, może podać tę informację do wiadomości publicznej lub nałożyć taki obowiązek na podmioty. Raz w roku właściwy organ przekazuje KE i ENISA sprawozdanie podsumowujące otrzymane zgłoszenia i podjęte działania.

Właściwe organy państw członkowskich UE powinny zapewniać utrzymanie integralności i dostępności publicznych sieci łączności elektronicznej. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji powinna przyczyniać się do zwiększania poziomu bezpieczeństwa łączności elektronicznej, poprzez

m.in. zapewnianie wiedzy i doradztwa, oraz propagować wymianę najlepszych praktyk. Właściwe organy powinny dysponować niezbędnymi środkami do wykonywania swoich obowiązków, w tym uprawnieniami do uzyskiwania informacji niezbędnych do oceny poziomu bezpieczeństwa sieci lub usług. Powinny być również uprawnione do pozyskiwania kompleksowych i wiarygodnych danych na temat przypadków rzeczywistych zagrożeń bezpieczeństwa, które wywarły znaczący wpływ na funkcjonowanie sieci lub usług. W stosownych przypadkach powinny udzielać im pomocy Zespoły Reagowania na Incydenty Związane z Bezpieczeństwem Komputerowym (CSIRT) utworzone na podstawie NIS. W szczególności CSIRT mogą być zobowiązane do dostarczania właściwym organom informacji o ryzyku i incydentach związanych z bezpieczeństwem zagrażającym publicznym sieciom łączności elektronicznej i publicznie dostępnym usługom łączności elektronicznej oraz zalecać metody radzenia sobie z tymi problemami (pkt 98 preambuły EKŁE).

W przypadku gdy zapewniany jest skuteczny i spełniający najwyższy poziom bezpieczeństwa danych kontakt ze wszystkimi zainteresowanymi użytkownikami końcowymi, niezależnie od miejsca lub państwa członkowskiego ich zamieszkania, państwa członkowskie powinny mieć możliwość wprowadzenia transmisji publicznych ostrzeżeń za pośrednictwem publicznie dostępnych usług łączności elektronicznej innych niż usługi ruchomej łączności interpersonalnej wykorzystujące numery i innych niż usługi transmisji wykorzystywane do celów nadawczych lub za pośrednictwem aplikacji mobilnej przesyłanej za pomocą usług dostępu do internetu. W celu informowania użytkowników końcowych przyjeżdżających do danego państwa członkowskiego o istnieniu takich publicznych systemów ostrzegania państwo to powinno zapewnić, aby ci użytkownicy końcowi otrzymywali automatycznie za pomocą SMS, niezwłocznie i bezpłatnie, łatwo zrozumiałe informacje dotyczące sposobu otrzymywania ostrzeżeń publicznych, w tym za pomocą ruchomych urządzeń końcowych nieobsługujących usług dostępu do internetu. Publiczne ostrzeżenia inne niż oparte na usługach ruchomej łączności interpersonalnej wykorzystujących numery powinny być przekazywane użytkownikom końcowym w sposób łatwy do otrzymania. W przypadku gdy publiczny system ostrzegania opiera się na aplikacji, nie powinna ona wymagać od użytkowników końcowych logowania się lub rejestrowania w danym organie ani u danego dostawcy aplikacji. Dane dotyczące lokalizacji użytkowników końcowych powinny być używane zgodnie z dyrektywą 2002/58/WE. Transmisja publicznych ostrzeżeń powinna być bezpłatna dla użytkowników końcowych (pkt 294 preambuły EKŁE).

Państwa UE zobowiązane są zapewnić, aby w przypadku szczególnego i znacznego zagrożenia wystąpienia incydentu związanego z bezpieczeństwem

w publicznych sieciach łączności elektronicznej lub w ramach dostępnych publicznie usług łączności elektronicznej podmioty udostępniające takie sieci lub świadczące takie usługi informowały swoich użytkowników, na których takie zagrożenie może mieć wpływ, o wszelkich możliwych środkach ochronnych lub naprawczych koniecznych do podjęcia przez użytkowników. W stosownych przypadkach podmioty powinny informować swoich użytkowników również o samym zagrożeniu (art. 40 ust. 3 EKŁE).

Dostawcy publicznych sieci łączności elektronicznej lub publicznie dostępnych usług łączności elektronicznej są zobowiązani poinformować użytkowników o szczególnych i istotnych zagrożeniach dla bezpieczeństwa oraz o środkach, które mogą podejmować w celu ochrony bezpieczeństwa łączności, np. przez zastosowanie szczególnych rodzajów oprogramowania lub technologii szyfrowania. Wymóg informowania użytkowników o takich zagrożeniach nie powinien zwalniać danego dostawcy usług z obowiązku podjęcia na własny koszt odpowiednich i natychmiastowych środków w celu zaradzenia wszelkim zagrożeniom bezpieczeństwa oraz przywrócenia normalnego poziomu bezpieczeństwa danej usługi. Udzielanie użytkownikowi takich informacji na temat zagrożeń bezpieczeństwa powinno odbywać się bezpłatnie (pkt 96 preambuły EKŁE).

Umowa pomiędzy dostawcą a podmiotem korzystającym z usług dostawy powinna określać, jaki rodzaj działań dostawca może podjąć w razie wystąpienia zdarzeń naruszających bezpieczeństwo, zagrożeń takimi zdarzeniami lub podatnością na wystąpienie takich wydarzeń. Ponadto umowa powinna precyzować wszelkie ustalenia dotyczące możliwości kompensacji lub zwrotu pieniędzy, jeśli dostawca w nieadekwatny sposób zareaguje na incydent związany z bezpieczeństwem, w tym jeżeli do zgłoszonego dostawcy incydentu związanego z bezpieczeństwem dochodzi z powodu znanych luk bezpieczeństwa w oprogramowaniu lub sprzęcie komputerowym, w związku z czym producent lub programista udostępnił poprawki, a dostawca nie zastosował ich ani nie podjął żadnych innych odpowiednich środków zaradczych (pkt 264 preambuły EKŁE).

Przepisy art. 40 EKŁE nie naruszają przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[2] oraz dyrektywy 2002/58 Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności

[2] Dz.Urz. UE. L Nr 119 z dnia 4.05.2016 r., s. 1.

elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[3] (art. 40 ust. 4 EKŁE), co oznacza, że poza wskazanymi przepisami EKŁE w zakresie ochrony danych osobowych zastosowanie mają postanowienia wspomnianej dyrektywy i rozporządzenia.

Komisja Europejska, w jak największym stopniu uwzględniając opinię ENISA, może przyjąć akty wykonawcze określające szczegółowo techniczne i organizacyjne środki, o których mowa w art. 40 ust. 1 EKŁE, a także format i procedury stosowane w odniesieniu do wymogów dotyczących zgłoszenia na podstawie art. 40 ust. 2 EKŁE (powiadamianie o incydentach). Powinny się one opierać w jak najszerszym zakresie na normach europejskich i międzynarodowych oraz nie uniemożliwiać państwom członkowskim przyjmowania dodatkowych wymogów służących osiągnięciu celów określonych w art. 40 ust. 1 EKŁE (art. 40 ust. 5 EKŁE).

Postanowienia art. 41 EKŁE dotyczą wdrożenia i egzekwowania postanowień w zakresie bezpieczeństwa sieci i usług. Zgodnie z art. 41 ust. 1 EKŁE państwa UE powinny zapewnić, by w celu wdrożenia art. 40 EKŁE właściwe organy były uprawnione do wydawania wiążących instrukcji, w tym instrukcji dotyczących środków wymaganych, aby zaradzić incydentowi związanemu z bezpieczeństwem lub aby zapobiec wystąpieniu takiego incydentu, gdy zidentyfikowano znaczne zagrożenie, oraz do określenia terminów wdrożenia podmiotom udostępniającym publiczne sieci łączności elektronicznej lub świadczącym publicznie dostępne usługi łączności elektronicznej.

Według art. 41 ust. 2 EKŁE państwa UE powinny zapewnić, aby właściwe organy były uprawnione do wymagania od podmiotów udostępniających publiczne sieci łączności elektronicznej lub świadczących publicznie dostępne usługi łączności elektronicznej: dostarczania informacji potrzebnych do oceny bezpieczeństwa ich sieci i usług, w tym do oceny udokumentowanych polityk bezpieczeństwa oraz poddania się audytowi bezpieczeństwa przeprowadzanemu przez wykwalifikowany niezależny podmiot lub właściwy organ i udostępnienia właściwemu organowi wyników takiego audytu. Koszty wspomnianego audytu powinien ponosić dostawca.

Państwa UE powinny także zapewnić, aby właściwe organy miały wszelkie uprawnienia niezbędne do badania przypadków nieprzestrzegania wymogów oraz ich wpływu na bezpieczeństwo sieci i usług (art. 41 ust. 3 EKŁE). Powinny także zapewnić w celu wdrożenia przepisów art. 40 EKŁE, aby właściwe organy dysponowały uprawnieniami pozwalającymi im zwracać się o pomoc do zespołu reagowania na incydenty związane z bezpieczeństwem

[3] Dz.Urz. UE. L Nr 201 z dnia 31.07.2002 r., s. 37.

komputerowym wyznaczonym na podstawie art. 9 dyrektywy NIS w związku z problemami wchodzącymi w zakres zadań CSIRT zgodnie z pkt 2 załącznika I do tej dyrektywy (art. 41 ust. 4 EKŁE). Właściwe organy, w stosownych przypadkach oraz zgodnie z prawem krajowym, powinny konsultować się i współpracować z odpowiednimi krajowymi organami ścigania, właściwymi organami w rozumieniu art. 8 ust. 1 NIS oraz krajowymi organami ds. ochrony danych (art. 41 ust. 5 EKŁE).

Dostawcy publicznych sieci łączności elektronicznej lub publicznie dostępnych usług łączności elektronicznej (lub zarówno sieci, jak i usług) powinni mieć obowiązek wprowadzania środków w celu ochrony bezpieczeństwa, odpowiednio, sieci lub usług, a także w celu zapobieżenia skutkom incydentów związanych z bezpieczeństwem lub minimalizacji tych skutków. Środki te powinny zapewniać poziom bezpieczeństwa sieci i usług proporcjonalny do istniejącego ryzyka z uwzględnieniem aktualnego stanu wiedzy i technologii. Przy opracowywaniu środków bezpieczeństwa należy brać pod uwagę co najmniej wszystkie stosowne aspekty następujących kwestii:

- w odniesieniu do bezpieczeństwa sieci i urządzeń – bezpieczeństwo fizyczne i bezpieczeństwo środowiska, bezpieczeństwo dostaw, kontrolę dostępu do sieci i integralność sieci;
- w odniesieniu do postępowania w przypadku incydentów związanych z bezpieczeństwem – procedury postępowania w przypadku incydentu związanego z bezpieczeństwem, zdolności wykrywania incydentów, zgłaszanie incydentów związanych z bezpieczeństwem i informowanie o nich;
- w odniesieniu do zarządzania ciągłością działalności – strategię ciągłości usług i plany awaryjne, zdolność w zakresie przywracania gotowości do pracy po katastrofie;
- w odniesieniu zaś do monitorowania, kontroli i testowania – strategie monitorowania i rejestrowania, ćwiczenia w zakresie planów awaryjnych, testowanie sieci i usług, oceny bezpieczeństwa i monitorowanie zgodności oraz zgodność z normami międzynarodowymi (pkt 94 preambuły EKŁE).

Z uwagi na rosnące znaczenie usług łączności interpersonalnej niewykorzystujących numerów państwa członkowskie powinny zapewnić, aby podlegały one również odpowiednim wymogom bezpieczeństwa zgodnie z ich specyficznym charakterem i istotną rolą w gospodarce. Dostawcy usług powinni również zapewnić poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka. Ze względu na to, że dostawcy usługi interpersonalnej łączności niewykorzystującej numerów zazwyczaj nie sprawują rzeczywistej kontroli nad transmisją sygnałów w sieciach, stopień ryzyka w przypadku takich usług można uznać za niższy pod pewnymi względami niż w przypadku tradycyjnych usług łączności

elektronicznej. Dlatego też, jeżeli tylko jest to uzasadnione aktualną oceną ryzyka dla bezpieczeństwa, środki podejmowane przez dostawców usługi interpersonalnej łączności niewykorzystujące numerów powinny być łagodniejsze. Takie samo podejście powinno być stosowane odpowiednio do usług łączności interpersonalnej wykorzystującej numery, jeżeli dostawca nie sprawuje rzeczywistej kontroli nad transmisją sygnału (pkt 95 preambuły EKŁE).

## 2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r.

W UE do niedawna obowiązywała dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[4]. Dyrektywa NIS wynikała ze Strategii Cyberbezpieczeństwa Unii Europejskiej opublikowanej 7 lutego 2013 r. NIS była wskazana jako środek realizacji jednego z głównych priorytetów – osiągnięcia odporności na zagrożenie cybernetyczne. Nowe elementy wprowadzone przez nią do europejskiego porządku prawnego były następujące:

1) stworzenie wspólnej siatki pojęciowej (incydent, sieci i systemy, postępowanie w razie incydentu);
2) ustanowienie zespołów CSIRT, organów właściwych oraz pojedynczego punktu kontaktowego w każdym państwie członkowskim;
3) wyodrębnienie operatorów usług kluczowych w wybranych sektorach gospodarki i nałożenie na nich nowych obowiązków;
4) wyróżnienie dostawców usług cyfrowych i nałożenie na nich nowych, ale łagodniejszych niż u operatorów, obowiązków;
5) nałożenie na państwa obowiązku przygotowania krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych;
6) określenie zasad współpracy pomiędzy państwami członkowskimi (Sieć CSIRT i Grupa Współpracy)[5].

Dyrektywa NIS zawierała przepisy w zakresie cyberbezpieczeństwa. Nakładała minimalne wymogi na zespoły CSIRT, określała podstawowe zasady identyfikacji operatorów usług kluczowych, określała minimalne wymogi bezpieczeństwa i progi zgłaszania incydentów dla dostawców usług cyfrowych oraz

[4] Dz.Urz. UE. L Nr 194 z dnia 19.07.2016 r., s. 1.

[5] A. Besiekierska (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019, uwaga nr 2–3 do art. 1.

nakłaniała do promowania normalizacji (zgodnie z zasadą neutralności technologicznej) i dobrowolnego zgłaszania incydentów[6]. Nakładała na państwa członkowskie szereg obowiązków, zobowiązując do powołania konkretnych instytucji oraz wprowadzenia mechanizmów współpracy. NIS zobowiązywała wszystkie państwa członkowskie do zagwarantowania minimalnego poziomu krajowych zdolności w dziedzinie bezpieczeństwa teleinformatycznego. Przepisy tej dyrektywy umożliwiły stworzenie zarówno scentralizowanego systemu bezpieczeństwa na poziomie krajowym, jak i podzielenie kompetencji pomiędzy różne podmioty. Dyrektywa dotyczyła trzech obszarów: instytucji, które powstały we wszystkich państwach członkowskich; współpracy na poziomie europejskim; zobowiązań w zakresie bezpieczeństwa sieci i informacji.

Zgodnie z pkt 6 preambuły NIS celem tej dyrektywy było skuteczne reagowanie na wyzwania związane z zapewnieniem bezpieczeństwa sieci i systemów informatycznych. Punkt 7 preambuły NIS stanowił, że w celu uwzględnienia wszystkich istotnych incydentów i ryzyk niniejsza dyrektywa powinna mieć zastosowanie zarówno do operatorów usług kluczowych, jak i dostawców usług cyfrowych. Obowiązki nakładane na operatorów usług kluczowych i dostawców usług cyfrowych nie powinny jednak mieć zastosowania do przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej w rozumieniu dyrektywy 2002/21, które podlegały szczególnym wymogom w zakresie bezpieczeństwa i integralności ustanowionym w tej dyrektywie. W Polsce implementacji do krajowego porządku prawnego dyrektywy NIS dokonała ustawa o krajowym systemie cyberbezpieczeństwa z 5 lipca 2018 r.[7], do której przygotowane zostały także akty wykonawcze[8].

---

[6] *Ibidem*, uwaga nr 2–3 do art. 1.

[7] T.j. Dz.U. z 2023 r. poz. 913 ze zm.

[8] Uchwała w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024; rozporządzenie w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo; rozporządzenie w sprawie progów uznania incydentu za poważny; rozporządzenie w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej; rozporządzenie w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu; rozporządzenie w sprawie zakresu działania oraz trybu pracy Kolegium do spraw Cyberbezpieczeństwa; rozporządzenie w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych.

## 3. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r.

W grudniu 2020 r. opublikowano projekt nowej dyrektywy (Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final)[9], czyli projekt dyrektywy NIS 2, która miała zastąpić obowiązującą dotychczas, wymienioną dyrektywę NIS. W uzasadnieniu dla wprowadzenia nowej dyrektywy wskazano m.in., że konieczność zmiany unijnych przepisów związana jest z pandemią COVID-19, która znacząco przyspieszyła transformację cyfrową społeczeństw i przedsiębiorstw, oraz na rosnącą liczbę ataków cybernetycznych. Projekt nowej dyrektywy miał również wyeliminować słabości związane ze stosowaniem przepisów dyrektywy NIS, spowodowane głównie brakiem zapewniania odpowiedniej współpracy i wymiany informacji pomiędzy państwami członkowskimi. Ponadto zauważono, że zakres zastosowania dyrektywy NIS jest już nieaktualny i nie obejmuje wszystkich podmiotów, które powinny mieć dodatkowe obowiązki w zakresie cyberbezpieczeństwa. W świetle projektu dyrektywy NIS 2 władze państw członkowskich powinny przede wszystkim: zapewnić funkcjonowanie odpowiednich organów związanych z cyberbezpieczeństwem, opracować krajowe strategie cyberbezpieczeństwa (w ramach których powinny zostać opracowane odpowiednie polityki, m.in. w zakresie rozwoju i promowania kompetencji dotyczących cyberbezpieczeństwa), a także zapewnić współpracę z właściwymi organami i CSIRT innych państw członkowskich (m.in. w ramach sieci CSIRT oraz grupy współpracy państw członkowskich).

Nowością w stosunku do dyrektywy NIS było wprowadzenie w projekcie dyrektywy NIS 2 obowiązku opracowania przez państwa członkowskie narodowego planu reagowania na kryzysy i incydenty bezpieczeństwa o dużej skali (ang. *incident and crisis response plan*). Plan ten powinien zawierać m.in. odpowiednie procedury, kanały przepływu informacji czy środki mające na celu przygotowanie organów państw członkowskich na wypadek wystąpienia incydentów cyberbezpieczeństwa o dużej skali.

W dniu 13 maja 2022 r. Rada (UE) i Parlament Europejski osiągnęły porozumienie w sprawie przepisów dotyczących środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii. Dyrektywa NIS 2 została przyjęta przez Parlament Europejski w dniu 14 listopada 2022 r., a następnie w dniu 28 listopada 2022 r. Rada (UE) przyjęła ten akt. Ostatecznie została

[9] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166 [dostęp: 6.02.2024 r.].

opublikowana w dniu 14 grudnia 2022 r. jako dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 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) (tekst mający znaczenie dla EOG).

Dyrektywa NIS 2 wprawdzie zastąpi obowiązującą dotychczas dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, ale jest ona kontynuacją dyrektywy NIS, gdyż zawiera bardziej szczegółowe rozwiązania, aby jeszcze bardziej zwiększyć odporność i zdolność reagowania na incydenty, zarówno w sektorze publicznym i prywatnym, jak i w całej UE.

NIS 2 została przyjęta, gdyż zakres zastosowania dyrektywy NIS był już nieaktualny i nie obejmował wszystkich podmiotów, na które powinny być nałożone dodatkowe obowiązki w zakresie cyberbezpieczeństwa. Zgodnie z NIS 2 należy przede wszystkim: zapewnić funkcjonowanie odpowiednich organów związanych z cyberbezpieczeństwem, opracować krajowe strategie cyberbezpieczeństwa (w ramach których powinny zostać opracowane odpowiednie polityki, m.in. w zakresie rozwoju i promowania kompetencji dotyczących cyberbezpieczeństwa), a także zapewnić współpracę z właściwymi organami i CSIRT innych państw członkowskich (m.in. w ramach sieci CSIRT oraz grupy współpracy państw członkowskich). NIS 2 zawiera także bardzo dużo nowych zaleceń i rekomendacji, jednocześnie bardzo szczegółowo określa wymagania, kompetencje i zadania dla istniejących oraz nowo utworzonych instytucji i organów zarówno unijnych, jak i krajowych, a także określa zasady współpracy pomiędzy tymi instytucjami i organami.

W uzasadnieniu dla wprowadzenia nowej dyrektywy wskazano m.in., że konieczność zmiany unijnych przepisów związana jest z rosnącą liczbą ataków cybernetycznych. NIS 2 ma wyeliminować słabości związane ze stosowaniem przepisów dyrektywy NIS, spowodowane głównie brakiem zapewniania odpowiedniej współpracy i wymiany informacji pomiędzy państwami członkowskimi.

Postanowienia art. 1 NIS 2 określają jej przedmiot. Zgodnie z art. 1 NIS 2 dyrektywa ta ustanawia środki mające na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w całej UE, aby poprawić funkcjonowanie rynku wewnętrznego. W tym celu niniejsza dyrektywa określa:

a) obowiązki państw członkowskich dotyczące przyjęcia krajowych strategii cyberbezpieczeństwa oraz wyznaczenia lub powołania właściwych organów, organów ds. zarządzania kryzysowego w cyberbezpieczeństwie, pojedynczych punktów kontaktowych ds. cyberbezpieczeństwa (pojedyncze punkty

kontaktowe) oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT);
b) środki zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązki w zakresie zgłaszania incydentów spoczywające na podmiotach w rodzaju tych, o których mowa w załączniku I lub II do tej dyrektywy, jak również na podmiotach zidentyfikowanych jako podmioty o charakterze krytycznym na podstawie dyrektywy 2022/2557;
c) zasady i obowiązki w zakresie wymiany informacji o cyberbezpieczeństwie;
d) obowiązki w zakresie nadzoru i egzekwowania przepisów spoczywające na państwach członkowskich.

Załącznik nr I do NIS 2 zawiera zestawienie tzw. sektorów kluczowych, a załącznik nr II wymienia tzw. sektory ważne. Postanowienia art. 2 NIS 2 określają z kolei jej zakres. Niniejsza dyrektywa ma zastosowanie do podmiotów publicznych lub prywatnych w rodzaju tych, o których mowa w załączniku I lub II, które kwalifikują się jako średnie przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia 2003/361/WE lub które przekraczają pułapy dla średnich przedsiębiorstw określone w ust. 1 tego artykułu oraz które świadczą usługi lub prowadzą działalność w UE.

Zgodnie z art. 2 ust. 2 NIS 2 niniejsza dyrektywa ma również zastosowanie do podmiotów w rodzaju tych, o których mowa w załączniku I lub II, w przypadku gdy:
a) usługi świadczone są przez:
   – dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej;
   – dostawców usług zaufania;
   – rejestry nazw domen najwyższego poziomu oraz dostawców usług systemów nazw domen;
b) podmiot jest jedynym w danym państwie członkowskim dostawcą usługi, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej;
c) zakłócenie usługi świadczonej przez podmiot mogłoby mieć znaczący wpływ na porządek publiczny, bezpieczeństwo publiczne lub zdrowie publiczne;
d) zakłócenie usługi świadczonej przez podmiot mogłoby prowadzić do powstania poważnego ryzyka systemowego, w szczególności w sektorach, w których takie zakłócenie mogłoby mieć wpływ transgraniczny;
e) podmiot ma charakter krytyczny ze względu na jego szczególne znaczenie na poziomie krajowym lub regionalnym dla konkretnego sektora lub rodzaju usługi lub dla innych współzależnych sektorów w państwie członkowskim;

f) podmiot jest podmiotem administracji publicznej:
   – na poziomie rządu centralnego, zdefiniowanym przez państwo członkowskie, zgodnie z prawem krajowym; lub
   – na poziomie regionalnym, zdefiniowanym przez państwo członkowskie zgodnie z prawem krajowym, który zgodnie z oceną opartą na analizie ryzyka świadczy usługi, których zakłócenie mogłoby mieć znaczący wpływ na krytyczną działalność społeczną lub gospodarczą.

NIS 2 ma zastosowanie także do podmiotów zidentyfikowanych jako podmioty mające charakter krytyczny na mocy dyrektywy 2022/2557, niezależnie od ich wielkości (art. 2 ust. 3 NIS 2). Dyrektywa ta ma zastosowanie również do podmiotów świadczących usługi rejestracji nazw domen, niezależnie od ich wielkości (art. 2 ust. 4 NIS 2). Państwa członkowskie mogą wreszcie postanowić, że niniejsza dyrektywa ma zastosowanie do:

a) podmiotów administracji publicznej na poziomie lokalnym;
b) instytucji edukacyjnych, zwłaszcza gdy prowadzą one działalność badawczą o krytycznym znaczeniu (art. 2 ust. 5 NIS 2).

Istotne postanowienie zawiera art. 2 ust. 6–7 NIS 2, zgodnie z którym dyrektywa ta nie ogranicza spoczywającego na państwach członkowskich obowiązku ochrony bezpieczeństwa narodowego oraz dla ich uprawnień do zabezpieczania innych podstawowych funkcji państwa, w tym zapewniania integralności terytorialnej państwa i utrzymywania porządku publicznego. NIS 2 nie ma także zastosowania do podmiotów administracji publicznej, które prowadzą działalność w dziedzinach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, w tym zapobiegania im, prowadzenia postępowań w sprawie przestępstw, ich wykrywania oraz ścigania.

Państwa członkowskie mogą zwolnić określone podmioty, które prowadzą działania w obszarach bezpieczeństwa narodowego, bezpieczeństwa publicznego, obronności lub egzekwowania prawa, w tym zapobieganie przestępstwom, prowadzenie postępowań w ich sprawie, wykrywanie ich i ściganie, lub które świadczą usługi wyłącznie na rzecz podmiotów administracji publicznej, o których mowa w art. 2 ust. 7 NIS 2, z obowiązków ustanowionych w art. 21 (środki zarządzania ryzykiem w cyberbezpieczeństwie) lub w art. 23 (obowiązki w zakresie zgłaszania incydentów), w odniesieniu do tych działań lub tych usług.

NIS 2 nie ma zastosowania do podmiotów, które państwa członkowskie zwolniły z zakresu stosowania rozporządzenia 2022/2554 zgodnie z art. 2 ust. 4 tego rozporządzenia (art. 2 ust. 10 NIS 2). Zgodnie z tym przepisem państwa członkowskie mogą wyłączyć z zakresu stosowania niniejszego rozporządzenia podmioty, o których mowa w art. 2 ust. 5 pkt 4–23 dyrektywy 2013/36, mające siedzibę na ich odpowiednich terytoriach. Jeżeli państwo członkowskie korzysta

z takiej możliwości, informuje KE o tym oraz o wszelkich późniejszych zmianach w tym zakresie. Komisja podaje te informacje do wiadomości publicznej na swojej stronie internetowej lub za pomocą innych łatwo dostępnych środków.

Obowiązki ustanowione w NIS 2 nie wiążą się z dostarczaniem informacji, których ujawnienie byłoby sprzeczne z podstawowymi interesami państw członkowskich w zakresie bezpieczeństwa narodowego, bezpieczeństwa publicznego lub obronności (art. 2 ust. 11 NIS 2). Postanowienia NIS 2 nie naruszają postanowień rozporządzenia 2016/679, dyrektywy 2002/58, dyrektywy 2011/93, dyrektywy 2013/40 oraz dyrektywy 2022/2557 (art. 2 ust. 12 NIS 2).

Zgodnie z art. 346 TFUE postanowienia traktatów nie stanowią przeszkody w stosowaniu następujących reguł:

a) żadne państwo członkowskie nie ma obowiązku udzielania informacji, których ujawnienie uznaje za sprzeczne z podstawowymi interesami jego bezpieczeństwa;
b) każde państwo członkowskie może podejmować środki, jakie uważa za konieczne w celu ochrony podstawowych interesów jego bezpieczeństwa, a które odnoszą się do produkcji lub handlu bronią, amunicją lub materiałami wojennymi.

Środki takie nie mogą negatywnie wpływać na warunki konkurencji na rynku wewnętrznym w odniesieniu do produktów, które nie są przeznaczone wyłącznie do celów wojskowych. Bez naruszenia przywołanych postanowień art. 346 TFUE informacje, które są poufne zgodnie z przepisami unijnymi lub krajowymi, takimi jak przepisy dotyczące tajemnicy przedsiębiorstwa, podlegają wymianie z Komisją i innymi odpowiednimi organami zgodnie z NIS 2 tylko wtedy, gdy wymiana taka jest niezbędna do stosowania niniejszej dyrektywy. Informacje podlegające wymianie ogranicza się do tego, co jest istotne dla celów takiej wymiany i proporcjonalne do jej celów. Podczas wymiany informacji zachowuje się poufność tych informacji oraz chroni się bezpieczeństwo i interesy handlowe danych podmiotów (art. 2 ust. 13 NIS 2). Podmioty, właściwe organy, pojedyncze punkty kontaktowe i CSIRT przetwarzają dane osobowe w zakresie niezbędnym do celów NIS 2 i zgodnie z rozporządzeniem 2016/679. Przetwarzanie danych osobowych na mocy niniejszej dyrektywy przez dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności elektronicznej odbywa się zgodnie z unijnymi przepisami o ochronie danych i unijnym prawem dotyczącym prywatności, w szczególności dyrektywą 2002/58 (art. 2 ust. 14 NIS 2).

Postanowienia art. 21 NIS 2 określają środki zarządzania ryzykiem w cyberbezpieczeństwie. Zgodnie z art. 21 ust. 1 NIS 2 państwa członkowskie powinny zapewnić, aby podmioty kluczowe i ważne wprowadzały odpowiednie i proporcjonalne

środki techniczne, operacyjne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu. Przy uwzględnieniu najnowszego stanu wiedzy oraz, w stosownych przypadkach, odpowiednich norm europejskich i międzynarodowych, a także kosztów wdrożenia środki, o których wcześniej mowa, zapewniają poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka. Oceniając proporcjonalność tych środków, należycie uwzględnia się stopień narażenia podmiotu na ryzyko, wielkość podmiotu i prawdopodobieństwo wystąpienia incydentów oraz ich dotkliwość, w tym ich skutki społeczne i gospodarcze.

Według art. 21 ust. 2 NIS 2 natomiast środki, o których mowa w art. 21 ust. 1 NIS 2, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy:

a) politykę analizy ryzyka i bezpieczeństwa systemów informatycznych;
b) obsługę incydentu;
c) ciągłość działania, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej oraz zarządzanie kryzysowe;
d) bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami;
e) bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie;
f) polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;
g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa;
h) polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania;
i) bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami;
j) w stosownych przypadkach – stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.

Zgodnie z art. 21 ust. 3 NIS 2 państwa członkowskie powinny zapewnić, aby rozważając, które ze środków w zakresie bezpieczeństwa łańcucha dostaw

(art. 21 ust. 2 lit. d NIS 2) są odpowiednie, podmioty uwzględniały podatności charakterystyczne dla każdego bezpośredniego dostawcy i usługodawcy oraz ogólną jakość produktów i praktyk cyberbezpieczeństwa dostawców i usługodawców, w tym ich procedury bezpiecznego opracowywania. Państwa członkowskie powinny również zapewnić, aby rozważając, które ze środków w zakresie bezpieczeństwa łańcucha dostaw są odpowiednie, uwzględniać wyniki skoordynowanych oszacowań ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw przeprowadzonych zgodnie z art. 22 ust. 1 NIS 2. Państwa członkowskie są obowiązane także zapewnić, aby podmiot, który stwierdzi, że nie spełnia środków określonych w art. 21 ust. 2 NIS 2, bez zbędnej zwłoki wprowadził wszelkie istotne, odpowiednie i proporcjonalne środki naprawcze (art. 21 ust. 4 NIS 2).

Do 17 października 2024 r. KE powinna przyjąć akty wykonawcze określające wymogi techniczne i metodykę dotyczącą środków, o których mowa w art. 21 ust. 2 NIS 2, w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych oraz platform sieci społecznościowych i dostawców usług zaufania. Komisja może przyjąć akty wykonawcze określające wymogi techniczne i metodykę, a w razie potrzeby również wymogi sektorowe dotyczące środków, o których mowa w art. 21 ust. 2 NIS 2, w odniesieniu do podmiotów kluczowych i ważnych innych niż te, o których mowa wcześniej. Przygotowując akty wykonawcze, KE na tyle, na ile to możliwe, stosuje się do norm międzynarodowych i europejskich, a także odpowiednich specyfikacji technicznych. Komisja wymienia się informacjami i wraz z ENISA współpracuje nad projektami aktów wykonawczych (art. 21 ust. 5 NIS 2).

Postanowienia art. 22 NIS 2 dotyczą skoordynowanych na poziomie Unii szacowań ryzyka krytycznych łańcuchów dostaw. Zgodnie z art. 22 ust. 1 NIS 2, NISCG we współpracy z KE i ENISA może przeprowadzać skoordynowane szacowanie ryzyka dla bezpieczeństwa określonych krytycznych łańcuchów dostaw usług ICT, systemów ICT lub produktów ICT, z uwzględnieniem technicznych i, w stosownych przypadkach, pozatechnicznych czynników ryzyka. Po konsultacji z NISCG i ENISA oraz w razie potrzeby z odpowiednimi zainteresowanymi stronami KE wskazuje konkretne krytyczne usługi ICT, systemy ICT lub produkty ICT, które można poddać skoordynowanemu oszacowaniu ryzyka dla bezpieczeństwa (art. 22 ust. 2 NIS 2).

Przepis art. 23 NIS 2 określa obowiązki w zakresie zgłaszania incydentów. Zgodnie z art. 23 ust. 1 NIS 2 każde państwo członkowskie powinno zapewnić, aby podmioty kluczowe i ważne bez zbędnej zwłoki zgłaszały swojemu

właściwemu CSIRT lub, jeżeli ma to zastosowanie, swojemu właściwemu organowi, incydent mający istotny wpływ na świadczenie przez nie usług, o którym mowa w art. 21 ust. 3 NIS 2 (poważny incydent). Incydent uznaje się za poważny, jeżeli:

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.

W stosownych przypadkach dane podmioty bez zbędnej zwłoki powinny powiadamiać odbiorców swoich usług o poważnych incydentach, które mogą mieć niekorzystny wpływ na świadczenie tych usług. Każde państwo członkowskie powinno zapewnić, aby podmioty te zgłaszały m.in. informacje umożliwiające CSIRT lub, jeżeli ma to zastosowanie, właściwemu organowi ustalenie transgranicznego wpływu incydentu. Samo zgłoszenie nie nakłada na podmiot zgłaszający zwiększonej odpowiedzialności. Jeżeli dane podmioty zgłoszą poważny incydent właściwemu organowi, państwo członkowskie powinno zapewnić, aby ten właściwy organ po otrzymaniu zgłoszenia przekazał je CSIRT.

Przepis art. 24 NIS 2 reguluje stosowanie europejskich programów certyfikacji cyberbezpieczeństwa. Zgodnie z art. 24 ust. 1 NIS 2, aby wykazać zgodność ze szczególnymi wymogami art. 21 NIS 2, państwa członkowskie mogą wymagać od podmiotów kluczowych i ważnych stosowania konkretnych produktów ICT, usług ICT i procesów ICT opracowanych przez dany podmiot kluczowy lub ważny lub nabytych od osób trzecich, certyfikowanych zgodnie z europejskimi programami certyfikacji cyberbezpieczeństwa przyjętymi na podstawie art. 49 rozporządzenia 2019/881. Ponadto państwa członkowskie powinny zachęcać podmioty kluczowe i ważne do korzystania z kwalifikowanych usług zaufania. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 38 NIS 2 w celu uzupełnienia niniejszej dyrektywy przez określenie, od których kategorii podmiotów kluczowych i ważnych należy wymagać stosowania certyfikowanych produktów ICT, usług ICT i procesów ICT lub uzyskania certyfikacji dla swoich własnych produktów ICT, usług ICT i procesów ICT na podstawie europejskiego programu certyfikacji cyberbezpieczeństwa przyjętego zgodnie z art. 49 rozporządzenia 2019/881. Te akty delegowane przyjmuje się w razie stwierdzenia niewystarczających poziomów cyberbezpieczeństwa i określa się w nich termin wdrażania. Przed przyjęciem takich aktów delegowanych Komisja przeprowadza ocenę skutków i prowadzi konsultacje (art. 24 ust. 2 NIS 2).

Rozdział VII NIS 2 zatytułowany jest *Nadzór i egzekwowanie przepisów.* Zgodnie z art. 31 ust. 1 NIS 2 państwa członkowskie powinny zapewnić, aby ich właściwe organy skutecznie monitorowały przestrzeganie niniejszej dyrektywy

i stosowały środki niezbędne do zagwarantowania tego przestrzegania. Państwa członkowskie mogą zezwolić ich właściwym organom na wprowadzenie hierarchii priorytetów w odniesieniu do zadań nadzorczych. Taka hierarchia priorytetów bazuje na podejściu uwzględniającym analizę ryzyka. W tym celu, wykonując zadania nadzorcze określone w art. 32 i 33 NIS 2, właściwe organy mogą określić metodykę nadzorczą pozwalającą ustalić hierarchię priorytetów w tych zadaniach na podstawie podejścia uwzględniającego analizę ryzyka (art. 31 ust. 2 NIS 2). Właściwe organy, odpowiadając na incydenty, które doprowadziły do naruszeń danych osobowych, ściśle współpracują z organami nadzorczymi, na mocy rozporządzenia 2016/679, bez ograniczania właściwości i zadań organów nadzorczych określonych w tym rozporządzeniu (art. 31 ust. 3 NIS 2). Nie naruszając krajowych ram ustawodawczych i instytucjonalnych, państwa członkowskie powinny zapewnić, aby nadzorując przestrzeganie NIS 2 przez podmioty administracji publicznej oraz nakładając środki egzekwowania przepisów w odniesieniu do naruszeń niniejszej dyrektywy, właściwe organy miały odpowiednie uprawnienia do podejmowania takich zadań w sposób niezależny pod względem operacyjnym wobec nadzorowanych podmiotów administracji publicznej. Państwa członkowskie mogą podjąć decyzję o nałożeniu na te podmioty odpowiednich, proporcjonalnych i skutecznych środków nadzoru i egzekwowania przepisów zgodnie z krajowymi ramami ustawodawczymi i instytucjonalnymi (art. 31 ust. 4 NIS 2).

Przepis art. 32 NIS 2 dotyczy środków nadzoru i egzekwowania przepisów dla podmiotów kluczowych. Zgodnie więc z art. 32 ust. 1–2 NIS 2 państwa członkowskie powinny zapewnić, aby środki nadzoru lub egzekwowania przepisów nakładane na podmioty kluczowe w odniesieniu do obowiązków określonych w niniejszej dyrektywie były skuteczne, proporcjonalne i odstraszające, stosownie do okoliczności każdego indywidualnego przypadku. Państwa członkowskie powinny zapewnić, aby wykonując uprawnienia nadzorcze wobec podmiotów kluczowych, właściwe organy były uprawnione do objęcia tych podmiotów co najmniej:

a) kontrolami na miejscu i nadzorem zdalnym, w tym wyrywkowymi kontrolami prowadzonymi przez przeszkolonych specjalistów;
b) regularnymi ukierunkowanymi audytami bezpieczeństwa prowadzonymi przez niezależną instytucję lub właściwy organ;
c) audytami doraźnymi, w tym w uzasadnionych przypadkach w związku z wystąpieniem poważnego incydentu lub z naruszeniem niniejszej dyrektywy przez podmiot kluczowy;
d) skanami bezpieczeństwa na podstawie obiektywnych, niedyskryminacyjnych, sprawiedliwych i przejrzystych kryteriów szacowania ryzyka, w razie potrzeby we współpracy z danym podmiotem;

e) wnioskami o udzielenie informacji niezbędnych do oceny środków zarządzania ryzykiem w cyberbezpieczeństwie przyjętych przez dany podmiot, w tym udokumentowanej polityki cyberbezpieczeństwa;
f) wnioskami o udzielenie dostępu do danych, dokumentów i informacji koniecznych do wykonywania ich zadań nadzorczych;
g) wnioskami o przedstawienie dowodów realizacji polityki cyberbezpieczeństwa, takich jak wyniki audytu bezpieczeństwa przeprowadzonego przez wykwalifikowanego audytora oraz odpowiednie dowody.

Ukierunkowane audyty bezpieczeństwa, o których mowa w art. 32 ust. 2 lit. b NIS 2, opierają się na oszacowaniach ryzyka przeprowadzonych przez właściwy organ lub badany podmiot bądź na innych dostępnych informacjach dotyczących ryzyka. Wyniki ukierunkowanych audytów bezpieczeństwa udostępnia się właściwemu organowi. Koszty takiego ukierunkowanego audytu bezpieczeństwa prowadzonego przez niezależną instytucję pokrywa podmiot poddawany audytowi, z wyjątkiem należycie uzasadnionych przypadków, gdy właściwy organ postanowi inaczej.

Z kolei przepis art. 33 NIS 2 dotyczy środków nadzoru i egzekwowania przepisów w odniesieniu do podmiotów ważnych. Zgodnie z art. 33 ust. 1–2 NIS 2 w przypadku otrzymania dowodu, wskazania lub informacji, że podmiot ważny rzekomo nie stosuje się do niniejszej dyrektywy, w szczególności jej w art. 21 (środki zarządzania ryzykiem w cyberbezpieczeństwie) i 23 (obowiązki w zakresie zgłaszania incydentów), państwa członkowskie powinny zapewnić, aby w razie potrzeby właściwe organy podjęły działania w postaci środków nadzoru ex *post*. Państwa członkowskie powinny zapewnić, aby środki te były skuteczne, proporcjonalne i odstraszające stosownie do okoliczności każdego indywidualnego przypadku. Państwa członkowskie powinny zapewnić, aby wykonując zadania nadzorcze wobec podmiotów ważnych, właściwe organy były uprawnione do objęcia tych podmiotów co najmniej:

a) kontrolami na miejscu i nadzorem zdalnym ex *post*, prowadzonymi przez przeszkolonych specjalistów;
b) ukierunkowanymi audytami bezpieczeństwa prowadzonymi przez niezależną instytucję lub właściwy organ;
c) skanami bezpieczeństwa na podstawie obiektywnych, niedyskryminacyjnych, sprawiedliwych i przejrzystych kryteriów szacowania ryzyka, w razie potrzeby we współpracy z danym podmiotem;
d) wnioskami o udzielenie informacji niezbędnych do oceny ex *post* środków zarządzania ryzykiem w cyberbezpieczeństwie, przyjętych przez dany podmiot, w tym udokumentowanej polityki cyberbezpieczeństwa;
e) wnioskami o udzielenie dostępu do danych, dokumentów i informacji koniecznych do wykonywania ich zadań nadzorczych;

f) wnioskami o przedstawienie dowodów realizacji polityki cyberbezpieczeństwa, takich jak wyniki audytu bezpieczeństwa przeprowadzonego przez wykwalifikowanego audytora oraz odpowiednie dowody.

Ukierunkowane audyty bezpieczeństwa, o których mowa w art. 33 ust. 2 lit. b NIS 2, opierają się na oszacowaniach ryzyka przeprowadzonych przez właściwy organ lub badany podmiot bądź na innych dostępnych informacjach o ryzyku. Wyniki ukierunkowanych audytów bezpieczeństwa udostępnia się właściwemu organowi. Koszty takiego ukierunkowanego audytu bezpieczeństwa prowadzonego przez niezależną instytucję pokrywa podmiot poddany audytowi, z wyjątkiem należycie uzasadnionych przypadków, gdy właściwy organ postanowi inaczej.

Przepis art. 34 NIS 2 określa ogólne warunki nakładania administracyjnych kar pieniężnych na podmioty kluczowe i ważne. Państwa członkowskie powinny zapewnić, aby administracyjne kary pieniężne nakładane na podmioty kluczowe i ważne zgodnie z art. 34 NIS 2 za naruszenia niniejszej dyrektywy były skuteczne, proporcjonalne i odstraszające, stosownie do okoliczności każdego indywidualnego przypadku (art. 34 ust. 1 NIS 2).

Podejmując decyzję o nałożeniu administracyjnej kary pieniężnej i o jej wysokości, w każdym indywidualnym przypadku należycie uwzględnia się co najmniej elementy wymienione w art. 32 ust. 7 NIS 2 (art. 34 ust. 3 NIS 2). Zgodnie więc z art. 32 ust. 7 NIS 2, przyjmując środki egzekwowania przepisów, właściwe organy powinny przestrzegać prawa do obrony oraz brać pod uwagę okoliczności każdego indywidualnego przypadku i należycie uwzględniać co najmniej:

a) wagę naruszenia i znaczenie naruszonych przepisów, przy czym za poważne należy uznać w każdym przypadku m.in. następujące naruszenia:
   - powtarzające się naruszenia;
   - niezgłoszenie lub nieusunięcie poważnych incydentów;
   - nieusunięcie uchybień zgodnie z wiążącymi nakazami właściwych organów;
   - utrudnianie prowadzenia audytów lub działań monitorujących nakazanych przez właściwy organ po stwierdzeniu naruszenia;
   - dostarczanie nieprawdziwych lub rażąco niedokładnych informacji w odniesieniu do środków zarządzania ryzykiem w cyberbezpieczeństwie lub obowiązków zgłaszania incydentów;
b) czas trwania naruszenia;
c) istotne wcześniejsze naruszenia ze strony danego podmiotu;
d) spowodowane szkody majątkowe i niemajątkowe, w tym straty finansowe lub gospodarcze, wpływ na inne usługi i liczbę użytkowników, których dotyka incydent;

e) umyślny lub nieumyślny charakter czynu ze strony sprawcy naruszenia;
f) środki zastosowane przez podmiot, aby zapobiec szkodom majątkowym i niemajątkowym lub je ograniczyć;
g) stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji;
h) stopień współpracy odpowiedzialnych osób fizycznych lub prawnych z właściwymi organami.

Państwa członkowskie powinny zapewnić, aby podmioty kluczowe, które naruszają postanowienia art. 21 lub 23 NIS 2, podlegały zgodnie z art. 34 ust. 2 i 3 NIS 2 administracyjnym karom pieniężnym, które przewidują w maksymalnej wysokości kary w wysokości co najmniej 10 mln euro lub co najmniej 2% łącznego rocznego światowego obrotu w poprzednim roku obrotowym przedsiębiorstwa, do którego należy podmiot kluczowy, przy czym zastosowanie ma kwota wyższa (art. 34 ust. 4 NIS 2). Analogiczny przepis dotyczy podmiotów ważnych. Inne są natomiast wysokości kar. Zgodnie więc z art. 34 ust. 5 NIS 2 państwa członkowskie powinny zapewnić, aby podmioty ważne, które naruszają postanowienia art. 21 lub 23 NIS 2, podlegały, zgodnie z art. 34 ust. 2 i 3 NIS 2, administracyjnym karom pieniężnym w maksymalnej wysokości co najmniej 7 mln euro lub 1,4% łącznego rocznego światowego obrotu w poprzednim roku obrotowym przedsiębiorstwa, do którego należy podmiot ważny, przy czym zastosowanie ma kwota wyższa.

Państwa członkowskie mogą natomiast także przewidzieć uprawnienie do nakładania okresowych kar pieniężnych w celu przymuszenia podmiotu kluczowego lub ważnego do zaprzestania naruszenia NIS 2, zgodnie z wcześniejszą decyzją właściwego organu (art. 34 ust. 6 NIS 2). W każdym przypadku nakładane kary pieniężne muszą być skuteczne, proporcjonalne i odstraszające. Do dnia 17 października 2024 r. państwo członkowskie powinno powiadomić KE o przepisach, które przyjęło, oraz powiadomić o ewentualnych późniejszych zmianach przepisów lub innych zmianach, które mają na nie wpływ (art. 34 ust. 8 NIS 2).

Zgodnie z postanowieniami art. 45 NIS 2 dyrektywa ta wchodzi w życie 20. dnia po jej opublikowaniu w Dzienniku Urzędowym UE. Natomiast zgodnie z art. 41 tej dyrektywy w ciągu 21 miesięcy od daty wejścia w życie NIS 2 (tj. styczeń 2025 r.) państwa członkowskie muszą przyjąć i opublikować przepisy niezbędne do wykonania NIS 2. W przypadku Polski będzie to nowa ustawa lub nowelizacja obowiązującej u.k.s.c. oraz nowe lub znowelizowane akty wykonawcze. Konieczne będą także zmiany w innych aktach prawnych z uwagi na potrzebę większej harmonizacji przepisów w zakresie Krajowego Planu Zarządzania Kryzysowego oraz działania Zespołu Incydentów Krytycznych i Rządowego Zespołu

Zarządzania Kryzysowego, funkcjonującego na podstawie ustawy o zarządzaniu kryzysowym. Konieczne będzie również opracowanie nowych projektów aktów wykonawczych w zakresie uregulowań NIS 2 wprowadzających nowe obowiązki, zmiany do obecnych obowiązków (np. wynikających z rozszerzonego zakresu podmiotów zobowiązanych) czy też z uwagi na wprowadzenie nowych instytucji, nieznanych w NIS, jak np. rejestry prowadzone przez organy UE. Nowe obowiązki dla państw członkowskich UE obejmują również obowiązki informacyjne dotyczące podmiotów kluczowych i ważnych (art. 3 ust. 3–6 dyrektywy NIS 2), a ich wykonanie również będzie wymagało stosownych uregulowań w polskim prawie.

Przepisy art. 5 NIS 2 określają sposób transpozycji przedmiotowej dyrektywy jako tzw. harmonizację minimalną. Oznacza to, iż postanowienia dyrektywy nie uniemożliwiają państwom członkowskim przyjęcia lub utrzymania przepisów zapewniających wyższy poziom cyberbezpieczeństwa, pod warunkiem że takie przepisy są spójne z obowiązkami państw członkowskich ustanowionymi w prawie UE.

W przeszłości zdarzało się nie dotrzymać terminu wdrożenia danej dyrektywy, ale terminowe (a nawet szybsze niż wymagane 21 miesięcy – określone w art. 41 NIS 2) wdrożenie dyrektywy NIS 2 jest bardzo pożądane zarówno z powodu rosnącej liczby naruszeń cyberbezpieczeństwa (w tym tzw. szeroko pojętych ataków hakerskich), jak i obecnej sytuacji geopolitycznej w Europie (wojna Ukraina–Rosja).

Wdrożenie NIS 2 z pewnością wiąże się z koniecznością poniesienia kosztów zarówno przez podmioty zobowiązane do realizacji obowiązków wynikających z NIS 2, jak i przez organy państwa. Uwzględniając panujące w branży IT tendencje w tym zakresie i rosnącą świadomość zagrożeń, głównym zadaniem państwa jest właściwa koordynacja, harmonizacja i synchronizacja wszelkich działań w obszarze cyberbezpieczeństwa, które bez właściwego zarządzania będą generować koszty, a jednocześnie nie przyniosą spodziewanych efektów. Większość nowych obowiązków określonych przez NIS 2 to obowiązki organizacyjne: zasady właściwej komunikacji, raportowania, kontroli, analizy ryzyka i zarządzania tym ryzykiem, przestrzegania zasad opracowanych przez dedykowane organy UE. Koszty konieczne do poniesienia w wyżej wymienionym zakresie, przy odpowiednim zarządzaniu cyberbezpieczeństwem, będą zdecydowanie mniejsze niż koszty wynikające z potencjalnych incydentów bezpieczeństwa.

Dyrektywa wprowadza także obowiązki dla organów unijnych, takie jak np. prowadzenie na szczeblu unijnym rejestrów podatności, bazy danych dotyczących rejestracji nazw domen czy też rejestrów podmiotów zobowiązanych w poszczególnych krajach, cykliczne opracowywanie przez ENISA (*Sprawozdania*

*o stanie cyberbezpieczeństwa w Unii*) oraz prowadzenie skoordynowanej oceny ryzyka krytycznych łańcuchów dostaw na poziomie UE. Wykonywanie nowych obowiązków przez organy unijne wiąże się z koniecznością współpracy organów krajowych z organami UE m.in. w zakresie zbierania i przekazywania informacji dotyczących danego kraju członkowskiego.

Z wprowadzenia nowych obowiązków wobec podmiotów zobowiązanych (takich jak m.in.: przeprowadzanie analizy ryzyka i opracowanie stosownych polityk, w tym polityki bezpieczeństwa systemów informatycznych, właściwa obsługa incydentów, zapewnienie ciągłości działania, właściwe zarządzanie kryzysowe, zapewnienie bezpieczeństwa łańcucha dostaw, obsługa i ujawnianie podatności, wprowadzenie procedur w zakresie testowania i audytu, wykorzystywania kryptografii i szyfrowania) wynika konieczność rozszerzenia zakresu działań nadzorczych, w tym kompetencji osób nadzorujących. Te uregulowania również powinny znaleźć odzwierciedlenie w przepisach wykonawczych.

## 4. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r.

Obecnie obowiązuje 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. Artykuł 1 lit. b tego rozporządzenia określa ramy ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa. Celem ich jest zapewnienie odpowiedniego poziomu cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT w Unii oraz uniknięcia rozdrobnienia rynku wewnętrznego w zakresie programów certyfikacji cyberbezpieczeństwa w UE. Ramy regulacyjne, o których mowa, nie naruszają przepisów szczegółowych dotyczących dobrowolnej lub obowiązkowej certyfikacji zawartych w innych aktach prawnych Unii. Rozporządzenie 2019/881 z uwagi na swój charakter obowiązuje bezpośrednio w Polsce oraz w każdym innym kraju członkowskim i nie wymaga wprowadzania, jak w przypadku dyrektyw do polskiego porządku prawnego.

Zgodnie z art. 2 pkt 9 rozporządzenia 2019/881 *Europejski program certyfikacji cyberbezpieczeństwa* oznacza kompleksowy zbiór przepisów, wymogów technicznych, norm i procedur ustanowionych na poziomie unijnym i mających zastosowanie do certyfikacji lub oceny zgodności określonych produktów ICT, usług ICT i procesów ICT. Według art. 2 pkt 10 rozporządzenia *Krajowy program*

*certyfikacji cyberbezpieczeństwa* oznacza kompleksowy zbiór przepisów, wymogów technicznych, norm i procedur określonych i przyjętych przez krajowy organ publiczny i mających zastosowanie do certyfikacji lub oceny zgodności objętych zakresem danego programu produktów ICT, usług ICT i procesów ICT. Zgodnie natomiast z art. 2 pkt 119 rozporządzenia *Europejski certyfikat cyberbezpieczeństwa* oznacza wydany przez odpowiedni organ dokument poświadczający, że dany produkt ICT, dana usługa ICT lub dany proces ICT zostały ocenione pod względem zgodności ze szczegółowymi wymogami bezpieczeństwa określonymi w europejskim programie certyfikacji cyberbezpieczeństwa.

Rozdział II (art. 5–12) rozporządzenia 2019/881 określa zadania ENISA. Przepis art. 5 pkt 4 rozporządzenia 2019/881 stanowi, że ENISA przyczynia się do opracowywania i wdrażania polityki i prawa Unii poprzez wkład w pracę grupy współpracy, przez zapewnianie wiedzy fachowej i pomoc. Przepis art. 11 NIS mówi natomiast o współpracy pomiędzy tymi dwoma instytucjami w zakresie przygotowywania wytycznych. Szereg postanowień rozporządzenia 2019/881 dotyczy wydawania wytycznych przez ENISA. Zgodnie z art. 5 pkt 2 rozporządzenia 2019/881 ENISA przyczynia się do opracowywania i wdrażania polityki i prawa Unii poprzez pomoc państwom członkowskim przy wdrażaniu polityki i prawa Unii w dziedzinie cyberbezpieczeństwa w sposób jednolity, w tym za pomocą wydawania opinii, wytycznych, udzielania porad i najlepszych praktyk dotyczących takich zagadnień, jak zarządzanie ryzykiem, zgłaszanie incydentów i wymiana informacji, jak również za pomocą ułatwiania wymiany najlepszych praktyk pomiędzy właściwymi organami w tym zakresie. Z kolei, zgodnie z art. 7 pkt 2 lit. b rozporządzenia 2019/881, ENISA współpracuje na poziomie operacyjnym i tworzy synergię z instytucjami, organami i jednostkami organizacyjnymi Unii, w tym z CERT-UE, ze służbami zajmującymi się cyberprzestępczością i z organami nadzoru zajmującymi się ochroną prywatności i danych osobowych w celu rozwiązywania kwestii będących przedmiotem wspólnego zainteresowania, m.in. poprzez zapewnianie doradztwa i wydawanie wytycznych w istotnych kwestiach związanych z cyberbezpieczeństwem. ENISA sporządza i publikuje wytyczne oraz opracowuje dobre praktyki dotyczące wymogów cyberbezpieczeństwa w zakresie produktów ICT, procesów ICT i usług ICT, we współpracy z krajowymi organami ds. certyfikacji cyberbezpieczeństwa oraz z przemysłem prowadzonej w formalny, ustrukturyzowany i przejrzysty sposób. ENISA opracowuje, we współpracy z państwami członkowskimi i przemysłem, porady i wytyczne dotyczące kwestii technicznych związanych z wymogami bezpieczeństwa dla operatorów usług kluczowych i dostawców usług cyfrowych, a także dotyczące już istniejących norm, w tym norm krajowych państw członkowskich (art. 8 ust. 3 i 6 rozporządzenia 2019/881).

Tytuł III rozporządzenia 2019/881 (art. 46 i n.), jest poświęcony ramom certyfikacji bezpieczeństwa. Zgodnie z art. 46 tego rozporządzenia ustanawia się europejskie ramy certyfikacji cyberbezpieczeństwa w celu poprawy warunków funkcjonowania rynku wewnętrznego poprzez zwiększenie poziomu cyberbezpieczeństwa w Unii oraz umożliwienie zharmonizowanego podejścia na poziomie unijnym do europejskich programów certyfikacji cyberbezpieczeństwa z myślą o stworzeniu jednolitego rynku cyfrowego w zakresie produktów ICT, usług ICT i procesów ICT. Europejskie ramy certyfikacji cyberbezpieczeństwa określają mechanizm ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa i potwierdzania, że produkty ICT, usługi ICT i procesy ICT, które oceniono zgodnie z tymi programami, są zgodne z określonymi wymogami bezpieczeństwa mającymi na celu zabezpieczenie dostępności, autentyczności, integralności lub poufności przechowywanych, przekazywanych lub przetwarzanych danych bądź funkcji lub usług oferowanych albo dostępnych za pośrednictwem tych produktów, usług i procesów w trakcie ich całego cyklu życia.

Zgodnie z art. 47 ust. 1–2 rozporządzenia 2019/881 komisja publikuje unijny kroczący program prac na rzecz europejskich programów certyfikacji cyberbezpieczeństwa, wskazujący strategiczne priorytety przyszłych europejskich programów certyfikacji cyberbezpieczeństwa. Unijny kroczący program prac zawiera w szczególności wykaz produktów ICT, usług ICT i procesów ICT lub ich kategorie, które mają możliwość korzystania z włączenia w zakres stosowania danego europejskiego programu certyfikacji cyberbezpieczeństwa. KE może zwrócić się do ENISA z wnioskiem o przygotowanie propozycji programu lub o przegląd istniejącego europejskiego programu cyberbezpieczeństwa na podstawie unijnego kroczącego programu prac (art. 48 ust. 1 rozporządzenia 2019/881). ENISA powinna wspierać i propagować opracowywanie oraz realizację ustanowionej w tytule III tego rozporządzenia polityki UE w zakresie certyfikacji cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT poprzez: monitorowanie na bieżąco zmian w powiązanych dziedzinach normalizacji i zalecanie odpowiednich specyfikacji technicznych do zastosowania przy tworzeniu europejskich programów certyfikacji cyberbezpieczeństwa zgodnie z art. 54 ust. 1 lit. c, w przypadkach gdy nie istnieją normy w danym zakresie, oraz przygotowywanie propozycji dotyczących europejskich programów certyfikacji cyberbezpieczeństwa dla produktów ICT, usług ICT i procesów ICT (art. 8 ust. 1 lit. a i b rozporządzenia 2019/881). ENISA powinna przyczyniać się do budowania zdolności związanych z procesami oceny i certyfikacji poprzez sporządzanie i wydawanie wytycznych, a także udzielania wsparcia państwom członkowskim na ich wniosek (art. 8 ust. 4 rozporządzenia 2019/881).

## 5. Zalecenia w sprawie cyberbezpieczeństwa sieci 5G

W UE przyjęte zostały także regulacje, które odnoszą się bezpośrednio do bezpieczeństwa infrastruktury i usług świadczonych w określonej technologii, czyli 5G. W dniu 26 marca 2019 r. Komisja Europejska przyjęła Zalecenia (UE) C/2019/2335 w sprawie cyberbezpieczeństwa sieci 5G. NISCG przygotował raport z dnia 9 października 2019 r. *EU coordinated risk assessment of the cybersecurity of 5G networks*[10], który zawiera analizę zagrożeń dla sieci 5G. W listopadzie 2019 r. ENISA w raporcie *ENISA Threat Landscape for 5G Networks*[11] przedstawiła katalog możliwych zagrożeń dla sieci 5G.

W dniu 29 stycznia 2020 r. został opublikowany raport NIS Cooperation Group, przygotowany we współpracy z KE i ENISA *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*[12]. NISCG została ustanowiona przez Dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii z dnia 6 lipca 2016 r.[13] Zgodnie z punktem 4 preambuły NIS „należy utworzyć grupę współpracy, złożoną z przedstawicieli państw członkowskich, Komisji oraz Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (zwanej dalej «ENISA») w celu wspierania i ułatwiania współpracy strategicznej między państwami członkowskimi w zakresie bezpieczeństwa sieci i systemów informatycznych".

NISCG składa się z przedstawicieli państw członkowskich, KE i ENISA. Zadania NISCG określa art. 11 NIS, który mówi o współpracy pomiędzy tymi podmiotami w zakresie przygotowywania rekomendacji. Z kolei rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 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) z dnia 17 kwietnia 2019 r.[14], zgodnie z nazwą powołuje i reguluje działanie ENISA (The European Union Agency for Cybersecurity).

Rozdział II (art. 5–12) rozporządzenia 2019/881 określa zadania ENISA. Przepis art. 5 pkt 4 rozporządzenia 2019/881 stanowi, że: ENISA przyczynia się do

---

10 https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049 [dostęp: 25.07.2023 r.].

11 https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks [dostęp: 30.08.2023 r.].

12 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures [dostęp: 25.02.2023 r.].

13 Dz.Urz. UE L 194 z dnia 19.07.2016 r.

14 Dz.Urz. UE L 151 z dnia 7.06.2019 r.

opracowywania i wdrażania polityki i prawa Unii poprzez wkład w prace grupy współpracy na podstawie art. 11 dyrektywy (UE) 2016/1148, przez zapewnianie wiedzy fachowej i pomocy. Szereg postanowień rozporządzenia 2019/881 dotyczy wydawania wytycznych przez ENISA. W szczególności, zgodnie z art. 5 pkt 2 rozporządzenia 2019/881, ENISA przyczynia się do opracowywania i wdrażania polityki i prawa Unii poprzez pomoc państwom członkowskim przy wdrażaniu polityki i prawa Unii w dziedzinie cyberbezpieczeństwa w sposób jednolity, w szczególności w związku z dyrektywą (UE) 2016/1148, w tym za pomocą wydawania opinii czy wytycznych.

Wspomniany *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures* (5G Toolbox) wskazuje i opisuje zestaw środków strategicznych i technicznych, a także odpowiadające im działania wspierające mające na celu zwiększenie ich skuteczności, które można wdrożyć w celu ograniczenia zidentyfikowanych zagrożeń w sprawozdaniu ze skoordynowanej przez UE oceny ryzyka cyberbezpieczeństwa sieci 5G. W szczególności wspomnieć należy o postanowieniach 5G Toolbox, o których mowa na s. 42, a zamieszczonych w punktach: 2. *Supplier-specific vulnerabilities* oraz 3. *Vulnerabilities stemming from dependency to individual suppliers*. W tabelarycznym zestawieniu ryzyk zawartych w 5G Toolbox chodzi o ryzyka wymienione na s. 35 i oznaczone symbolami SM03 i SM04.

Dokument 5G Toolbox pod względem prawnym ma charakter wytycznych, zbliżonych, ale nie takich samych jak wytyczne wydawane przez ENISA. Wytyczne wydawane są na podstawie postanowień dyrektywy, ale nie są postanowieniami dyrektywy. Wytyczne NISCG (5G Toolbox) nie są przepisami prawa polskiego, gdyż nie są postanowieniami rozporządzenia UE lub dyrektywy UE, które to postanowienia zostały wprowadzone do polskiego porządku prawnego. Wytyczne NISCG powinny być uwzględniane analogicznie jak wytyczne ENISA.

Uwzględnianie wytycznych NISCG może następować w zasadzie w dwojakiej formie. Po pierwsze, w procesie przygotowywania aktów prawnych. Po drugie, w zakresie stosowania i interpretacji przepisów powszechnie obowiązujących, w szczególności przez organy regulacyjne. Zgodnie z art. 175d p.t. minister właściwy do spraw informatyzacji, wydając rozporządzenie, powinien brać pod uwagę wytyczne Komisji Europejskiej oraz Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA) w tym zakresie. Przepis ten nie wspomina natomiast o Grupie Współpracy NIS. Wskazane już jednak zostało, że w skład Grupy Współpracy NIS wchodzą przedstawiciele ENISA. Przepis art. 11 NIS mówi o współpracy pomiędzy tymi dwiema instytucjami w zakresie przygotowywania rekomendacji. Przyjąć więc można, że minister właściwy do spraw informatyzacji może także uwzględnić, przygotowując rozporządzenie, wytyczne Grupy Współpracy NIS.

KE przyjęła komunikat COM (2020)50 *Secure 5G deployment in the EU – Implementing the EU Toolbox*[15], w którym zatwierdziła wnioski z 5G Toolbox i podkreśliła znaczenie ich skutecznego oraz szybkiego wdrożenia, a także wezwała państwa członkowskie do podjęcia konkretnych kroków w celu ich wdrożenia. NISCG, przy wsparciu KE oraz ENISA, przygotowała w lipcu 2020 r. *Report on Member states' progress in implementing the EU Toolbox on 5G cybersecurity*[16]. W dniu 10 grudnia 2020 r. ENISA opublikowała wytyczne w celu zapewnienia wspólnego podejścia do bezpieczeństwa sieci i usług łączności elektronicznej (ang. *Guideline on Security Measures under the EECC*)[17]. Uzupełnieniem wytycznych ENISA z 10 grudnia 2020 r. był *5G Supplement – to the Guideline on Security Measures under the EECC*[18]. W suplemencie dotyczącym 5G skupiono się na cyberbezpieczeństwie sieci 5G na poziomie polityk bezpieczeństwa określonych w 5G Toolbox.

W grudniu 2020 r. Komisja dokonała przeglądu skutków zalecenia 2019/2335, a w szczególności osiągniętych etapów wdrożenia[19]. 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 skutecznego ograniczania ryzyka w całej UE[20]. Zalecenia zostały przygotowane także przez ECA w raporcie ze stycznia 2022[21]. ECA wskazało, że państwa członkowskie zastosowały rozbieżne podejścia do stosowania sprzętu od dostawców wysokiego ryzyka lub rodzaju i zakresu stosowanych ograniczeń. Raport ECA mówi o potrzebie dostarczenia

---

15 https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64481 [dostęp: 22.01.2023 r.].

16 https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity [dostęp: 24.04.2023 r.].

17 https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc/ [dostęp: 20.03.2023 r.].

18 https://www.enisa.europa.eu/publications/5g-supplement-security-measures-under-eecc/ [dostęp: 20.04.2023 r.].

19 *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: 14.03.2023 r.].

20 *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: 14.01.2023 r.].

21 *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 r.].

dalszych wskazówek lub podejmowania działań wspierających, które dotyczą kluczowych elementów 5G Toolbox 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[22].

Z kolei w swoim zaleceniu z dnia 9 grudnia 2022 r. Rada UE zwróciła się do agencji NISCG o przyspieszenie trwających prac nad oceną ryzyka bezpieczeństwa cybernetycznego i odporności europejskich infrastruktur i sieci komunikacyjnych[23]. W dniu 15 czerwca 2023 r. został opublikowany przygotowany przez NISCG *Second report on Member States' Progress in implementing the EU Toolbox on 5G Cybersecurity*[24]. W niniejszym raporcie przedstawiono 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 przyjąć ramy prawne, aby władze krajowe mogły oceniać profil ryzyka dostawców i na tej podstawie stosować ograniczenia. Według tego raportu uregulowania prawne (ang. *legislative framework*), 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 zakresie wprowadzania ograniczeń dla dostawców wysokiego ryzyka (ang. *high-risk suppliers*) spośród tych krajów 10 wdrożyło restrykcje na dostawców wysokiego ryzyka, 3 pracują nad wdrożeniem odpowiednich regulacji do przepisów krajowych, a 14 krajów nie dokonało tego. W raporcie wskazano, że w przypadku braku działań ze strony państw członkowskich we wdrażaniu 5G Toolbox w UE KE rozważy dalsze działania mające na celu zwiększenie odporności rynku wewnętrznego, w tym zbadanie możliwych ścieżek legislacyjnych, nie naruszając regulacji w państwach członkowskich, które już wdrożyły ograniczenia zgodnie z 5G Toolbox, przy poszanowaniu kompetencji państw członkowskich w zakresie bezpieczeństwa narodowego[25].

---

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

[23] *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 r.].

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

[25] https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity, p. 6, 22, 24 [dostęp: 26.07.2023 r.].

# Rozdział II
# Bezpieczeństwo sieci i usług w łączności elektronicznej w prawie polskim i w dokumentach programowych

## 1. Bezpieczeństwo sieci i usług w łączności elektronicznej w prawie polskim

### 1.1. Prawo telekomunikacyjne

*1.1.1. Bezpieczeństwo i integralność sieci oraz usług telekomunikacyjnych*

Ustawa o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw z dnia 16 listopada 2012 r.[1] wprowadziła m.in. nowy dział VIIa. Zmieniony został art. 175 p.t. oraz dodane zostały nowe art. 175a–175e p.t. Nowela z 16 listopada 2012 r. dokonała w zakresie swojej regulacji wdrożenia następujących dyrektyw Unii Europejskiej:

a) dyrektywy Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniającej dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów[2];
b) dyrektywy Parlamentu Europejskiego i Rady 2009/140/WE z dnia 25 listopada 2009 r. zmieniającej dyrektywy 2002/21/WE w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej, 2002/19/WE w sprawie dostępu do sieci i usług łączności elektronicznej oraz wzajemnych połączeń oraz 2002/20/WE w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej[3].

W szczególności nowela z 16 listopada 2012 r. dokonała implementacji nowego rozdziału IIIa dyrektywy 2002/21/WE w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej, dotyczącego bezpieczeństwa i integralności sieci oraz usług. Artykuł 13a dyrektywy 2002/21/WE zobowiązywał do

---

1 Dz.U. z 2012 r. poz. 1445.
2 Dz.Urz. UE L 337 z 18.12.2009 r., s. 11.
3 Dz.Urz. UE L 337 z 18.12.2009 r., s. 37.

stosowania właściwych środków technicznych i organizacyjnych w razie wystąpienia zagrożenia dla bezpieczeństwa sieci i usług, zapewniających poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka, z uwzględnieniem aktualnego stanu wiedzy i technologii. Przedsiębiorstwa zostały zobowiązane do ochrony integralności sieci w celu zapewnienia ciągłości świadczenia usług oraz do powiadamiania regulatora o każdym naruszeniu bezpieczeństwa. Zgodnie z art. 13b dyrektywy 2002/21/WE regulator powinien być uprawniony do wydawania przedsiębiorcom wiążących instrukcji w sprawach bezpieczeństwa sieci i usług, żądania od nich informacji oraz poddania się na własny koszt audytowi bezpieczeństwa. Treść przepisów dotyczących bezpieczeństwa i integralności sieci oraz usług została dodatkowo zmodyfikowana w związku z implementacją w prawie krajowym przepisów dyrektywy 2016/1148. Implementacja została dokonana ustawą z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, która znowelizowała również ustawę – Prawo telekomunikacyjne.

Dział VIIA zatytułowany *Bezpieczeństwo i integralność sieci i usług telekomunikacyjnych* zawiera przepisy art. 175–175e p.t. Zgodnie z art. 175 ust. 1 p.t. dostawca publicznie dostępnych usług telekomunikacyjnych, a jeżeli jest to konieczne – także operator publicznej sieci telekomunikacyjnej, jest zobowiązany podjąć środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa i integralności sieci, usług oraz przekazu komunikatów w związku ze świadczonymi usługami. Podjęte środki powinny zapewniać poziom bezpieczeństwa odpowiedni do stopnia ryzyka, przy uwzględnieniu najnowocześniejszych osiągnięć technicznych oraz kosztów wprowadzenia tych środków. Bezpieczeństwo i integralność usług są związane z zachowaniem stabilnych warunków dostarczania usług abonentom przy założonej funkcjonalności usług[4]. Dostawca usług jest zobowiązany do informowania użytkowników o wystąpieniu szczególnego ryzyka naruszenia bezpieczeństwa sieci wymagającego podjęcia środków wykraczających poza środki techniczne i organizacyjne podjęte przez dostawcę usług, a także o istniejących możliwościach zapewnienia bezpieczeństwa i związanych z tym kosztach (art. 175 ust. 2 p.t.).

Według art. 175a ust. 1 p.t. przedsiębiorcy telekomunikacyjni są obowiązani niezwłocznie informować Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług, o podjętych działaniach zapobiegawczych i środkach naprawczych oraz podjętych przez przedsiębiorcę działaniach, o których mowa w art. 175 p.t.

[4] Zob. S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2019, uwaga 2 do art. 175. Zob. także w sprawie typowych zagrożeń sieci i usług: M. Betkier, J. Górski, *Ochrona sieci przed zagrożeniami*, „Prawo i Regulacje Świata Telekomunikacji i Mediów" 2010, nr 2, s. 64 i n.

i art. 175c p.t. Prezes UKE przekazuje informacje, o których mowa w art. 175a ust. 1 p.t., jeżeli dotyczą one zdarzeń będących incydentami w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa, CSIRT właściwemu dla zgłaszającego przedsiębiorcy telekomunikacyjnego, zgodnie z art. 26 ust. 5–7 tej ustawy, z wyłączeniem informacji stanowiących tajemnicę przedsiębiorstwa (art. 175a ust. 1a p.t.). Przekazanie, o którym mowa w art. 175a ust. 1a p.t., następuje w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji (art. 175a ust. 1b p.t.). Minister właściwy do spraw informatyzacji został upoważniony do określenia, w drodze rozporządzenia, wzoru formularza do przekazywania informacji, o których mowa w art. 175a ust. 1 p.t., kierując się koniecznością zapewnienia Prezesowi UKE informacji niezbędnych do właściwego realizowania jego obowiązków (art. 175a ust. 2 p.t.). Na podstawie tej delegacji ustawowej zostało wydane przez ministra cyfryzacji rozporządzenie z dnia 20 września 2018 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług[5]. Z kolei przepis art. 175a ust. 2a p.t. przyznał ministrowi właściwemu do spraw informatyzacji delegację do określenia, w drodze rozporządzenia, kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług, biorąc pod uwagę w szczególności wartość procentową użytkowników, na których naruszenie bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych miało wpływ, czas trwania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych powodującego niedostępność lub ograniczenie dostępności sieci bądź usług telekomunikacyjnych oraz rekomendacje i wytyczne Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA). Na podstawie art. 175a ust. 2a p.t. zostało wydane rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług[6].

W praktyce więc, zgodnie z art. 175a p.t., przedsiębiorca ma obowiązek niezwłocznego poinformowania Prezesa UKE o naruszeniu bezpieczeństwa lub integralności, podjętych działaniach zapobiegawczych i środkach naprawczych oraz innych działaniach w tym zakresie. Zgodnie z obowiązującym formularzem raportowym, w części IV.4, przedsiębiorca powinien określić przyczynę

[5] Dz.U. z 2018 r. poz. 1831.

[6] Dz.U. z 2018 r. poz. 1830.

zaistniałego naruszenia, przy czym jedną z opcji jest wskazanie, że przyczyną taką był cyberatak. W przypadku natomiast, gdy zdarzenie miało charakter incydentu w rozumieniu u.k.s.c., tj. incydentu w zakresie cyberbezpieczeństwa, Prezes UKE przekazuje informację właściwemu CSIRT. Prezes UKE jest też uprawniony do korzystania z systemu teleinformatycznego tworzonego na potrzeby krajowego systemu cyberbezpieczeństwa, o którym mowa w art. 46 u.k.s.c. Określone w rozporządzeniu z dnia 20 września 2018 r. progi uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług telekomunikacyjnych są uniwersalne i odnoszą się w praktyce do ciągłości działania usługi (czasu niedostępności) w relacji do zakresu objętych użytkowników. Zapewnia to, że naruszenia (incydenty) związane z cyberprzestrzenią będą raportowane, a informacje te zostaną przekazane właściwym CSIRT.

Obecnie istnieje rozdział pomiędzy regulacją właściwą przedsiębiorcom telekomunikacyjnym (komunikacji elektronicznej) a regulacjami właściwymi dla krajowego systemu cyberbezpieczeństwa. W przyszłości, czyli po implementacji NIS 2, może dojść do wprowadzenia jednolitego modelu regulacji w zakresie cyberbezpieczeństwa, w którym regulacjami z zakresu krajowego systemu cyberbezpieczeństwa będą objęci także przedsiębiorcy telekomunikacyjni. Prezentowane były jednak poglądy opowiadające się za utrzymaniem stanu, w którym istniałyby dwa nakładające się reżimy zgłaszania incydentów bezpieczeństwa i incydentów telekomunikacyjnych, jeden wynikający z p.k.e., a drugi z k.s.c. (po wejściu w życie noweli lub nowej ustawy k.s.c.). W przypadku przyjęcia tego modelu oznaczałoby to, że obowiązki w zakresie bezpieczeństwa regulowane byłyby dwutorowo. Wtedy konieczne byłoby zapewnienie pełnego i precyzyjnego rozdziału pomiędzy incydentami w rozumieniu p.k.e. oraz incydentami w rozumieniu k.s.c. Występowały bowiem istotne różnice nie tylko na poziomie podstawowych definicji, ale także co do zakresu objętych regulacjami podmiotów. Powinien być wtedy także zapewniony odpowiednio długi okres *vacatio legis* na wprowadzenie nowych rozwiązań. Wskazywano, że obowiązki raportowe przedsiębiorców komunikacji elektronicznej powinny zostać utrzymane jedynie wobec Prezesa UKE, a w każdym razie powinien istnieć wyłącznie jeden kanał zgłoszeń. Niezależnie od przyjętego ostatecznie sposobu regulacji istotne jest, aby konkretny przedsiębiorca komunikacji elektronicznej odpowiadał tylko za bezpieczeństwo i integralność swoich usług i swojej infrastruktury. Projektowane przepisy nie powinny wkraczać w tę sferę, powodując nałożenie na tych przedsiębiorców szerszych obowiązków, gdyż byłaby to ingerencja w konkurencyjny rynek rozwiązań w zakresie bezpieczeństwa teleinformatycznego.

Według art. 175b ust. 1 p.t. Prezes UKE informuje o wystąpieniu naruszenia bezpieczeństwa lub integralności sieci lub usług organy regulacyjne innych państw członkowskich oraz Europejską Agencję do spraw Bezpieczeństwa Sieci i Informacji (ENISA), jeżeli uzna charakter tego naruszenia za istotny. Prezes UKE publikuje na stronie internetowej UKE informację, o której mowa wcześniej, lub nakłada na przedsiębiorcę telekomunikacyjnego, w drodze decyzji, obowiązek podania jej do publicznej wiadomości, wskazując sposób jej publikacji, jeżeli uzna, że leży to w interesie publicznym (art. 175b ust. 2 p.t.). Prezes UKE w terminie do końca lutego każdego roku przekazuje Komisji Europejskiej oraz Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji sprawozdanie za rok poprzedni zawierające informacje o naruszeniach i działaniach, o których mowa w art. 175b ust. 1 i 2 p.t. oraz w art. 175a ust. 1 p.t. (art. 175b ust. 3 p.t.). Na podstawie informacji, o których mowa w art. 175a p.t., uzyskanych od przedsiębiorców telekomunikacyjnych, Prezes UKE corocznie w terminie do dnia 30 kwietnia opracowuje i przekazuje ministrowi właściwemu do spraw informatyzacji raport o zgłoszonych zagrożeniach i ewentualnych podjętych przez przedsiębiorców telekomunikacyjnych działaniach zapobiegawczych i środkach naprawczych (art. 175b ust. 4 p.t.).

Przepisy art. 175b p.t. implementują do krajowego porządku prawnego wymóg art. 13a ust. 3 dyrektywy 2002/21 nakazujący informowanie przez regulatora krajowego innych organów regulacyjnych w państwach członkowskich UE oraz Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji o naruszeniach bezpieczeństwa sieci i usług. Zgodnie z art. 13a dyrektywy 2002/21 przedsiębiorcy powinni zgłaszać krajowemu organowi regulacyjnemu naruszenia bezpieczeństwa mające znaczący wpływ na sieci lub usługi. Natomiast krajowy organ regulacyjny powinien przekazywać takie informacje innym regulatorom oraz ENISA „w stosownych przypadkach".

Zgodnie z art. 175c ust. 1 p.t. przedsiębiorca telekomunikacyjny, z uwzględnieniem art. 160 ust. 2 p.t. (obowiązek zachowania tajemnicy), podejmuje proporcjonalne i uzasadnione środki mające na celu zapewnienia bezpieczeństwa i integralności sieci, usług oraz przekazu komunikatów związanych ze świadczonymi usługami, w tym:

1) eliminację przekazu komunikatu, który zagraża bezpieczeństwu sieci lub usług;
2) przerwanie lub ograniczenie świadczenia usługi telekomunikacyjnej na zakończeniu sieci, z którego następuje wysyłanie komunikatów zagrażających bezpieczeństwu sieci lub usług.

Przedsiębiorca telekomunikacyjny informuje Prezesa UKE niezwłocznie o podjęciu tych środków, jednak nie później niż w ciągu 24 godzin od ich

podjęcia. W informacji zamieszcza się dane niezbędne do identyfikacji zagrożeń bezpieczeństwa sieci lub usług oraz przekazu komunikatów związanych ze świadczonymi usługami, ze wskazaniem podjętych środków naprawczych (art. 175c ust. 2 p.t.). Prezes UKE może, w drodze decyzji, zakazać stosowania środków, o których wcześniej mowa, jeżeli uzna, że nie są one proporcjonalne lub uzasadnione lub nie realizują celów, o których mowa w tym przepisie (art. 175c ust. 3 p.t.). W przypadku podjęcia opisywanych środków przedsiębiorca telekomunikacyjny nie odpowiada za niewykonanie lub nienależyte wykonanie usług telekomunikacyjnych w zakresie wynikającym z podjętych środków. Zasady tej nie stosuje się w przypadku wydania decyzji, o której mowa w art. 175c ust. 3 p.t. (art. 175c ust. 4 p.t.). Przedsiębiorca telekomunikacyjny może informować innych przedsiębiorców telekomunikacyjnych i podmioty zajmujące się bezpieczeństwem teleinformatycznym o zidentyfikowanych zagrożeniach, o których mowa w art. 175c ust. 1 p.t. Informacja może zawierać dane niezbędne do identyfikacji oraz ograniczenia zagrożenia (art. 175c ust. 5 p.t.).

Według art. 175d p.t. minister właściwy do spraw informatyzacji może określić, w drodze rozporządzenia, minimalne środki techniczne i organizacyjne oraz metody zapobiegania zagrożeniom, o których mowa w art. 175a ust. 1 p.t. i art. 175c ust. 1 p.t., jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług, biorąc pod uwagę wytyczne Komisji Europejskiej oraz Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji w tym zakresie.

Zgodnie z art. 175e ust. 1 p.t. Prezes UKE publikuje na stronie internetowej UKE aktualne informacje o:

1) potencjalnych zagrożeniach związanych z korzystaniem przez abonentów z usług telekomunikacyjnych;
2) rekomendowanych środkach ostrożności i najbardziej popularnych sposobach zabezpieczania telekomunikacyjnych urządzeń końcowych przed oprogramowaniem złośliwym lub szpiegującym;
3) przykładowych konsekwencjach braku lub nieodpowiedniego zabezpieczenia telekomunikacyjnych urządzeń końcowych.

Informacje te publikowane są przez przedsiębiorców telekomunikacyjnych na ich stronach internetowych (art. 175e ust. 2 p.t.). Obowiązek publikacji na stronach internetowych może zostać zrealizowany przez umieszczenie na stronie odnośnika do miejsca na stronie internetowej UKE lub innego podmiotu zajmującego się bezpieczeństwem sieci, w którym zamieszczone są informacje wymagane zgodnie z art. 175e ust. 1 p.t. (art. 175e ust. 3 p.t.).

### *1.1.2. Wymagania bezpieczeństwa w postępowaniach selekcyjnych*

Obecna konstrukcja rozdziału częstotliwości przewidziana w ustawie – Prawo telekomunikacyjne odbywa się na dwuetapowo: postępowanie selekcyjne, np. aukcja, oraz drugi etap w postaci dokonania rezerwacji. Te dwa etapy są jednak ściśle związane. Warunki postępowań selekcyjnych są ściśle określone. Uczestnicy muszą wiedzieć, na jakich warunkach przystępują np. do aukcji. Kwestie te regulują akty wykonawcze do Prawa telekomunikacyjnego oraz dokumentacja, np. aukcyjna, wydawane przez Prezesa UKE. Ważne jest więc, aby uczestnik znał warunki uczestnictwa w aukcji, na jakich otrzyma przydział częstotliwości, jeżeli wygra postępowanie selekcyjne. Nie jest dopuszczalne rozwiązanie, uwzględniając treść rozdziału prawa telekomunikacyjnego dotyczącego przeprowadzania postępowań selekcyjnych i przydziału częstotliwości (art. 114 p.t. i n.), aby zwycięzcy postępowań selekcyjnych dowiadywali się o dodatkowych obowiązkach, dopiero gdy wydana zostanie decyzja rezerwacyjna (art. 115 p.t.).

Przepis art. 115 ust. 1 p.t. określa wymagania, które powinna zawierać rezerwacja częstotliwości. Zgodnie z art. 115 ust. 1 pkt 10 p.t. rezerwacja częstotliwości powinna zawierać m.in. wymagania dotyczące bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i usług ustalone przez Prezesa UKE z uwzględnieniem rekomendacji i wytycznych Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji, po zasięgnięciu opinii Kolegium, o którym mowa w art. 64 u.k.s.c. („Kolegium"), jeżeli rezerwacja jest dokonywana po przeprowadzeniu aukcji, o której mowa w art. 116 ust. 1 pkt 2 p.t. Przepis art. 115 ust. 1 pkt 10 p.t. dodany został przez art. 14 pkt 8 ustawy z dnia 14 maja 2020 r. o zmianie niektórych ustaw w zakresie działań osłonowych w związku z rozprzestrzenianiem się wirusa SARS-CoV-2[7], która weszła w życie 16 maja 2020 r. Wątpliwości budziło wprowadzenie tego rodzaju zmian aktem prawnym, którego celem była walka z koronawirusem, tym bardziej że aukcja była i jest prowadzona zdalnie, a więc bez bezpośrednich fizycznych kontaktów jej uczestników z UKE czy pomiędzy uczestnikami. Wątpliwości powstają także co do uzasadnienia wiązania rozdysponowania częstotliwości, którą regulują przepisy działu IV p.t. (*Gospodarowanie częstotliwościami i numeracją*), z bezpieczeństwem infrastruktury, która jest uregulowana w dziale VIIA p.t. (*Bezpieczeństwo i integralność sieci i usług telekomunikacyjnych*). W przypadku rozdysponowywania częstotliwości aspekt bezpieczeństwa może być związany właśnie z tym procesem, np. poprzez weryfikację czy podmiot, który ubiega się o częstotliwości, nie stwarza zagrożenia dla interesów Polski. Przedmiotem rozdysponowywania częstotliwości nie jest natomiast infrastruktura telekomunikacyjna i nie powinna

[7] Dz.U. z 2020 r. poz. 875.

ona na tym etapie postępowania być przedmiotem dodatkowych wymagań, w szczególności w zakresie bezpieczeństwa.

Odpowiednio, zgodnie z art. 36 ustawy z dnia 14 maja 2020 r., został zmieniony art. 65 ust. 1 u.k.s.c., określający sprawy, w których Kolegium wyraża opinie. W art. 65 k.s.c. w ust. 1 po pkt 1 dodany został pkt 1a w brzmieniu: „planowanych do ustalenia przez Prezesa Urzędu Komunikacji Elektronicznej w projekcie rozstrzygnięcia decyzji w sprawie rezerwacji częstotliwości, o którym mowa w art. 118 ust. 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2019 r. poz. 2460 oraz z 2020 r. poz. 374, 695 i 875), jeżeli ta decyzja jest wydawana po przeprowadzeniu aukcji, o której mowa w art. 116 ust. 1 pkt 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne".

W związku z wprowadzonymi zmianami powstało pytanie, dlaczego wprowadzone uregulowanie dotyczyło tylko jednego rodzaju postępowania selekcyjnego, tj. aukcji, a nie innych, np. przetargu czy konkursu. Charakter i zakres wprowadzonych zmian wskazywał na instrumentalne tworzenie przepisów rangi ustawowej, tj. w celu doprowadzenia do unieważnienia konkretnego i to w sensie faktycznym, a więc prowadzonego w danym momencie postępowania selekcyjnego. Trudno zaakceptować takie podejście legislacyjne. Problemy te powinny być bowiem rozwiązywane na gruncie obowiązujących przepisów, przez powołane do tego organy regulacyjne.

Wskazać także należy, że w art. 65 po ust. 1 dodany został ust. 1a w brzmieniu: „Opinia w sprawie projektu rozstrzygnięcia decyzji, o której mowa w ust. 1 pkt 1a, wydawana jest przez Kolegium w terminie 14 dni od dnia otrzymania projektu przekazanego do zaopiniowania przez Prezesa Urzędu Komunikacji Elektronicznej". Przepis ten ma głównie charakter porządkujący poprzez zakreślenie, w jakim terminie powinna być przygotowana opinia przez Kolegium. Nie określa natomiast, jaki charakter jest tej opinii, tj. czy jest ona wiążąca dla Prezesa UKE, czy tylko wyraża stanowisko Kolegium, z którym Prezes UKE powinien się zapoznać, ale nie musi go uwzględnić. Kwestia ta może w praktyce odgrywać istotną rolę. Warto zauważyć, że w przeszłości podobny problem występował, gdy chodzi o charakter opinii Prezesa Urzędu Ochrony Konkurencji i Konsumentów. Zgodnie z ustawą – Prawo telekomunikacyjne Prezes UKE w przypadku niektórych decyzji regulacyjnych powinien zasięgać opinii Prezesa UOKiK. Ostatecznie ukształtowało się stanowisko, także w drodze wykładni sądowej, że opinia Prezesa UOKiK nie ma charakteru wiążącego. Prezes musi jej zasięgnąć, gdyż brak takiego stanowiska ze strony Prezesa UOKiK będzie naruszeniem proceduralnym, ale nie jest tym stanowiskiem (opinią) Prezesa UOKiK związany. Przyjąć należy, że jest podobnie w przypadku opinii Kolegium. Prezes UKE nie jest związany przygotowaną przez Kolegium opinią. Kolegium jest działającym przy

Radzie Ministrów tylko organem opiniodawczo-doradczym w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa (art. 64 u.s.k.c.), którego opinie nie mają mocy wiążącej.

Wreszcie wprowadzone zmiany wywoływały wątpliwości także dlatego, że przepisy obecnego prawa telekomunikacyjnego miały przestać obowiązywać z uwagi na konieczność wprowadzenia do polskiego porządku prawnego do grudnia 2020 r. Dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej. Tym bardziej że toczyły się prace nad projektem ustawy – Prawo łączności elektronicznej, którego celem było wdrożenie regulacji EKŁE. Innymi słowy, ustawodawca przyjąłby przepisy ustawy, które obowiązywałyby kilka miesięcy. Przepisy dotyczące rozdysponowania częstotliwości muszą być spójne z tymi, które są zawarte w EKŁE. Nie mogą być przyjmowane w sposób wybiórczy. Dział III EKŁE (art. 45 i n.) reguluje gospodarkę częstotliwościami, ale przepisy określające sposoby przyznawania częstotliwości nie przewidują uzależnienia ich rozdysponowania od kwestii związanych z szeroko rozumianym bezpieczeństwem.

Zmiany dokonane w p.t. oraz u.k.s.c. oznaczają, że w decyzjach rezerwacyjnych muszą być zawarte wymagania w zakresie bezpieczeństwa, których treść powinna być wcześniej zaopiniowana przez Kolegium. Treść wymagań bezpieczeństwa przygotowuje najpierw Prezes UKE, a następnie przedstawia Kolegium do wyrażenia opinii. Można mieć wątpliwości co do potrzeby wprowadzania wymagań dotyczących bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i usług do treści decyzji rezerwacyjnej. Wymagania w zakresie bezpieczeństwa i integralności sieci i usług telekomunikacyjnych są bowiem już określone w przepisach powszechnie obowiązujących w postaci art. 175–175e p.t. oraz w rozporządzeniu wydanym na podstawie art. 175d p.t. Wydaje się nadmiarowe wprowadzanie takich wymagań do decyzji rezerwacyjnych, skoro obowiązują już w tym zakresie przepisy powszechne, a po drugie, może dojść do kolizji prawnych, gdyby okazało się, że wymagania w zakresie bezpieczeństwa wprowadzone do decyzji rezerwacyjnych są sprzeczne z przepisami powszechnie obowiązującymi lub nie mają podstaw prawnych w przepisach powszechnie obowiązujących. Dokładnie taka sytuacja zaistniała po przeprowadzonej w 2023 r. aukcji na częstotliwości 3600–3800 MHz, gdy w postępowaniu rezerwacyjnym przeprowadzonym po zakończeniu aukcji w grudniu 2023 r. zostały wydane decyzje rezerwacyjne, w których znalazły się postanowienia zawierające wymagania w zakresie bezpieczeństwa sieci i usług telekomunikacyjnych, które nie mają jednak oparcia w obowiązujących przepisach prawa. Dlatego Prezes

UKE, starając się rozwiązać potencjalny konflikt prawny, zawarł w tych decyzjach rezerwacyjnych, a konkretnie w załączniku nr 4 do tych decyzji, odnośnie do tych wymagań bezpieczeństwa, swoistą klauzulę o następującej treści: „Poszczególne postanowienia Wymagań mają zastosowanie, o ile obowiązujące przepisy prawa nie stanowią inaczej. Postanowienia Wymagań należy tak interpretować, aby je pogodzić z obowiązującymi przepisami. W przypadkach niedających się pogodzić kolizji z obowiązującymi przepisami, przepisy prawa powszechnie obowiązującego mają pierwszeństwo i wchodzą w miejsce postanowień niniejszego Załącznika, z którymi są one niezgodne".

Przepis art. 14 pkt 9 ustawy z dnia 14 maja 2020 r. dodał natomiast w art. 118d po ust. 1 kolejne ust. 1a i 1b. Zgodnie więc z nowym brzmieniem art. 118d ust. 1a p.t. „Prezes UKE unieważnia z urzędu przetarg, aukcję albo konkurs w przypadku, gdy projekt rozstrzygnięcia decyzji w sprawie rezerwacji częstotliwości opublikowany wraz z ogłoszeniem o przetargu, aukcji albo konkursie i dokumentacją przetargu, aukcji albo konkursu nie zawiera wszystkich elementów, o których mowa w art. 115 ust. 1". Natomiast według art. 118d ust. 1b p.t. „unieważnienia przetargu, aukcji albo konkursu z przyczyny, o której mowa w ust. 1a, Prezes UKE dokonuje niezwłocznie". W uzasadnieniu do projektu art. 14 pkt 9 ustawy z dnia 14 maja 2020 r. wyjaśniono, że w art. 118d p.t. proponuje się wprowadzenie przepisów, zgodnie z którymi w przypadku, gdy projekt rozstrzygnięcia decyzji w sprawie rezerwacji częstotliwości opublikowany wraz z ogłoszeniem o przetargu, aukcji albo konkursie i dokumentacją przetargu, aukcji albo konkursu nie zawiera wszystkich elementów, o których mowa w art. 115 ust. 1 p.t., Prezes UKE unieważnia z urzędu przetarg, aukcję albo konkurs. Szersze uzasadnienie w tym zakresie przedstawiono w serwisie rządowym (www.gov.pl). Doprowadziło to do powstania w aukcji wątpliwości formalnych, które mogły podważyć cały proces w postępowaniu sądowym, przez co jego uczestnicy nie mieliby pewności inwestycyjnej dotyczącej przedsięwzięć finansowych. Intencją rządu było jednak jak najszybsze wprowadzenie do Polski komercyjnie funkcjonującej sieci piątej generacji (5G) i dotrzymanie terminów określonych w Europejskiej Agendzie Cyfrowej. Dlatego mając na uwadze możliwe konsekwencje, a także wspomniane wyżej kwestie związane z bezpieczeństwem, podjęto decyzję o konieczności powtórzenia całego postępowania.

Zarówno dodanie do art. 118d p.t. po ust. 1 kolejnych postanowień ust. 1a i 1b, jak i uzasadnienie wprowadzenia tych zmian budziło jednak wątpliwości. Wskazane już zostało, że etap pierwszy polega na wyłonieniu w trybie selekcyjnym podmiotu, który uzyska częstotliwości. Kończy ten etap wyłonienie podmiotu, który wygrał przykładowo aukcję i ogłoszenie jej wyników (art. 118b–c p.t.). Przepis art. 118d p.t. reguluje kwestie związane z unieważnieniem przetargu

(art. 118d p.t.). Dotyczy jednak zdarzeń i spraw, które odbyły się w tym etapie postępowania. Wniosek taki wynika po prostu z treści art. 118d p.t., który określa przyczyny i powody unieważnienia aukcji, związane właśnie z tym etapem. Nie mogą więc być z powodów prawnych (obecnej konstrukcji rozdysponowywania częstotliwości), ale także po prostu logicznych powodem unieważnienia tego etapu postępowania, okoliczności, które w nim nie występowały, gdyż dotyczą dopiero drugiego etapu postępowania, który ma nastąpić, a który dotyczy postępowania rezerwacyjnego (decyzji rezerwacyjnej).

Tego rodzaju zmiany są trudne także do zaakceptowania pod względem legislacyjnym. Mogą prowadzić do naruszenia zasady *lex retro non agit*. Wprowadzono bowiem rozwiązania, które działają wstecz, i to w sytuacji, gdy przepisy obowiązujące były jeszcze stosowane w praktyce, gdyż aukcja wprawdzie została zawieszona, ale była nadal w toku. Taka konstrukcja przepisów jest rzadko stosowana, gdyż oznacza w praktyce, że ustawodawca wprowadza dodatkowy wymóg do postępowania aukcyjnego, i wskazuje, że gdy go nie będzie w tym postępowaniu, które się już toczy (a co jest oczywiste, że go nie ma, bo dopiero po rozpoczęciu postępowania wymóg ten się pojawił), to go unieważni.

W związku z wprowadzonymi nowymi regulacjami należy zwrócić uwagę na postanowienia art. 118d ust. 1 p.t., który stanowi, że „Prezes UKE z urzędu lub na wniosek uczestnika przetargu, aukcji albo konkursu złożony w terminie 21 dni od dnia ogłoszenia wyników przetargu, aukcji albo konkursu, w drodze decyzji, unieważnia przetarg, aukcję albo konkurs, jeżeli zostały rażąco naruszone przepisy prawa lub interesy uczestników przetargu, aukcji albo konkursu". Z uwagi na postanowienia art. 118d ust. 1 p.t., określające przyczyny unieważnienia postępowań selekcyjnych, powstają wątpliwości co do sytuacji, w której przyczynę unieważnienia postępowania selekcyjnego miałoby stanowić – obok rażącego naruszenia przepisów prawa lub interesów uczestników przetargu, aukcji albo konkursu – także uchybienie nie tylko niemające przymiotu rażącego, ale w ogóle niestanowiące naruszenia przepisów prawa. W art. 115 ust. 1 p.t. ujęte są bowiem elementy obligatoryjne decyzji rezerwacyjnej, a nie projektu takiej decyzji. Przepis art. 115 ust. 1 p.t. mówi bowiem o rezerwacji częstotliwości, a nie projekcie decyzji rezerwacyjnych, jak stanowi art. 118d ust. 1a p.t. Zastosowanie przepisu art. 118d ust. 1a p.t. prowadzić będzie do sytuacji, w której brak jednego z elementów w projekcie decyzji stanowić będzie przesłankę obligatoryjnego unieważnienia postępowania selekcyjnego (chociaż projekt decyzji rezerwacyjnej nie ma wpływu na jego przebieg), natomiast ujęcie takiego elementu, a następnie jego zmiana w decyzji wydanej po zakończeniu postępowania selekcyjnego nie będzie wywoływać żadnych konsekwencji. Należy także zauważyć, że przepis art. 118d ust. 1b p.t. tworzy określoną

gradację przesłanek unieważnienia postępowania selekcyjnego, którą trudno uznać za prawidłową, uznając wadliwość ogłoszonego projektu decyzji rezerwacyjnej za wymagającą w pierwszej kolejności reakcji organu niż rażące naruszenie przepisów prawa lub interesów uczestników postępowania selekcyjnego. Nie jest także wyjaśnione, dlaczego unieważnienie postępowania selekcyjnego z innych (ważniejszych) powodów miałoby nie następować bez nieuzasadnionej zwłoki, a tylko z powodu braku wskazanych w art. 118d ust. 1a p.t. elementów.

Zgodnie z art. 71 ust. 1 ustawy z dnia 14 maja 2020 r. przepisy art. 14 pkt 8 i 9 tej ustawy stosuje się do ogłoszonych przed dniem wejścia w życie niniejszej ustawy przetargów, konkursów i aukcji. Natomiast według art. 71 ust. 2 tej ustawy w przypadku, gdy w ogłoszonym przetargu, konkursie lub aukcji przed dniem wejścia w życie niniejszej ustawy zostały złożone oferty, Prezes UKE zwraca niezwłocznie złożone oferty uczestnikom, a wpłacone przez uczestników przetargu albo aukcji wadium oddaje w terminie 21 dni od dnia unieważnienia przetargu albo aukcji z przyczyny, o której mowa w art. 118d ust. 1a p.t.

Uczestnicy postępowania selekcyjnego powinni być poinformowani, czy i jakiej treści została przedstawiona opinia Kolegium, z uwagi na jej znaczenie dla postępowania selekcyjnego i jego uczestników. Wprowadzone ustawą z dnia 14 maja 2020 r. nowe przepisy nie zawierają jednak regulacji w tym zakresie.

### 1.2. Rozporządzenie Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług

Rozporządzenie Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług[8], zostało wydane na podstawie art. 175d p.t. Upoważnienie zawarte w art. 175d p.t. do wydania rozporządzenia ma charakter fakultatywny. Upoważnienie to daje podstawę do określenia w drodze rozporządzenia minimalnych środków technicznych i organizacyjnych oraz metod zapobiegania istotnym zagrożeniom bezpieczeństwa i integralności sieci oraz usług, o których mowa w art. 175a ust. 1 p.t. i art. 175c p.t., jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług. Środki ustalane i stosowane samodzielnie przez przedsiębiorcę na podstawie zasad określonych w art. 175 p.t. można uznać

[8] Dz.U. z 2020 r. poz. 1130.

za standardowe. Podwyższony poziom bezpieczeństwa przedsiębiorca może zapewniać na podstawie art. 175 ust. 2 p.t. Upoważnienie dotyczy również minimalnych środków zapobiegania zagrożeniom określonym w art. 175c ust. 1 p.t., wynikającym z aktywności użytkownika zakończenia sieci, która polega na wysyłaniu komunikatów generujących zagrożenia określone w tym przepisie. Gdy wydaje się rozporządzenie, niezbędne jest uwzględnienie wytycznych Komisji Europejskiej oraz Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji w tym zakresie (ENISA, obecnie pod zmienioną nazwą: Europejska Agencja do spraw Cyberbezpieczeństwa). Przepisy rozporządzenia powinny być neutralne technologicznie. Nie mogą podawać konkretnych rozwiązań, a jedynie wskazywać na cel zastosowania środków technicznych.

Paragraf 1 rozporządzenia z 22 czerwca 2020 r. określa minimalne środki techniczne i organizacyjne, zwane dalej „środkami", oraz metody zapobiegania zagrożeniom, o których mowa w art. 175a ust. 1 i art. 175c ust. 1 p.t., jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług. W uzasadnieniu rozporządzenia wyjaśniono, że zarówno w interesie obywateli, jak i państwa jest, aby przedsiębiorcy telekomunikacyjni mieli obowiązek stosowania konkretnych rozwiązań w celu zapewnienia bezpieczeństwa sieci iusługtelekomunikacyjnych. Wraz z rozwojem technologii zwiększa się także liczba zagrożeń, które mogą wpłynąć na bezpieczeństwo i integralność sieci oraz usług telekomunikacyjnych, utrudniać życie obywatelom oraz niekorzystnie wpływać na sprawne funkcjonowanie państwa. W obecnej sytuacji przedsiębiorcy telekomunikacyjni sami decydują, jakie rodzaje środków technicznych i organizacyjnych chcą zastosować, aby zapewnić bezpieczeństwo sieci i usług telekomunikacyjnych. Brakuje jednolitych standardów prawnych, które działając w interesie obywateli, obligowałyby przedsiębiorców telekomunikacyjnych do stosowania konkretnych rodzajów rozwiązań w zakresie bezpieczeństwa.

Postanowienia art. 175 ust. 1 p.t. są transpozycją art. 13a dyrektywy 2002/21 (dyrektywy ramowej). Państwa członkowskie mają informować się wspólnie oraz ENISA o istotnych incydentach bezpieczeństwa w telekomunikacji. Na podstawie tych informacji ENISA publikuje raporty o bezpieczeństwie w telekomunikacji. Raport ENISA z 2018 r. opierał się na 169 istotnych incydentach zgłoszonych do ENISA przez kraje członkowskie UE oraz EFTA. Spośród nich 51% miało wpływ na telefonię mobilną i internet mobilny. Główną przyczyną (62% z ogółu zgłoszonych) incydentów bezpieczeństwa były awarie systemów, polegające najczęściej na awariach sprzętowych lub błędach oprogramowania. Awarie sprzętowe najczęściej dotyczyły przełączników sieciowych, ruterów, stacji bazowych sieci mobilnej, sterowników i systemów zasilania. Około 18% zgłoszonych

incydentów było związanych z błędami ludzkimi. Dotyczyły średnio 1,2 mln połączeń. W porównaniu z poprzednimi latami zwiększyła się liczba incydentów związanych ze skutkami działalności natury – śniegu, burz, pożarów lasów (około 17% zgłoszonych incydentów). Podczas tego rodzaju incydentów przez 96 godzin użytkownicy sieci nie mogli uzyskać do niej dostępu i stracili średnio 56,8 tys. użytkownikogodzin, co było najwyższym wynikiem spośród wszystkich incydentów. Ataki z wykorzystaniem szkodliwego oprogramowania stanowiły około 2% zgłoszonych incydentów. Spośród wszystkich incydentów 18% stanowiły awarie po stronie trzeciej. Około 1/3 incydentów miało wpływ na dostępność do numeru alarmowego 112[9].

Według raportu UKE w 2018 r. zgłoszono Prezesowi UKE 198 przypadków naruszeń bezpieczeństwa. Pięć z nich dotyczyło obszaru całego kraju, cztery obszaru kilku województw, a reszta dotyczyła obszaru gmin (157 przypadków obejmowało obszary od 1 do 10 gmin, 30 przypadków obejmowało obszary powyżej 10 gmin). Najbardziej ucierpieli w wyniku naruszeń użytkownicy telefonii komórkowej i internetu mobilnego (odpowiednio 525 tys. oraz 100 tys. użytkowników). W zdecydowanej większości przypadków naruszenia dotyczyły dostępu do numerów alarmowych (190 przypadków), 22 przypadki dotyczyły integralności sieci, a dwa dotyczyły zagrożeń cyberbezpieczeństwa. Najczęstszymi przyczynami naruszeń były awarie sprzętu i oprogramowania (168 przypadków). Dewastacja infrastruktury spowodowała 16 naruszeń, przerwa w zasilaniu – 6, a błąd ludzki – 5. Marginalne były przyczyny spowodowane klęską żywiołową i cyberatakiem. W uzasadnieniu rozporządzenia z 22 czerwca 2020 r. wskazuje się, że z powyższych danych wynika, iż aby zwiększyć bezpieczeństwo w telekomunikacji, przedsiębiorcy telekomunikacyjni powinni kłaść większy nacisk na bezpieczeństwo sprzętowe i oprogramowania, odpowiednie szkolenie pracowników w zakresie najnowszych technologii, a także ochronę infrastruktury sieciowej przed warunkami atmosferycznymi. Mając na uwadze zjawisko konwergencji telekomunikacji i teleinformatyki, w nadchodzącym okresie należy spodziewać się zwiększenia liczby naruszeń spowodowanych cyberatakami. Istotne jest też, aby przedsiębiorcy zwracali uwagę na dobór strony trzeciej (podwykonawców, usługodawców), nie tylko na ich poziom techniczny oraz merytoryczny, ale także na sposób zarządzania bezpieczeństwem. Ze względu na interes społeczny ważne jest zapobieganie niedostępności numerów alarmowych. W Polsce najczęściej incydenty dotyczyły obszaru kilku gmin – toteż należy podjąć działania, aby obywatele tych obszarów nie byli dyskryminowani

[9] ENISA, *Annual Report Telecom Security Incidents 2017*, https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2017 [dostęp: 19.09.2023 r.].

w dostępie do telekomunikacji. Rozporządzenie ma na celu wprowadzenie ogólnych standardów bezpieczeństwa telekomunikacyjnego na terenie całego kraju. Dzięki temu wszyscy obywatele będą mieli pewność, że wszyscy przedsiębiorcy telekomunikacyjni tak samo sprawnie i szybko reagują na incydenty, które uniemożliwiają korzystanie z usług telekomunikacyjnych.

W uzasadnieniu rozporządzenia z 22 czerwca 2020 r. wskazuje się także, że obecny stan prawny nakłada na przedsiębiorców telekomunikacyjnych obowiązek podejmowania proporcjonalnych i uzasadnionych środków mających na celu zapewnienie bezpieczeństwa oraz integralności sieci i usług. Brak za to regulacji zawierającej określenie minimalnych środków technicznych i organizacyjnych oraz metod zapobiegania zagrożeniom, o których mowa w art. 175a ust. 1 i art. 175c ust. 1 p.t. Rozporządzenie wypełnia tę lukę, jednak nie nakłada nowych obowiązków, a jedynie precyzuje istniejące. Przedsiębiorcy telekomunikacyjni są obowiązani stosować wskazane w rozporządzeniu środki w swojej działalności. Warto jednak zauważyć, że mają one minimalny charakter i nie są nowymi przedsięwzięciami. Podobne regulacje istnieją w innych krajach. Wielu przedsiębiorców telekomunikacyjnych już obecnie stosuje środki, o których mowa w rozporządzeniu.

Zgodnie z § 2 rozporządzenia z 22 czerwca 2020 r. przedsiębiorca telekomunikacyjny:

1) opracowuje i aktualizuje dokumentację dotyczącą bezpieczeństwa i integralności sieci i usług zawierającą opis środków, o których mowa w pkt 2–13;
2) opracowuje i aktualizuje wykaz elementów infrastruktury telekomunikacyjnej i systemów informatycznych, których naruszenie bezpieczeństwa lub integralności będzie miało istotny wpływ na funkcjonowanie sieci lub usług o znaczeniu kluczowym dla funkcjonowania przedsiębiorcy, zwanych dalej „kluczową infrastrukturą";
3) identyfikuje zagrożenia bezpieczeństwa lub integralności sieci lub usług;
4) ocenia prawdopodobieństwo wystąpienia oddziaływania zagrożeń na bezpieczeństwo lub integralność sieci lub usług;
5) zapewnia i stosuje środki minimalizujące skutki wystąpienia oddziaływań zagrożeń na bezpieczeństwo lub integralność sieci lub usług;
6) ustanawia zasady i procedury dostępu do kluczowej infrastruktury i przetwarzanych danych, obejmujące przypisanie odpowiedzialności za kluczową infrastrukturę w zakresie odpowiednim do realizowanych zadań;
7) zabezpiecza dostęp do kluczowej infrastruktury, monitoruje ten dostęp i wskazuje środki reagowania na nieuprawniony dostęp lub próbę takiego dostępu;
8) ustanawia zasady bezpiecznego zdalnego przetwarzania danych;

9) stosuje, wynikające z oceny prawdopodobieństwa wystąpienia oddziaływania zagrożeń, środki zabezpieczające dla poszczególnych kategorii danych;
10) zawierając umowy mające istotny wpływ na funkcjonowanie sieci lub usług, identyfikuje zagrożenia dla bezpieczeństwa tych sieci lub usług, związane z zawieranymi umowami;
11) zapewnia monitorowanie i dokumentowanie funkcjonowania sieci i usług telekomunikacyjnych mające na celu wykrycie naruszenia bezpieczeństwa lub integralności sieci lub usług, o których mowa w art. 175a p.t. i ustalenie przyczyn takiego naruszenia;
12) ustala wewnętrzne procedury zgłaszania naruszeń bezpieczeństwa lub integralności sieci lub usług, o których mowa w art. 175a p.t., oraz umożliwia użytkownikom końcowym dokonywanie zgłoszeń wszelkich naruszeń bezpieczeństwa lub integralności sieci lub usług;
13) przeprowadza ocenę bezpieczeństwa sieci i usług telekomunikacyjnych:
    a) co najmniej raz na dwa lata,
    b) po każdym:
        – stwierdzonym naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych o istotnym wpływie na funkcjonowanie sieci lub usług, w zakresie objętym naruszeniem, oraz
        – wykryciu podatności zwiększającej poziom ryzyka wystąpienia naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych o istotnym wpływie na funkcjonowanie sieci lub usług, w zakresie objętym wykrytą podatnością.

W uzasadnieniu rozporządzenia z 22 czerwca 2020 r. wskazano, że przepisy § 2 tego rozporządzenia określają minimalne środki techniczne i organizacyjne oraz metody, które obejmą ogólną działalność telekomunikacyjną. Według projektodawców trudno jest jednoznacznie określić metody, jakie mają stosować przedsiębiorcy. Stosowanie określonych rozwiązań zależy od przeprowadzonej oceny ryzyka, posiadanej wiedzy o wykrytych naruszeniach bezpieczeństwa i integralności oraz wykrytych podatnościach. To od przyjętych lub planowanych środków technicznych i organizacyjnych zależy stosowanie konkretnych metod zapobiegania zagrożeniom. Metoda to świadomie stosowany sposób działania prowadzący do uzyskania planowanego rezultatu. W niniejszym przypadku chodzi o zapobieganie zagrożeniom. Projektodawcy zauważają, że jednoznaczne określenie metod będzie też kłopotliwe ze względu na istniejące różnice między przedsiębiorcami – zarówno w przyjętym modelu biznesowym, jak i wielkości czy obszarze działania. Dlatego też nie jest możliwe wskazanie metod zapobiegania zagrożeniom w bardziej skonkretyzowany sposób, zachowując równocześnie neutralność technologiczną. Dopiero

w następstwie analizy ryzyka przedsiębiorca będzie mógł wybrać właściwy środek zabezpieczający.

W uzasadnieniu rozporządzenia z 22 czerwca 2020 r. wyjaśniono także, że ze względu na to, iż rozporządzenie dotykać będzie bardzo zróżnicowaną grupę podmiotów, aby uniknąć nakładania nadmiernych obciążeń, konieczny jest duży poziom ogólności przepisów. Konkretne środki zastosowane przez przedsiębiorców muszą bowiem zależeć od przeprowadzonych przez nich analiz ryzyka. Wśród wskazanych środków dominują te o charakterze czysto organizacyjnym (określone w § 2 pkt 1, 3–6, 8, 10, 12–13), jednak istotne są też o charakterze technicznym–sporządzenie wykazu kluczowej infrastruktury (pkt 2), zabezpieczenie dostępu do niej i monitorowanie dostępu (pkt 7), stosowanie środków zabezpieczających dla poszczególnych kategorii danych (pkt 9), monitorowanie i dokumentowanie funkcjonowania sieci (pkt 11). Należy wskazać, że w większości przypadków środki wskazane w rozporządzeniu mają mieszany charakter. Nie jest to wyjątkowa sytuacja w prawodawstwie. Przykładowo przepisy art. 24 i 25 RODO odnoszą się do środków organizacyjnych i technicznych, nie wskazując jednak różnic między nimi. RODO wprost odnosi się do pseudonimizacji czy minimalizacji danych, nie wskazując jednoznacznie, czy te środki mają charakter środka organizacyjnego czy technicznego.

Przepis art. 175c p.t. wskazuje na otwarty katalog proporcjonalnych i uzasadnionych środków, które podejmuje przedsiębiorca telekomunikacyjny, mając na celu zapewnienie bezpieczeństwa i integralności sieci, usług oraz przekazu komunikatów związanych ze świadczonymi usługami. Rozporządzenie to uzupełnia ten katalog o niezbędne elementy do zapewnienia proporcjonalności tego działania. Środki, o których mowa w art. 175c p.t., czyli eliminacja przekazu komunikatu, który zagraża bezpieczeństwu sieci lub usług oraz przerwanie lub ograniczenie świadczenia usługi telekomunikacyjnej na zakończeniu sieci, z którego następuje wysyłanie komunikatów zagrażających bezpieczeństwu sieci lub usług, muszą być stosowane w zgodzie z tym rozporządzeniem. Dla zapewnienia skutecznego stosowania tych środków przedsiębiorca musi dokonać szacowania ryzyka, ocenić, co szkodzi infrastrukturze i usługom, a także monitorować sieć w celu wykrywania zagrożeń. Rozporządzenie będzie zatem uzupełnieniem do stosowania art. 175c p.t.

Obowiązki zawarte w § 2 rozporządzenia z 29 czerwca 2020 r. wynikają z wytycznych ENISA dotyczących minimalnych środków bezpieczeństwa[10], o których mowa w art. 13a dyrektywy 2009/140, i posiadają pełne odniesienie do

[10] ENISA, Technical Guideline on Minimum Security Measures, https://www.enisa.europa.eu/publications/technical-guideline-on-minimum-security-measures [dostęp 17.09.2023 r.].

wspomnianych wytycznych. W EKŁE istnieje bardzo podobna podstawa prawna (art. 40 i 41). W uzasadnieniu rozporządzenia z 22 czerwca 2020 r. wyjaśniono, że zarządzanie bezpieczeństwem zależne jest w szczególności od prawidłowego funkcjonowania dwóch procesów: procesu identyfikacji zasobów (zwanych też aktywami) oraz procesu zarządzania ryzykiem. Wprowadzenie konkretnych zabezpieczeń technicznych i organizacyjnych, w wyspecyfikowanych w wytycznych ENISA obszarach, wynika z postępowania z oszacowanym ryzykiem. Aby ułatwić stosowanie przepisów § 2 rozporządzenia również u małych i średnich przedsiębiorców, odstąpiono od technicznego języka wytycznych i uproszczono niektóre wymogi. Różnice w stosowaniu rozporządzenia mają charakter faktyczny, a nie prawny. Środki w rozporządzeniu są skalowalne i sposób ich wdrożenia jest zależny od wielkości i profilu działania przedsiębiorcy. Upoważnienie ustawowe odnosi się do dostawców i operatorów bez rozróżnienia na wielkość działalności przedsiębiorcy, zatem nie jest możliwe rozróżnianie obowiązków w samej treści rozporządzenia. W uzasadnieniu wskazano, że ten sam cel zabezpieczenia w wielu przypadkach można osiągnąć zarówno środkami organizacyjnymi, jak i technicznymi. Biorąc pod uwagę, że rozporządzenie skierowane jest do operatorów o różnej skali prowadzonej działalności, w rozporządzeniu wskazano cel zabezpieczenia. Środki do osiągnięcia celu zabezpieczenia pozostawione są do wyboru przez operatora.

W części uzasadnienia rozporządzenia z 22 czerwca 2020 r., w zakresie oceny skutków regulacji, wskazuje się, że zastosowanie środków technicznych i organizacyjnych oraz metod zapobiegania zagrożeniom wskazanym w rozporządzeniu może wymusić zmiany w organizacji oraz aktualizację istniejących rozwiązań technicznych. Granicą stosowania dywersyfikacji (uniezależnienia się od jednego dostawcy) jest utrzymanie interoperacyjności usług u danego przedsiębiorcy. Pozwala to dużym przedsiębiorcom na stosowanie, podobnie jak robią obecnie, strategii chroniących ich działalności przed tzw. *vendor lock-in*. Warto też wskazać, że ten wymóg dotyczy głównie dużych operatorów i to tylko zajmujących się wdrażaniem sieci 5G. Środki przewidziane w rozporządzeniu są skalowalne i sposób ich wdrożenia jest zależny od wielkości i profilu działania przedsiębiorcy. Upoważnienie ustawowe odnosi się do dostawców i operatorów bez rozróżnienia na wielkość działalności przedsiębiorcy, zatem nie jest możliwe rozróżnianie obowiązków w samej treści rozporządzenia. Ten sam cel zabezpieczenia w wielu przypadkach można więc osiągnąć zarówno środkami organizacyjnymi, jak i technicznymi. Biorąc pod uwagę, że rozporządzenie skierowane jest do operatorów o różnej skali prowadzonej działalności, w rozporządzeniu wskazano cel zabezpieczenia. Środki do osiągnięcia celu zabezpieczenia pozostawione są natomiast do wyboru przez operatora.

W uzasadnienia rozporządzenia z 22 czerwca 2020 r. wyjaśnia się także cel i znaczenie poszczególnych punktów zawartych w § 2 tego rozporządzenia. W pkt 1 § 2 rozporządzenia z 22 czerwca 2020 r. wskazuje na obowiązek prowadzenia odpowiedniej dokumentacji dotyczącej bezpieczeństwa i integralności sieci i usług. Musi ona obejmować opis wszystkich podjętych środków. Zachowanie udokumentowanych informacji o środkach bezpieczeństwa jest istotne nie tylko z punktu widzenia organu nadzoru, ale przede wszystkim dla samej organizacji, jako podstawa do wyciągania wniosków i usprawniania działania. Zgodnie z § 2 pkt 2 rozporządzenia z 22 czerwca 2020 r. niezbędne jest posiadanie wykazu elementów infrastruktury telekomunikacyjnej i systemów informatycznych mających istotny wpływ na funkcjonowanie sieci lub usług o kluczowym znaczeniu dla przedsiębiorcy. Posiadanie wykazu jest punktem wyjścia do oceny, czy sieć jest podatna na zagrożenia cyberbezpieczeństwa oraz czy wykorzystywany w niej sprzęt spełnia wymogi bezpieczeństwa. Szczegółowy wykaz powinien obejmować te elementy infrastruktury telekomunikacyjnej i systemów informatycznych, które mają istotny wpływ na funkcjonowanie sieci lub usług o kluczowym znaczeniu dla przedsiębiorcy. Nie jest zatem konieczne prowadzenie wykazu całej infrastruktury (taką funkcję pełni już wykaz prowadzony przez Prezesa UKE), a tylko jego części, których naruszenie bezpieczeństwa lub integralności będzie miało istotny wpływ na funkcjonowanie sieci lub usług o znaczeniu kluczowym dla funkcjonowania przedsiębiorcy. Do decyzji przedsiębiorcy pozostaje identyfikacja poszczególnych elementów, ale celowe pominięcie lub niewłaściwa identyfikacja najistotniejszych elementów sieci może prowadzić do uznania, że ten środek nie został zastosowany. Opracowanie wykazu dla sieci i usług o kluczowym znaczeniu jest jednym z najważniejszych środków. Jeśli przedsiębiorca ma infrastrukturę, która nie jest kluczowa dla jego działalności, to nie wydaje się zasadne podnoszenie dla niej wymogów bezpieczeństwa. Odrębnie wskazano „elementy infrastruktury telekomunikacyjnej" i „systemy informatyczne". Poza typowymi elementami infrastruktury przedsiębiorca powinien zidentyfikować także systemy informatyczne, które nie wypełniają definicji infrastruktury telekomunikacyjnej, a są istotne dla świadczenia usług (np. systemy CRM czy OSS). Punkty 3–5 § 2 rozporządzenia z 22 czerwca 2020 r. to opisowo określone środki prowadzące do zarządzania ryzykiem w organizacji. Przedsiębiorca powinien identyfikować zagrożenia (przy czym za punkt wyjścia identyfikacji powinny służyć dokumenty ENISA w tym zakresie, np. ENISA Threat Landscape)[11], oceniać prawdo-

[11] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 [dostęp: 15.01.2023 r.].

podobieństwo oddziaływania tych zagrożeń na bezpieczeństwo oraz zapewniać i stosować środki minimalizujące skutki oddziaływania tych zagrożeń. Preferowane są rozwiązania ENISA, które są oparte na europejskim porządku prawnym i identyfikują typowe dla europejskiej infrastruktury zagrożenia. Nie wyklucza to jednak stosowania innych metodyk. Identyfikacja zagrożeń może opierać się także na polskich normach (np. z rodziny ISO 27000), rekomendacjach i standardach NIST serii SP 800[12] czy też dobrych praktykach pokroju ITIL czy Resilia. Nic nie stoi na przeszkodzie, aby opierać się na zagranicznych rozwiązaniach, takich jak Federal Information Processing Standards[13] ze Stanów Zjednoczonych albo Katalog Wymagań Bezpieczeństwa[14] opracowany przez Bundesnetzagentur i BSI z Niemiec. Istotne jest, aby zidentyfikować wszystkie poważne zagrożenia dla działania sieci i usług. Punkty 6–9 § 2 rozporządzenia z 22 czerwca 2020 r. regulują środki związane z dostępem do zasobów. Zgodnie z punktem 6 przedsiębiorca powinien ustanowić zasady i procedury dostępu do kluczowej infrastruktury wraz z przypisaniem odpowiedzialności za tę infrastrukturę. Dostęp i odpowiedzialność powinny być zgodne z zakresem realizowanych zadań. Nie chodzi tu wyłącznie o dostęp fizyczny, ale przede wszystkim o uprawnienia w rozumieniu systemów IT (ang. *privilege and access control*). Punkt 7 uzupełnia powyższe, wskazując konieczność zabezpieczania dostępu do zasobów i monitorowanie tego dostępu, pkt 8 nakazuje ustanowić zasady dotyczące zdalnego przetwarzania danych, a pkt 9 – zabezpieczyć te dane. Trzeba w tym miejscu zaakcentować konieczność kategoryzacji danych i stosowania właściwych dla nich środków zabezpieczających. Nie wszystkie dane wymagają równego poziomu bezpieczeństwa i powinno to znaleźć odzwierciedlenie w działaniach przedsiębiorcy. Na marginesie należy wskazać, że środki zabezpieczające wynikające z oceny prawdopodobieństwa nie zwalniają z realizacji obowiązków określonych w innych przepisach, takich jak ochrona danych osobowych czy ochrona informacji niejawnych. Punkt 10 § 2 rozporządzenia z 22 czerwca 2020 r. wskazuje na konieczność uwzględniania tzw. bezpieczeństwa prawnego, rozszerzając obowiązek identyfikacji zagrożeń także w tym obszarze. Przy zawieraniu umów, które mogą mieć wpływ na bezpieczeństwo (umowy serwisowe, outsourcing usług lub procesów, przeniesienie działalności poza centralę itp.), przedsiębiorca powinien zidentyfikować

[12] NIST, Computer Security Resource Center, https://csrc.nist.gov/publications/sp800 [dostęp: 15.01.2023 r.].

[13] NIST, Current Federal Information Processing Standards, https://www.nist.gov/itl/current-fips [dostęp: 15.01.2023 r.].

[14] Bundesnetzagentur, Katalog von Sicherheitsanforderungen, https://www.bundesnetzagentur.de [dostęp: 15.01.2023 r.].

wynikające z umowy ryzyka dla konkretnych sieci czy usług. Część zagrożeń nie wynika ze szkodliwych działań podmiotów trzecich, a z błędów czy innej działalności osób dopuszczonych do sieci i usług. Zagrożenia mogą mieć charakter nie tylko operacyjny, ale też prawny lub dotyczą zgodności prawnej (ang. *compliance*), np. w zakresie przetwarzania danych osobowych przez podmioty trzecie, lub nadmiernego dostępu do infrastruktury. Punkt 11 § 2 rozporządzenia z 22 czerwca 2020 r. dotyczy monitorowania i dokumentowania funkcjonowania sieci i usług telekomunikacyjnych (element tzw. bezpieczeństwa operacyjnego). Dzięki właściwie prowadzonemu monitorowaniu sieci jest możliwe wykrywanie występujących anomalii i odróżnianie awarii od celowych ataków. Bez wykrywania naruszeń nie jest możliwe ich zgłaszanie zgodnie z art. 175a p.t. Punkt 12 § 2 rozporządzenia z 22 czerwca 2020 r. uzupełnia obowiązek ustawowy z art. 175a p.t. dotyczący zgłaszania naruszeń. Kluczowe jest w tym wypadku posiadanie procedury regulującej zgłaszanie incydentów w organizacji oraz przez użytkowników końcowych. Dokonywanie zgłoszeń przez użytkowników można umożliwić w ramach istniejącej pomocy technicznej bądź zgłoszenia mailowego. Punkt 13 § 2 rozporządzenia z 22 czerwca 2020 r. zawiera wytyczne dotyczące okresowej oceny bezpieczeństwa. Okresowe sprawdzanie systemów co dwa lata wydaje się standardową, zalecaną praktyką. Nie musi być to koniecznie pełen audyt. Nie jest też sugerowane, aby była to ocena zlecana na zewnątrz. Może to zostać dokonane własnymi środkami przedsiębiorcy. Konieczne jest sprawdzenie bezpieczeństwa po każdym istotnym incydencie oraz po pojawieniu się istotnej podatności – o ile logiczne jest, że nie należy wtedy sprawdzać całej sieci, o tyle niezbędne jest zbadanie powiązań i ocena, czy konkretny incydent nie wpłynął na resztę infrastruktury i usług. Niektóre państwa członkowskie wykorzystywały wytyczne ENISA w swoich regulacjach prawnych, jak np. Grecja, która wykorzystała rekomendacje ENISA w regulacjach wydanych przez właściwy organ ds. bezpieczeństwa komunikacji i prywatności[15], czy Rumunia, w której organ właściwy ds. telekomunikacji – ANCOM, wykorzystał także rekomendacje ENISA[16]; podobnie w Słowacji propozycje ENISA zostały wykorzystane przez Urząd Regulacji

[15] Regulacja przez organ właściwy ds. bezpieczeństwa komunikacji i prywatności: http://www.adae.gr/fileadmin/docs/nomoi/kanonismoi/Kanonismos_FEK_1742_B_15_07_2013_asfaleia_akeraiotita__ADAE_205_2013.pdf – za raportem ENISA dotyczącym implementacji art. 13a Dyrektywy 2009/140/WE: https://resilience.enisa.europa.eu/article-13/state-of-play-2015-public-report [dostęp: 17.09.2023 r.].

[16] Decyzja organu właściwego ds. telekomunikacji ANCOM – http://www.ancom.ro/en/uploads/forms_files/decizie_2013_512_en1381320558.pdf [ dostęp: 17.09.2023 r.].

Łączności Elektronicznej i Usług Pocztowych[17], w Holandii zaś wykorzystał je organ właściwy ds. telekomunikacji – Agentschap Telecom[18].

W uzasadnieniu rozporządzenia z 22 czerwca 2020 r. wskazano także, że trwa wdrażanie instalacji 5G. Sieci najnowszej generacji w modelu *non standalone* będą współpracowały ze starszymi sieciami i innymi technologiami, jednak w docelowym modelu *standalone* nie będą wymagały tego wsparcia, co zwiększy ich wydajność i szybkość. Oznacza to, że już teraz należy przygotować odrębne środki bezpieczeństwa i integralności sieci 5G. Nie powoduje to różnego traktowania przedsiębiorców telekomunikacyjnych. Wymogi są wyodrębnione w rozporządzeniu ze względu na stosowaną technologię, a nie cechy identyfikujące przedsiębiorcę. Główną cechą wyróżniającą sieć 5G w warstwie dostępowej jest tzw. New Radio, czyli interfejs radiowy pozwalający na obsługiwanie danych w nowym podejściu (wysoki przepływ danych, niskie opóźnienia, połączenia wielu urządzeń końcowych), modeli komunikacji (ruch IP, ruch poza IP, *short data bursts* itp.) i różnych protokołów sesji (IPv4, IPv6, IPv4v6 etc.). Równie istotnymi cechami wyróżniającymi sieci 5G są, w warstwie szkieletowej, możliwość dzielenia sieci na warstwy (Network Slicing), możliwość świadczenia usług w punkcie dostępowym sieci (Mobile Edge Computing) oraz ułatwienie tworzenia nowych usług (Network Capability Exposure oraz Flexible Mobile Service Steering). Wszystkie powyższe cechy powodują, że konieczne okazuje się rozróżnienie środków technicznych w zależności od stosowanej technologii.

Zgodnie z § 3 ust. 1 rozporządzenia z 22 czerwca 2020 r. przedsiębiorca telekomunikacyjny dostarczający sieć piątej generacji (5G), określoną w dokumencie technicznym – Raporcie ETSI TR 121 915 V.15.0.0. (2019–10) lub dokumencie go zastępującym, realizując środki, o których mowa w § 2 pkt 3–5, w ramach tej sieci:

1) uwzględnia rekomendacje, o których mowa w art. 33 ust. 4 u.k.s.c. (rekomendacje Pełnomocnika Rządu do spraw Cyberbezpieczeństwa dotyczące stosowania urządzeń informatycznych lub oprogramowania);
2) stosuje strategię skutkującą brakiem uzależnienia się od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług;
3) zapewnia podwyższanie odporności na zakłócenia sieci i usług telekomunikacyjnych.

[17] Regulacja wydana przez Urząd Regulacji Łączności Elektronicznej i Usług Pocztowych: https://www.teleoff.gov.sk/data/files/27461.pdf [dostęp: 17.09.2023 r.].

[18] Minimalne wymagania dla zachowania ciągłości działania: https://www.agentschaptelecom.nl/documenten/brochures/2016/november/1/minimale-eisen-continuiteitsplan-telecomaanbieders [dostęp: 17.09.2023 r.].

W uzasadnieniu rozporządzenia z 22 czerwca 2020 r. wyjaśniono, że w Polsce nie ma zwyczaju definiowania generacji sieci komórkowych, stąd konieczne jest odwołanie się do specyfikacji, czyli raportu technicznego ETSI TR 121 915 V.15.0.0., który zawiera niezbędne informacje dotyczące wstępnej fazy wdrażania sieci 5G. Rozporządzenie precyzuje zobowiązania z art. 175 p.t. przez wskazanie, że konieczne jest, aby przedsiębiorca telekomunikacyjny dostarczający sieci 5G, w zakresie bezpieczeństwa i integralności sieci i usług: identyfikował zagrożenia bezpieczeństwa lub integralności sieci lub usług; oceniał prawdopodobieństwo oddziaływania tych zagrożeń; zapewniał i stosował środki minimalizujące skutki wystąpienia oddziaływania tych zagrożeń. Są to elementy zarządzania ryzykiem w organizacji, niezbędne do poprawnego zabezpieczenia sieci i usług.

W uzasadnieniu rozporządzenia z 22 czerwca 2020 r. wyjaśniono także, że wszystkie działania wskazane w § 3 tego rozporządzenia uzupełniają zarządzanie ryzykiem w organizacji (§ 2 pkt 3–5 rozporządzenia z 22 czerwca 2020 r.). Są one specyficzne dla powstających sieci 5G i będą stosowane przez podmioty, które te sieci budują. Przepis ten stanowi wytyczną do stosowania pozostałych środków wymienionych w rozporządzeniu. Przedstawione w § 3 środki nie oznaczają automatycznego wprowadzania zmian w sieci poszczególnych przedsiębiorców. Wszelkie działania powinny być poprzedzone analizą ryzyka i oceną, w jaki sposób wdrożenie tych środków wpłynie na poziom bezpieczeństwa danej sieci. Stanowi to mniej restrykcyjne podejście niż nakładanie środków bezpieczeństwa bezpośrednio na sieć.

Zgodnie z § 3 ust. 1 pkt 1 rozporządzenia z 22 czerwca 2020 r., dokonując zarządzania ryzykiem, przedsiębiorca dostarczający sieć 5G w ramach tej sieci, uwzględnia rekomendacje, o których mowa w art. 33 ust. 4 u.k.s.c. (rekomendacje Pełnomocnika Rządu do spraw Cyberbezpieczeństwa). W uzasadnieniu rozporządzenia z 22 czerwca 2020 r. wyjaśniono, że istotne jest, aby w ramach szacowania ryzyka przedsiębiorcy uwzględniali rekomendacje Pełnomocnika Rządu do spraw Cyberbezpieczeństwa. Nie oznacza to konieczności automatycznego ich stosowania i wprowadzania do sieci danego przedsiębiorcy telekomunikacyjnego. Ważne jest jedynie, aby przedsiębiorca świadomie planował kolejne kroki prowadzące do zapewnienia cyberbezpieczeństwa swojej sieci. Rekomendacje Pełnomocnika Rządu ds. Cyberbezpieczeństwa dotyczą stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Nie oznaczają one automatycznie konieczności pozbycia się sprzętu z sieci. Wskazują jedynie na możliwe zagrożenia wynikające ze stosowania określonych urządzeń. Rekomendacje mogą mieć również charakter pozytywny (wskazywać

zalecany sprzęt) oraz wskazywać określony sposób korzystania (np. rodzaje systemów, w których zaleca się korzystać z określonego sprzętu lub oprogramowania). W uzasadnieniu wyjaśniono także, że ujęcie rekomendacji w tym punkcie nie oznacza, iż przedsiębiorcy są włączani w procedurę dotyczącą uwzględniania stosowania rekomendacji i nadzoru określoną w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Zgodnie z § 3 ust. 1 pkt 2 rozporządzenia z 22 czerwca 2020 r. przedsiębiorca telekomunikacyjny uwzględnia rekomendacje Pełnomocnika Rządu do spraw Cyberbezpieczeństwa (art. 33 ust. 4 u.k.s.c.), stosuje strategię skutkującą brakiem uzależnienia się od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług. W uzasadnieniu tego rozporządzenia wyjaśniono, że obecne trendy europejskie akcentują ochronę łańcucha dostaw w działalności gospodarczej. Zgodne jest to z interesami samych przedsiębiorców, którzy chronią się przed uzależnieniem od jednego dostawcy (tzn. *vendor lock*), kiedy planują własne sieci. Dywersyfikacja w niektórych przypadkach będzie bardzo utrudniona. Stąd nie wskazuje się procentowo, ile urządzeń powinno być od różnych producentów, a jedynie zwraca się uwagę na konieczność stosowania odpowiedniej strategii w tym zakresie. Granicą stosowania dywersyfikacji u danego przedsiębiorcy będzie konieczność zapewnienia interoperacyjności usług. Jednocześnie powiązanie powyższych elementów z procesem szacowania ryzyka (określonym w § 2 ust. 3–5 rozporządzenia z 29 czerwca 2020 r.) pozwoli na świadome i oparte na ryzyku podejście do budowy stabilnej i bezpiecznej sieci 5G.

Wprowadzenie dla przedsiębiorców telekomunikacyjnych wymogu unikania uzależnienia od jednego producenta poszczególnych elementów sieci telekomunikacyjnej może być jednak uznane za wyjście poza delegację ustawową sformułowaną w art. 175d p.t. Delegacja ustawowa dotyczy środków technicznych i organizacyjnych oraz metod zapobiegania zagrożeniom, o których mowa w art. 175a ust. 1 p.t. i art. 175c ust. 1 p.t. Nie dotyczy natomiast kwestii związanych z zakupem elementów sieci telekomunikacyjnej przez przedsiębiorców telekomunikacyjnych od producentów infrastruktury telekomunikacyjnej.

Wreszcie, zgodnie z § 3 ust. 1 pkt 3 rozporządzenia z 22 czerwca 2020 r., przedsiębiorca telekomunikacyjny zapewnia podwyższanie odporności na zakłócenia sieci i usług telekomunikacyjnych. W uzasadnieniu rozporządzenia wyjaśniono, że zamiast wskazywania konieczności redundancji poszczególnych elementów sieci wskazuje się na konieczność podwyższania odporności (ang. *resilience*) sieci i usług. W rozporządzeniu nie wskazano szczegółowych metod, gdyż można to osiągnąć na różne sposoby, np. redundancję sprzętu czy zapewnienie roamingu krajowego.

Według z § 3 ust. 2 rozporządzenia z 22 czerwca 2020 r. przedsiębiorca telekomunikacyjny prowadzi dokumentację działań ujętych w § 3 ust. 1 tego rozporządzenia. Rozporządzenie wskazuje na prowadzenie dokumentacji jako środek organizacyjny służący zapewnieniu bezpieczeństwa lub integralności sieci. Należy jednak zauważyć, że istnienie niezbędnej dokumentacji w zakresie wykazu aktywów czy też procedur dotyczących zgłaszania naruszeń określonych zgodnie z art. 175a p.t. jest dobrą praktyką i bez niej trudno jest realizować zobowiązania ustawowe.

Zgodnie z § 4 rozporządzenia z 22 czerwca 2020 r. rozporządzenie weszło w życie po upływie 6 miesięcy od dnia jego ogłoszenia. Należy zwrócić uwagę, że obowiązek zabezpieczania sieci istnieje w ustawie – Prawo telekomunikacyjne od 2004 r. i to właśnie art. 175 tej ustawy jest podstawą prawną nakładania obowiązków na przedsiębiorcę. Niniejsze rozporządzenie jedynie wskazuje środki, które mają stosować przedsiębiorcy, realizując obowiązek ustawowy.

### 1.3. Ustawa o krajowym systemie cyberbezpieczeństwa

Obecnie obowiązuje ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. Zgodnie z art. 1 ust. 1 u.k.s.c. określa ona:

1) organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;
2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy;
3) zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Według art. 2 ust. 2 k.s.c. ustawy nie stosuje się do:

1) przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów;
2) dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE[19];
3) podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu. U.k.s.c. nie obejmuje więc trzech grup podmiotów. Dwa pierwsze przypadki wynikają wprost z implementacji dyrektywy NIS, trzeci to wyłączenie wynikające

[19] Dz.Urz. UE L 257 z 28.08.2014 r., s. 73.

z konieczności zapewnienia bezpieczeństwa narodowego. Spośród tych trzech wyłączeń dwa są całkowite – dotyczą dostawców usług zaufania oraz podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu, oraz jedno częściowe (wyłączenie o charakterze podmiotowo-przedmiotowym) – odnoszące się do przedsiębiorców telekomunikacyjnych w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów[20].

Wskazane już zostało, że zgodnie z art. 1 ust. 2 pkt 1 u.k.s.c. ustawy o krajowym systemie cyberbezpieczeństwa nie stosuje się – w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów – do przedsiębiorców telekomunikacyjnych, w wypadku których kwestie te regulują przepisy ustawy – Prawo telekomunikacyjne (art. 175–175e p.t.). Rozwiązanie to jest zgodne z podejściem przyjętym w NIS. Według art. 1 ust. 3 NIS wymogi dotyczące bezpieczeństwa i zgłaszania incydentów przewidziane w niniejszej dyrektywie nie mają zastosowania do przedsiębiorstw, którzy podlegali wymogom art. 13a i 13b dyrektywy 2002/21, ani do dostawców usług zaufania. Postanowienia art. 13a i 13b dyrektywy 2002/21 zawarte są w rozdziale IIIa tej dyrektywy, który poświęcony jest właśnie bezpieczeństwu i integralności sieci i usług. Postanowienia rozdziału IIIa dyrektywy 2002/21 zostały zaimplementowane do nowego rozdziału VIIA zatytułowanego *Bezpieczeństwo i integralność sieci i usług telekomunikacyjnych*. Ustawa z dnia 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw[21] wprowadziła po art. 175 p.t. przepisy art. 175a–175e p.t.

Wprawdzie zgodnie z art. 1 ust. 2 pkt 1 u.k.s.c. nie stosuje się jej do przedsiębiorców telekomunikacyjnych w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów, jednakże należy mieć na uwadze, że u.k.s.c. definiuje usługi cyfrowe oraz usługi kluczowe świadczone w istotnych dla gospodarki, społeczeństwa i bezpieczeństwa państwa sektorach, podsektorach oraz przez określone ustawą podmioty i nakłada na nie szczegółowe wymagania związane z zapewnieniem bezpieczeństwa. Ważne jest w tym kontekście to, że stosowanie nowych technologii, w szczególności opartych na 5G, wpłynie nie tylko na korzystanie z internetu do celów prywatnych, ale przede wszystkim usprawni funkcjonowanie całego przemysłu, w tym przedsiębiorstw o strategicznym znaczeniu dla państwa. To właśnie branże przemysłowe (w tym wymienione w załącznikach nr 1 i 2 do u.k.s.c.) mają być pierwszymi klientami, ponieważ

[20] W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019, uwaga 2 do art. 1.

[21] Dz.U. z 2012 r. poz. 1445.

5G sprzyja internetowi rzeczy, na którym coraz częściej one się opierają. Należy uwzględnić, że operatorzy usług kluczowych, podmioty działające w określonych sektorach czy świadczące zdefiniowany rodzaj usług będą wymagały współpracy i wykorzystania sieci 5G eksploatowanej przez podmioty, które uzyskają prawa do pasm wykorzystywanych w technologii 5G. Współpraca operatorów usług kluczowych czy dostawców usług cyfrowych z dostawcami sieci 5G będzie wymagała uwzględnienia określonych u.k.s.c. wymagań.

Ustawa o krajowym systemie cyberbezpieczeństwa stanowi implementację dyrektywy NIS, ale wykracza poza implementację minimalną. Zakres ustawy został poszerzony o wybrane elementy bezpieczeństwa narodowego (współpraca zespołów CSIRT, incydenty krytyczne) i instytucjonalne (utworzenie funkcji Pełnomocnika Rządu do spraw Cyberbezpieczeństwa oraz Kolegium do spraw Cyberbezpieczeństwa). Rozszerzono również zakres przedmiotowy, obejmując więcej sektorów gospodarki w stosunku do dyrektywy NIS. Doprecyzowano też ogólne przepisy z dyrektywy NIS, tworząc model uwzględniający polską specyfikę w ramach unijnego prawa. Wybrano tryb wyznaczania operatorów usług kluczowych w drodze decyzji administracyjnej. Wskazano szczegółowo obowiązki operatorów. Wydzielono zespoły CSIRT oraz podzielono odpowiedzialność organów właściwych do spraw cyberbezpieczeństwa według sektorów gospodarki i działów administracji rządowej. Rozdzielono w ten sposób część techniczną systemu od części administracyjnej. Podzielono zadania ochrony cyberprzestrzeni RP na część cywilną i wojskową[22].

Ustawa o krajowym systemie cyberbezpieczeństwa określa organizację krajowego systemu cyberbezpieczeństwa (art. 4 k.s.c.). Każda grupa podmiotów (operatorzy usług kluczowych, dostawcy usług cyfrowych, podmioty publiczne, CSIRT, organy właściwe, Pojedynczy Punkt Kontaktowy, wybrani ministrowie) ma określone zadania, uprawnienia i obowiązki związane z zapewnieniem cyberbezpieczeństwa. Określa sposób nadzoru i kontroli przez organy właściwe nad wybranymi uczestnikami systemu (rozdział 11 k.s.c.)[23].

Zgodnie z dyrektywą NIS nie stosowało się jej wymogów dotyczących bezpieczeństwa i zgłaszania incydentów do przedsiębiorców, którzy podlegali wymogom art. 13a i 13b dyrektywy 2002/21, transponowanej do polskiego prawa przez p.t. w art. 175 i n., ani do dostawców usług zaufania, którzy podlegają wymogom określonym w art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym

[22] A. Besiekierska (red.), *Ustawa o krajowym…*, uwaga 5–6 do art. 1.

[23] *Ibidem*, uwaga 7–8 do art. 1.

oraz uchylającego dyrektywę 1999/93/WE (rozporządzenie eIDAS)[24]. Zgodnie z motywami dyrektywy NIS przedsiębiorcy telekomunikacji na mocy dyrektywy 2002/21 podlegają już szczególnym wymogom bezpieczeństwa w zakresie udostępniania publicznych sieci łączności i świadczenia publicznie dostępnej usługi łączności elektronicznej w rozumieniu prawa telekomunikacyjnego[25].

W oparciu o art. 6 u.k.s.c. zostało wydane rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych[26]. Rozporządzenie to określa wykaz usług kluczowych, o których mowa w art. 5 ust. 2 pkt 1 u.k.s.c., oraz progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, stanowiące załącznik do rozporządzenia. Rozporządzenie to nie wyodrębnia jednak ani sektora telekomunikacyjnego, ani przedsiębiorców telekomunikacyjnych. Przed wydaniem tego rozporządzenia pojawiały się propozycje, aby wprowadzić sektor telekomunikacyjny oraz podmioty prowadzące działalność telekomunikacyjną na listę usług kluczowych, o których mowa w art. 4 pkt 1 u.k.s.c. W ten sposób organ właściwy do spraw cyberbezpieczeństwa mógłby wydać decyzję o uznaniu danego operatora telekomunikacyjnego za operatora usługi kluczowej. W takiej sytuacji rekomendacje z art. 33 ust. 4 u.k.s.c. stałyby się już nie fakultatywne, ale obligatoryjne. Potencjalnie wprowadzenie usług telekomunikacyjnych i operatorów telekomunikacyjnych do wykazu usług kluczowych, w połączeniu z przepisami art. 33 ust. 4a–4b u.k.s.c., które zaczęły obowiązywać od 1 stycznia 2021 r., stworzyłoby więc system, w którym pełnomocnik mógłby wydawać rekomendacje z urzędu, które to rekomendacje byłyby dla operatorów telekomunikacyjnych wiążące.

Należy przypomnieć, że zgodnie z art. 33 ust. 4 u.k.s.c. Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa („Pełnomocnik") po uzyskaniu opinii Kolegium do Spraw Cyberbezpieczeństwa („Kolegium") wydaje, zmienia lub odwołuje rekomendacje dotyczące stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Wydawanie rekomendacji, o których mowa w art. 33 ust. 4 u.k.s.c., jest częścią uregulowań zawartych w art. 33 u.k.s.c. Postanowienia art. 33 u.k.s.c. wprowadzają instytucję badania lub oceny bezpieczeństwa stosowanego sprzętu lub oprogramowania. Zgodnie z art. 33 ust. 1 u.k.s.c. CSIRT MON, CSIRT NASK lub CSIRT GOV może przeprowadzić badanie urządzenia informatycznego lub oprogramowania w celu identyfikacji

[24] Dz.Urz. UE L 257 z 28.08.2014 r., s. 73.

[25] A. Besiekierska (red.), *Ustawa o krajowym*…, uwaga nr 9–10 do art. 1.

[26] Dz.U. z 2018 r. poz. 1806.

podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, co może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Według art. 33 ust. 3 u.k.s.c. CSIRT MON, CSIRT NASK lub CSIRT GOV w przypadku identyfikacji wskazanych podatności składa wniosek w sprawie wskazanych wcześniej rekomendacji do Pełnomocnika Rządu do spraw Cyberbezpieczeństwa. Opisane rekomendacje nie mają przymiotu decyzji administracyjnej. W uzasadnieniu do ustawy wskazano, że rekomendacje są środkiem pozytywnym, co oznacza, że mogą one tylko rekomendować dane oprogramowanie lub uznać za niepożądane. Rekomendacje są środkiem dobrowolnym, co oznacza, że nie mogą wiązać prywatnych podmiotów, a więc także operatorów telekomunikacyjnych. Rekomendacje mają charakter abstrakcyjny, co z kolei oznacza, że pełnomocnik powinien poinformować o wydaniu rekomendacji wszystkie podmioty krajowego systemu cyberbezpieczeństwa, których może dotyczyć podatność[27].

Wskazane już zostało, że rekomendacje są dobrowolne, ale w praktyce możliwy jest element nacisku w postaci wystąpienia przez pełnomocnika do podmiotu nadzorującego. Brak realizacji rekomendacji nie jest wprost objęty żadną sankcją. Informacja o niedostosowaniu się do rekomendacji może być jednak zinterpretowana przez organ właściwy jako wskazówka do wszczęcia kontroli. Jeśli rekomendacja dotyczyła konkretnej podatności i nakazywała jej usunięcie, może być zastosowany przepis o przymusie usuwania podatności (art. 11 ust. 1 pkt 6 u.k.s.c.)[28]. Niedostosowanie się do niego jest zagrożone administracyjną karą pieniężną[29] do 20 tys. zł za każdą nieusuniętą podatność (art. 73 ust. 3 pkt 8 u.k.s.c.).

Rekomendacje wiążą natomiast podmioty, które są w krajowym systemie cyberbezpieczeństwa, co oznacza, że podmioty mają obowiązek udzielenia odpowiedzi w zakresie sposobu realizacji rekomendacji. Podmiot krajowego systemu cyberbezpieczeństwa może złożyć zastrzeżenia do rekomendacji. Podmioty, które wchodzą w skład krajowego systemu cyberbezpieczeństwa,

---

[27] Zob. W. Kitler, J. Taczkowska-Olszewska, F. Rodoniewicz, *Ustawa o krajowym…*, t. 7 do art. 33; A. Besiekierska (red.), *Ustawa o krajowym…*, t. 6 do art. 33.

[28] Zob. A. Besiekierska (red.), *Ustawa o krajowym…*, t. 6–7 do art. 33.

[29] Zob. szerzej w sprawie administracyjnej kary pieniężnej: A. Gronkiewicz, A. Ziółkowska, *Sankcja administracyjna w korporacjach zawodowych w odniesieniu do samorządów zaufania publicznego*, w: M. Lewicki, R. Lewicka, G. Stahl (red.), *Sankcje administracyjne. Blaski i cienie*, Warszawa 2011, s. 202 i n.; M. Wincenciak, *Sankcje w prawie administracyjnym i procedura ich wymierzania*, Warszawa 2008, s. 17 i n.

wymienia art. 4 u.k.s.c.[30] Wśród nich jest także kategoria operatora usługi kluczowej. Operatorem usługi kluczowej jest podmiot posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej (usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymieniona w wykazie usług kluczowych, stanowiącym załącznik nr 1 do u.k.s.c.). Załącznik nr 1 w ramach sektora czy podsektora nie wymienia infrastruktury telekomunikacyjnej czy szerzej telekomunikacji. Używane jest jednak określenie „infrastruktura cyfrowa", które nie może być utożsamiane z infrastrukturą telekomunikacyjną. W załączniku nr 1 do u.k.s.c. wymienia się w ostatniej rubryce infrastrukturę cyfrową, do której zalicza się: podmioty, które świadczą usługi DNS, podmioty prowadzące punkt wymiany ruchu internetowego (IXP), stanowiącego obiekt sieciowy, który umożliwia połączenie międzysystemowe pomiędzy więcej niż dwoma niezależnymi systemami autonomicznymi, głównie do celów ułatwienia wymiany ruchu internetowego, podmioty zarządzające rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD). Pomimo że jest to bardzo mały wycinek działalności największych operatorów telekomunikacyjnych, to jednak należałoby uznać, że w tym zakresie prowadzą taką działalność w ramach sektora usług kluczowych. Nie zostały jednak formalnie za takie podmioty uznane.

Zgodnie z art. 33 ust. 4a–4b u.k.s.c. w przypadku uzyskania przez pełnomocnika informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego, pełnomocnik będzie mógł jednak wydać rekomendacje z urzędu. Przed wydaniem rekomendacji w trybie art. 33 ust. 4a u.k.s.c. pełnomocnik przeprowadza konsultację z CSIRT MON, CSIRT NASK lub CSIRT GOV. Przepisy art. 33 ust. 4a–4b u.k.s.c. zostały wprowadzone ustawą z dnia 11 września 2019 r. – Przepisy wprowadzające ustawę – Prawo zamówień publicznych[31], które weszły w życie z dniem 1 stycznia 2021 r.

Przepis art. 41 u.k.s.c. określa organy właściwe do spraw cyberbezpieczeństwa[32]. Zgodnie z art. 41 pkt 8 u.k.s.c. organem właściwym do spraw cyberbezpieczeństwa dla sektora infrastruktury cyfrowej jest minister właściwy do spraw

[30] Zob. szerzej C. Banasiński, W. Nowak, *Europejski i krajowy system cyberbezpieczeństwa*, w: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018, s. 161 i n.; P. Trąbiński, *Podział kompetencji* w zapewnianiu cyberbezpieczeństwa, w: G. Szpor, A. Gryszczyńska (red.), *Internet. Strategie bezpieczeństwa. Internet: security strategy*, Warszawa 2017, s. 76 i n.

[31] Dz.U. z 2019 r. poz. 2020.

[32] Zob. szerzej w sprawie organów właściwych do spraw cyberbezpieczeństwa: C. Banasiński, *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, w: *idem* (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018, s. 27–31.

informatyzacji. Według art. 45 ust. 1 pkt 1 u.k.s.c. minister właściwy do spraw informatyzacji jest odpowiedzialny m.in. za monitorowanie wdrażania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej oraz realizację planów działań na rzecz jej wdrożenia.

### 1.4. Ustawa o zarządzaniu kryzysowym

Ustawa o zarządzaniu kryzysowym określa organy właściwe w sprawach zarządzania kryzysowego oraz ich zadania i zasady działania w tej dziedzinie, a także zasady finansowania zadań zarządzania kryzysowego (art. 1 u.z.k.). Zarządzanie kryzysowe to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej (art. 2 u.z.k.). Zgodnie z art. 3 pkt 2 u.z.k. infrastrukturę krytyczną stanowią systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje w szczególności systemy łączności i sieci teleinformatycznych. Z kolei europejska infrastruktura krytyczna oznacza systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia i instalacje kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, wyznaczone w systemach w zakresie energii elektrycznej, ropy naftowej i gazu ziemnego oraz transportu drogowego, kolejowego, lotniczego, wodnego, śródlądowego, żeglugi oceanicznej, żeglugi morskiej bliskiego zasięgu i portów, zlokalizowane na terytorium państw członkowskich Unii Europejskiej, których zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie (art. 3 pkt 2a u.z.k.).

Ustawa o zarządzaniu kryzysowym przewiduje utworzenie Krajowego Planu Zarządzania Kryzysowego oraz wojewódzkie, powiatowe i gminne plany zarządzania kryzysowego, zwane dalej „planami zarządzania kryzysowego" (art. 5 ust. 1 u.z.k.).

Zgodnie z art. 5b ust. 1 u.z.k. Rada Ministrów powinna przyjąć w drodze uchwały Narodowy Program Ochrony Infrastruktury Krytycznej, zwany dalej

„programem", którego celem jest stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej, w szczególności w zakresie:

1) zapobiegania zakłóceniom funkcjonowania infrastruktury krytycznej;
2) przygotowania na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną;
3) reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej;
4) odtwarzania infrastruktury krytycznej.

Na podstawie art. 5b ust. 9 u.z.k. zostało wydane rozporządzenie Rady Ministrów w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej z dnia 30 kwietnia 2010 r.[33]

Ochrona infrastruktury krytycznej obejmuje: gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej; opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej; odtwarzanie infrastruktury krytycznej; współpracę między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochrony (art. 6 ust. 1 u.z.k.). Do ochrony infrastruktury krytycznej zobowiązani są właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej, którzy mają obowiązek ich ochrony, w szczególności przez przygotowanie i wdrażanie, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywanie własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia (art. 6 ust. 5 u.z.k.). Właściciele, posiadacze samoistni i zależni, będący jednocześnie operatorami usług kluczowych w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa, uwzględniają w planach ochrony infrastruktury krytycznej dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych zgodnie z zakresem informacji określonym w przepisach wydanych na podstawie art. 10 ust. 5 u.k.s.c. (art. 6 ust. 5b u.z.k.). Zgodnie z art. 5 ust. 1 u.k.s.c. operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do tej ustawy, mający jednostkę organizacyjną na terytorium Polski, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. Sektory, podsektory oraz rodzaje podmiotów określa załącznik nr 1 do u.k.s.c.

Rada Ministrów sprawuje zarządzanie kryzysowe na terytorium Polski. W przypadkach niecierpiących zwłoki zarządzanie kryzysowe sprawuje minister

[33] Dz.U. z 2010 r. Nr 83, poz. 541.

właściwy do spraw wewnętrznych, zawiadamiając niezwłocznie o swoich działaniach Prezesa Rady Ministrów. Decyzje podjęte przez ministra właściwego do spraw wewnętrznych podlegają rozpatrzeniu na najbliższym posiedzeniu Rady Ministrów. Prezes Rady Ministrów, z zachowaniem przepisów o ochronie informacji niejawnych, określa, w drodze zarządzenia, wykaz przedsięwzięć i procedur systemu zarządzania kryzysowego z uwzględnieniem zobowiązań wynikających z członkostwa w Organizacji Traktatu Północnoatlantyckiego oraz organy odpowiedzialne za ich uruchamianie (art. 7 u.z.k.). W sytuacji kryzysowej Prezes Rady Ministrów może, z własnej inicjatywy albo na wniosek Szefa Kancelarii Prezesa Rady Ministrów lub ministra kierującego działem administracji rządowej, wydawać polecenia obowiązujące:

1) organy administracji rządowej;
2) państwowe osoby prawne oraz państwowe jednostki organizacyjne mające osobowość prawną;
3) organy jednostek samorządu terytorialnego, samorządowe osoby prawne oraz samorządowe jednostki organizacyjne niemające osobowości prawnej;
4) osoby prawne i jednostki organizacyjne niemające osobowości prawnej oraz przedsiębiorców (art. 7a ust. 1 u.z.k.).

Polecenia są wydawane w celu:

1) zapewnienia właściwego funkcjonowania, ochrony, wzmocnienia lub odbudowy infrastruktury krytycznej;
2) przejęcia kontroli nad sytuacją kryzysową, której wpływ na poziom bezpieczeństwa ludzi, mienia lub środowiska jest szczególnie negatywny;
3) usunięcia skutków sytuacji kryzysowej, o której mowa w poprzednim punkcie (art. 7a ust. 2 u.z.k.).

Polecenia są wydawane w drodze decyzji administracyjnej, podlegają natychmiastowemu wykonaniu z chwilą ich doręczenia lub ogłoszenia oraz nie wymagają uzasadnienia (art. 7a ust. 3 u.z.k.). Polecenia nie mogą dotyczyć rozstrzygnięć co do istoty sprawy załatwianej w drodze decyzji administracyjnej, a także nie mogą dotyczyć czynności operacyjno-rozpoznawczych, dochodzeniowo-śledczych oraz czynności z zakresu ścigania wykroczeń (art. 7a ust. 5 u.z.k.).

Wydając polecenie wobec osób prawnych i jednostek organizacyjnych niemających osobowości prawnej oraz przedsiębiorców, Prezes Rady Ministrów wyznacza ministra kierującego działem administracji rządowej odpowiedzialnego za zawarcie umowy z podmiotem albo wyznacza do jej zawarcia Szefa Kancelarii Prezesa Rady Ministrów (art. 7b ust. 1 u.z.k.). Wykonywanie zadań objętych poleceniem wydanym w stosunku do tych podmiotów następuje na podstawie umowy zawartej z podmiotem przez ministra kierującego działem

administracji rządowej albo przez Szefa Kancelarii Prezesa Rady Ministrów i jest finansowane ze środków budżetu państwa z części budżetowej, której dysponentem jest, odpowiednio, minister albo szef Kancelarii Prezesa Rady Ministrów (art. 7b ust. 2 u.z.k.).

Przy Radzie Ministrów został utworzony Rządowy Zespół Zarządzania Kryzysowego, zwany dalej „Zespołem", jako organ opiniodawczo-doradczy właściwy w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego. W skład Zespołu wchodzą:

1) Prezes Rady Ministrów – przewodniczący;
2) Minister Obrony Narodowej i minister właściwy do spraw wewnętrznych – zastępcy przewodniczącego;

2a) minister właściwy do spraw administracji publicznej;

3) Minister Spraw Zagranicznych;
4) Minister Koordynator Służb Specjalnych – jeżeli został powołany zgodnie z art. 8 ust. 1–2 u.z.k.).

Do zadań zespołu należy w szczególności przygotowywanie propozycji użycia sił i środków niezbędnych do opanowania sytuacji kryzysowych oraz doradzanie w zakresie koordynacji działań organów administracji rządowej, instytucji państwowych i służb w sytuacjach kryzysowych (art. 9 ust. 1 pkt 1–2 u.k.).

## 2. Bezpieczeństwo sieci i usług łączności elektronicznej w polskich dokumentach programowych

### 2.1. Plan działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń

Dotychczas obowiązywało stare rozporządzenie Rady Ministrów z dnia 4 stycznia 2010 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń[34]. Obowiązywał model regulacji, zgodnie z którym wymagania bezpieczeństwa określone w NIS nie dotyczyły przedsiębiorców telekomunikacyjnych. Zgodnie z art. 1 ust. 3 NIS wymogi dotyczące bezpieczeństwa i zgłaszania incydentów przewidziane w niniejszej dyrektywie nie miały zastosowania do przedsiębiorstw, które podlegały wymogom art. 13a i 13b dyrektywy 2002/21. Postanowienia art. 13a i 13b dyrektywy 2002/21 zawarte były w rozdziale IIIa, który poświęcony był właśnie bezpieczeństwu i integralności sieci i usług. W szczególności art. 13a ust. 1 dyrektywy 2002/21/

[34] Dz.U. z 2010 r. Nr 15, poz. 77.

WE nakładał na państwa członkowskie obowiązek zapewnienia, aby przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej podejmowały właściwe środki techniczne i organizacyjne w razie wystąpienia zagrożenia dla bezpieczeństwa sieci lub usług. Zgodnie natomiast z art. 13b dyrektywy 2002/21 regulator powinien być uprawniony do wydawania przedsiębiorcom wiążących instrukcji w sprawach bezpieczeństwa sieci i usług, żądania od nich informacji oraz poddania się na własny koszt przez nich audytowi bezpieczeństwa. Postanowienia rozdziału IIIa dyrektywy 2002/21 zostały zaimplementowane do nowego rozdziału VIIA prawa telekomunikacyjnego zatytułowanego *Bezpieczeństwo i integralność sieci i usług telekomunikacyjnych*. Ustawa z dnia 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw[35] wprowadziła po art. 175 p.t. przepisy art. 175a–175e p.t. Plany działań przedsiębiorców telekomunikacyjnych w sytuacjach szczególnych zagrożeń były przygotowywane w praktyce przez przedsiębiorców telekomunikacyjnych od wielu lat. Nie było z nimi problemów, gdyż stanowiły powtarzalną czynność o charakterze administracyjnym. Kilkudziesięciostronicowe plany były przygotowywane według tego samego schematu.

Rozporządzenie Rady Ministrów w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń z dnia 19 sierpnia 2020 r. zostało wydane na podstawie art. 176a ust. 5 p.t. Zgodnie z § 1 rozporządzenia z dnia 19 sierpnia 2020 r. określa ono:

1) rodzaje, zawartość, tryb sporządzania oraz aktualizacji przez przedsiębiorcę telekomunikacyjnego, zwanego dalej „przedsiębiorcą", planu działań w przypadku wystąpienia:
   a) sytuacji kryzysowych,
   b) stanów nadzwyczajnych,
   c) bezpośrednich zagrożeń dla bezpieczeństwa lub integralności infrastruktury telekomunikacyjnej przedsiębiorcy lub świadczonych przez niego usług – zwanych dalej „sytuacjami szczególnych zagrożeń";
2) organy uzgadniające plan działań w sytuacjach szczególnych zagrożeń, zwany dalej „planem", oraz zakres tych uzgodnień;
3) rodzaje przedsiębiorców obowiązanych do uzgadniania zawartości planu;
4) rodzaje działalności telekomunikacyjnej niepodlegającej obowiązkowi sporządzania planu;
5) rodzaje przedsiębiorców niepodlegających obowiązkowi sporządzania planu.

[35] Dz.U. z 2012 r. poz. 1445.

Nowela z dnia 5 lipca 2018 r., która weszła w życie 28 sierpnia 2018 r.[36], wprowadziła do art. 176a ust. 2 pkt 4 p.t. problematykę cyberbezpieczeństwa. Obowiązujące obecnie rozporządzenie wprowadza więc nowe elementy, które powinny zawierać plany w sytuacjach szczególnych zagrożeń w postaci wymagań w zakresie cyberbezpieczeństwa infrastruktury telekomunikacyjnej świadczonych usług. Zgodnie z § 6 ust. 1 pkt 2 rozporządzenie z dnia 19 sierpnia 2020 r. przedsiębiorca sporządzający plan dokonuje analizy i oceny bezpieczeństwa i integralności wykorzystywanej infrastruktury telekomunikacyjnej i świadczonych usług, w tym ochrony przed wystąpieniem incydentów w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, na podstawie dostępnych informacji o zaistniałych incydentach oraz potencjalnych przyczynach ich wystąpienia. Pojęcia „zagrożenie cyberbezpieczeństwa" oraz „incydent" są zdefiniowane w art. 2 u.k.s.c. Zagrożenie cyberbezpieczeństwa to potencjalna przyczyna wystąpienia incydentu. Incydent to zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.

Przepis § 6 ust. 1 pkt 2 rozporządzenia z dnia 19 sierpnia 2020 r. odnosi się do zagrożeń cyberbezpieczeństwa, w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Zgodnie natomiast z art. 1 ust. 2 pkt 1 u.k.s.c. ustawy o krajowym systemie cyberbezpieczeństwa nie stosuje się – w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów – do przedsiębiorców telekomunikacyjnych, w wypadku których kwestie te regulują przepisy ustawy – Prawo telekomunikacyjne (art. 175 i n. p.t.). Ustawa o krajowym systemie cyberbezpieczeństwa nie ma zastosowania do przedsiębiorców telekomunikacyjnych i dostawców usług zaufania, którzy zostali już objęci europejskimi i krajowymi wymaganiami sektorowymi z zakresu bezpieczeństwa. W związku z powyższym powstaje pytanie o podstawę prawną odesłania w rozporządzeniu z dnia 19 sierpnia 2020 r. wydawanym w oparciu o art. 176a p.t. do przepisów u.k.s.c., które zgodnie z art. 1 ust. 2 pkt 1 u.k.s.c. nie mają zastosowania.

Problem ten dostrzegał sam projektodawca, który na s. 11 uzasadnienia projektu rozporządzenia z dnia 19 sierpnia 2020 r. w wersji z dnia 18 maja 2020 r. wyjaśniał, że potrzebę analizy rozszerzono o zagrożenia cyberbezpieczeństwa i ich wpływ na bezpieczeństwo i integralność. Takie podejście, według projektodawcy, wynika z przepisów ustawy o krajowym systemie cyberbezpieczeństwa, zmieniających przepisy art. 176a ust. 1 pkt 3 i ust. 2 pkt 4 ustawy. Projektodawca wyjaśnił, że u.k.s.c. nie obejmuje przedsiębiorców telekomunikacyjnych, co oznacza, że nie są oni elementem krajowego systemu cyberbezpieczeństwa

[36] Dz.U. z 2018 r. poz. 1560.

i nie mają obowiązków związanych z uczestnictwem w tym systemie. Projektodawca uznał jednak, że racjonalne wydaje się, aby wykonując swoją działalność telekomunikacyjną, przeprowadzali analizy incydentów i zabezpieczali swoje sieci i usługi.

## 2.2. Strategia Cyberbezpieczeństwa Polski

W okresie prac nad wdrożeniem dyrektywy NIS do polskiego porządku prawnego prowadzone były prace nad Strategią Cyberbezpieczeństwa RP, które zostały przyjęte przez Radę Ministrów w listopadzie 2017 r.[37] Po wejściu w życie u.k.s.c. na podstawie art. 68 tej ustawy Rada Ministrów przygotowała uchwałę *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*, („Strategia Cyberbezpieczeństwa"), stanowiącą załącznik do uchwały. Strategia to dokument, który określa strategiczne cele rządu polskiego w zakresie cyberbezpieczeństwa. Zgodnie z tą strategią kluczowe jest, aby systemy informacyjne, operatorzy usług kluczowych, operatorzy infrastruktury krytycznej, dostawcy usług cyfrowych oraz administracja publiczna były odporne na incydenty w cyberprzestrzeni.

W rozdziale zatytułowanym *Zwiększenie cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury krytycznej* wskazano, iż technologie informatyczne wykorzystywane przez operatorów usług kluczowych, dostawców usług cyfrowych, operatorów infrastruktury krytycznej (w tym operatorów telekomunikacyjnych) stanowią element krytyczny dla ciągłości działania państwa oraz zapewniania bezpieczeństwa obywatelom. Co więcej, bezpieczeństwo najważniejszych sektorów gospodarki, ze szczególnym uwzględnieniem sektora energii, zależy od zapewnienia niezakłóconego działania przemysłowych systemów sterowania. Dlatego zapewnienie cyberbezpieczeństwa zarówno IT, jak i OT będzie traktowane przez rząd jako priorytet. Wyrazem tego są przygotowywane już analizy dotyczące doprecyzowania wymagań bezpieczeństwa niezbędnych do spełnienia przez operatorów telekomunikacyjnych, szczególnie przy budowie sieci 5G, która w przyszłości będzie podstawą funkcjonowania państwa w zakresie mobilnej telekomunikacji. Zakłada się, że będą w tym obszarze konieczne zmiany prawne, aby umożliwić odpowiednią kontrolę nad zapewnieniem cyberbezpieczeństwa.

Oprócz tego, mając na uwadze, że odpowiedzialność za zapewnienie bezpieczeństwa usług leży przede wszystkim po stronie podmiotów je świadczących, rząd podejmie działania wspierające budowanie zdolności i kompetencji

[37] Uchwała nr 52/2017 Rady Ministrów z 27.04.2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022.

w zakresie cyberbezpieczeństwa wśród operatorów usług kluczowych, operatorów infrastruktury krytycznej oraz dostawców usług cyfrowych, uwzględniając ich różnorodną specyfikę i różny stopień dojrzałości w zakresie cyberbezpieczeństwa. Ponadto rząd będzie wspierał te podmioty w reagowaniu na incydenty istotne, krytyczne i poważne, szczególnie w przypadku wystąpienia incydentów ponadsektorowych. W pierwszej kolejności zostanie zapewniona spójność działań w zakresie opracowywania kryteriów identyfikacji operatorów infrastruktury krytycznej i operatorów usług kluczowych, uwzględniająca potrzebę włączenia tych podmiotów do systemu zarządzania kryzysowego. Proces ten przebiegał będzie we współpracy ze wszystkimi sektorami. Wykorzystując mechanizmy przewidziane prawem, rekomendowane będą minimalne wymagania w zakresie cyberbezpieczeństwa ze szczególnym uwzględnianiem zarządzania ciągłością działania.

W Strategii Cyberbezpieczeństwa wskazano, że analogicznym reżimem objęci zostaną dostawcy usług cyfrowych. Rząd uwzględnił międzynarodową specyfikę tych podmiotów oraz konieczność zapewnienia takich regulacji, sprzyjające rozwojowi rynku cyfrowego w Polsce. Stąd działania w tym obszarze będą prowadzone na forum europejskim, przede wszystkim w ramach NISCG, a także w ramach współpracy transatlantyckiej z brytyjskimi i amerykańskimi instytucjami stymulującymi podnoszenie standardów cyberbezpieczeństwa przez dostawców usług cyfrowych. Na potrzeby zarządzania cyberbezpieczeństwem na poziomie krajowym wdrożona zostanie wspólna metodyka statycznego i dynamicznego szacowania ryzyka, uwzględniająca specyfikę poszczególnych sektorów, a także operatorów infrastruktury krytycznej, operatorów usług kluczowych i dostawców usług cyfrowych. Metodyka i narzędzia umożliwiające statyczne i dynamiczne szacowania ryzyka dla systemów teleinformatycznych powstają w ramach projektu Narodowej Platformy Cyberbezpieczeństwa finansowanego przez Narodowe Centrum Badań i Rozwoju. Metodyka i narzędzia umożliwiające statyczne i dynamiczne szacowanie ryzyka dla systemów teleinformatycznych są także opracowywane w ramach projektu badawczego *Narodowa Platforma Cyberbezpieczeństwa*, realizowanego przez Naukową i Akademicką Sieć Komputerową i finansowanego przez Narodowe Centrum Badań i Rozwoju w ramach Programu CyberSecIdent – Cyberbezpieczeństwo i e-Tożsamość. W dokumencie Strategia Cyberbezpieczeństwa wskazano również, że wykorzystując potencjał intelektualny ekspertów zgromadzonych w komitetach technicznych Polskiego Komitetu Normalizacyjnego, ośrodkach naukowych, akademickich i instytutach badawczych, a także w zainteresowanych podmiotach publicznych i prywatnych, opracowane zostaną nowe standardy lub nastąpi przełożenie istniejących norm i standardów na konkretne rekomendacje w zakresie ich wdrażania. W celu

zwiększenia odporności systemów informacyjnych administracji publicznej na cyberzagrożenia niezbędne jest opracowanie Narodowych Standardów Cyberbezpieczeństwa jako zbioru wymagań organizacyjnych i technicznych dotyczących bezpieczeństwa m.in. aplikacji, urządzeń mobilnych serwerów i sieci, stacji roboczych, modeli chmur obliczeniowych.

Według Strategii Cyberbezpieczeństwa zapewnienie cyberbezpieczeństwa wymaga stosowania zabezpieczeń organizacyjnych i technicznych na wszystkich etapach cyklu życia systemów teleinformatycznych. Działania te składają się na tzw. bezpieczny łańcuch dostaw, który obejmuje projektowanie, budowę, wdrażanie, eksploatację oraz wycofywanie z użycia. Przez pojęcie łańcucha dostaw należy rozumieć system, na który składają się podsystemy produkcji, dystrybucji, transportu, magazynowania oraz recyklingu komponentów systemów teleinformatycznych, jak również ich instalacja, uruchomienie, bieżące utrzymanie, serwisowanie oraz naprawy. Ważnym elementem zapewnienia jakości w łańcuchu dostaw będzie ocena i certyfikacja produktów (w szczególności oprogramowania, urządzeń i usług). Priorytetowe w tym zakresie będzie utworzenie, a następnie utrzymanie i rozwój krajowego systemu oceny i certyfikacji cyberbezpieczeństwa bazującego na działalności akredytowanych jednostek oceniających zgodność, co umożliwi Polsce uzyskanie pełnego i rozpoznawanego na arenie europejskiej i międzynarodowej statusu państwa producenta w dziedzinie rozwiązań cyberbezpieczeństwa.

Zgodnie ze Strategią Cyberbezpieczeństwa Polska aktywnie włączy się w prace nad ustanowieniem europejskich programów certyfikacji cyberbezpieczeństwa zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych. Działania na poziomie krajowym będą obejmowały, w szczególności, wyznaczenie krajowego organu ds. certyfikacji cyberbezpieczeństwa, który będzie wydawał europejskie certyfikaty cyberbezpieczeństwa oraz nadzorował krajowe jednostki oceniające zgodność produktów, usług i procesów z wymaganiami określonymi w europejskich programach certyfikacji cyberbezpieczeństwa oraz współpracował z krajową jednostką akredytującą – Polskim Centrum Akredytacji, w celu monitorowania i nadzorowania działalności akredytowanych jednostek oceniających zgodność w odniesieniu do wymagań rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881. Efektem tych działań będzie zdobycie na poziomie krajowym zdolności do wspierania polskich producentów, którzy uzyskując europejskie certyfikaty cyberbezpieczeństwa, będą mogli skuteczniej konkurować na jednolitym rynku cyfrowym UE. Zostaną określone konkretne zadania oraz działania dla organów administracji rządowej wraz z harmonogramem ich

realizacji. Wskazane też zostaną źródła finansowania oraz mierniki pozwalające na określenie stopnia realizacji konkretnego działania.

Istotne kwestie odnośnie do wdrażania usług opartych na technologii 5G zostały podniesione w *Opinii Rady ds. Cyfryzacji do Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*. Pozytywnie oceniono wskazanie konieczności doprecyzowania wymagań bezpieczeństwa niezbędnych do spełnienia przez operatorów telekomunikacyjnych, szczególnie przy budowie sieci 5G, oraz wprowadzenie zmian prawnych umożliwiających odpowiednią kontrolę nad zapewnieniem cyberbezpieczeństwa. Zwrócono uwagę, iż w obliczu dynamicznie rozwijających się technologii związanych m.in. z internetem rzeczy istnieje konieczność nie tylko zapewnienia bezpieczeństwa produktu, usługi lub procesu już na etapie projektowania (ang. *security by design*), ale także potrzeba odniesienia tej zasady do ochrony danych i prywatności (ang. *privacy by design*).

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 jest efektem prac sformułowanych w innych wcześniejszych dokumentach dotyczących cyberbezpieczeństwa Polski i rozwoju sług w sieci 5G. W szczególności należy wskazać na Narodowy Plan Szerokopasmowy. W dokumencie tym omówione zostały plany rozwoju sieci 5G pod kątem m.in. wykorzystania do świadczenia usług szerokopasmowej transmisji danych, modeli budowy sieci 5G i źródeł jej finansowania (w tym m.in. trzech odrębnych sieci finansowanych wyłącznie przez operatorów, z częściowym udziałem środków publicznych, albo jednej sieci ze współudziałem środków publicznych). Główne prace dotyczące dokumentu NPS przypadają na 2018 r., ale były także kontynuowane w 2019 r.

Wskazać należy także na dokument *Strategia 5G dla Polski*. Przewiduje on, że Cyberbezpieczeństwo sieci 5G będzie kluczowym wyzwaniem, ponieważ niezawodność komunikacji będzie miała decydujące znaczenie dla dostarczania usług, szczególnie w przypadku komunikacji krytycznej. Nie tylko na poziomie zapewnienia usług sieciowych, ale także w warstwach wyższych związanych ze świadczeniem konkretnych usług. Architektury bezpieczeństwa wykorzystujące sieci 5G w warstwach aplikacyjnych będą musiały zmierzyć się z wyzwaniami, takimi jak: wypracowanie nowych modeli świadczenia usług, zastosowanie nowych modeli ustanawiania związków zaufania między poszczególnymi uczestnikami komunikacji w danym ekosystemie i między różnymi ekosystemami; zapewnienie użytkownikowi prawa do zachowania prywatności; wypracowanie zasad i modeli niezawodnej współpracy pomiędzy gestorami poszczególnych usług i systemów, a także użytkowników w sytuacji zagrożenia bezpieczeństwa czy zaistnienia incydentów.

Działania w zakresie rozwoju infrastruktury sieci 5G w Polsce muszą uwzględniać aspekty bezpieczeństwa, niezawodności oraz odporności na uszkodzenia (ang. *resilience*) od początkowego etapu projektowania rozwiązań. Od początku musi być także budowana świadomość zróżnicowanej roli podmiotów odpowiedzialnych za dostarczanie sieci, usług transmisji, szeroko pojętych usług telekomunikacyjnych, które dla zapewnienia kompleksowego bezpieczeństwa powinny być realizowane przez dostawców usług społeczeństwa informacyjnego. W Strategii Cyberbezpieczeństwa w zakresie infrastruktury sieci 5G wskazano jako konieczne śledzenie prac i zapewnienie zastosowania rozwiązań przyjętych przez organizacje normalizacyjne, takie jak:

- 3GPP – w obszarze architektury sieci, uwierzytelniania, zarządzania kluczami kryptograficznymi, bezpieczeństwa sieci wirtualnych (ang. *network slicing*), bezpieczeństwa i prywatności urządzeń abonenckich;
- ETSI, NFV – w obszarze zarządzania bezpieczeństwem i monitorowania NFV, zarządzania zaufaniem, specyfikacjami technicznymi bezpiecznych komponentów;
- IETF – w obszarze protokołów komunikacyjnych, ONF (Open Network Foundation) – w zakresie sieci definiowanych programowo;
- ISO, IEC – w obszarze lekkiej kryptografii (ang. *lightweight cryptography*), kryptografii kwantowej, bezpieczeństwa informacji, metod ewaluacji bezpieczeństwa, zarządzania tożsamością i prywatnością, internetu rzeczy, bezpieczeństwa pojazdów itp.;
- WTSA, ITU – w szczególności w obszarach standaryzacji dla rozwiązań IoT, sieci telekomunikacyjnych;
- GSMA – w zakresie rozwoju technologii mobilnych i ich bezpieczeństwa w obszarach takich jak IoT security, IoT big data, *smart cities*, *connected vehicles* czy ustanowienia dobrych praktyk polityki regulacyjnej.

W powyższym zakresie minister cyfryzacji będzie dążyć do skoordynowanego wsparcia dla prac normalizacyjnych realizowanych na poziomie krajowym, europejskim i międzynarodowym przez grupy eksperckie, które mogą działać, także przy porozumieniu na rzecz strategii 5G dla Polski. W prace powinni również zostać włączeni przedstawiciele Polskiego Komitetu Normalizacyjnego, tak aby skorzystać z ich doświadczenia dla uniknięcia powielania prac i tworzenia mnogości standardów. Dla efektywnej realizacji celów minister cyfryzacji będzie dążyć do zapewnienia wsparcia podmiotów realizujących politykę rozwoju i innowacyjności, takich jak Narodowe Centrum Badań i Rozwoju oraz Polska Agencja Rozwoju Przedsiębiorczości, a także w ramach europejskich programów badawczych (takich jak Horyzont 2020 oraz programy przewidywane do uruchomienia w latach następnych).

W Strategii Cyberbezpieczeństwa wskazano także na potrzebę opracowania i wdrażania komponentów sprzętowych i programowych. Obszar ten będzie w znacznym stopniu wspierany przez inicjowane w ramach Strategii Cyberbezpieczeństwa zaawansowane programy badawczo-rozwojowe mogące dać efektywne narzędzia z obszaru bezpieczeństwa sieci 5G. Kluczowe działania to:

- opracowywanie rozwiązań sprzętowo-programowych zapewniających realizację zasady bezpieczeństwa E2E (ang. *end to end*), w tym nowe komponenty z wbudowanymi elementami bezpieczeństwa, takie jak urządzenia abonenckie, obsługowe i bezobsługowe, które będą zdolne do ochrony swojej tożsamości sieciowej w silnym, odpornym na manipulacje systemie zarządzania tożsamością;
- opracowywanie technik i metod przeciwdziałania nowym, zaawansowanym atakom na infrastrukturę dostępową i aplikacje, w tym na architekturę zaufania.

W Strategii Cyberbezpieczeństwa zauważa się, że w wypadku zastosowań krytycznych dla zdrowia lub życia albo mających znaczny wymiar ekonomiczny, np. w infrastrukturze krytycznej, kluczowe staje się zapewnienie, że oferowane rozwiązanie spełnia wymagania bezpieczeństwa w obu znaczeniach tego terminu (ang. *safety* oraz *security*), które często już się przenikają. Z tego względu konieczne są następujące kierunki działań:

- opracowywanie metod i technik efektywnego testowania nowych urządzeń oraz ciągłego sprawdzania integralności urządzeń będących w eksploatacji (zarówno komponentów sieci, jak i urządzeń końcowych);
- realizowanie jako wspólnych przedsięwzięć przemysłu (dostawców), normalizatorów i legislatorów formujących prawny kontekst odpowiedzialności za bezpieczeństwo produktu i promujących takich producentów (dostawców), którzy będą sami dostarczać rozwiązania możliwe do prostego przetestowania;
- wypracowanie metod zapewniających stabilne aktualizowanie oprogramowania urządzeń końcowych, w szczególności z uwagi na luki bezpieczeństwa oraz wycofywanie urządzeń z eksploatacji;
- zdefiniowanie i uzgodnienie możliwych działań w przypadku stwierdzenia działania urządzeń końcowych w sposób zagrażający bezpieczeństwu;
- rozwój krajowych kompetencji systemu oceny i certyfikacji zgodnego z normą Common Criteria (ISO 15408) o zakresie ewaluacji komponentów sieci 5G oraz usług budowanych na takich sieciach i urządzeń tam stosowanych w niezbędnym zakresie;
- znaczne rozszerzenie o metody i techniki ewaluacji bezpieczeństwa oraz prywatności aktualnie prowadzone prace dotyczące budowy polskiego systemu oceny i certyfikacji bezpieczeństwa produktów IT, a w szczególności

internetu pojazdów (IoV), telemedycyny, aplikacji mobilnych, komponentów sieci 5G, w tym oprogramowania wirtualizacyjnego funkcji sieciowych.

Strategia Cyberbezpieczeństwa wskazuje, że działania te należy prowadzić w sposób niegenerujący dodatkowych procesów certyfikujących, a umożliwiający podejmowanie części istotnych procesów oceny i certyfikacji bez konieczności korzystania z innych ośrodków zagranicznych. Ten kierunek działania powinien być prowadzony lub koordynowany przez jednostki naukowo-badawcze realizujące projekt KSO3C, a także – w szerokim porozumieniu – z istniejącą siecią jednostek certyfikujących, laboratoriów dokonujących ocen i pomiarów, wzorcowania i kalibracji w obszarze telekomunikacji i automatyki przemysłowej, z udziałem Polskiego Centrum Akredytacji. Podjęte zostaną również działania zmierzające do poszerzenia programu badawczo-rozwojowego w NCBiR (CyberSecIdent) o zagadnienia związane z metodami i technikami ewaluacji bezpieczeństwa (i prywatności) dotyczące sieci 5G.

Strategia Cyberbezpieczeństwa zajmuje się także kwestiami dotyczącymi testów funkcjonowania sieci 5G. Obecni na polskim rynku operatorzy telekomunikacyjni, jak również dostawcy sprzętu, planują testy kluczowych komponentów sieci 5G zarówno w laboratorium, jak i na wybranych stacjach bazowych oraz innych obiektach – w zależności od charakteru i zakresu poszczególnych badań i eksperymentów. Przeprowadzenie pełnego pilotażu E2E (ang. *end-to-end*) usług oferowanych przez sieć 5G jest uwarunkowane zakończeniem prac standaryzacyjnych, gotowością pasm testowych, gotowością infrastruktury oraz zaangażowaniem partnerów publicznych i przemysłowych. Do efektywnego przeprowadzenia testów sieci 5G na terenie Polski niezbędne są:

- zdefiniowane standardy;
- dostępność sprzętu dla sieci szkieletowej;
- dostępność terminali abonenckich i/lub modułów M2M,
- przeznaczenie dostępnych segmentów widmowych o odpowiednich szerokościach w pasach częstotliwości przeznaczonych dla sieci 5G;
- przyjęcie modelu i zakresu programu testów;
- wspomaganie badań naukowo-rozwojowych, w szczególności zwiększających zaangażowanie partnerów przemysłowych;
- zapewnienie udziału w testach podmiotów niezależnych, np. uczelni, instytutów badawczych, samorządów, co dodatkowo stworzy możliwość ich przeprowadzenia w formule partnerstwa publiczno-prywatnego.

W dniu 15 lipca 2019 r. Ministerstwo Cyfryzacji przesłało zgodnie z planem do Komisji Europejskiej informacje odnośnie do szacowania ryzyka dla sieci 5G oraz proponowanych działań mitygujących. Wypełniony formularz oraz analiza zostały przekazane grupie roboczej przy KE w celu ich analizy przez Komisję

Europejską i ENISA. Analiza została przygotowana przez zespół roboczy powołany przez ministra cyfryzacji z udziałem ekspertów MC, NASK PIB, IŁ oraz ABW pod przewodnictwem Pełnomocnika Rządu do spraw Cyberbezpieczeństwa. Następnie wyniki analizy zostały zaakceptowane przez Kolegium do spraw Cyberbezpieczeństwa.

Komisja Europejska monitoruje konkurencyjność cyfrową państw członkowskich przy pomocy sprawozdań dotyczących indeksu gospodarki cyfrowej i społeczeństwa cyfrowego. Zbiór sprawozdań obejmuje zarówno profile poszczególnych krajów, jak i rozdziały tematyczne. Z zakresu obszaru bezpieczeństwa wskazano w dokumencie, że Polska zapowiedziała nową strategię POPC na lata 2021–2027, która obejmie zaawansowane umiejętności cyfrowe w dziedzinie cyberbezpieczeństwa, obliczenia wielkiej skali (HPC) i sztuczną inteligencję (AI).

Na początku 2018 r. Polska opublikowała projekt strategii *5G dla Polski*, w której nakreślono niezbędne zmiany legislacyjne mające ułatwić wprowadzanie sieci 5G, a także cele pośrednie i ogólne. Wstępny plan zakładał ogłoszenie aukcji pasma 700 MHz do 2020 r., jednak na początku 2019 r. Polska powiadomiła Komisję o swoim zamiarze opóźnienia tego procesu do dnia 30 czerwca 2022 r. w związku z nierozwiązaną kwestią koordynacji pasma z państwami trzecimi. W celu rozwiązania tego problemu Polska zwróciła się również o pomoc do KE. Znaczne rozdrobnienie częstotliwości w paśmie 3,4–3,8 GHz wymaga odpowiednich narzędzi zmiany zagospodarowania częstotliwości, aby możliwe było skuteczne zarządzanie nimi na potrzeby wprowadzania sieci 5G. W tym celu rząd zaproponował szereg poprawek legislacyjnych mających na celu ogólne polepszenie przepisów dotyczących organizacji aukcji pasma oraz służących ułatwieniu wprowadzenia sieci 5G. Wszystkie zainteresowane strony są zgodne jednak co do tego, że istnieje ryzyko opóźnienia wprowadzenia sieci 5G w Polsce z uwagi na niskie limity dotyczące pól elektromagnetycznych oraz duże rozdrobnienie częstotliwości przeznaczonych na 5G. W 2023 r. została przeprowadzona aukcja na częstotliwości 5G, którą wygrali czterej działający na polskim rynku telekomunikacyjnym operatorzy mobilni. Następnie zostało wszczęte przez Prezesa UKE postępowanie rezerwacyjne, które zakończyło się wydaniem w grudniu 2023 r. dla wskazanych czterech operatorów mobilnych decyzji rezerwacyjnych przyznających im częstotliwości z pasma 3,4–3,8 GHz, niezbędne do świadczenia usług w technologii 5G.

# Rozdział III
## Założenia i kierunek zmian prawa polskiego w zakresie komunikacji elektronicznej i systemu cyberbezpieczeństwa

## 1. Prawo komunikacji elektronicznej

W dniu 9 grudnia 2022 r. został skierowany do sejmu rządowy projekt ustawy – Prawo komunikacji elektronicznej (druk sejmowy nr 2861). P.k.e. kompleksowo reguluje m.in. kwestie wykonywania działalności polegającej na zapewnieniu komunikacji elektronicznej, regulowania rynków komunikacji elektronicznej, warunki gospodarowania częstotliwościami, zasobami orbitalnymi oraz zasobami numeracji, a także prawa i obowiązki użytkowników, zasady przetwarzania danych telekomunikacyjnych i ochrony tajemnicy komunikacji elektronicznej. Dotychczas materia ta była regulowana ustawą z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, która ma być zastąpiona p.k.e. Potrzeba opracowania nowej ustawy wynika z konieczności wdrożenia do polskiego porządku prawnego przepisów dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej. Zastąpienie dotychczasowej ustawy p.t. nowym aktem prawnym uzasadnione jest zakresem i liczbą zmian oraz koniecznością uporządkowania, przeredagowania i niejednokrotnie uproszczenia dotychczas funkcjonujących przepisów z zakresu ustawy p.t.[1]

Przepis art. 1 ust. 1 pkt 4 p.k.e. stanowi, że p.k.e. określa zadania i obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie komunikacji elektronicznej. Dział I rozdział 5 p.k.e. jest więc poświęcony obowiązkom na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Pojęcia (wyrażenia) „obronność" i „bezpieczeństwo" państwa właściwe są m.in. dla ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny[2], w której występują te określenia. Natomiast „bezpieczeństwo i porządek publiczny" właściwe jest m.in. dla Konstytucji RP oraz ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym[3].

Projekt nie wyjaśnia, co należy rozumieć przez pojęcie bezpieczeństwa sieci i usług. We wcześniejszej wersji projektu p.k.e. przepis art. 2 pkt 4 wskazywał, że oznacza to: „zdolność sieci telekomunikacyjnych lub usług telekomunikacji

---

1 Zob. uzasadnienie p.k.e.

2 Dz.U. z 2022 r. poz. 655 ze zm.

3 Dz.U. z 2002 r. Nr 113, poz. 985 ze zm.

elektronicznej do odpierania wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność: a) tych sieci lub usług, b) przetwarzanych danych i treści objętych tajemnicą komunikacji elektronicznej, c) innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy". Pozytywnie należało ocenić wprowadzenie do projektu definicji bezpieczeństwa sieci i usług, zwłaszcza że w obowiązującej ustawie p.t. brak takiej definicji. Zwrócić jednak należy uwagę na niespójność pomiędzy definicją bezpieczeństwa sieci i usług zawartą w EKŁE (art. 2 pkt 21 EKŁE) a tą zawartą we wcześniejszej wersji projektu p.k.e. Projekt p.k.e. pomijał istotną, zawartą w EKŁE, przesłankę „danego poziomu pewności" w kontekście zdolności odpierania przez sieć i usługi łączności elektronicznej działań naruszających m.in. dostępność, autentyczność konkretnej sieci i usług.

W rozdziale 5 działu pierwszego p.k.e. uregulowane zostały kwestie dotyczące obowiązku stosowania przez przedsiębiorców telekomunikacyjnych środków zapewniających bezpieczeństwo sieci lub usług oraz obowiązku sporządzania planu działań w sytuacjach szczególnych zagrożeń. Przedmiotem ochrony w tym rozdziale są bezpieczeństwo i integralność sieci, usług i przekazu komunikatów[4]. Przedmiotem ochrony są też substancja i funkcjonalność sieci oraz jej zdolność do świadczenia usług. Bezpieczeństwo i integralność usług są związane z zachowaniem stabilnych warunków dostarczania usług abonentom przy założonej funkcjonalności usług[5].

Przedsiębiorcy telekomunikacyjni są zobowiązani do wykonywania zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w zakresie i na warunkach określonych w ustawie p.k.e. i w przepisach odrębnych. Usługi telekomunikacyjne są bowiem często wykorzystywane do popełniania przestępstw. Niemniej jednak realizacja tych obowiązków może prowadzić do naruszania danych osobowych użytkowników usług telekomunikacyjnych. W związku z tym państwa członkowskie UE mogą podejmować działania legislacyjne, które ograniczają zakres ochrony danych osobowych z uwagi na wymagania w zakresie bezpieczeństwa państwa, obronności, bezpieczeństwa publicznego, zwalczania przestępczości i realizacji innych ważnych interesów państw członkowskich oraz ochrony danych osobowych osób fizycznych. W zakresie ochrony danych osobowych środki powinny

[4] M. Rogalski, *Projekt ustawy Prawo komunikacji elektronicznej – zagadnienia wybrane*, „Krytyka Prawa" 2021, nr 2, s. 130 i n.

[5] Najczęściej występujące zagrożenia bezpieczeństwa sieci i usług przedstawiają M. Betkier, J. Górski, *Ochrona sieci przed zagrożeniami*, „Prawo i Regulacje Świata Telekomunikacji i Mediów" 2010, nr 2, s. 64 i n.

być dostosowane do stanu wiedzy technicznej oraz kosztu ich wdrożenia oraz powinny uwzględniać charakter, zakres i cele przetwarzania oraz ryzyko naruszenia praw i wolności podmiotów[6].

Przepis art. 15 dyrektywy 2002/58 określa zakres stosowania niektórych przepisów dyrektywy 95/46. Zgodnie z art. 15 ust. 1 dyrektywy 2002/58 państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, 8 ust. 1–4, i art. 9 tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (tj. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy 95/46.

Przepisy rozdziału 5 działu I nie zawierają rozwiązań szczegółowych w zakresie ochrony danych wykraczających poza ochronę tajemnicy telekomunikacyjnej, gdyż wymogi szczegółowe zależą od przyjętego sposobu realizacji wskazanych zadań i określone są przepisami odrębnymi, w tym w szczególności przepisami ustawy o ochronie informacji niejawnych i ustawy o ochronie danych osobowych oraz RODO. Przepisy tych aktów prawnych mają zastosowanie niezależnie od minimalnego standardu bezpieczeństwa danych telekomunikacyjnych, określonego w rozdziale 5 ustawy działu I p.k.e. Przykładowo więc prezes UODO będzie mógł zarówno występować do przedsiębiorców komunikacji elektronicznej na podstawie art. 52 u.o.d.o. w celu zapewnienia skutecznej ochrony danych osobowych[7], jak i prowadzić kontrolę działalności przedsiębiorców w sprawach naruszeń danych osobowych oraz wydawać zalecenia na podstawie art. 58 RODO.

Przepis art. 39 ust. 1 p.k.e. określa obowiązki przedsiębiorców telekomunikacyjnych w sytuacji wystąpienia szczególnego zagrożenia. Zgodnie z art. 2 pkt 65 p.k.e. sytuacja szczególnego zagrożenia oznacza sytuację:

a) wymagającą współpracy przedsiębiorców komunikacji elektronicznej z organami administracji publicznej i innymi podmiotami wykonującymi zadania w zakresie ratownictwa, niesienia pomocy, zarządzania kryzysowego, utrzymania porządku publicznego oraz obronności i bezpieczeństwa państwa:

---

[6] Zob. szerzej D. Lubasz, w: E. Bielak-Jomaa, D. Lubasz, *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 695 i n.; P. Litwiński (red.), P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018, s. 501 i n.

[7] Zob. G. Sibiga, *Wystąpienie – nowa kompetencja Generalnego Inspektora Ochrony Danych Osobowych*, dodatek do „Monitora Prawniczego" 2011, nr 3, s. 1027 i n.

- w przypadku wystąpienia sytuacji kryzysowej, w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[8],
- w czasie obowiązywania stanów nadzwyczajnych,
- w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny,

b) stanowiącą bezpośrednie zagrożenie dla bezpieczeństwa sieci i usług komunikacji elektronicznej.

Sytuacje szczególnego zagrożenia oznaczają więc zamknięty katalog zdarzeń zdefiniowanych w przepisach, do których p.k.e. odsyła. Według art. 3 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym sytuacja kryzysowa oznacza sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków.

Pojęcie sytuacji szczególnych zagrożeń występuje w XI Rozdziale Konstytucji RP i związane jest z wprowadzaniem stanów nadzwyczajnych (stanu wojennego, stanu wyjątkowego, stanu klęski żywiołowej)[9]. Zgodnie z art. 228 ust. 1 Konstytucji RP w sytuacji szczególnych zagrożeń, gdy zwykłe środki konstytucyjne nie są wystarczające, może zostać wprowadzony odpowiedni stan nadzwyczajny. Stan nadzwyczajny może być wprowadzony tylko na podstawie ustawy, w drodze rozporządzenia, które podlega dodatkowemu podaniu do publicznej wiadomości (art. 228 ust. 2 Konstytucji RP). Do stanów nadzwyczajnych należy zaliczyć: stan wojenny, stan wyjątkowy czy stan klęski żywiołowej. Stan wojenny można wprowadzić na części albo na całym terytorium państwa w razie zewnętrznego zagrożenia państwa, zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji. Stan wojenny wprowadza Prezydent Rzeczypospolitej na wniosek RM (art. 229 Konstytucji RP)[10]. Stan wyjątkowy może być wprowadzony na części albo na całym terytorium państwa w razie zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego. Wprowadza go Prezydent Rzeczypospolitej na wniosek RM na czas oznaczony, nie dłuższy niż 90 dni. Przedłużenie stanu wyjątkowego może nastąpić tylko raz za zgodą Sejmu

[8] Dz.U. z 2022 r. poz. 261, 583 i 2185.

[9] Zob. szerzej L. Garlicki, *Polskie prawo konstytucyjne*, Warszawa 2002, s. 424–426; K. Prokop, *Stany nadzwyczajne w Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, Białystok 2005, s. 9 i n.

[10] Zob. także ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz.U. z 2002 r. Nr 156, poz. 1301 ze zm.).

i na czas nie dłuższy niż 60 dni (art. 230 Konstytucji RP)[11]. W celu zapobieżenia skutkom katastrof naturalnych lub awarii technicznych noszących znamiona klęski żywiołowej oraz ich usunięcia RM może wprowadzić na czas oznaczony, nie dłuższy niż 30 dni, stan klęski żywiołowej na części albo na całym terytorium państwa. Przedłużenie tego stanu może nastąpić za zgodą Sejmu (art. 232 Konstytucji RP)[12].

Przepis art. 39 ust. 1 p.k.e. nakłada na przedsiębiorcę telekomunikacyjnego obowiązek posiadania oraz wprowadzonego do stosowania planu działań w sytuacjach szczególnych zagrożeń. Pojęcie przedsiębiorców telekomunikacyjnych jest zdefiniowane w art. 2 pkt 40 p.k.e. i obejmuje dostawców usług telekomunikacyjnych oraz operatorów. Statusu przedsiębiorcy telekomunikacyjnego nie mają podmioty eksploatujące sieci niepubliczne. Przedsiębiorcami telekomunikacyjnymi są natomiast dostawcy usług działający w sieciach niepublicznych. Plany te powinny być aktualne i uzgodnione z odpowiednimi służbami. Obowiązek ich przygotowania spoczywa na wszystkich przedsiębiorcach telekomunikacyjnych. Przepis art. 39 ust. 1 p.k.e. przewiduje jednak wyjątek w zakresie tego obowiązku, gdyż zgodnie z ust. 9 pkt 7 art. 39 p.k.e. RM może określić w drodze rozporządzenia rodzaje działalności telekomunikacyjnej lub rodzaje przedsiębiorców telekomunikacyjnych niepodlegających obowiązkowi sporządzania planu. Pojęcie zagrożenia nie jest zdefiniowane i dlatego należy przyjąć, że chodzi o jakiekolwiek niebezpieczeństwo, niezależnie od tego, co jest jego źródłem, tj. działanie sił przyrody czy też błędy człowieka.

Plany działań przygotowywane na wypadek wystąpienia sytuacji szczególnego zagrożenia powinny dotyczyć zagadnień wymienionych w przepisie art. 39 ust. 1 p.k.e. Użyte na początku przepisu art. 39 ust. 1 p.k.e. określenie „w szczególności" oznacza, że przedstawiony w tym przepisie zakres tematyczny nie ma charakteru wyczerpującego i plany mogą regulować także inne zagadnienia. W planach mogą być przewidziane zarówno środki osobowe, jak i rzeczowe, które powinny zapewniać ochronę infrastruktury telekomunikacyjnej w sytuacjach szczególnych zagrożeń oraz przed nieuprawnionym dostępem.

Plany powinny w szczególności dotyczyć współpracy z innymi przedsiębiorcami telekomunikacyjnymi, w tym z zagranicznymi przedsiębiorcami telekomunikacyjnymi, w sytuacjach szczególnych zagrożeń (art. 39 ust. 1 pkt 1 p.k.e.). Poza współpracą z przedsiębiorcami telekomunikacyjnymi plany powinny określać

[11] Zob. także ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz.U. z 2002 r. Nr 113, poz. 985 ze zm.).

[12] Zob. także ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. z 2002 r. Nr 62, poz. 558 ze zm.).

także współpracę z podmiotami i służbami wykonującymi zadania w zakresie ratownictwa, niesienia pomocy ludności, zadania na rzecz obronności, cyberbezpieczeństwa, bezpieczeństwa państwa oraz bezpieczeństwa porządku publicznego, a także z podmiotami właściwymi w sprawach zarządzania kryzysowego, wskazanymi przez organy uzgadniające w ramach uzgodnień projektów planów (art. 39 ust. 1 pkt 2 p.k.e.). Podmioty, służby i zadania we wskazanym zakresie określają w szczególności: ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym[13]; ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej[14]; ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej[15]; ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[16].

Plan powinien przewidywać środki techniczne i organizacyjne zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych danych, a także poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka, minimalizujące w szczególności wpływ, jaki na sieci telekomunikacyjne, usługi komunikacji elektronicznej lub podmioty korzystające z tych sieci lub usług może mieć wystąpienie sytuacji szczególnego zagrożenia przy uwzględnieniu aktualnego stanu wiedzy technicznej oraz kosztów wprowadzenia tych środków (art. 39 ust. 1 pkt 3 p.k.e.).

Plan powinien przewidywać utrzymanie ciągłości dostarczania publicznych sieci telekomunikacyjnych lub świadczenia publicznie dostępnych usług telekomunikacyjnych (art. 39 ust. 1 pkt 4 p.k.e.). Utrzymanie ciągłości dostarczania publicznych sieci telekomunikacyjnych lub świadczenia publicznie dostępnych usług telekomunikacyjnych oznacza zapewnienie nieprzerwanego dostarczania sieci lub świadczenia usług. Zgodnie z art. 2 pkt 5 p.k.e. dostarczanie sieci telekomunikacyjnej oznacza przygotowanie sieci telekomunikacyjnej w sposób umożliwiający świadczenie w niej usług, jej eksploatację, nadzór nad nią lub zapewnianie dostępu telekomunikacyjnego. Z kolei świadczenie usług telekomunikacyjnych oznacza wykonywanie usług za pomocą własnej sieci, z wykorzystaniem sieci innego operatora lub sprzedaż we własnym imieniu i na własny rachunek usługi telekomunikacyjnej wykonywanej przez innego dostawcę usług telekomunikacyjnych (art. 2 pkt 69 p.k.e.). Natomiast publicznie dostępna usługa telekomunikacyjna oznacza usługę telekomunikacyjną dostępną dla ogółu użytkowników (art. 2 pkt 46 p.k.e.).

Plany powinny regulować kwestie związane z utrzymaniem ciągłości, a w przypadku jej utraty odtwarzanie dostarczania publicznych sieci telekomunikacyjnych

[13] Dz.U. z 2006 r. Nr 191, poz. 1410 ze zm.
[14] Dz.U. z 2002 r. Nr 62, poz. 558 ze zm.
[15] Dz.U. z 1991 r. Nr 81, poz. 351 ze zm.
[16] Dz.U. z 2007 r. Nr 89, poz. 590 ze zm.

lub przywrócenie świadczenia publicznie dostępnych usług telekomunikacyjnych, z uwzględnieniem pierwszeństwa dla podmiotów i służb, wykonujących zadania w zakresie ratownictwa, niesienia pomocy ludności, zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, a także dla podmiotów właściwych w sprawach zarządzania kryzysowego, wskazanych w ramach uzgodnień planów przez organy uzgadniające plany, w przypadku utraty ciągłości dostarczania tych sieci lub usług (art. 39 ust. 1 pkt 5 p.k.e.).

Plan powinien określać techniczne i organizacyjne przygotowanie do realizacji obowiązków, o których mowa w art. 40 ust. 1 pkt 3 p.k.e. (art. 39 ust. 1 pkt 6 p.k.e.). Przepis art. 40 ust. 1 pkt 3 p.k.e. dotyczy sytuacji, gdy Prezes UKE w drodze decyzji zobowiąże przedsiębiorcę telekomunikacyjnego do ograniczenia zakresu lub obszaru:

a) eksploatacji publicznych sieci telekomunikacyjnych i urządzeń telekomunikacyjnych;
b) świadczenia niektórych publicznie dostępnych usług telekomunikacyjnych;
c) używania urządzeń radiowych.

W planie powinien być określony sposób udostępniania urządzeń telekomunikacyjnych, o którym mowa w art. 41 ust. 1 p.k.e., przez przedsiębiorców telekomunikacyjnych (art. 39 ust. 1 pkt 7 p.k.e.). Zgodnie z art. 41 ust. 1 p.k.e. w planie powinien być określony sposób nieodpłatnego udostępniania urządzeń telekomunikacyjnych niezbędnych do przeprowadzenia akcji ratowniczej innemu przedsiębiorcy telekomunikacyjnemu lub podmiotowi, o którym mowa w art. 39 ust. 1 pkt 2 p.k.e.

Zgodnie z art. 39 ust. 1 pkt 8 p.k.e. plan powinien zawierać ewidencję i gromadzenie rezerw przeznaczonych na utrzymanie ciągłości świadczenia publicznie dostępnych usług telekomunikacyjnych i ich odtworzenia w sytuacji szczególnego zagrożenia oraz współpracę z dostawcami sprzętu i usług serwisowych i naprawczych.

Przedsiębiorca telekomunikacyjny sporządza plan w terminie 12 miesięcy od dnia powstania obowiązku jego sporządzenia (art. 39 ust. 2 p.k.e.). Przedsiębiorca telekomunikacyjny sporządza projekt planu na podstawie danych, określonych w przepisach wydanych na podstawie art. 39 ust. 9 p.k.e., udostępnionych przez organy uzgadniające plan, obejmujących w szczególności kwestie bezpieczeństwa środowiskowego, a także potrzeby w zakresie świadczenia, utrzymania i odtwarzania usług telekomunikacyjnych oraz dostępu telekomunikacyjnego. Organy uzgadniające plan mogą wskazać inne organy administracji rządowej właściwe do udostępnienia tych danych w terminie 7 dni od otrzymania wystąpienia. Dane są udostępniane w terminie 14 dni od dnia otrzymania wystąpienia przedsiębiorcy o udostępnienie danych (art. 39 ust. 3 p.k.e.).

Przedsiębiorca telekomunikacyjny sporządzający plan dokonuje uzgodnienia projektu planu z organami uzgadniającymi plan. Organy te uzgadniają projekt planu i przesyłają potwierdzenie jego uzgodnienia w terminie 30 dni od dnia otrzymania projektu planu albo odmawiają uzgodnienia projektu planu, określając przyczynę braku uzgodnienia, oraz wyznaczają termin jego uzupełnienia i ponownego przesłania do uzgodnienia nie krótszy niż 14 dni. Niezajęcie stanowiska przez organ uzgadniający plan w terminie 30 dni od dnia otrzymania projektu planu jest równoznaczne z uzgodnieniem projektu planu (art. 39 ust. 4 p.k.e.). Przedsiębiorca telekomunikacyjny przekazuje Prezesowi UKE projekt planu uzgodniony z organami uzgadniającymi plan. Prezes UKE dokonuje sprawdzenia kompletności planu, a w przypadku stwierdzenia braku kompletności określa zakres i termin uzupełnienia nie krótszy niż 14 dni (art. 39 ust. 5 p.k.e.).

Plan zachowuje ważność przez 3 lata od daty jego wprowadzenia do stosowania przez przedsiębiorcę (art. 39 ust. 6 p.k.e.). Podlega aktualizacji przed upływem wskazanego wcześniej terminu, w przypadku wystąpienia okoliczności wpływających na jego zawartość, określonych w przepisach wydanych na podstawie art. 39 ust. 9 p.k.e., albo na wniosek organu uzgadniającego plan lub wskazanego przez ten organ innego organu administracji rządowej, w przypadku zmiany danych (art. 39 ust. 7 p.k.e.).

Zgodnie z art. 39 ust. 8 p.k.e. w przypadku wystąpienia sytuacji szczególnego zagrożenia lub po uzyskaniu informacji o jej wystąpieniu od podmiotów, o których mowa w art. 39 ust. 1 pkt 2 p.k.e., przedsiębiorca telekomunikacyjny jest zobowiązany do niezwłocznego przystąpienia do realizacji działań określonych w przygotowanych przez siebie planach. Decyzję co do tego, czy przystąpić do realizacji działań określonych planem, podejmuje zatem przedsiębiorca telekomunikacyjny. „Niezwłoczna" realizacja oznacza podjęcie działań w możliwie najszybszym czasie. „Możliwie najszybszym", tj. takim, na jaki pozwalają okoliczności konkretnie zaistniałego zdarzenia.

Przepis art. 39 ust. 9 p.k.e. stanowi podstawę do wydania rozporządzenia Rady Ministrów z w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń[17]. Przygotowany został projekt rozporządzenia Rady Ministrów w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacji szczególnego zagrożenia. Zgodnie z § 1 tego rozporządzenia określa ono:

1) szczegółową zawartość planu działań w sytuacji szczególnego zagrożenia, zwanego dalej „planem", oraz tryb jego sporządzania;

[17] Zob. także M. Koselski, *Sporządzenie planów działań operatorów publicznych w sytuacjach szczególnych zagrożeń*, „Biuletyn Urzędu Regulacji Telekomunikacji i Poczty" 2003, nr 2, s. 15 i n.

2) zakres danych udostępnianych przedsiębiorcy telekomunikacyjnemu, zwanemu dalej „przedsiębiorcą", przez organy uzgadniające plan lub przez organy administracji rządowej właściwe do ich udostępnienia;
3) tryb uzgadniania planu, jego uzupełnienia w przypadku braku kompletności oraz wprowadzenia do stosowania przez przedsiębiorcę;
4) szczegółowe okoliczności aktualizacji planu oraz jej tryb;
5) organy uzgadniające plan oraz zakres tych uzgodnień;
6) sposób i zakres przekazywania planu organom uzgadniającym plan;
7) rodzaje działalności telekomunikacyjnej lub rodzaje przedsiębiorców niepodlegających obowiązkowi sporządzania planu. Według § 2 ust. 1 tego projektu rozporządzenia obowiązkowi sporządzenia planu nie podlega przedsiębiorca:
   a) którego roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były równe kwocie 10 mln zł lub mniejsze od tej kwoty lub
   b) który wykonuje działalność telekomunikacyjną:
      – polegającą wyłącznie na dostarczaniu powiązanych usług,
      – wyłącznie na obszarze mniejszym od granic administracyjnych jednego powiatu, z wyłączeniem miasta na prawach powiatu w rozumieniu ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym[18],
      – polegającą wyłącznie na dostarczaniu sieci lub łączy telekomunikacyjnych dzierżawionych od innego przedsiębiorcy,
      – polegającą wyłącznie na sprzedaży we własnym imieniu i na własny rachunek usługi telekomunikacyjnej świadczonej przez innego dostawcę usług,
      – polegającą wyłącznie na rozprowadzaniu lub rozpowszechnianiu programów radiofonicznych lub telewizyjnych,
      – polegającą wyłącznie na świadczeniu usług dostępu do sieci Internet za pośrednictwem sieci telekomunikacyjnej obsługującej do 1000 zakończeń sieci posiadających własny adres IP,
      – wyłącznie za pośrednictwem sieci telekomunikacyjnej innego przedsiębiorcy telekomunikacyjnego.

Wymienione wcześniej kryteria wyłączające obowiązek sporządzenia planu nie mają zastosowania do przedsiębiorców:

1) realizujących zadania na rzecz Sił Zbrojnych, o których mowa w art. 648 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny[19];

[18] Dz.U. z 2022 r. poz. 1526.
[19] Dz.U. z 2002 r. poz. 655 i 974.

2) posiadających decyzje i będących stronami umów, o których mowa w art. 807 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny.

Zgodnie z art. 439 ust. 1 pkt 4 p.k.e. kto nie wypełnia lub nienależycie wypełnia obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, o których mowa w art. 39 ust. 1, 2, 7 i 8 p.k.e., podlega karze pieniężnej. Niezależnie od kar pieniężnych Prezes UKE może nałożyć na kierującego przedsiębiorstwem telekomunikacyjnym, w szczególności osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego przedsiębiorcy telekomunikacyjnego lub związku takich przedsiębiorców, karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy (art. 439 ust. 4 p.k.e.).

Zgodnie z art. 40 ust. 1 p.k.e. Prezes UKE w sytuacji szczególnego zagrożenia może, w drodze decyzji, nałożyć na przedsiębiorcę telekomunikacyjnego obowiązki dotyczące:

1) utrzymania ciągłości dostarczania publicznych sieci telekomunikacyjnych lub świadczenia publicznie dostępnych usług telekomunikacyjnych,
2) odtwarzania dostarczania publicznych sieci telekomunikacyjnych lub przywrócenia świadczenia publicznie dostępnych usług telekomunikacyjnych, z uwzględnieniem pierwszeństwa dla:
   a) podmiotów wykonujących zadania w zakresie ratownictwa, niesienia pomocy ludności, a także zadania na rzecz obronności, cyberbezpieczeństwa, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego oraz podmiotów właściwych w sprawach zarządzania kryzysowego,
   b) operatorów usług kluczowych, o których mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,
   c) operatorów infrastruktury krytycznej, o których mowa w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym

   – w przypadku utraty ciągłości dostarczania tych sieci lub usług;
3) ograniczenia zakresu lub obszaru:
   a) eksploatacji publicznych sieci telekomunikacyjnych i urządzeń telekomunikacyjnych,
   b) świadczenia niektórych publicznie dostępnych usług telekomunikacyjnych,
   c) używania urządzeń radiowych

   – kierując się rozmiarem zagrożenia i potrzebą ograniczenia jego skutków, uwzględniając zasady minimalizowania negatywnych skutków nałożonych obowiązków dla ciągłości lub ograniczenia świadczenia publicznie dostępnych usług telekomunikacyjnych i dla działalności gospodarczej przedsiębiorcy telekomunikacyjnego.

Przepis art. 40 p.k.e. dotyczy decyzji podejmowanych w sytuacjach szczególnych zagrożeń. W art. 40 ust. 1 p.k.e. utrzymane zostały przepisy art. 178 p.t., dotyczące uprawnienia Prezesa UKE do utrzymania, w drodze decyzji, ciągłości świadczenia usług telekomunikacyjnych lub dostarczania sieci albo wprowadzania ograniczeń w tym zakresie. Decyzje takie są wydawane przez Prezesa UKE. Powinno je poprzedzać postępowanie zmierzające do ustalenia sytuacji szczególnego zagrożenia oraz stwierdzenia, jaka decyzja, spośród decyzji wymienionych w art. 40 ust. 1 p.k.e., powinna być wydana. Decyzje Prezesa UKE są decyzjami administracyjnymi skierowanymi do konkretnych podmiotów, a nie decyzjami obowiązującymi wszystkich przedsiębiorców telekomunikacyjnych lub podmioty niebędące przedsiębiorcami telekomunikacyjnymi.

Przepis art. 40 ust. 1 p.k.e. wymienia trzy rodzaje obowiązków, które mogą być nałożone w drodze decyzji Prezesa UKE. Prezes UKE może wydać decyzję nakładającą obowiązek utrzymania ciągłości dostarczania publicznych sieci telekomunikacyjnych lub świadczenia publicznie dostępnych usług telekomunikacyjnych (art. 40 ust. 1 pkt 1 p.k.e.). Ustawa nie precyzuje dokładnie, jakich elementów sieci telekomunikacyjnej, usług czy grup użytkowników dotyczą te obowiązki, z czego należy wnioskować, że dotyczą one całej sieci i wszystkich świadczonych usług, ale o charakterze publicznym. Podmiotami, do których są adresowane wskazane obowiązki, są zarówno operatorzy („dostarczania sieci telekomunikacyjnej"), jak i dostawcy usług („świadczenie usług telekomunikacyjnych"). Nakładając te obowiązki, Prezes UKE jest obowiązany uwzględniać pierwszeństwo dla podmiotów koordynujących działania ratownicze, podmiotów właściwych w sprawach zarządzania kryzysowego, służb ustawowo powołanych do niesienia pomocy, a także innych podmiotów realizujących zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Operatorzy i dostawcy usług są więc zobowiązani w pierwszym rzędzie realizować wskazane obowiązki na rzecz wymienionych wcześniej podmiotów i służb.

Na przedsiębiorcę telekomunikacyjnego może być nałożony przez Prezesa UKE w drodze decyzji, w przypadku wystąpienia szczególnego zagrożenia, obowiązek odtwarzania dostarczania publicznych sieci telekomunikacyjnych lub przywrócenia świadczenia publicznie dostępnych usług telekomunikacyjnych, z uwzględnieniem pierwszeństwa dla podmiotów wskazanych w tym przepisie, w przypadku utraty ciągłości dostarczania tych sieci lub usług (art. 40 ust. 1 pkt 2 p.k.e.). Zgodnie z art. 5 ust. 1 u.k.s.c. operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do tej ustawy, mający jednostkę organizacyjną na terytorium Polski, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. Załącznik nr 1 do tej ustawy określa rodzaje podmiotów uznanych za operatorów usług

kluczowych. Zgodnie z art. 2 pkt 16 wymienionej ustawy usługa kluczowa oznacza usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych.

Zgodnie z art. 3 pkt 2 u.z.k. przez pojęcie infrastruktury krytycznej należy rozumieć systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje systemy:

a) zaopatrzenia w energię, surowce energetyczne i paliwa,
b) łączności,
c) sieci teleinformatycznych,
d) finansowe,
e) zaopatrzenia w żywność,
f) zaopatrzenia w wodę,
g) ochrony zdrowia,
h) transportowe,
i) ratownicze,
j) zapewniające ciągłość działania administracji publicznej,
k) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Na przedsiębiorcę telekomunikacyjnego może być nałożony przez Prezesa UKE w drodze decyzji, w przypadku wystąpienia szczególnego zagrożenia, obowiązek ograniczenia zakresu lub obszaru eksploatacji publicznych sieci telekomunikacyjnych i urządzeń telekomunikacyjnych (art. 40 ust. 1 pkt 3 lit. a p.k.e.). Prezes UKE może także w drodze decyzji nałożyć na przedsiębiorcę telekomunikacyjnego, w przypadku wystąpienia szczególnego zagrożenia, obowiązek ograniczenia zakresu lub obszaru świadczenia niektórych publicznie dostępnych usług telekomunikacyjnych (art. 40 ust. 1 pkt 3 lit. b p.k.e.). Decyzja powinna wskazywać, jakie publicznie dostępne usługi telekomunikacyjne powinny być niedostępne. Z uwagi na wskazanie w przepisie, że obowiązek ten dotyczy ograniczenia „niektórych" usług, nie można na podstawie tego przepisu ograniczyć dostępu do wszystkich publicznie dostępnych usług telekomunikacyjnych. Przepis ten mówi także o „ograniczeniu" dostępu do publicznie dostępnych usług telekomunikacyjnych, co oznacza, że nie jest możliwe „wyłączenie" tych usług, ale tylko ograniczenie dostępu do nich. Podmiotami, na które jest nakładany ten obowiązek, są przedsiębiorcy telekomunikacyjni.

Pośrednie skutki decyzji wydanej na podstawie art. 40 ust. 1 pkt 3 p.k.e. dotyczą także stosunków umownych z użytkownikami sieci danego operatora.

W przypadku bowiem realizowania przez operatora telekomunikacyjnego decyzji Prezesa UKE wydanej na podstawie art. 40 ust. 1 pkt 3 lit. b p.k.e. abonenci oraz użytkownicy usług telekomunikacyjnych tego operatora nie będą mogli korzystać z jego usług. Zgodnie z art. 371 ust. 1 p.k.e. do odpowiedzialności przedsiębiorców komunikacji elektronicznej za niewykonanie lub nienależyte wykonanie usługi komunikacji elektronicznej mają zastosowanie przepisy Kodeksu cywilnego. Powstaje pytanie o wzajemne relacje pomiędzy postanowieniami Rozdziału 4 w Dziale VII, określającymi odpowiedzialność za niewykonanie lub nienależyte wykonanie usług telekomunikacyjnych (art. 371 i n. p.k.e.), a postanowieniami rozdziału 5 działu I dotyczącymi obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego (art. 39 i n. p.k.e.). Z jednej bowiem strony podmiot świadczący usługi telekomunikacyjne jest odpowiedzialny wobec klienta z tytułu niewykonania lub nienależytego wykonania usług telekomunikacyjnych, a z drugiej strony ustawodawca zobowiązuje go do zaprzestania świadczenia tych usług w sytuacjach określonych w p.k.e. na żądanie uprawnionych podmiotów. Zasadą jest obowiązek świadczenia przez przedsiębiorcę telekomunikacyjnego usług telekomunikacyjnych, wyjątkiem natomiast sytuacja, gdy jest zobowiązany do zaprzestania świadczenia tych usług. Postanowienia rozdziału 5 działu I zawierają regulacje odnoszące się do sytuacji wyjątkowych lub nadzwyczajnych. Przewidują one szczególne obowiązki, które dotyczą zastosowania środków będących odstępstwem od zasady swobodnego i nieskrępowanego przez państwo prowadzenia działalności gospodarczej. Ustawa upoważnia uprawniony organ do skorzystania z tych nadzwyczajnych środków tylko wówczas, gdy w wyniku oceny określonego zagrożenia podjętej przez organ działający w imieniu państwa, uzna je za właściwe i niezbędne. Należy więc przyjąć, że Prezes UKE, nakładając na danego przedsiębiorcę telekomunikacyjnego obowiązek przewidziany w art. 40 ust. 1 pkt 3 lit. b p.k.e., niejako automatycznie zwalnia go z obowiązku zapewnienia ciągłości świadczenia usług telekomunikacyjnych na obszarze, którego decyzja dotyczy. Skutki takiego zwolnienia będą obejmować niemożność korzystania z połączeń w sieci telekomunikacyjnej także w celach np. ratowniczych. W chwili wydania przedmiotowej decyzji Prezes UKE zawsze dokonuje wszechstronnej oceny jej skutków i ma świadomość ich wystąpienia[20].

Do oceny skutków niewykonania lub nienależytego wykonania zobowiązań przedsiębiorcy telekomunikacyjnego w stosunku do klientów w związku z realizacją decyzji Prezesa UKE wydanej w trybie art. 40 ust. 1 pkt 3 lit. b p.k.e. będą

[20] M. Rogalski, *Specobowiązki przedsiębiorców telekomunikacyjnych*, „Prawo Teleinformatyczne" 2007, nr 1, s. 41–42.

miały zastosowanie przepisy kodeksu cywilnego. Przy założeniu, że po stronie przedsiębiorcy telekomunikacyjnego nie będzie można znaleźć zawinienia, będzie można przyjąć brak podstaw odpowiedzialności deliktowej na podstawie art. 415 k.c. Odmiennie będzie się przedstawiać odpowiedzialność kontraktowa przedsiębiorcy telekomunikacyjnego związana z niewykonaniem lub nienależytym wykonaniem zobowiązań polegających na zapewnieniu świadczenia usług telekomunikacyjnych dla klienta. W takich sytuacjach przedsiębiorca telekomunikacyjny będzie mógł zwolnić się od odpowiedzialności wobec klientów poprzez wykazanie, że niewykonanie lub nienależyte wykonanie zobowiązań, polegające na ograniczeniu obszaru, na którym były świadczone usługi, było następstwem okoliczności, za które nie ponosi odpowiedzialności. Okolicznością tą będzie wykonanie przez przedsiębiorcę telekomunikacyjnego obowiązku przewidzianego w art. 40 ust. 1 pkt 3 lit. b p.k.e. Do sporów dotyczących ewentualnych roszczeń klientów przeciwko przedsiębiorcom telekomunikacyjnym może być wówczas dopozwany Skarb Państwa.

Na przedsiębiorcę telekomunikacyjnego może być nałożony przez Prezesa UKE w drodze decyzji, w przypadku wystąpienia szczególnego zagrożenia, obowiązek ograniczenia zakresu lub obszaru używania urządzeń radiowych (art. 41 ust. 1 pkt 3 lit. c p.k.e.). Definicję urządzenia radiowego zawiera art. 2 pkt 73 p.k.e. Przyjąć należy, że w przypadku wydania decyzji na podstawie art. 40 ust. 1 pkt 3 p.k.e. przedsiębiorca telekomunikacyjny powinien poinformować klientów o utrudnieniach w korzystaniu z usług telekomunikacyjnych będących następstwem wydania tej decyzji. Przepisy p.k.e. nie zabraniają poinformowania klientów o takich utrudnieniach, a ponadto należy zwrócić uwagę na kwestię cywilnoprawnej oceny ewentualnych skutków takich utrudnień. Pomijając stronę techniczną sposobu przekazania informacji, treść nie powinna być zbyt szczegółowa, aby nie zniweczyć celu, dla którego decyzja zostanie wydana. Treść komunikatów powinna być oczywiście uzgodniona ze specjalistami z zakresu problematyki bezpieczeństwa.

W praktyce może powstać problem wyboru określonego rozwiązania technologicznego dla zrealizowania celu wskazanego w decyzji Prezesa UKE. Przykładowo może się okazać, że jest możliwe zastosowanie rozwiązania, które pozwala ograniczyć zakres świadczonych usług telekomunikacyjnych na ściśle określonym obszarze, ale z drugiej strony, z uwagi na propagacyjne właściwości fal radiowych, nie zapewnia pełnej pewności, że nastąpi całkowity brak możliwości wykonywania połączeń na tym obszarze. Rozwiązanie to jest korzystne dla przedsiębiorcy telekomunikacyjnego i klientów, gdyż możliwość realizacji połączeń jest wyłączona tylko na ściśle określonym obszarze. Nie jest natomiast korzystne dla służb odpowiedzialnych za bezpieczeństwo, gdyż nie daje im

całkowitej gwarancji, że nie zostanie zrealizowane żadne połączenie na wybranym obszarze. Inne z kolei rozwiązanie zapewnia stuprocentową gwarancję całkowitego ograniczenia eksploatacji sieci w którymkolwiek z miejsc danego obszaru, ale realizacja tego rozwiązania oznacza brak możliwości wykonywania połączeń w promieniu kilkudziesięciu kilometrów. W takich sytuacjach należy rozważyć skorzystanie z rozwiązań przewidzianych w art. 42 p.k.e., czyli nie wyłączenia całej sieci telekomunikacyjnej na danym obszarze, ale zastosowania odpowiednich urządzeń, które uniemożliwiają wykonywanie połączeń telefonicznych na określonym obszarze. Z pewnością jest to rozwiązanie mniej uciążliwe dla użytkowników sieci telekomunikacyjnych i pozwala na osiągnięcie zamierzonych celów przez służby odpowiedzialne za bezpieczeństwo[21].

Prezes UKE, nakładając na przedsiębiorców telekomunikacyjnych obowiązki w sytuacji wystąpienia szczególnego zagrożenia, powinien kierować się rozmiarem zagrożenia i potrzebą ograniczenia jego skutków. Powinien także przestrzegać zasady minimalizowania negatywnych skutków nałożonych obowiązków dla ciągłości lub ograniczenia świadczenia publicznie dostępnych usług telekomunikacyjnych i dla działalności gospodarczej przedsiębiorcy telekomunikacyjnego. Środki zastosowane w sytuacji szczególnego zagrożenia powinny być proporcjonalne do stopnia zagrożenia. Sytuacja musi stanowić realne zagrożenie[22].

Prezes UKE, wydając decyzję, musi z jednej strony dokonać oceny rozmiaru zagrożenia, uwzględniając potrzebę ograniczenia jego skutków, z drugiej jednak strony musi uwzględniać interes konsumentów oraz przedsiębiorcy telekomunikacyjnego. Wyrażają się one w potrzebie przestrzegania zasady minimalizowania negatywnych skutków nałożonych obowiązków dla ciągłości świadczenia usług i dla działalności gospodarczej przedsiębiorcy telekomunikacyjnego. Ustawa nie wskazuje, która z tych dyrektyw ma pierwszeństwo. Należy więc uznać, że konieczność ograniczenia skutków zagrożenia oraz interes konsumentów i przedsiębiorców telekomunikacyjnych mają takie samo znaczenie. Prezes UKE, wydając decyzję, powinien więc w takim samym stopniu uwzględniać obie te dyrektywy.

Zgodnie z art. 40 ust. 2 p.k.e. Prezes UKE w przypadku ogłoszenia jednego ze stopni alarmowych CRP, o których mowa w art. 15 ust. 2 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych[23], może, w drodze decyzji, nałożyć na przedsiębiorcę telekomunikacyjnego obowiązki, o których mowa w art. 40 ust. 1 pkt 3 p.k.e., kierując się wytyczną wskazaną w art. 40 ust. 1 p.k.e. Według

[21] *Ibidem*, s. 42–43.

[22] L. Wiśniewski, *Stany nadzwyczajne w projekcie nowej Konstytucji RP*, w: T. Jasudowicz (red.), *Prawa człowieka w sytuacjach nadzwyczajnych ze szczególnym uwzględnieniem prawa i praktyki polskiej*, Toruń 1997, s. 152.

[23] Dz.U. z 2021 r. poz. 2234 oraz z 2022 r. poz. 583 i 655.

natomiast art. 40 ust. 3 p.k.e. Prezes UKE w przypadku wystąpienia trwałych lub cyklicznych zakłóceń urządzenia radiowego wykorzystywanego bezpośrednio na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego może, w drodze decyzji, nałożyć na przedsiębiorcę telekomunikacyjnego obowiązek, o którym mowa w art. 40 ust. 1 pkt 3 lit. c p.k.e., kierując się wytyczną wymienioną w art. 40 ust. 1 p.k.e. Prezes UKE wydaje decyzje, o których mowa w art. 40 ust. 1–3 p.k.e., z urzędu lub na uzasadniony wniosek ministra obrony narodowej, komendanta głównego Policji, komendanta Centralnego Biura Śledczego Policji, komendanta Centralnego Biura Zwalczania Cyberprzestępczości, komendanta wojewódzkiego Policji, komendanta głównego Straży Granicznej, komendanta Oddziału Straży Granicznej, komendanta głównego Żandarmerii Wojskowej, szefa Agencji Bezpieczeństwa Wewnętrznego, szefa Służby Kontrwywiadu Wojskowego lub komendanta Służby Ochrony Państwa. Prezes UKE może więc wydać decyzje z urzędu lub na wniosek. Wydając decyzje z urzędu, powinien ocenić, czy wystąpiła sytuacja szczególnego zagrożenia. W przypadku złożenia wniosku o wydanie decyzji Prezes UKE także ocenia, czy zachodzą podstawy do jej wydania, i może odmówić jej wydania.

Przepis art. 40 ust. 4 p.k.e. zezwala Prezesowi UKE na wydanie decyzji w formie ustnej oraz odstąpienie od jej uzasadnienia w całości lub części. Przesłanką do wydania decyzji w takiej formie są względy bezpieczeństwa państwa. Zgodnie bowiem z art. 14 § 2 k.p.a. sprawy mogą być załatwiane ustnie, gdy przemawia za tym interes strony, a przepis prawa nie stoi temu na przeszkodzie. Przyjmuje się, że wyrażenie „gdy przemawia za tym interes strony" należy uważać za równoznaczne pod względem znaczenia z określeniem „gdy strona się zgadza". Treść „oświadczenia" strony co do zgody musi mieć wyraźny charakter. Wyrażenia zgody nie można domniemywać. W sytuacji istnienia jakichkolwiek wątpliwości, a zwłaszcza gdy w ocenie organu za ustnym załatwieniem sprawy przemawia interes strony, organ obowiązany jest zwrócić się do strony o jej stanowisko. Brak zgody nakłada na organ administracji publicznej obowiązek zastosowania formy pisemnej. W przypadku ustnego załatwienia sprawy treść oraz istotne motywy takiego załatwienia powinny być utrwalone w aktach w formie protokołu lub podpisanej przez stronę adnotacji. W uchwale z dnia 13 października 1997 r. NSA w składzie pięciu sędziów stwierdził, że „ogłoszenie ustne decyzji administracyjnej, jako wyjątek od zasady pisemności, wymaga utrwalenia tej czynności na piśmie w drodze sporządzenia protokołu (art. 67 § 2 pkt 5 k.p.a.), który powinien odpowiadać wymaganiom art. 68 i 107 k.p.a. w zakresie koniecznych elementów decyzji"[24]. Składniki decyzji administracyjnej formu-

[24] FPK 13/97, ONSA 1998, nr 1, poz. 17, LEX nr 31616.

łuje art. 107 § 1 k.p.a. Wobec braku wyraźnego określenia tej kwestii należy przyjąć, że powyższy przepis ma zastosowanie do decyzji pisemnych i decyzji ogłoszonych ustnie, z tym że w odniesieniu do decyzji ustnych niektóre wymagania określone w art. 107 § 1 k.p.a. z natury rzeczy nie będą mogły być spełnione, np. podpis osoby upoważnionej do wydania decyzji. Przepis art. 107 § 1 k.p.a. do niezbędnych elementów decyzji zalicza uzasadnienie faktyczne i prawne. Od uzasadnienia decyzji można odstąpić w dwóch przypadkach – gdy decyzja uwzględnia w całości żądanie strony (nie dotyczy to jednak decyzji rozstrzygających sporne interesy stron oraz decyzji wydanych na skutek odwołania) oraz gdy z dotychczasowych przepisów ustawowych wynikała możliwość zaniechania lub ograniczenia uzasadnienia ze względu na interes bezpieczeństwa państwa. Przepis art. 40 ust. 4 p.k.e. stanowi więc przepis szczególny pozwalający na odstąpienie od uzasadnienia decyzji w całości lub w części, jeżeli wymagają tego względy bezpieczeństwa państwa. Decyzja ogłoszona ustnie doręczana jest temu przedsiębiorcy telekomunikacyjnemu na piśmie w terminie 14 dni od dnia jej ogłoszenia (art. 40 ust. 4 p.k.e.).

Zgodnie z art. 40 ust. 5 p.k.e. Prezes UKE może, w przypadku wprowadzenia stanu nadzwyczajnego, podwyższenia stanu gotowości obronnej państwa w razie zewnętrznego zagrożenia bezpieczeństwa państwa albo wydania postanowienia o dniu, w którym rozpoczyna się czas wojny, albo wystąpienia przez właściwy organ z wnioskiem o wprowadzenie stanu nadzwyczajnego, podwyższenia stanu gotowości obronnej państwa w razie zewnętrznego zagrożenia bezpieczeństwa państwa albo wydania tego postanowienia, w drodze decyzji, na uzasadniony wniosek podmiotu, o którym mowa w art. 40 ust. 4 p.k.e., na czas określony nałożyć na przedsiębiorcę telekomunikacyjnego obowiązek ograniczenia zakresu lub obszaru wykorzystania zasobów częstotliwości radiowych, kierując się wytyczną, o której mowa w art. 40 ust. 1 p.k.e., oraz minimalizacją skutków związanych z roszczeniem odszkodowawczym, o którym mowa w art. 40 ust. 9 p.k.e. Przepis art. 40 ust. 5 p.k.e. jest nową regulacją w stosunku do ustawy – Prawo telekomunikacyjne. Wprowadzenie powyższego ograniczenia, w okresie zewnętrznego zagrożenia bezpieczeństwa państwa, w sytuacji, gdy ogłoszony zostanie np. stan wojenny albo wyjątkowy, ma kluczowe znaczenie dla tworzenia warunków funkcjonowania i działań Sił Zbrojnych RP w określonych sytuacjach operacyjnych w zakresie czasowego dostępu do dodatkowych zasobów widma częstotliwości radiowych będących w dyspozycji przedsiębiorców telekomunikacyjnych (zob. uzasadnienie do art. 40 p.k.e.).

Prezes UKE, wydając decyzję, o której mowa w art. 40 ust. 5 p.k.e., musi kierować się zasadą minimalizowania skutków wydania decyzji dla prowadzonej działalności telekomunikacyjnej oraz skutków związanych z roszczeniem

odszkodowawczym. Decyzję Prezes UKE wydaje na czas określony, nie dłuższy niż czas trwania opisanej sytuacji (ust. 6). W przypadku wprowadzenia takiego ograniczenia przedsiębiorca telekomunikacyjny nie uiszcza opłaty za prawo dysponowania częstotliwością, o której mowa w art. 24 ust. 1 p.k.e., za okres wprowadzenia ograniczenia (art. 40 ust. 7 p.k.e.). Zgodnie z art. 40 ust. 8 p.k.e. Prezes UKE może, na uzasadniony wniosek podmiotu, o którym mowa w art. 40 ust. 4 p.k.e., zezwolić na wykorzystywanie na czas określony, nie dłuższy niż czas, na który wydana została decyzja, o której mowa w art. 40 ust. 5 p.k.e., zasobów częstotliwości radiowych, o których mowa w art. 40 ust. 5 p.k.e. Zgodnie z art. 40 ust. 9 p.k.e. przedsiębiorcy przysługuje również prawo do wystąpienia z roszczeniem odszkodowawczym z tytułu poniesionych strat. Do roszczeń o odszkodowanie z tytułu strat poniesionych przez przedsiębiorcę telekomunikacyjnego wskutek wydania decyzji, o której mowa w art. 40 ust 5 p.k.e., stosuje się odpowiednio przepisy ustawy z dnia 22 listopada 2002 r. o wyrównywaniu strat majątkowych wynikających z ograniczenia w czasie stanu nadzwyczajnego wolności i praw człowieka i obywatela[25],

Decyzjom wydanym na podstawie art. 40 ust. 1–3 i 5 p.k.e. nadaje się rygor natychmiastowej wykonalności (art. 40 ust. 10 p.k.e.), co oznacza, że decyzja podlega wykonaniu w trybie natychmiastowym. Podmiot, który otrzymuje decyzję zaopatrzoną w rygor natychmiastowej wykonalności, ma obowiązek wykonania jej zgodnie z treścią. Złożenie do Prezesa UKE wniosku o ponowne rozpoznanie sprawy nie wstrzymuje wykonania decyzji. Decyzja musi być wykonana najszybciej, jak to możliwe, czyli bez zbędnej zwłoki. W przypadku nadania decyzji rygoru natychmiastowej wykonalności bezpośrednie skutki prawne decyzji dla podmiotu, do którego decyzja ta jest skierowana, będą polegały na powstaniu po stronie tego podmiotu obowiązku jej wykonania, zanim decyzja stanie się ostateczna, tj. przed upływem 14-dniowego terminu na wniesienie wniosku o ponowne rozpatrzenie sprawy, a w przypadku złożenia takiego wniosku – przed ponownym wydaniem decyzji przez organ administracji. W związku z tym, że opisany skutek prawny nadania decyzji rygoru natychmiastowej wykonalności ma wyjątkowy charakter, Prezes UKE powinien przed nadaniem decyzji rygoru natychmiastowej wykonalności przeanalizować wnikliwie stan faktyczny oraz przesłanki jej nadania, gdyż rygor natychmiastowej wykonalności powinien być nadawany tylko w sytuacji oczywistej konieczności.

Rygor natychmiastowej wykonalności może być wstrzymany za zasadach ogólnych. Zgodnie z art. 61 § 3 p.p.s.a. po przekazaniu sądowi skargi sąd może na wniosek skarżącego wydać postanowienie o wstrzymaniu wykonania

[25] Dz.U. z 2002 r. poz. 1955.

w całości lub w części aktu lub czynności, „jeżeli zachodzi niebezpieczeństwo wyrządzenia znacznej szkody lub spowodowania trudnych do odwrócenia skutków, z wyjątkiem przepisów prawa miejscowego, które weszły w życie, chyba że ustawa szczególna wyłącza wstrzymanie ich wykonania. Odmowa wstrzymania wykonania aktu lub czynności przez organ nie pozbawia skarżącego złożenia wniosku do sądu. Dotyczy to także aktów wydanych lub podjętych we wszystkich postępowaniach prowadzonych w granicach tej samej sprawy". Przepis art. 61 § 3 p.p.s.a. reguluje instytucję tzw. ochrony tymczasowej w postępowaniu sądowo-administracyjnym[26]. Podstawowym celem ochrony tymczasowej jest ochrona strony skarżącej przed skutkami wykonania zaskarżonej decyzji, które mogą być trudne do odwrócenia po ewentualnym jej uchyleniu przez sąd[27].

Podmiot zobowiązany do wykonania decyzji w trybie art. 40 ust. 1 p.k.e. może złożyć do Prezesa UKE wniosek o ponowne rozpatrzenie sprawy, jeżeli nie zgadza się z treścią jego decyzji. W przypadku podtrzymania decyzji przez Prezesa UKE przysługuje mu skarga do WSA. W przypadku zaskarżenia decyzji wydanej na podstawie art. 40 ust. 1 p.k.e. z pewnością ocenie podlegać będzie „wystąpienie sytuacji szczególnego zagrożenia", której zaistnienie stanowi podstawę wydania decyzji. Przepisy p.k.e. nie zwalniają bowiem Prezesa UKE od uzasadnienia decyzji, także w tym zakresie, tzn. wykazania wystąpienia sytuacji szczególnego zagrożenia, która uzasadniałaby wydanie decyzji.

Zgodnie z art. 15 ust. 2 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych[28] w przypadku zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej albo w przypadku wystąpienia takiego zdarzenia można wprowadzić jeden z czterech stopni alarmowych CRP:

1) pierwszy stopień alarmowy CRP (stopień ALFA-CRP);
2) drugi stopień alarmowy CRP (stopień BRAVO-CRP);
3) trzeci stopień alarmowy CRP (stopień CHARLIE-CRP);
4) czwarty stopień alarmowy CRP (stopień DELTA-CRP).

W przypadku ogłoszenia jednego z tych stopni alarmowych CRP Prezes UKE może w drodze decyzji nałożyć na przedsiębiorcę telekomunikacyjnego obowiązki, o których mowa w art. 40 ust. 1 pkt 3 p.k.e., czyli ograniczyć zakres lub obszar:

---

[26] Zob. szerzej R. Hauser, M. Wierzbowski (red.), *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, Warszawa 2023, uwagi do art. 61.

[27] Zob. postanowienie NSA z 29 maja 2015 r., sygn. II GZ 251/15, CBOSA; postanowienie WSA w Poznaniu z 25 czerwca 2019 r., sygn. IV SA/Po 425/19, CBOSA.

[28] Dz.U. z 2016 r. poz. 904 ze zm.

a) eksploatacji publicznych sieci telekomunikacyjnych i urządzeń telekomunikacyjnych;
b) świadczenia niektórych publicznie dostępnych usług telekomunikacyjnych;
c) używania urządzeń radiowych.

Podejmując taką decyzję, Prezes UKE musi się kierować rozmiarem zagrożenia i potrzebą ograniczenia jego skutków, uwzględniając zasady minimalizowania negatywnych skutków nałożonych obowiązków dla ciągłości lub ograniczenia świadczenia publicznie dostępnych usług telekomunikacyjnych i dla działalności gospodarczej przedsiębiorcy telekomunikacyjnego.

Zgodnie z art. 41 ust. 1 p.k.e. przedsiębiorca telekomunikacyjny w sytuacji szczególnego zagrożenia jest obowiązany do nieodpłatnego udostępniania urządzeń telekomunikacyjnych niezbędnych do przeprowadzenia akcji ratowniczej innemu przedsiębiorcy telekomunikacyjnemu lub podmiotowi, o którym mowa w art. 39 ust. 1 pkt 2 p.k.e., biorąc pod uwagę konieczność utrzymania ciągłości wykonywania działalności telekomunikacyjnej przez tego przedsiębiorcę. Obowiązek ten powstaje w przypadku wystąpienia sytuacji szczególnego zagrożenia. „Sytuacja szczególnego zagrożenia" jest zdefiniowana w art. 2 pkt 65 p.k.e. Natomiast „urządzenie telekomunikacyjne" definiuje art. 2 pkt 74 p.k.e. Urządzenia telekomunikacyjne są udostępniane nieodpłatnie. Przy udostępnianiu tych urządzeń powinna być zachowana zasada minimalizowania negatywnych skutków takiego udostępnienia dla ciągłości wykonywania działalności telekomunikacyjnej przez przedsiębiorcę. Podstawę prawną takiego nieodpłatnego przekazania urządzeń telekomunikacyjnych może stanowić umowa użyczenia (art. 710 i n. k.c.). Obowiązek, o którym mowa w art. 41 ust. 1 p.k.e., nie dotyczy urządzeń telekomunikacyjnych:

1) przewidzianych przez przedsiębiorcę telekomunikacyjnego sporządzającego plan, o którym mowa w art. 39 ust. 1 p.k.e., do realizacji działań, o których mowa w art. 39 ust. 1 pkt 4 i 5 p.k.e.;
2) wykorzystanych dla zapewnienia telekomunikacji na potrzeby obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego (art. 41 ust. 2 p.k.e.).

Analogiczny jak na przedsiębiorców telekomunikacyjnych obowiązek nieodpłatnego udostępniania urządzeń telekomunikacyjnych (art. 41 ust. 1 p.k.e.) został nałożony także na podmioty niebędące przedsiębiorcami telekomunikacyjnymi, używające radiowych urządzeń nadawczych lub nadawczo-odbiorczych (zob. art. 2 pkt 73 p.k.e.) stosowanych w służbach radiokomunikacyjnych (zob. art. 2 pkt 59 p.k.e.). Podmioty te w sytuacjach szczególnych zagrożeń są także obowiązane do nieodpłatnego udostępniania urządzeń telekomunikacyjnych niezbędnych do przeprowadzenia akcji ratowniczej podmiotom koordynującym

działania ratownicze, podmiotom właściwym w sprawach zarządzania kryzysowego, służbom ustawowo powołanym do niesienia pomocy, a także innym podmiotom realizującym zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego (art. 41 ust. 3 p.k.e.). Zarządzanie kryzysowe to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej (art. 2 u.z.k.). Z kolei sytuacja kryzysowa to sytuacja wpływająca negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołująca znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków (art. 3 pkt 1 u.z.k.).

Zgodnie z art. 41 ust. 4 p.k.e. przepisy dotyczące obowiązków przedsiębiorców telekomunikacyjnych oraz podmiotów niebędących przedsiębiorcami telekomunikacyjnymi w zakresie nieodpłatnego udostępniania urządzeń telekomunikacyjnych w sytuacjach szczególnych zagrożeń stosuje się odpowiednio podczas przeprowadzania akcji ratowniczej o zasięgu międzynarodowym, co najmniej w zakresie ustalonym umowami międzynarodowymi, których RP jest stroną. Obowiązki przedsiębiorców telekomunikacyjnych i podmiotów niebędących przedsiębiorcami telekomunikacyjnymi będą musiały być więc odpowiednio realizowane także w przypadku akcji ratowniczych, niebędących sytuacjami szczególnych zagrożeń, gdy mają one zasięg międzynarodowy. Obowiązki te powinny być realizowane co najmniej w zakresie wyznaczonym umowami międzynarodowymi. Dotyczy to zarówno umów wielostronnych (np. Międzynarodowa konwencja o ratownictwie morskim, przyjęta przez Międzynarodową Organizację Morską w Londynie dnia 28 kwietnia 1989 r.[29]), jak i dwustronnych (np. umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Słowackiej o współpracy i wzajemnej pomocy podczas katastrof, klęsk żywiołowych i innych poważnych wypadków, podpisana w Bratysławie dnia 24 stycznia 2000 r.[30]).

Zgodnie z art. 41 ust. 5 p.k.e. urządzenia telekomunikacyjne, o których mowa w art. 41 ust. 1 p.k.e., oraz radiowe urządzenia nadawcze lub nadawczo-odbiorcze (art. 41 ust. 3 p.k.e.) udostępnia się na podstawie pisemnego żądania innego przedsiębiorcy telekomunikacyjnego (zob. art. 41 ust. 1 p.k.e.), podmiotu

[29] Dz.U. z 2006 r. Nr 207, poz. 1523.

[30] Dz.U. z 2004 r. Nr 36, poz. 327.

wskazanego w art. 39 ust. 1 pkt 2 p.k.e. lub w art. 41 ust. 3 p.k.e. W sprawach niecierpiących zwłoki, w przypadku opisanym w art. 41 ust. 3 p.k.e., gdy wydanie żądania na piśmie nie jest możliwe, urządzenie to udostępnia się na podstawie ustnego żądania przedstawiciela tego podmiotu.

Według art. 41 ust. 6 p.k.e. zwrot urządzenia telekomunikacyjnego (zob. art. 41 ust. 1 p.k.e.) oraz radiowego urządzenia nadawczego lub nadawczo-odbiorczego (zob. art. 41 ust. 3 p.k.e.) następuje po ustaniu przyczyny udostępnienia, w terminie i miejscu określonym przez przedsiębiorcę telekomunikacyjnego lub podmiot niebędący przedsiębiorcą telekomunikacyjnym odpowiednio z innym przedsiębiorcą telekomunikacyjnym, o którym mowa w art. 41 ust. 1 p.k.e., art. 39 ust. 1 pkt 2 p.k.e. lub w art. 41 ust. 3 p.k.e. Z czynności zwrotu sporządza się protokół.

Nową regulacją w stosunku do przepisów poprzedniej ustawy – Prawo telekomunikacyjne jest przepis art. 41 ust. 8 p.k.e., który stanowi, że do roszczeń o odszkodowanie z tytułu utraty albo zniszczenia urządzenia telekomunikacyjnego udostępnionego podmiotowi, o którym mowa w art. 41 ust. 1 p.k.e., oraz radiowego urządzenia nadawczego lub nadawczo-odbiorczego udostępnionego podmiotom wskazanym w art. 41 ust. 3 p.k.e., stosuje się odpowiednio przepisy ustawy z dnia 22 listopada 2002 r. o wyrównywaniu strat majątkowych wynikających z ograniczenia w czasie stanu nadzwyczajnego wolności i praw człowieka i obywatela, a do roszczeń o odszkodowanie z tytułu utraty albo zniszczenia urządzenia telekomunikacyjnego udostępnionego innemu przedsiębiorcy telekomunikacyjnemu stosuje się przepisy Kodeksu cywilnego.

Zgodnie z art. 439 ust. 1 pkt 4 p.k.e. kto nie wypełnia lub nienależycie wypełnia obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, o których mowa w art. 41 ust. 1 i 3 p.k.e., podlega karze pieniężnej. Niezależnie od kar pieniężnych Prezes UKE może nałożyć na kierującego przedsiębiorstwem telekomunikacyjnym, w szczególności osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego przedsiębiorcy telekomunikacyjnego lub związku takich przedsiębiorców, karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy (art. 441 ust. 4 p.k.e.).

W ustawie zrezygnowano z przepisu zawartego w poprzednim art. 179 ust. 2 p.t. ze względu na fakt, że nie zawiera żadnej normy prawnej, lecz jedynie informację, że przedsiębiorca wykonuje obowiązki zawarte w planach, decyzjach i umowach, celem przygotowania i utrzymania wskazanych elementów sieci telekomunikacyjnych na potrzeby systemu kierowania bezpieczeństwem narodowym. Takie obowiązki nie dotyczą wszystkich przedsiębiorców telekomunikacyjnych, ale tylko tych, których te decyzje, umowy i plany obowiązują.

Taki przepis może być niezrozumiały dla przedsiębiorcy telekomunikacyjnego (zwłaszcza małego, prowadzącego działalności na niewielkim obszarze kraju), którego nie dotyczą powyższe decyzje, umowy i plany[31].

Przepis art. 41 ust. 9 p.k.e. stanowi podstawę dla RM do określenia, w drodze rozporządzenia, trybu nieodpłatnego udostępniania urządzeń telekomunikacyjnych niezbędnych do przeprowadzenia akcji ratowniczej oraz radiowych urządzeń nadawczych lub nadawczo-odbiorczych stosowanych w służbach radiokomunikacyjnych przez podmioty niebędące przedsiębiorcami telekomunikacyjnymi, odpowiednio przez przedsiębiorców telekomunikacyjnych oraz podmioty niebędące przedsiębiorcami telekomunikacyjnymi, a także tryb i sposób ich zwrotu, mając na uwadze konieczność zachowania zasady minimalizowania negatywnych skutków udostępniania tych urządzeń oraz brak możliwości ich zwrotu ze względu na utratę lub zniszczenie.

Projekt rozporządzenia Rady Ministrów w sprawie trybu nieodpłatnego udostępniania urządzeń telekomunikacyjnych oraz radiowych urządzeń nadawczych lub nadawczo-odbiorczych[32] przewiduje w § 1, że rozporządzenie to będzie określać:

1) tryb nieodpłatnego udostępniania urządzeń telekomunikacyjnych oraz radiowych urządzeń nadawczych lub nadawczo-odbiorczych w sytuacji szczególnego zagrożenia:
   a) przez przedsiębiorcę telekomunikacyjnego urządzeń telekomunikacyjnych niezbędnych do przeprowadzenia akcji ratowniczej innemu przedsiębiorcy telekomunikacyjnemu lub podmiotowi, o którym mowa w art. 39 ust. 1 pkt 2 ustawy,
   b) przez podmioty niebędące przedsiębiorcami telekomunikacyjnymi radiowych urządzeń nadawczych lub nadawczo-odbiorczych stosowanych w służbach radiokomunikacyjnych podmiotom koordynującym działania ratownicze, podmiotom właściwym w sprawie zarządzania kryzysowego, służbom ustawowo powołanym do niesienia pomocy, a także innym podmiotom realizującym zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego;
2) tryb i sposób zwrotu urządzeń telekomunikacyjnych oraz radiowych urządzeń nadawczych lub nadawczo-odbiorczych.

Zgodnie z art. 42 p.k.e. w przypadkach i na zasadach określonych w przepisach odrębnych minister obrony narodowej, komendant główny Policji, komendant

[31] Zob. uzasadnienie do art. 41 p.k.e.

[32] Projekt p.k.e. zawiera poza uzasadnieniem także projekty aktów wykonawczych, które powinny być wydane na podstawie przepisów p.k.e.

Centralnego Biura Śledczego Policji, komendant Centralnego Biura Zwalczania Cyberprzestępczości, komendant wojewódzki Policji, komendant główny Straży Granicznej, komendant Oddziału Straży Granicznej, komendant główny Żandarmerii Wojskowej, komendant Oddziału Żandarmerii Wojskowej, szef Agencji Bezpieczeństwa Wewnętrznego, szef Służby Kontrwywiadu Wojskowego, komendant Służby Ochrony Państwa oraz szef Krajowej Administracji Skarbowej mogą zarządzić o zastosowaniu urządzeń uniemożliwiających telekomunikację na określonym obszarze.

Przepis art. 42 p.k.e. zawiera zamknięty katalog organów, które mogą dysponować środkami uniemożliwiającymi na określonym, ograniczonym obszarze świadczenie usług telekomunikacyjnych. Przypadki oraz warunki, kiedy może nastąpić ograniczenie telekomunikacji na danym obszarze, określają przepisy odrębne. Przykładem takiego przepisu jest art. 18c ustawy z dnia 6 kwietnia 1990 r. o Policji[33]. Zgodnie z tym przepisem w przypadkach, o których mowa w art. 18 ust. 1 niniejszej ustawy lub w art. 22 ust. 1 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, komendant główny Policji lub komendant wojewódzki Policji może zarządzić zastosowanie przez Policję urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wyeliminowania zagrożenia lub jego skutków, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych. O zastosowaniu tych urządzeń komendant główny Policji lub komendant wojewódzki Policji niezwłocznie informuje Prezesa Urzędu Komunikacji Elektronicznej.

Ograniczenie komunikacji następuje poprzez zarządzenie zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze. Definicja telekomunikacji (art. 2 pkt 70 p.k.e.) wskazuje, że chodzi o ograniczenie nie tylko komunikacji głosowej, ale wszelkich innych form komunikacji objętych pojęciem telekomunikacji. Ograniczenie telekomunikacji może nastąpić tylko na określonym obszarze, którego precyzyjne określenie może w praktyce nastręczać trudności z uwagi na technologiczne uwarunkowania, np. w zakresie funkcjonowania nadajników telefonii ruchomej, co może być związane z możliwością wykorzystania np. telefonów komórkowych w celach terrorystycznych poprzez uruchamianie ładunków wybuchowych. Podmiotami uprawnionymi do zarządzenia zastosowania urządzeń ograniczających telekomunikację są wymienione w art. 42 p.k.e. Przepis ten wyłącza możliwość dochodzenia odszkodowań przez przedsiębiorców telekomunikacyjnych. Nie wyłącza to oczywiście takich roszczeń odszkodowawczych, gdy zarządzenie ograniczenia telekomunikacji nastąpiło z naruszeniem przepisów prawa.

[33] Dz.U. z 1990 r. Nr 30, poz. 179 ze zm.

Postanowienia art. 96 przepisów wprowadzających[34] określają, które z aktów wykonawczych wydanych na podstawie ustawy – Prawo telekomunikacyjne i jak długo będą obowiązywać. Wśród tych aktów wykonawczych wymienia się ważne rozporządzenie Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług[35]. Rozporządzenie określa minimalne środki techniczne i organizacyjne oraz metody zapobiegania zagrożeniom, o których mowa w art. 175a ust. 1 i art. 175c ust. 1 p.t., jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług. Oznaczać to będzie, że do dnia wydania nowego rozporządzenia na podstawie przepisów p.k.e. obowiązywać będzie rozporządzenie Ministra Cyfryzacji z dnia 22 czerwca 2020 r.

## 2. Projekt noweli ustawy o krajowym systemie cyberbezpieczeństwa

W dniu 3 lipca 2023 r. został skierowany do Sejmu projekt ustawy – o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (druk sejmowy nr 3457). W uzasadnieniu tej noweli wskazano, że ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, uchwalona w 2018 r., tworzy podstawy prawno-instytucjonalne dla cyberbezpieczeństwa na poziomie krajowym. U.k.s.c. jest implementacją dyrektywy NIS. Krajowy system cyberbezpieczeństwa tworzy wiele podmiotów, przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych oraz podmioty publiczne, na które nałożono obowiązki związane z zapewnieniem bezpieczeństwa informacji, a także obsługą incydentów. Operatorzy usług kluczowych zostali podzieleni według sektorów i podsektorów wskazanych w załączniku nr 1 do u.k.s.c. Dla każdego sektora ustanowiono organ właściwy do spraw cyberbezpieczeństwa („organ właściwy"), który odpowiada za identyfikację i wyznaczanie operatorów usług kluczowych oraz nadzór i kontrolę nad przestrzeganiem przepisów ustawy w danym sektorze. Obecnie ani przedsiębiorcy telekomunikacyjni, ani dostawcy usług zaufania nie są podmiotami krajowego systemu cyberbezpieczeństwa. W uzasadnieniu wskazano, że projekt z dnia 3 lipca 2023 r. służy realizacji celów Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata

[34] Projekt ustawy – Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej.

[35] Dz.U. z 2020 r. poz. 1130.

2019–2024, jakimi są podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym. Projekt realizuje także cel szczegółowy tej strategii, odnoszący się do rozwoju krajowego systemu cyberbezpieczeństwa poprzez ewaluację przepisów prawa dotyczących cyberbezpieczeństwa. Ponadto projekt realizuje cele wskazanej strategii w odniesieniu do zapewnienia bezpieczeństwa łańcucha dostaw i utworzenia krajowego systemu certyfikacji cyberbezpieczeństwa.

W związku z prowadzonymi pracami nad projektem z 3 lipca 2023 r. należy zwrócić uwagę, że została przyjęta nowa dyrektywa NIS 2, która musi być implementowana do polskiego porządku prawnego. Pomimo świadomości konieczności implementacji NIS 2 prowadzone były od dawna prace nad nowelą ustawy o krajowym systemie cyberbezpieczeństwa, gdyż rozpoczęły się we wrześniu 2020 r. Do chwili obecnej powstało już 10 wersji projektu ustawy zmieniającej ustawę o k.s.c. Kolejne wersje projektu z dnia 3 lipca 2023 r. wzbudzały kontrowersje, gdyż projekt ten w minimalnym stopniu odzwierciedlał zmiany wprowadzone nową dyrektywą NIS 2.

Powstaje więc pytanie, czy nie lepszym rozwiązaniem jest dokonanie implementacji nowej dyrektywy NIS 2 zamiast przyjmowania noweli ustawy o krajowym systemie cyberbezpieczeństwa, skoro w perspektywie najbliższych miesięcy przepisy te będą musiały być zmienione w związku właśnie z koniecznością implementacji dyrektywy NIS 2. Przyjęcie projektu z dnia 3 lipca 2023 r. oznaczać może wprowadzenie rozwiązań niespójnych i niezgodnych z projektem dyrektywy NIS 2. Byłyby wprowadzane indywidualne rozwiązania krajowe w sytuacji posiadanej już przez projektodawcę wiedzy o przyjętych unijnych przepisach NIS 2 i kierunkach zmian wskazywanych tą dyrektywą.

Ponadto należy zauważyć, że wyniki analizy przepisów NIS 2 w porównaniu z obecną treścią u.k.s.c. wskazują, iż w przypadku nowelizacji obecnej u.k.s.c. implementacja NIS 2 spowoduje konieczność ponownego uchwalenia prawie połowy (44%) przepisów znajdujących się obecnie w projekcie z dnia 3 lipca 2023 r. W zdecydowanej większości tych przepisów określone są zadania i obowiązki podmiotów podlegających regulacjom u.k.s.c., co spowoduje konieczność weryfikacji wszystkich opracowanych na podstawie zmienionej u.k.s.c. polityk, procedur, zasad współpracy. Wskazane zmiany nie dotyczą konieczności wprowadzenia do u.k.s.c. przepisów implementujących zupełnie nowe rozwiązania, nieprzewidziane w NIS, ale wymagane przez NIS 2, co pokazuje duży zakres koniecznych zmian.

Zastrzeżenia budzi więc prowadzenie dalszych prac legislacyjnych nad dwiema nowelami u.k.s.c. w tym samym czasie, tj. jednej wynikającej z konieczności implementacji przepisów unijnych, a drugiej, stanowiącej kontynuację

trwających prac nad nowelą k.s.c. Wskazane jest prowadzenie jednej noweli, będącej wynikiem konieczności wdrożenia NIS 2, albo po prostu rozpoczęcie prac nad całkowicie nową ustawą o krajowym systemie cyberbezpieczeństwa, która implementowałaby NIS 2. Ewentualna nowela mogłaby być uzupełniona o regulacje, których potrzeba przyjęcia może wynikać z obecnego projektu z dnia 3 lipca 2023 r. Przyjmowanie natomiast przepisów w drodze kolejnej noweli u.k.s.c. mogło zagrozić terminowej transpozycji NIS 2, a także spowodować wprowadzenie rozwiązań niespójnych z dyrektywą NIS2. W praktyce mogło to wywoływać rozbieżne interpretacje przepisów. Prowadzenie prac zarówno nad wdrożeniem NIS 2, jak i nowelą k.s.c. spowodować mogłoby dla przedsiębiorców, zwłaszcza mniejszych i średnich, także dodatkowe koszty związane najpierw z wprowadzeniem obowiązków z noweli u.k.s.c., a następnie analogicznych lub zmodyfikowanych obowiązków wynikających z wdrożenia NIS 2 (innymi słowy, mogłoby dojść do „podwójnego" realizowania obowiązków). Za takim podejściem do sposobu transpozycji dyrektywy NIS 2 przemawiają także przykłady wdrożenia innych dyrektyw wprowadzających istotne zmiany w danym obszarze, jak np. wdrożenie dyrektywy EKŁE, które postanowiono przeprowadzić poprzez uchwalenie całkowicie nowej ustawy – Prawo komunikacji elektronicznej, a nie poprzez nowelizację ustawy – Prawo telekomunikacyjne.

Zgodnie z art. 1 pkt 2 lit. a projektu z dnia 3 lipca 2023 r. w art. 1 ust. 1 k.s.c. dodano m.in. nowy pkt 4 w brzmieniu: „4) zadania i obowiązki przedsiębiorców komunikacji elektronicznej w zakresie wymogów dotyczących bezpieczeństwa sieci lub usług komunikacji elektronicznej i zgłaszania incydentów telekomunikacyjnych". W ten sposób kwestie związane z bezpieczeństwem sieci lub usług komunikacji elektronicznej przeniesiono do u.k.s.c. W uzasadnieniu projektu z dnia 3 lipca 2023 r. wyjaśniono, że dostosowaniu do projektowanych zmian o charakterze systemowym uległ także art. 1 ust. 2. W związku z wynikającym z implementacji art. 40 i 41 EKŁE włączeniem do krajowego systemu cyberbezpieczeństwa przedsiębiorców komunikacji elektronicznej konieczne było uchylenie pkt 1 w art. 1 ust. 2, zgodnie z którym przepisów obowiązującej ustawy nie stosuje się do tych przedsiębiorców[36].

Projekt z dnia 3 lipca 2023 r. nadaje nowe brzmienie art. 2 u.k.s.c. Przepis art. 2 pkt 2 projektu z dnia 3 lipca 2023 r. wprowadza nową definicję bezpieczeństwa sieci lub usług komunikacji elektronicznej, które oznacza „zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania, przy zakładanym poziomie ryzyka, wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność: a) tych sieci lub usług,

[36] Zob. s. 19 uzasadnienia projektu z dnia 3 lipca 2023 r.

b) przetwarzanych informacji objętych tajemnicą komunikacji elektronicznej, c) innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy". Przepis ten stanowi wdrożenie art. 2 pkt 21 EKŁE.

Przepis art. 2 pkt 11 projektu z dnia 3 lipca 2023 r. formułuje także definicję cyberbezpieczeństwa, które oznacza działania niezbędne do ochrony systemów informacyjnych, użytkowników takich systemów oraz innych podmiotów przed cyberzagrożeniami, a art. 2 pkt 12 przewiduje definicję cyberzagrożenia, którym są wszelkie potencjalne okoliczności, zdarzenia lub działania, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć na systemy informacyjne, użytkowników takich systemów oraz na inne podmioty. Rozporządzenie 2019/881 wprowadziło definicję cyberbezpieczeństwa, która różni się od tej stosowanej na gruncie obowiązującej u.k.s.c. Z tego względu wprowadzono nową definicję cyberbezpieczeństwa. Natomiast dotychczasowemu brzmieniu definicji cyberbezpieczeństwa odpowiada definicja bezpieczeństwa systemów informacyjnych[37].

## 2.1. Zadania i obowiązki przedsiębiorców komunikacji elektronicznej w zakresie wymogów dotyczących bezpieczeństwa

W projekcie z dnia 3 lipca 2023 r. dodany został nowy Rozdział 4a zatytułowany *Zadania i obowiązki przedsiębiorców komunikacji elektronicznej w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów* (art. 20a–20h). W uzasadnieniu projektu wyjaśniono, że współczesne społeczeństwo informacyjne jest zależne od usług dostarczanych przez przedsiębiorców komunikacji elektronicznej, bez których nie jest możliwy przepływ informacji. Z tego powodu, zarówno na poziomie europejskim, jak i krajowym, istotne jest, aby sieci telekomunikacyjne i usługi komunikacji elektronicznej zapewniały odpowiednio wysoki poziom bezpieczeństwa. Obecnie przedsiębiorcy telekomunikacyjni już na podstawie dotychczas obowiązujących przepisów Działu VIIA p.t. są obowiązani stosować środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług. Ponadto byli obowiązani informować Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług, o podjętych działaniach zapobiegawczych i środkach naprawczych oraz podjętych przez przedsiębiorcę działaniach. Prezes UKE jednak nie miał kompetencji reagowania na te naruszenia. Zauważyć należy, że

[37] Zob. s. 20 uzasadnienia projektu z dnia 3 lipca 2023 r.

podmioty świadczące publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów do tej pory w ogóle nie były prawnie obowiązane stosować środki bezpieczeństwa związane z usługami komunikacji interpersonalnej. Wyjątkiem w tym zakresie były wymogi narzucone unijnymi przepisami o ochronie danych osobowych. Proponowane przepisy z jednej strony stanowią ewolucję przepisów działu VIIA p.t., a z drugiej wdrożenie EKŁE. Wzmocniona zostanie rola Prezesa UKE w zakresie badania środków technicznych i organizacyjnych stosowanych przez przedsiębiorców komunikacji elektronicznej[38].

Zgodnie więc z art. 20a ust. 1 projektu z dnia 3 lipca 2023 r. przedsiębiorca komunikacji elektronicznej, w celu zapewnienia ciągłości świadczenia usług komunikacji elektronicznej lub dostarczania sieci telekomunikacyjnej, jest obowiązany uwzględniać możliwość wystąpienia sytuacji szczególnego zagrożenia. W art. 20a ust. 1 projektu z dnia 3 lipca 2023 r. nakładany jest na przedsiębiorcę komunikacji elektronicznej ogólny obowiązek brania pod uwagę w swojej działalności możliwości wystąpienia sytuacji szczególnego zagrożenia. Katalog tych sytuacji obejmuje stan nadzwyczajny, sytuację kryzysową oraz bezpośrednie zagrożenie dla bezpieczeństwa sieci i usług komunikacji elektronicznej. Przepis ten odzwierciedla obecny art. 176a ust. 1 p.t.[39]

Według art. 20a ust. 2 pkt 1 projektu z dnia 3 lipca 2023 r. przedsiębiorca komunikacji elektronicznej przeprowadza systematyczne szacowanie ryzyka wystąpienia sytuacji szczególnego zagrożenia co najmniej raz w roku. Przedsiębiorcy komunikacji elektronicznej są obowiązani do prowadzenia systematycznego szacowania ryzyka wystąpienia sytuacji szczególnego zagrożenia (art. 20 ust. 2 pkt 1 projektu z dnia 3 lipca 2023 r.). Po zidentyfikowaniu ryzyk są obowiązani wdrożyć środki techniczne i organizacyjne zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych danych, a także poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka (art. 20 ust. 2 pkt 2 projektu z dnia 3 lipca 2023 r.). Przepisy te są implementacją art. 40 ust. 1 EKŁE. W motywie 95 EKŁE prawodawca unijny zwrócił uwagę, że podmioty świadczące usługi komunikacji interpersonalnej niewykorzystujące numerów zazwyczaj nie sprawują rzeczywistej kontroli nad transmisją sygnałów w sieciach. Sytuacja taka może również w niektórych przypadkach dotyczyć dostawcy usług łączności interpersonalnej wykorzystującej numery. W takich sytuacjach środki techniczne i organizacyjne mające zapewnić bezpieczeństwo sieci i usług komunikacji elektronicznej powinny być

[38] Zob. s. 34 uzasadnienia projektu z dnia 3 lipca 2023 r.

[39] Zob. s. 34 uzasadnienia projektu z dnia 3 lipca 2023 r.

łagodniejsze. Uwzględniono to w projektowanych przepisach, wskazując, że środki techniczne i organizacyjne podejmowane przez przedsiębiorców komunikacji elektronicznej powinny zapewniać poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka, co również bierze pod uwagę sytuację dostawcy usług łączności interpersonalnej wykorzystującej numery. Inne środki będą stosować duzi operatorzy sieci mobilnych, dysponujący infrastrukturą telekomunikacyjną, a inne mali przedsiębiorcy, jak np. osiedlowi dostawcy usługi dostępu do internetu[40].

Zgodnie z art. 20a ust. 2 pkt 2 projektu z dnia 3 lipca 2023 r. przedsiębiorca komunikacji elektronicznej podejmuje środki techniczne i organizacyjne zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych danych, a także poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka, minimalizujące w szczególności wpływ, jaki na sieci telekomunikacyjne, usługi komunikacji elektronicznej lub podmioty korzystające z tych sieci lub usług może mieć wystąpienie sytuacji szczególnego zagrożenia, dotyczące następujących obszarów:

a) zapewnienia bezpieczeństwa infrastruktury telekomunikacyjnej;
b) postępowania w przypadku wystąpienia sytuacji szczególnego zagrożenia;
c) odtwarzania dostarczania sieci telekomunikacyjnych lub przywracania świadczenia usług komunikacji elektronicznej;
d) monitorowania, kontroli i testowania sieci telekomunikacyjnych lub usług komunikacji elektronicznej – przy uwzględnieniu aktualnego stanu wiedzy technicznej oraz kosztów wprowadzenia tych środków.

W art. 20a ust. 2 pkt 2 projektu z dnia 3 lipca 2023 r. wskazane zostały obligatoryjne obszary środków technicznych i organizacyjnych, które wynikają z motywu 94 EKŁE. Środki te można przykładowo podzielić na:

1) środki dotyczące zapewnienia bezpieczeństwa infrastruktury telekomunikacyjnej, np.:
   – bezpieczeństwo fizyczne i środowiskowe,
   – bezpieczeństwo łańcuchów dostaw,
   – kontrola dostępu do sieci,
   – zapewnienie integralności sieci;
2) środki dotyczące postępowania w sytuacji szczególnego zagrożenia:
   – procedury obsługi incydentu telekomunikacyjnego,
   – zdolności w zakresie wykrywania incydentów telekomunikacyjnych,
   – procedury raportowania incydentów telekomunikacyjnych oraz komunikacji;

[40] Zob. s. 34–35 uzasadnienia projektu z dnia 3 lipca 2023 r.

3) środki dotyczące odtwarzania dostarczania sieci telekomunikacyjnych lub przywracania świadczenia usług komunikacji elektronicznej, np.:
   – zapewnienie planów ciągłości działania usług,
   – zapewnienie zdolności do odtwarzania awaryjnego usług i sieci;
4) środki w zakresie monitorowania, audytowania i testowania np.:
   – przygotowanie polityk monitorowania i logowania,
   – przeprowadzanie ćwiczeń w zakresie planów ciągłości działania,
   – testowanie sieci i usług,
   – przeprowadzania oceny bezpieczeństwa sieci i usług komunikacji elektronicznej[41].

Przedsiębiorca komunikacji elektronicznej byłby zobowiązany dokumentować prowadzenie analizy ryzyka oraz wdrożenie środków bezpieczeństwa (art. 20a ust. 2 pkt 3 projektu z dnia 3 lipca 2023 r.). Dokumentowanie tych środków jest zgodne z powszechnie uznanymi normami technicznymi (ISO 27001), jak również pozwala na rozliczalność tych działań oraz skuteczne przeprowadzenie audytu i kontroli. W celu uproszczenia prowadzenia dokumentacji w art. 20a ust. 3 projektu z dnia 3 lipca 2023 r. wskazano, że przedsiębiorcy komunikacji elektronicznej sporządzający plan działania w sytuacji szczególnego zagrożenia będą dokumentować w tym planie wdrożenie środków technicznych i organizacyjnych, o których mowa w art. 20a ust. 2 pkt 2 projektu z dnia 3 lipca 2023 r.

Ważną kwestią jest zapewnienie przepływu informacji między zespołami CSIRT, prezesem UKE oraz przedsiębiorcami komunikacji elektronicznej. Zaproponowano więc, aby co do zasady przedsiębiorcy komunikacji elektronicznej byli obowiązani wyznaczyć dwie osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Dane tych osób byłyby przekazywane do Prezesa UKE (art. 20a ust. 2 pkt 4 projektu z dnia 3 lipca 2023 r.). Z obowiązku wyznaczenia wskazanych osób wyłącza się mikroprzedsiębiorców, małych przedsiębiorców oraz średnich przedsiębiorców, gdyż mogłoby to stanowić zbyt duże obciążenie dla tej grupy podmiotów (art. 20a ust. 2 pkt 6 projektu z dnia 3 lipca 2023 r.).

W projekcie z dnia 3 lipca 2023 r. zaproponowano, podobnie jak w obecnie obowiązujących przepisach (art. 175d p.t.), aby minister właściwy do spraw informatyzacji mógł określić, dla danego rodzaju działalności wykonywanej przez przedsiębiorcę komunikacji elektronicznej, minimalny zakres środków technicznych i organizacyjnych stosowanych w celu zapewnienia bezpieczeństwa sieci

[41] Zob. E. Vytogianni, M. Dekker, *Security Supervision under the EECC*, s. 15–16; European Union Agency for Cybersecurity (ENISA), https://www.enisa.europa.eu/publications/supporting-the-implementation-of-theeuropean-electronic-commmunications-code-eecc [dostęp: 7.02.2024 r.].

i usług komunikacji elektronicznej (art. 20a ust. 7 projektu z dnia 3 lipca 2023 r.). Przy wydawaniu rozporządzenia minister powinien wziąć pod uwagę:

- rekomendacje międzynarodowe o charakterze specjalistycznym (będą to mogły być w szczególności normy techniczne, dokumenty ENISA, akty wykonawcze Komisji Europejskiej wydane na podstawie art. 40 ust. 5 EKŁE czy też inne dokumenty specjalistyczne organizacji międzynarodowych);
- skalę działalności wykonywanej przez przedsiębiorcę komunikacji elektronicznej;
- potrzebę podejmowania przez tego przedsiębiorcę działań zapewniających bezpieczeństwo sieci lub usług komunikacji elektronicznej.

Przewidziano możliwość wydawania kilku rozporządzeń na podstawie art. 20a ust. 7 projektu z dnia 3 lipca 2023 r. – odrębnie dla każdego rodzaju działalności. W uzasadnieniu wyjaśniono, że konieczność zapewnienia ministrowi właściwemu do spraw informatyzacji takiej kompetencji wynika z faktu krytycznego znaczenia usług telekomunikacyjnych dla społeczeństwa informacyjnego. Wiele usług jest zależnych od usług telekomunikacyjnych, przykładowo centra przetwarzania danych potrzebują redundantnych łączy telekomunikacyjnych, aby mogły świadczyć swoje usługi. Dlatego konieczne jest, aby dla tego sektora minister mógł wydać minimalne wymagania co do środków bezpieczeństwa, aby zapewnić jednolity poziom bezpieczeństwa danego rodzaju usług komunikacji elektronicznej[42].

W art. 20b ust. 1 projektu z dnia 3 lipca 2023 r. uregulowano uprawnienie Prezesa UKE do dokonywania oceny podjętych przez przedsiębiorcę komunikacji elektronicznej środków zapewniających bezpieczeństwo sieci i usług. Na jego żądanie przedsiębiorca poinformuje go o podjętych środkach (art. 20b ust. 2 projektu z dnia 3 lipca 2023 r.). Obowiązek ten jest zgodny z art. 41 ust. 2 lit. a EKŁE. Żądanie Prezesa UKE zawiera:

1) wskazanie podmiotu obowiązanego do przekazania informacji;
2) datę;
3) wskazanie zakresu żądanych informacji oraz okresu, którego dotyczą;
4) wskazanie celu, jakiemu informacje mają służyć;
5) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni;
6) pouczenie o zagrożeniu karą (art. 20b ust. 3 projektu z dnia 3 lipca 2023 r.).

W wyniku przeprowadzonej przez Prezesa UKE oceny mogą powstać uzasadnione wątpliwości co do stosowania przez przedsiębiorcę komunikacji elektronicznej właściwych środków technicznych i organizacyjnych. W projekcie

[42] Zob. s. 36–37 uzasadnienia projektu z dnia 3 lipca 2023 r.

z dnia 3 lipca 2023 r. zaproponowano więc, aby w takiej sytuacji Prezes UKE mógł nałożyć, w drodze decyzji, na przedsiębiorcę komunikacji elektronicznej obowiązek:

- właściwego zastosowania lub uzupełnienia środków technicznych lub organizacyjnych, w określonym przez Prezesa UKE terminie (art. 20b ust. 4 pkt 1 projektu z dnia 3 lipca 2023 r.), co stanowi implementację art. 41 ust. 1 EKŁE, lub
- poddania się audytowi bezpieczeństwa, którego wyniki przedsiębiorca udostępnia Prezesowi UKE (art. 20b ust. 4 pkt 2 projektu z dnia 3 lipca 2023 r.), co stanowi z kolei implementację art. 41 ust. 2 lit. b EKŁE.

W uzasadnieniu projektu z dnia 3 lipca 2023 r. wyjaśniono, że celowo w przepisie art. 20b ust. 4 pkt 1 użyto funktora „lub", ponieważ zależnie od konkretnej sytuacji u przedsiębiorcy komunikacji elektronicznej może zaistnieć potrzeba nakazania uzupełnienia tylko środka technicznego lub tylko środka organizacyjnego albo i jednego, i drugiego[43]. Zgodnie więc art. 20b ust. 4 pkt 1 projektu z dnia 3 lipca 2023 r. Prezes UKE może, w drodze decyzji, nałożyć na przedsiębiorcę komunikacji elektronicznej obowiązek „właściwego zastosowania lub uzupełnienia środków technicznych lub organizacyjnych". Tymczasem art. 41 ust. 1 EKŁE stanowi, że „Państwa członkowskie zapewniają, aby w celu wdrożenia art. 40 właściwe organy były uprawnione do wydawania wiążących instrukcji – w tym instrukcji dotyczących środków wymaganych […]". Przepis ten mówi o wydawaniu przez odpowiednie organy w decyzji „wiążących instrukcji", a nie *„środków* technicznych lub organizacyjnych". Przepis art. 20b ust. 4 projektu z dnia 3 lipca 2023 r. powinien więc zostać zmieniony i brzmieć następująco: „Prezes UKE może, w drodze decyzji, nałożyć na przedsiębiorcę komunikacji elektronicznej obowiązek:

1) zastosowania dodatkowych wiążących instrukcji – w tym instrukcji dotyczących środków wymaganych, kierując się potrzebą zapewnienia ich proporcjonalności do zidentyfikowanego stopnia ryzyka;
2) w przypadku powstania uzasadnionych wątpliwości co do stosowania właściwych środków bezpieczeństwa, poddania się, na własny koszt, audytowi bezpieczeństwa przeprowadzanemu przez wykwalifikowany, wybrany przez przedsiębiorcę podmiot i udostępnienia Prezesowi UKE wyników takiego audytu".

Prezes UKE może więc zarządzić przeprowadzenie audytów tylko w sytuacji, w której istnieje uzasadniona obawa, iż przedsiębiorca nie stosuje wystarczających środków bezpieczeństwa.

---

[43] Zob. s. 37 uzasadnienia projektu z dnia 3 lipca 2023 r.

W przypadku jednak, gdyby art. 20b ust. 4 projektu z dnia 3 lipca 2023 r. nie został zmieniony, postanowienia art. 20b projektu powinny być uzupełnione o ustęp 7, zgodnie z którym: *Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, wytyczne w zakresie stosowania technicznych i organizacyjnych środków, o których mowa w art. 20a ust. 2 pkt 2, kierując się potrzebą zapewnienia ich proporcjonalności do zidentyfikowanego stopnia ryzyka oraz zasady minimalizacji kosztów związanych z ich wdrażaniem*. Określenie w rozporządzeniu wytycznych w zakresie stosowania dodatkowych technicznych i organizacyjnych środków, o których mowa w art. 20a ust. 2 pkt 2 projektu z dnia 3 lipca 2023 r., zapewniłoby jasność i przejrzystość zarówno dla Prezesa UKE, jak i dla przedsiębiorców komunikacji elektronicznej, co do tego, jakie mogą być konkretnie stosowane odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa sieci lub usług.

Uprawnienie Prezesa UKE do nałożenia, w drodze decyzji administracyjnej, obowiązku właściwego zastosowania lub uzupełnienia środków technicznych bądź organizacyjnych służy m.in. przeciwdziałaniu ryzykom związanych z błędną konfiguracją sieci, które może prowadzić do poważnych incydentów telekomunikacyjnych, lub ryzykom związanym z niewystarczającą kontrolą dostępu. Prezes UKE będzie mógł także, na podstawie art. 20b projektu z dnia 3 lipca 2023 r., nakazać uzupełnić środki organizacyjne, np. związane z bezpieczeństwem fizycznym obiektów infrastruktury telekomunikacyjnej lub dostępem osób z zewnątrz, np. serwisantów dostawcy, do kluczowej infrastruktury. Określając termin na wdrożenie dodatkowych środków, Prezes UKE powinien kierować się z jednej strony koniecznością jak najszybszego ich wdrożenia, a z drugiej zaś powinien być to obiektywnie termin realny do wykonania przez przedsiębiorcę (art. 20b ust. 5 projektu z dnia 3 lipca 2023 r.)[44].

Z kolei celem audytu bezpieczeństwa byłaby ocena zastosowanych przez przedsiębiorcę środków zapewniających bezpieczeństwo sieci lub usług komunikacji elektronicznej. Audyt musiałby być przeprowadzony przez podmiot niezależny od przedsiębiorcy komunikacji elektronicznej, który zostałby zobligowany do przeprowadzenia audytu. Do tego audytu byłyby stosowane odpowiednio postanowienia art. 15 ust. 2 pkt 1 i 2 oraz ust. 3–5 u.k.s.c. Odpowiednie stosowanie przepisów art. 15 ust. 2 u.k.s.c (w zakresie spełniania wymogów formalnych przez podmioty przeprowadzające audyt) wynika z różnic w wymaganych wiedzy i doświadczeniu, w zależności od zakresu przedmiotowego audytu, który miałby być przeprowadzony.

[44] Zob. s. 37 uzasadnienia projektu z dnia 3 lipca 2023 r.

Przepis art. 15 u.k.s.c. określa, jakie podmioty mogą przeprowadzić audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, czyli świadczenia bardzo ważnej usługi. Podmioty przeprowadzające taki audyt powinny spełniać wysokie standardy. Zgodnie z art. 15 ust. 2 pkt 1 i 2 u.k.s.c. audyt może być przeprowadzony przez:

1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz.U. z 2022 r. poz. 1854), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
2) co najmniej dwóch audytorów posiadających:
   a) certyfikaty określone w przepisach wydanych na podstawie art. 15 ust. 8 u.k.s.c.[45] lub
   b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
   c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.

Przepis art. 15 ust. 3 u.k.s.c. wyjaśnia, że za praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych uważa się udokumentowane wykonanie w ciągu ostatnich trzech lat przed dniem rozpoczęcia audytu trzech audytów w zakresie bezpieczeństwa systemów informacyjnych lub ciągłości działania albo wykonywanie audytów bezpieczeństwa systemów informacyjnych lub ciągłości działania w wymiarze czasu pracy nie mniejszym niż 1/2 etatu, związanych z:

1) przeprowadzaniem audytu wewnętrznego pod nadzorem audytora wewnętrznego;
2) przeprowadzaniem audytu zewnętrznego pod nadzorem audytora wiodącego;
3) przeprowadzaniem audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;

[45] Na podstawie tego przepisu zostało wydane rozporządzenie Ministra Cyfryzacji w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu z dnia 12 października 2018 r. (Dz.U. z 2018 r. poz. 1999).

4) wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[46];
5) wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[47].

Audytor jest obowiązany do zachowania w tajemnicy informacji uzyskanych w związku z przeprowadzanym audytem, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych (art. 15 ust. 4 u.k.s.c.). Na podstawie zebranych dokumentów i dowodów audytor sporządza pisemne sprawozdanie z przeprowadzonego audytu i przekazuje je operatorowi usługi kluczowej wraz z dokumentacją z przeprowadzonego audytu (art. 15 ust. 5 u.k.s.c.).

Przy przeprowadzaniu audytów, o których mowa w art. 20b projektu z dnia 3 lipca 2023 r., nie zawsze wystarczające byłoby spełnienie przesłanki „praktyki w zakresie audytu bezpieczeństwa systemów informacyjnych", gdyż niezbędne mogą być wiedza i doświadczenie w zakresie funkcjonowania specyficznych rozwiązań telekomunikacyjnych. Wykonujący audyt bezpieczeństwa muszą być niezależni od przedsiębiorcy komunikacji elektronicznej, u którego prowadzony jest audyt bezpieczeństwa (art. 20b ust. 6 projektu z dnia 3 lipca 2023 r.)[48].

W art. 20c projektu z dnia 3 lipca 2023 r. uregulowano obowiązki przedsiębiorcy komunikacji elektronicznej po wykryciu incydentu telekomunikacyjnego. W uzasadnieniu projektu wyjaśniono, że przedsiębiorca obsługiwałby każdy incydent telekomunikacyjny, który u niego wystąpi. Dla przykładu oznaczałoby to, że dostawca usługi dostępu do internetu byłby obowiązany zainterweniować, jeżeli np. z powodów technicznych nastąpi przerwa lub pogorszenie jakości świadczenia tej usługi. Oczywiście rodzaje podejmowanych działań w ramach obsługi incydentu telekomunikacyjnego różniłyby się w zależności od przyczyny incydentu telekomunikacyjnego czy sieci lub usług dotkniętych tym incydentem. Obowiązek ten zwiększyłby bezpieczeństwo świadczonych usług komunikacji elektronicznej. Przedsiębiorca komunikacji elektronicznej zapewniłby dostęp do rejestrowanych incydentów zespołom CSIRT poziomu krajowego i CSIRT Telco. Jest to związane z tym, że CSIRT poziomu krajowego może zmienić klasyfikację konkretnego incydentu telekomunikacyjnego, a także z uprawnieniami zespołów CSIRT w związku z reagowaniem na incydenty telekomunikacyjne. Równocześnie mógłby przekazywać do zespołów CSIRT informacje o cyberzagrożeniach, podatnościach i incydentach, które mogłyby mieć negatywny wpływ

[46] Dz.U. z 2020 r. poz. 224.
[47] Dz.U. z 2022 r. poz. 623.
[48] Zob. s. 37–38 uzasadnienia projektu z dnia 3 lipca 2023 r.

na bezpieczeństwo sieci lub usług komunikacji elektronicznej, a także o wykorzystywanych technologiach. Uprawnienie to wzmacniałby przepływ informacji między przedsiębiorcami komunikacji elektronicznej a zespołami CSIRT. Bazując na tej wiedzy, zespoły CSIRT mogłyby dokonać analizy podatności czy analizy zagrożeń, co zwiększyłoby ich możliwości reagowania na incydenty telekomunikacyjne. Wiąże się to także z zadaniem zespołów CSIRT wskazanym w art. 32 ust. 4 u.k.s.c.[49] W przypadku kontynuowania prac nad zaproponowanym w projekcie z dnia 3 lipca 2023 r. przepisem art. 20c należałoby doprecyzować, że obowiązek dotyczy wyłącznie sieci telekomunikacyjnych lub usług komunikacji elektronicznej tego przedsiębiorcy. Niezbędne jest bowiem zapewnienie, aby przepisy nie były rozumiane rozszerzająco i nie pozwalały na obarczanie jednych podmiotów obowiązkami, które *de facto* należą do innych podmiotów.

Przepis art. 20d projektu z dnia 3 lipca 2023 r. reguluje zasady zgłaszania incydentów telekomunikacyjnych przez przedsiębiorców komunikacji elektronicznej. Obowiązkowemu zgłoszeniu podlegałby poważny incydent telekomunikacyjny. Przedsiębiorca komunikacji elektronicznej byłby obowiązany uznać incydent telekomunikacyjny za poważny incydent telekomunikacyjny, jeżeli spełnił on progi określone w rozporządzeniu ministra właściwego do spraw informatyzacji (art. 20d ust. 1 pkt 1 projektu z dnia 3 lipca 2023 r.). Obowiązek informacyjny dotyczyłby więc szczególnego rodzaju incydentów telekomunikacyjnych, które w znaczny i istotny sposób oddziałują na funkcjonowanie społeczeństwa. Z tego powodu państwo powinno być poinformowane o tym fakcie oraz powinno mieć odpowiednie możliwości reakcji na tego rodzaju zdarzenie[50].

Przedsiębiorcy telekomunikacyjni przekazywaliby do zespołu CSIRT Telco informację o wystąpieniu poważnego incydentu telekomunikacyjnego nie później niż w ciągu ośmiu godzin od chwili jego wystąpienia, według aktualnej wiedzy, jaką dysponują w tym czasie (art. 20d ust. 1 pkt 2 oraz 20e ust. 3 projektu z dnia 3 lipca 2023 r.). Informację tę uzupełnialiby w trakcie obsługi incydentu telekomunikacyjnego. Co do zasady zgłoszenie byłoby przekazywane w postaci elektronicznej. W przypadku braku możliwości przekazania go w postaci elektronicznej przy użyciu innych dostępnych środków komunikacji (art. 20d ust. 2 projektu z dnia 3 lipca 2023 r.). W uzasadnieniu projektu wyjaśniono, że podczas obsługi poważnego incydentu telekomunikacyjnego przedsiębiorcy komunikacji elektronicznej byliby zobowiązani współpracować z zespołami CSIRT Telco i właściwym zespołem CSIRT GOV, CSIRT MON lub CSIRT NASK. W ramach tej współpracy przekazywaliby niezbędne dane do tych zespołów, aby ułatwić

[49] Zob. s. 38 uzasadnienia projektu z dnia 3 lipca 2023 r.

[50] Zob. s. 38–39 uzasadnienia projektu z dnia 3 lipca 2023 r.

reagowanie na incydent telekomunikacyjny. Zespół CSIRT Telco przekazywałby niezwłocznie, w ciągu ośmiu godzin, informację o tym zgłoszeniu do właściwego dla danego przedsiębiorcy komunikacji elektronicznej zespołu CSIRT GOV, CSIRT MON lub CSIRT NASK. Rozwiązanie to zapewniłoby jeden punkt kontaktowy dla zgłoszeń incydentów telekomunikacyjnych, z drugiej strony zapewniłoby obieg informacji między zespołami CSIRT. Przewiduje się, że przekazywanie informacji pomiędzy CSIRT odbywałoby się za pomocą systemu teleinformatycznego, o którym mowa w art. 46 u.k.s.c.[51]

1) Postanowienia art. 20d ust. 3 projektu z dnia 3 lipca 2023 r. przewidują, że minister właściwy do spraw informatyzacji określi w rozporządzeniu progi uznania incydentu telekomunikacyjnego za poważny incydent telekomunikacyjny. Tworząc upoważnienie ustawowe, wzięto pod uwagę parametry istotności wpływu incydentu telekomunikacyjnego wskazane w art. 40 ust. 2 EKŁE. Progi te można podzielić na:
   a) ilościowe:
      – liczbę użytkowników, na których incydent telekomunikacyjny miał wpływ,
      – czas trwania skutków incydentu telekomunikacyjnego,
      – obszar, na którym wystąpiły skutki incydentu telekomunikacyjnego;
   b) jakościowe:
      – zakres wpływu incydentu telekomunikacyjnego na funkcjonowanie sieci i usług,
      – wpływ incydentu telekomunikacyjnego na zachowanie tajemnicy komunikacji elektronicznej,
      – wpływ incydentu telekomunikacyjnego na świadczenie usług kluczowych oraz funkcjonowanie infrastruktury krytycznej w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym,
      – wpływ incydentu telekomunikacyjnego na połączenia do numerów alarmowych,
      – wpływ incydentu telekomunikacyjnego na wykonywanie obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Wydając rozporządzenie, minister powinien uwzględnić rekomendacje ENISA, która czyni to celem wsparcia organów regulacyjnych państw UE[52]. Z projektowanych regulacji wynikało więc, że incydent miałby być klasyfikowany jako telekomunikacyjny na podstawie progów. Niemniej jednak przepis

[51] Zob. s. 39 uzasadnienia projektu z dnia 3 lipca 2023 r.

[52] *Ibidem*.

art. 2 projektu z dnia 3 lipca 2023 r., zawierający wyjaśnienie pojęć używanych w projektowanej noweli, wprowadza także definicję incydentu telekomunikacyjnego. W praktyce mogłoby dojść do incydentu, który spełniałby kryteria telekomunikacyjnego według definicji, ale nie spełniałby kryteriów według progów. Powstałoby pytanie, czy wówczas incydent byłby telekomunikacyjny. Mogłoby dojść do paradoksalnej sytuacji z uwagi na obie definicje: według jednej definicji incydent byłby telekomunikacyjny, a według drugiej nie.

Przepis art. 20d ust. 3 projektu z dnia 3 lipca 2023 r. określa katalog przesłanek, który został zmodyfikowany wobec postanowień EKŁE, w szczególności poprzez nieuwzględnienie wskazanej w EKŁE przesłanki „wpływu na działalność ekonomiczną i społeczną". W to miejsce wprowadzono szeroki katalog okoliczności, tj.: wpływ incydentu bezpieczeństwa na zachowanie tajemnicy komunikacji elektronicznej; wpływ incydentu bezpieczeństwa na świadczenie usług kluczowych w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz funkcjonowanie infrastruktury krytycznej w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym; wpływ incydentu bezpieczeństwa na połączenia do numerów alarmowych. Należałoby rozważyć usunięcie przesłanki wpływu na usługi kluczowe oraz infrastrukturę krytyczną. W przypadku bowiem, gdyby w rozporządzeniu określono odrębne progi odnoszące się wyłącznie do tego zakresu, wykonanie obowiązku zgłoszenia mogłoby być niemożliwe. Z perspektywy operatora zobowiązanego do dokonania zgłoszenia trudne do ustalenia byłoby, czy dany incydent miał wpływ na usługi kluczowe (lista takich operatorów nie jest jawna) lub infrastrukturę krytyczną (lista obiektów jest zastrzeżona). Ewentualne zgłoszenie incydentu mającego wpływ w tym zakresie byłoby faktycznie możliwe jedynie w przypadku, gdyby operator miał wiedzę w zakresie takiego wpływu lub sam był operatorem usługi kluczowej lub posiadaczem infrastruktury krytycznej.

Przepis art. 20e projektu z dnia 3 lipca 2023 r. zawiera szczegółowe postanowienia dotyczące zawartości zgłoszenia poważnego incydentu telekomunikacyjnego. Pozwoliłyby one zebrać podstawowe dane o tym incydencie, takie jak dane o podmiocie dotkniętym incydentem, liczbę użytkowników, na których poważny incydent telekomunikacyjny miał wpływ oraz na usługi kluczowe, usługi cyfrowe czy obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Dane te są niezbędne, aby CSIRT Telco mógł skutecznie reagować na poważne incydenty telekomunikacyjne. Ponadto dzięki tym informacjom CSIRT poziomu krajowego zyskają informacje niezbędne do bieżącego szacowania ryzyka na poziomie krajowym[53].

[53] Zob. s. 40 uzasadnienia projektu z dnia 3 lipca 2023 r.

Przede wszystkim zgłoszenie musiałoby zawierać informacje, od kogo pochodzi – od jakiego podmiotu (art. 20e ust. 1 pkt 1 projektu z dnia 3 lipca 2023 r.). Następnie musiałyby być wskazane dane osoby (imię, nazwisko, numer telefonu, adres poczty elektronicznej) zgłaszającej incydent oraz dane osoby uprawnionej do zgłaszania wyjaśnień (art. 20e ust. 1 pkt 2–3 projektu z dnia 3 lipca 2023 r.). Mogą to być dwie różne osoby albo jedna, która wypełnia dwie funkcje. Istotne jest, aby CSIRT Telco wiedział, kto zgłasza incydent telekomunikacyjny i kto może udzielić wyjaśnień[54].

Zgodnie z art. 20e ust. 1 pkt 4 projektu z dnia 3 lipca 2023 r. zgłoszenie powinno także zawierać opis wpływu incydentu telekomunikacyjnego na sieci i usługi, w tym:

a) sieci telekomunikacyjne, na które poważny incydent telekomunikacyjny miał wpływ,
b) usługi komunikacji elektronicznej zgłaszającego, na które poważny incydent telekomunikacyjny miał wpływ,
c) liczbę użytkowników usługi komunikacji elektronicznej, na których poważny incydent telekomunikacyjny miał wpływ,
d) moment wystąpienia i wykrycia poważnego incydentu telekomunikacyjnego oraz czas jego trwania,
e) zasięg geograficzny obszaru, którego dotyczy poważny incydent telekomunikacyjny,
f) wpływ poważnego incydentu telekomunikacyjnego na świadczenie usługi kluczowej przez operatorów usług kluczowych, jeżeli jest znany,
g) wpływ poważnego incydentu telekomunikacyjnego na świadczenie usługi cyfrowej przez dostawców usług cyfrowych, jeżeli jest znany,
h) przyczynę zaistnienia poważnego incydentu telekomunikacyjnego i sposób jego przebiegu oraz skutki jego oddziaływania na sieci telekomunikacyjne lub świadczone usługi komunikacji elektronicznej,
i) wpływ poważnego incydentu telekomunikacyjnego na połączenia z numerami alarmowymi,
j) wpływ poważnego incydentu telekomunikacyjnego na możliwość realizacji zadań lub obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Projekt zakładał, że zgłoszenie poważnego incydentu telekomunikacyjnego będzie zawierało opis wpływu tego zdarzenia na świadczenie usługi kluczowej przez operatorów usług kluczowych oraz usług cyfrowych przez dostawców usług cyfrowych, jeżeli ten wpływ jest znany. W uzasadnieniu wyjaśniono, że

[54] *Ibidem*.

interpretować to należy w ten sposób, iż jeżeli przedsiębiorca komunikacji elektronicznej uzyskał informację, np. w drodze negocjacji biznesowych, od swojego usługobiorcy, że jest operatorem usługi kluczowej – to powinien wskazać w zgłoszeniu, czy poważny incydent telekomunikacyjny miał wpływ na świadczenie usługi kluczowej. To samo w przypadku dostawców usług cyfrowych. Szczególnie tych dostawców świadczących usługi przetwarzania w chmurze. Centra przetwarzania danych wymagają, do swojego codziennego funkcjonowania, niezawodnych, redundantnych łączy telekomunikacyjnych. Natomiast jeśli przedsiębiorca komunikacji elektronicznej obiektywnie nie jest w stanie wskazać, czy poważny incydent telekomunikacyjny wpłynął na operatorów usług kluczowych czy dostawców usług cyfrowych, to nie musiałby wypełniać tej części zgłoszenia. Podobny przepis znajduje się w art. 12 ust. 1 pkt 4 lit. e u.k.s.c.[55]

W zgłoszeniu powinien być także opisany wpływ poważnego incydentu telekomunikacyjnego na:

- połączenia z numerami alarmowymi – o każdym przypadku niedostępności numerów ustalonych w ustawie lub w planie numeracji krajowej dla publicznych sieci telekomunikacyjnych udostępnianych służbom ustawowo powołanym do niesienia pomocy powinno wiedzieć państwo, ponieważ numery te służą pomocy obywatelom;
- możliwość realizacji zadań lub obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Chodzi o obowiązki określone obecnie w dziale VIII. *Obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego* ustawy – Prawo telekomunikacyjne, a później w art. 39 i następnych ustawy – Prawo komunikacji elektronicznej. Zalicza się do nich m.in. zadania i obowiązki w zakresie przygotowania i utrzymywania wskazanych elementów sieci telekomunikacyjnych dla zapewnienia telekomunikacji na potrzeby systemu kierowania bezpieczeństwem narodowym. Stanowią one kluczowe obowiązki z punktu widzenia obronności państwa, dlatego jeżeli wydarzył się poważny incydent telekomunikacyjny, to państwo powinno wiedzieć, w jaki sposób wpływa to na realizację tych obowiązków[56].

W uzasadnieniu projektu wyjaśniono także, że ze względu na współzależność sieci telekomunikacyjnych incydenty telekomunikacyjne w jednym państwie mogą mieć wpływ na usługi w drugim państwie UE, np. w przypadku tranzytu połączeń. Dlatego zgłoszenie poważnego incydentu telekomunikacyjnego powinno zawierać informację o transgranicznych skutkach tego zdarzenia.

[55] *Ibidem*.

[56] Zob. s. 40–41 uzasadnienia projektu z dnia 3 lipca 2023 r.

Dzięki temu CSIRT MON, CSIRT NASK lub CSIRT GOV będą w stanie ocenić, czy poważny incydent telekomunikacyjny dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej. W zgłoszeniu powinno być także wskazane, jakie działania zapobiegawcze i naprawcze podjął przedsiębiorca komunikacji elektronicznej w związku z poważnym incydentem telekomunikacyjnym. Przykładowo czy np. dokonano zabezpieczenia logów. Jest to istotne, ponieważ dzięki temu CSIRT Telco czy CSIRT poziomu krajowego będą wiedziały, co zostało zrobione, a w czym należy pomóc zgłaszającemu podczas reagowania na to zdarzenie. Oczywiście zakładano, że zgłoszenie może zawierać inne istotne informacje – pozostawia się to do decyzji zgłaszającego. Ważne jest samo zgłoszenie poważnego incydentu telekomunikacyjnego, nawet jeżeli przedsiębiorca nie miałby pełnej informacji o tym zdarzeniu. Dopiero po dłuższej analizie mógłby uzyskać informacje, np. o przyczynie tego zdarzenia. Dlatego wprowadzono regułę, że zgłaszający miał przekazać informacje znane mu w chwili dokonywania zgłoszenia, ale w trakcie obsługi incydentu telekomunikacyjnego musiałby uzupełnić to zgłoszenie[57].

Zgodnie z art. 20e ust. 4 projektu z dnia 3 lipca 2023 r. przedsiębiorca komunikacji elektronicznej mógłby przekazać, w niezbędnym zakresie, w zgłoszeniu, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do obsługi incydentu telekomunikacyjnego przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco mógłby zwrócić się do przedsiębiorcy komunikacji elektronicznej o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do obsługi incydentu telekomunikacyjnego (art. 20e ust. 5 projektu z dnia 3 lipca 2023 r.). W zgłoszeniu przedsiębiorca komunikacji elektronicznej oznaczałby informacje stanowiące tajemnice prawnie chronione, w tym tajemnicę przedsiębiorstwa (art. 20e ust. 6 projektu z dnia 3 lipca 2023 r.).

Postanowienia art. 20e ust. 4–6 projektu z dnia 3 lipca 2023 r. szeroko określają uprawnienia CSIRT. Tajemnice prawnie chronione stanowią bardzo szeroki katalog, wykraczający poza tajemnicę przedsiębiorstwa czy tajemnicę telekomunikacyjną. Kwestii tych dotyczy kilkadziesiąt ustaw znajdujących się obecnie w obrocie prawnym. W praktyce może wystąpić sytuacja, gdy przedsiębiorca telekomunikacyjny nie będzie zobowiązany do ich zachowania. Nie zawsze bowiem będzie on w pełni dysponentem danej informacji, tj. nie w każdym przypadku będzie dotyczyła ona wyłączenie jego samego i tym samym będzie mógł przekazać ją CSIRT bez ryzyka naruszenia praw innych podmiotów.

[57] Zob. s. 41 uzasadnienia projektu z dnia 3 lipca 2023 r.

W niektórych przypadkach, aby możliwe było przekazanie takich informacji, potrzebne byłoby uzyskanie zgody sądu. Ponadto przekazanie pełnych informacji w zakresie tajemnicy komunikacji elektronicznej może budzić wątpliwości, czy np. treść indywidualnych komunikatów jest niezbędna CSIRT do wykonywania jego zadań. W każdym wypadku to CSIRT powinien być odpowiedzialny za precyzyjne wskazanie, jakie informacje, w tym ewentualne tajemnice, mają zostać przekazane. Wskazanie i doprecyzowanie zakresu przekazywanych danych związanych z daną tajemnicą nie powinno być obowiązkiem przedsiębiorcy i rodzić z tego tytułu jego odpowiedzialność. Powinien być także określony minimalny termin na udzielenie odpowiedzi przez przedsiębiorcę, który powinien być proporcjonalny do zakresu wniosku[58].

Zgodnie z art. 20f ust. 1 projektu z dnia 3 lipca 2023 r. przedsiębiorca komunikacji elektronicznej udostępniałby na swojej stronie internetowej informacje o:

1) potencjalnych zagrożeniach związanych z korzystaniem przez użytkowników z usług komunikacji elektronicznej;
2) rekomendowanych środkach ostrożności i najbardziej popularnych sposobach zabezpieczania telekomunikacyjnych urządzeń końcowych przed oprogramowaniem złośliwym lub szpiegującym;
3) przykładowych konsekwencjach braku lub nieodpowiedniego zabezpieczenia telekomunikacyjnych urządzeń końcowych.

Przepis art. 20f projektu z dnia 3 lipca 2023 r. regulowałby obowiązki informacyjne przedsiębiorcy komunikacji elektronicznej wobec użytkowników końcowych. Postanowienia ust. 1 nakładałyby obowiązki dotyczące wzmacniania świadomości użytkowników z zakresu bezpieczeństwa. Dzięki temu użytkownicy mieliby dostęp do wiedzy, która umożliwiłaby im bezpieczne korzystanie z usług komunikacji elektronicznej[59].

Przepis art. 20f ust. 1 projektu z dnia 3 lipca 2023 r. stanowi implementację art. 40 ust. 3 EKŁE. Dodatkowy obowiązek informacyjny określony w art. 20f ust. 1 występuje w przypadku, gdy ujawnienie naruszenia bezpieczeństwa sieci lub usług leży w interesie publicznym. W takim przypadku Prezes UKE podaje informację do wiadomości publicznej na stronie internetowej UKE. Alternatywne rozwiązanie polega na zobowiązaniu przedsiębiorcy telekomunikacyjnego w drodze decyzji administracyjnej do podania informacji do wiadomości publicznej, we wskazany w decyzji sposób. Decyzji takiej ze względu na charakter sprawy można nadać rygor natychmiastowej wykonalności. Przedsiębiorca wykonuje obowiązek informacyjny na własny koszt.

---

58 Zob. s. 42 uzasadnienia projektu z dnia 3 lipca 2023 r.

59 *Ibidem*.

Przepis art. 20f ust. 1 projektu z dnia 3 lipca 2023 r. zobowiązuje Prezesa UKE do publikowania na swojej stronie internetowej aktualnych informacji o zagrożeniach związanych z korzystaniem z usług, w szczególności o zagrożeniach dla telekomunikacyjnych urządzeń końcowych. Przepis dotyczy telekomunikacyjnych urządzeń końcowych, czyli urządzeń telekomunikacyjnych przeznaczonych do podłączenia bezpośrednio lub pośrednio do zakończeń sieci. Telekomunikacyjne urządzenie końcowe dla potrzeb związanych ze stosowaniem omawianego przepisu powinno być rozumiane w sposób szeroki, jako urządzenie wykorzystywane do komunikowania, które może być jedynie pośrednio dołączone do zakończenia sieci. W szczególności informacja publikowana powinna obejmować ochronę komputerów i innych urządzeń przetwarzających informacje, pośrednio przyłączonych do sieci telekomunikacyjnej. Typowe informacje publikowane przez Prezesa UKE zawierają ostrzeżenia i wskazówki dotyczące korzystania z usług w instytucjach szczególnie narażonych na ryzyka (np. szkoły, instytucje edukacyjne), korzystania z niektórych funkcji urządzeń końcowych (np. funkcji oddzwaniania na prezentowane numery telefoniczne), korzystania z niektórych uprawnień (np. prawa do „bycia zapomnianym w Internecie"), ryzyk dotyczących posługiwania się urządzeniami końcowymi (np. ryzyk związanych z kupnem kradzionego telefonu, podmianą karty SIM). Informacje publikowane są na stronie Centrum Informacji Konsumenckiej UKE.

Przepis art. 20f ust. 1 projektu z dnia 3 lipca 2023 r. zobowiązuje do wskazania potencjalnych zagrożeń związanych z usługami telekomunikacyjnymi. Zagrożenia te są zróżnicowane w zależności od rodzaju usługi i sposobu korzystania z niej. Typowe zagrożenia są związane z korzystaniem z usług o podwyższonej opłacie, wykorzystywaniem usług telekomunikacyjnych do realizacji transakcji finansowych i handlowych, kradzieżą usług telekomunikacyjnych i utratą kontroli nad wysokością należności za wykorzystane usługi. Przepis zobowiązuje do publikowania informacji o najbardziej popularnych sposobach zabezpieczenia urządzeń przed oprogramowaniem złośliwym lub szpiegującym. Oprogramowanie złośliwe oznacza wszelkie aplikacje i funkcje mające szkodliwe, nielegalne lub niszczące działanie w stosunku do zasobów urządzenia. Występuje w różnych postaciach i powoduje zmiany w programach wykorzystywanych przez urządzenia końcowe, multiplikuje, zmienia lub usuwa aplikacje lub pliki, absorbuje zasoby urządzenia, umożliwia dostęp do urządzenia końcowego poza wiedzą i kontrolą jego użytkownika oraz zdalne wykonywanie operacji na tym urządzeniu, a także inne efekty niepożądane lub szkodliwe w stosunku do użytkownika urządzenia (wirusy, robaki, trojany, backdoory itp.). Oprogramowanie szpiegujące służy do zbierania informacji o użytkowniku, bez jego wiedzy i zgody, w szczególności informacji o odwiedzanych adresach internetowych,

wykorzystywanych usługach, hasłach dostępowych, kodach. Oprogramowanie to może służyć do śledzenia całej aktywności użytkownika poprzez odczyt wszystkich operacji wykonywanych na urządzeniu końcowym. Informacja powinna ostrzegać przed niebezpieczeństwami poprzez wskazywanie przykładowych konsekwencji braku lub nieodpowiedniego zabezpieczenia urządzeń (np. utrata danych, kontroli nad funkcjonowaniem urządzenia, szkody majątkowe związane z nielegalnym wykorzystaniem dostępu do danych, ułatwienie zewnętrznych ataków, ujawnienie haseł, kodów i innych danych dostępowych do usług). Prezes UKE powinien wskazywać te konsekwencje nieodpowiedniego zabezpieczenia urządzeń końcowych.

Przedsiębiorca jest zobowiązany do publikowania informacji przygotowanych przez Prezesa UKE na swojej stronie internetowej. Ustawa przewiduje możliwość wykonania obowiązku informacyjnego poprzez odesłanie na stronie internetowej przedsiębiorcy do strony Prezesa UKE lub innego podmiotu zajmującego się bezpieczeństwem sieci, gdzie są zamieszczone odpowiednie informacje. Przepisy nie stanowią przeszkody, aby przedsiębiorca poza odesłaniem do stron właściwego organu administracji publikował informacje dotyczące specyficznych zagadnień ochrony przed zagrożeniami związanymi z usługami, które świadczy, oraz urządzeniami końcowymi wykorzystywanymi do korzystania z tych usług. Dostawcy usług o większej skali działania prowadzą specjalne strony poświęcone ochronie przed zagrożeniami. Zaniechanie publikacji informacji wymaganych lub odesłania do właściwych stron internetowych Prezesa UKE jest zagrożone karą pieniężną w stosunku do przedsiębiorcy telekomunikacyjnego lub w stosunku do osoby kierującej przedsiębiorstwem telekomunikacyjnym.

Kolejne ustępy art. 20f, tj. ust. 2 i 3 projektu z dnia 3 lipca 2023 r., dotyczą już sytuacji, w której doszłoby do wystąpienia szczególnego i znacznego zagrożenia wystąpienia incydentu telekomunikacyjnego. Za szczególne zagrożenie uznano takie, które nie jest typowym lub generalnie występującym zagrożeniem, a które stwarza ryzyka dla użytkownika[60]. Zgodnie więc z art. 20f ust. 2 projektu z dnia 3 lipca 2023 r. w przypadku szczególnego i znacznego zagrożenia wystąpienia incydentu telekomunikacyjnego przedsiębiorca komunikacji elektronicznej informowałby swoich użytkowników, na których takie zagrożenie mogło mieć wpływ, o możliwych środkach zapobiegawczych, które użytkownicy ci mogliby podjąć, oraz związanych z tym kosztach. Przedsiębiorca komunikacji elektronicznej

[60] Zob. European Union Agency for Cybersecurity, *Cyber threats outreach in telecom. Guidelines for national authorities and telecom providers on outreach to users about cyber threats*, 2022, s. 21, https://www.enisa.europa.eu/publications/cyber-threats-outreachin-telecom [dostęp: 8.02.2024 r.].

informowałby tych użytkowników o samym zagrożeniu, jeżeli nie spowoduje to zwiększenia poziomu ryzyka dla bezpieczeństwa sieci lub usług komunikacji elektronicznej. W uzasadnieniu projektu z dnia 3 lipca 2023 r. wyjaśniono, że nie jest intencją projektodawcy nakładanie obowiązku informowania użytkowników o każdym zagrożeniu wystąpienia incydentu telekomunikacyjnego. Takie podejście spowodowałoby znaczne obciążenie działów bezpieczeństwa przedsiębiorców. Ponadto, po pewnym czasie wysyłania częstych wiadomości o drobnych zagrożeniach, użytkownicy mogliby zacząć je ignorować, co byłoby niepożądane. Tak jak wyżej wspomniano – obowiązki te pojawiałyby w sytuacji szczególnego i znacznego zagrożenia wystąpienia incydentu telekomunikacyjnego[61]. Pomocą dla przedsiębiorcy komunikacji elektronicznej przy dostosowaniu się do tych wymogów byłyby publikacje ENISA[62].

Ponadto, zgodnie z art. 20f ust. 3 projektu z dnia 3 lipca 2023 r., przedsiębiorca komunikacji elektronicznej informowałby, w tym na swojej stronie internetowej, o incydencie telekomunikacyjnym i jego wpływie na dostępność świadczonych usług, jeżeli w jego ocenie ten wpływ jest istotny. Przepis ten stanowił implementację art. 40 ust. 3 zdanie drugie EKŁE. Przedsiębiorca telekomunikacyjny powinien więc poinformować użytkowników o wystąpieniu szczególnego ryzyka naruszenia bezpieczeństwa sieci wykraczającego poza zwykły poziom ryzyka i standardowe środki bezpieczeństwa. Obowiązek ten wykonuje dostawca usług w stosunku do użytkowników korzystających z jego usług. Jednocześnie, jeżeli istnieją możliwości podniesienia bezpieczeństwa sieci, użytkownicy powinni być o nich poinformowani. Jeżeli podniesienie poziomu bezpieczeństwa wymaga dodatkowych nakładów, użytkownicy powinni być poinformowani o dodatkowych kosztach. Stosowanie dodatkowych środków, a w szczególności urządzeń podnoszących poziom bezpieczeństwa przekazu, nie może naruszać obowiązujących wymogów dotyczących funkcjonowania sieci. Poza obowiązkiem informowania użytkowników przepis art. 20f ust. 3 projektu z dnia 3 lipca 2023 r. nie nakłada na dostawcę obowiązków dotyczących stosowania dodatkowych zabezpieczeń sieci. Przepis ten ma jedynie na celu umożliwienie użytkownikom dostosowania poziomu indywidualnych zabezpieczeń do ich potrzeb, związanych z ochroną dostępu do sieci, funkcjonalności usług oraz treści przekazywanej informacji. Przedsiębiorca może odpłatnie oferować dodatkowe środki zabezpieczające. Przedsiębiorca telekomunikacyjny może także informować innych przedsiębiorców telekomunikacyjnych i podmioty wchodzące

[61] Zob. s. 43 uzasadnienia projektu z dnia 3 lipca 2023 r.

[62] Zob. https://www.enisa.europa.eu/publications/cyber-threats-outreach-in-telecom [dostęp: 8.02.2024].

w skład krajowego systemu cyberbezpieczeństwa o incydentach bezpieczeństwa i wykrytych podatnościach.

Zgodnie z art. 20g projektu z dnia 3 lipca 2023 r. w przypadku stwierdzenia przesyłania komunikatów elektronicznych zagrażających bezpieczeństwu sieci lub usług komunikacji elektronicznej przedsiębiorca komunikacji elektronicznej mógłby zastosować środki polegające na:

1) zablokowaniu przesłania takiego komunikatu;
2) ograniczeniu albo przerwaniu świadczenia usługi komunikacji elektronicznej – w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny stwierdzenia zagrożenia.

Przepis art. 20g projektu z dnia 3 lipca 2023 r. utrzymuje co do zasady obowiązki z art. 175c p.t. Przepis art. 175c ust. 4 p.t. stanowi, że przedsiębiorca telekomunikacyjny nie odpowiada za niewykonanie lub nienależyte wykonanie usług telekomunikacyjnych w zakresie wynikającym z art. 175c ust. 1 p.t. Zdecydowano się zrezygnować z tego rodzaju wyłączenia odpowiedzialności z mocy ustawy. Blokowanie komunikatu elektronicznego, tudzież przerwanie świadczenia usługi komunikacji elektronicznej, powinno być środkiem ostatecznym mającym zapewnić bezpieczeństwo sieci lub usług komunikacji elektronicznej. Przedsiębiorca komunikacji elektronicznej, aby zwolnić się z odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi, musiałby wykazać, że zastosowanie środków z art. 20g projektu z dnia 3 lipca 2023 r. było niezbędne, konieczne oraz nie było innych środków umożliwiających w danej sytuacji zareagowanie na zagrożenie[63].

Zgodnie z art. 20h ust. 1 projektu z dnia 3 lipca 2023 r. Prezes UKE, kierując się rekomendacjami ENISA dotyczącymi raportowania incydentów telekomunikacyjnych:

1) informowałby o wystąpieniu poważnego incydentu telekomunikacyjnego organy regulacyjne innych państw członkowskich oraz ENISA, jeżeli uznałby charakter tego incydentu za istotny;
2) przekazywałby KE oraz ENISA sprawozdanie za rok poprzedni zawierające informacje o poważnych incydentach telekomunikacyjnych.

Przepis ten stanowił implementację art. 40 ust. 2 ostatnie zdanie EKŁE. Wypełniał obowiązki informacyjne Polski wobec UE, której jednym z celów jest zapewnienie wysokiego poziomu odporności sieci i usług komunikacji elektronicznej na swoim terytorium. Bez tych danych nie jest możliwe prowadzenie ewaluacji dotychczasowej polityki w tym obszarze[64].

---

[63] Zob. s. 43 uzasadnienia projektu z dnia 3 lipca 2023 r.

[64] *Ibidem*.

3) Zgodnie z art. 20h ust. 2 projektu z dnia 3 lipca 2023 r. w przypadkach uzasadnionych interesem publicznym Prezes UKE mógłby udostępniać na stronie podmiotowej Biuletynu Informacji Publicznej Urzędu Komunikacji Elektronicznej informację o wystąpieniu poważnego incydentu telekomunikacyjnego. Prezes UKE informowałby niezwłocznie, w terminie nie dłuższym niż trzy dni, przedsiębiorcę komunikacji elektronicznej, u którego wystąpił poważny incydent telekomunikacyjny, o opublikowaniu wskazanej informacji, wraz ze wskazaniem adresu elektronicznego, pod którym udostępniona jest ta informacja (art. 20h ust. 3 projektu z dnia 3 lipca 2023 r.). Przedsiębiorca komunikacji elektronicznej byłby obowiązany udostępniać na swojej stronie internetowej informację o wystąpieniu poważnego incydentu telekomunikacyjnego oraz umieścić adres elektroniczny, niezwłocznie, nie później niż w terminie trzech dni od dnia otrzymania wskazanej informacji (art. 20h ust. 4 projektu z dnia 3 lipca 2023 r.). Prezes UKE mógłby, w drodze decyzji, nałożyć na przedsiębiorcę komunikacji elektronicznej, obowiązek podania do publicznej wiadomości informacji o wystąpieniu poważnego incydentu telekomunikacyjnego, wskazując sposób jej publikacji, jeżeli wskazane wcześniej sposoby opublikowania informacji w niewystarczającym stopniu służą ochronie interesu publicznego (art. 20h ust. 5 projektu z dnia 3 lipca 2023 r.). Celem tych przepisów było zapewnienie możliwości poinformowania społeczeństwa, np. o przyczynach nagłej niedostępności usług komunikacji elektronicznej, która dotknęłaby duże miasto czy nawet większy obszar. Brak informacji o przyczynach takich zdarzeń mógłby doprowadzić do paniki lub do niezadowolenia społecznego, co byłoby niepożądane [65].

## 2.2. Uregulowania w zakresie dostawców sprzętu i usług ICT

Poza zmianami dotyczącymi ściśle kwestii związanych z cyberbezpieczeństwem pojawiają się nowe uregulowania, dotychczas niewystępujące w polskim systemie prawnym, a dotyczące oceny dostawców sprzętu, usług i oprogramowania ICT (art. 1 pkt 58 i n. projektu dnia 3 lipca 2023 r.). Problematyka ta jest niezwykle ważna, gdyż tego rodzaju oceny prowadzić będą do wiążącego kształtowania polityki zakupowej w zakresie sprzętu i oprogramowania przedsiębiorców telekomunikacyjnych. Konsekwencją takiej oceny może być w skrajnym przypadku wyeliminowanie z rynku konkretnego podmiotu gospodarczego.

Zgodnie z art. 64 projektu (art. 1 pkt 58 projektu z dnia 3 lipca 2023 r.) przy Radzie Ministrów działa Kolegium jako organ opiniodawczo-doradczy

[65] *Ibidem*.

w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowych, CSIRT Telco, CSIRT INT, Prezesa UKE i organów właściwych do spraw cyberbezpieczeństwa. Według art. 64a ust. 1 projektu (art. 1 pkt 59 projektu z dnia 3 lipca 2023 r.) przewodniczący Kolegium, działając z urzędu lub na wniosek innego członka Kolegium, może zlecić CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych przez podmioty określone w art. 66a ust. 1 projektu z dnia 3 lipca 2023 r., uwzględniającej informacje przekazane przez państwa członkowskie lub organy Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego oraz przez sektor prywatny. Przewodniczący Kolegium, działając z urzędu lub na wniosek innego członka Kolegium, może zlecić CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania, o którym mowa w art. 66a ust. 2 projektu z dnia 3 lipca 2023 r., sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT (art. 1 pkt 59 projektu z dnia 3 lipca 2023 r.). Wskazane zadania są wykonywane w ramach ustawowych zadań odpowiednio CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT (art. 64a ust. 3 projektu z dnia 3 lipca 2023 r.).

W projektowych zmianach art. 65 k.s.c. rozszerzono także katalog zadań Kolegium do Spraw Cyberbezpieczeństwa m.in. o wyrażanie opinii o decyzji w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. W art. 65 ust. 1 pkt 1a u.k.s.c. otrzymał nowe brzmienie: „planowanych do ustalenia przez Prezesa UKE w projekcie rozstrzygnięcia decyzji w sprawie rezerwacji częstotliwości, o którym mowa w art. 110 ust. 2 ustawy z dnia … – Prawo komunikacji elektronicznej, jeżeli ta decyzja jest wydawana po przeprowadzeniu aukcji, o której mowa w art. 104 ust. 3 pkt 2 ustawy z dnia … – Prawo komunikacji elektronicznej". Ponadto dodano pkt 8 w brzmieniu:

„8) decyzji w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka".

Projekt z dnia 3 lipca 2023 r. w art. 66 w ust. 5 dodał również inne dodatkowe kompetencje dla Kolegium. Zgodnie z nowymi punktami 4–8 Kolegium:

„4) może zlecić CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług, o której mowa w art. 64a ust. 1;

5) może zlecić CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT, o której mowa w art. 64a ust. 2;

6) może wnioskować o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka, o którym mowa w art. 66a ust. 1;
7) powołuje zespół opiniujący, o którym mowa w art. 66a ust. 12 pkt 1, oraz wskazuje przedstawicieli członków Kolegium wchodzących w jego skład;
8) rozstrzyga spór, o którym mowa w art. 66a ust. 12 pkt 2, wskazując właściwego członka zespołu opiniującego".

Projekt z dnia 3 lipca 203 r. w pkt 62 po art. 66 dodał nowe art. 66a–66e w brzmieniu:

„Art. 66a.

4) 1. Minister właściwy do spraw informatyzacji, w celu ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, może wszcząć z urzędu albo na wniosek przewodniczącego Kolegium postępowanie w sprawie uznania dostawcy produktów ICT, usług ICT lub procesów ICT, zwanego dalej «dostawcą sprzętu lub oprogramowania», które są wykorzystywane przez:
5) podmioty krajowego systemu cyberbezpieczeństwa, o których mowa w art. 4 pkt 1 i 2 oraz 3–20,
6) przedsiębiorców komunikacji elektronicznej obowiązanych posiadać aktualne i uzgodnione oraz wprowadzone do stosowania plany działań w sytuacji szczególnego zagrożenia,
7) właścicieli lub posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym

– za dostawcę wysokiego ryzyka".

W uzasadnieniu projektu z 3 lipca 2023 r. wyjaśniono, że zawarty w rozdziale I Konstytucji art. 20 stanowi o ustroju gospodarczym Rzeczypospolitej Polskiej. Opiera się on m.in. na wolności prowadzenia działalności gospodarczej, która polega na możliwości podejmowania działalności gospodarczej w wybranej formie, swobodnego podejmowania decyzji gospodarczych oraz decyzji w sprawie zakończenia działalności. Z kolei art. 22 Konstytucji dopuszcza ograniczenie wolności działalności gospodarczej w drodze ustawy ze względu na ważny interes publiczny. W ślad za tym artykułem Trybunał Konstytucyjny podkreślał w swoim orzecznictwie, że wolność działalności gospodarczej nie ma charakteru absolutnego. W jednym z wyroków TK zaznaczył, że działalność gospodarcza może podlegać różnego rodzaju ograniczeniom w stopniu większym niż prawa i wolności o charakterze osobistym bądź politycznym. Państwo może więc wprowadzić takie przepisy ustawowe, które pozwolą zminimalizować niekorzystne skutki mechanizmów wolnorynkowych, jeżeli skutki te ujawniają się

w sferze, która nie może pozostać obojętna dla państwa ze względu na ochronę powszechnie uznawanych wartości[66]. Z kolei w innym orzeczeniu TK zaznaczył, że rezygnacja z niezbędnych środków kontroli przez państwo niektórych dziedzin gospodarki mogłaby doprowadzić do zagrożenia bezpieczeństwa państwa, porządku publicznego, a także prawno-międzynarodowym zobowiązaniom państwa[67]. W tym kontekście wskazywano, że bezpieczeństwo państwa zostało uznane przez Trybunał Konstytucyjny za element dobra wspólnego, a każdy obywatel jest zobowiązany do troski o dobro wspólne. Obowiązkiem Rady Ministrów jest zapewnienie bezpieczeństwa wewnętrznego i zewnętrznego państwa (art. 146 ust. 4 pkt 7 i 8 Konstytucji)[68].

W uzasadnieniu dalej wyjaśniono, że projektodawca zaproponował wprowadzenie mechanizmu pozwalającego na uznanie określonego dostawcy sprzętu lub oprogramowania dla szczególnego rodzaju podmiotów gospodarczych i społecznych, za dostawcę wysokiego ryzyka. Wskazane w decyzji zakresy produktów ICT, rodzaje usług ICT lub konkretne procesy ICT pochodzące od dostawcy wysokiego ryzyka będą musiały być wycofane z tych podmiotów. Rozwiązanie to ma na celu zapewnienie ochrony ważnego interesu państwowego w postaci bezpieczeństwa państwa[69].

W uzasadnieniu projektu z dnia 3 lipca 2023 r. wyjaśniono, że obecnie nie ma żadnych środków prawnych umożliwiających nakazanie wycofywania z eksploatacji produktów ICT, usług ICT i procesów ICT zagrażających bezpieczeństwu kluczowych podmiotów w Polsce, a przez to funkcjonowaniu państwa. W szczególności dotyczy to kluczowych przedsiębiorców telekomunikacyjnych, którzy będą świadczyć usługi, bazując na mobilnych sieciach 5G[70]. Sieć 5G będzie oferowała możliwość przetwarzania znacznie większej liczby danych oraz wyższe prędkości przekazywania danych w porównaniu do dotychczasowej

---

66 Wyrok TK z dnia 8 kwietnia 1998 r., sygn. akt K 10/97, OTK ZU 1998, nr 3, poz. 29.

67 Wyrok TK z dnia 10 października 2001 r., sygn. akt K 28/01, OTK ZU 2001, nr 7, poz. 212.

68 Uzasadnienie projektu z dnia 3 lipca 2023 r. s. 78.

69 *Ibidem*.

70 Komisja Europejska zdefiniowała sieć 5G jako: „zbiór wszystkich istotnych elementów infrastruktury sieciowej z zakresu technologii łączności ruchomej i bezprzewodowej, wykorzystywanej na potrzeby łączności i usług o wartości dodanej, o zaawansowanych parametrach eksploatacyjnych, takich jak bardzo wysoka prędkość przesyłu danych i przepustowość łączy, łączność charakteryzująca się niskim opóźnieniem, ekstremalnie wysoka niezawodność bądź zdolność obsługi dużej liczby podłączonych urządzeń. Mogą one obejmować elementy dotychczasowych sieci wykorzystujących technologię łączności ruchomej i bezprzewodowej poprzednich generacji, takich jak 4G lub 3G. Sieci 5G należy rozumieć jako obejmujące wszystkie istotne części sieci". Pkt II.2.a Zalecenie Komisji (UE) 2019/534 z dnia 26 marca 2019 r. Cyberbezpieczeństwo sieci 5G (Dz.Urz. UE L 88 z 29.03.2019, s. 42).

sieci 3G oraz 4G. Dzięki sieci 5G możliwe będzie podłączenie znacznie większej liczby urządzeń internetu rzeczy niż do tej pory. Umożliwi to znacznie większe możliwości przekazywania danych pomiędzy obywatelami oraz wpłynie pozytywnie na rozwój gospodarki. Wdrożenie sieci 5G wiąże się z ryzykami, szczególnie tymi związanymi z bezpieczeństwem. Dzięki tym sieciom będzie możliwe świadczenie wielu usług niezbędnych do funkcjonowania rynku wewnętrznego oraz utrzymania i realizacji podstawowych funkcji społecznych i gospodarczych – takich jak energetyka, transport, bankowość i opieka zdrowotna oraz systemy sterowania produkcją. Potencjalny cyberatak mógłby doprowadzić do naruszenia dostępności danej usługi na niespotykaną dotąd skalę. Możliwy byłby atak na sieć 5G, który doprowadziłby do przejęcia kontroli nad infrastrukturą krytyczną, jak np. sieci energetyczne. Przejęcie kontroli nad siecią 5G mogłoby doprowadzić do naruszenia poufności ogromnej liczby przesyłanych danych. Skutki takich incydentów byłyby bardzo poważne[71].

Przewidziane w art. 66a projektu z dnia 3 lipca 2023 r. postępowanie w sprawie uznania dostawcy produktów ICT, usług ICT lub procesów ICT, za dostawcę wysokiego ryzyka, kończy się wydaniem decyzji, która jest w znaczeniu faktycznym i prawnym rozstrzygnięciem o istotnych prawach i obowiązkach podmiotów gospodarczych działających na rynku telekomunikacyjnym w Polsce. Stanowi ona ograniczenie praw podmiotów gospodarczych. W uzasadnieniu projektu wskazano już, że art. 22 Konstytucji RP dopuszcza ograniczenie wolności działalności gospodarczej, ale to ograniczenie, zgodnie z przywołanym przepisem, „jest dopuszczalne tylko w drodze ustawy i tylko ze względu na ważny interes publiczny". Musi więc być wykazany „ważny interes publiczny" uzasadniający tworzenie tego rodzaju ograniczeń. W uzasadnieniu projektu temu ważnemu zagadnieniu poświęca się zaledwie kilka ogólnych zdań. Należy natomiast wyjaśnić, dlaczego ochrona bezpieczeństwa rozumiana jako interes publiczny uzasadnia tak daleko idące zmiany w przepisach, ograniczające prawa przedsiębiorców. W doktrynie i orzecznictwie TK wskazuje się, że aby ustanawiane przez organy władzy publicznej ograniczenia wolności działalności gospodarczej były ograniczeniami usprawiedliwionymi (a tym samym by były one konstytucyjnie legalne), muszą być one nie tylko ukierunkowane na realizację ważnego interesu publicznego, ale równocześnie muszą też być względem tego ważnego interesu publicznego proporcjonalne. Proporcjonalność ustanawianych ograniczeń jest (obligatoryjną) materialną przesłanką usprawiedliwiającą te ograniczenia, przy czym obowiązek spełniania tej przesłanki przez organy władzy publicznej (kreujące ograniczenia wolności działalności gospodarczej) wynika z art. 31

[71] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 79.

ust. 3 Konstytucji RP, mówiącego o wymogu „konieczności" ustanawianych ograniczeń[72]. Powinno być wyjaśnione, dlaczego zamierzonego celu, którym jest zapewnienie cyberbezpieczeństwa, nie można osiągnąć w inny, mniej radykalny sposób niż poprzez wykluczenie konkretnego przedsiębiorcy z rynku dostaw sprzętu telekomunikacyjnego. Projektodawcy powinni w szczególności wyjaśnić, dlaczego i w jakim zakresie, dobru w postaci zapewnienia bezpieczeństwa, mają ustąpić inne dobra, takie jak swoboda prowadzenia działalności gospodarczej, i dlaczego mają one uzasadniać podejmowanie działań o charakterze dyskryminującym, w stosunku do określonych dostawców. Ochrona wolności działalności gospodarczej oznacza nie tylko nakaz równouprawnienia podmiotów gospodarczych, ale przede wszystkim zakaz ich arbitralnej dyskryminacji[73]. Spowoduje to wzrost kosztów dla operatorów telekomunikacyjnych i obywateli, związany z ograniczeniem konkurencji w następstwie ewentualnego wykluczenia określonych dostawców z dostarczania sprzętu oraz koniecznością usunięcia sprzętu już zainstalowanego w sieci operatorów. Konsekwencje finansowe, w szczególności w zakresie możliwości wzrostu cen usług telekomunikacyjnych dla obywateli oraz kosztów dla operatorów, powinny być wyliczone, gdyż tylko wtedy można dokonać prawidłowej oceny skutków finansowych wprowadzonych ograniczeń. Obywatele i przedsiębiorcy powinni wiedzieć, jakie są skutki finansowe i gospodarcze tych regulacji. W zakresie skutków gospodarczych i finansowych w uzasadnieniu projektu wspomina się tylko o kosztach związanych z powoływaniem nowych struktur administracyjnych z zakresu cyberbezpieczeństwa, a w części poświęconej ocenie skutków regulacji, w zakresie wpływu na konkurencyjność oraz przedsiębiorców wspomina się tylko o zmianie obowiązków informacyjnych, a w ogóle nie wskazuje się na skutki ekonomiczne lub finansowe tych regulacji, co jest niezgodne z rzeczywistością, gdyż w sposób oczywisty taki wpływ będzie liczony nawet w miliardach złotych, a będzie on związany z potencjalną koniecznością eliminacji sprzętu tego dostawcy przez operatorów, którzy poniosą realne koszty wymiany sprzętu.

W uzasadnieniu projektu z 3 lipca 2023 r. przypomniano, że kwestia bezpieczeństwa sieci 5G została podjęta na poziomie unijnym. W motywie 3 i 4 zaleceń Komisji (UE) 2019/534 wskazano, że: „(3) Z powodu uzależnienia wielu usług o krytycznym znaczeniu od sieci 5G konsekwencje systemowych i rozległych zakłóceń byłyby szczególnie poważne. W rezultacie zapewnienie

[72] M. Safjan, L. Bosek, *Konstytucja RP. Tom I. Komentarz do art. 1–86*, Warszawa 2016, Nb 102–105 do art. 22.

[73] J. Ciapała, *Konstytucyjna wolność działalności gospodarczej w Rzeczypospolitej Polskiej*, Szczecin 2009, s. 268.

cyberbezpieczeństwa sieci 5G jest kwestią o strategicznym znaczeniu dla Unii w czasie, gdy cyberataki przybierają na sile i są coraz bardziej wyrafinowane. (4) Ponadnarodowy charakter infrastruktury stanowiącej podstawę ekosystemu cyfrowego, która charakteryzuje się siecią wzajemnych powiązań, jak również transgraniczny charakter zagrożeń oznaczają, że wszelkie istotne luki bezpieczeństwa lub cyberincydenty dotyczące sieci 5G występujące w jednym państwie członkowskim miałyby wpływ na całą Unię. Dlatego też należy przewidzieć środki w celu zapewnienia wysokiego wspólnego poziomu cyberbezpieczeństwa sieci 5G". Komisja zaleciła, aby państwa członkowskie przeprowadziły krajową ocenę ryzyka bezpieczeństwa sieci 5G Komisji oraz ENISA. Ponadto Komisja zaleciła, że na podstawie krajowej oceny ryzyka państwa członkowskie powinny:

a) zaktualizować wymogi w zakresie bezpieczeństwa oraz metody zarządzania ryzykiem stosowane w odniesieniu do sieci 5G;
b) zaktualizować odpowiednie obowiązki nakładane na przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej zgodnie z art. 13a i 13b dyrektywy 2002/21/WE;
c) obwarować ogólne zezwolenia warunkami dotyczącymi zabezpieczenia sieci publicznych przed nieuprawnionym dostępem oraz uzyskać od przedsiębiorstw uczestniczących w przyszłych postępowaniach o udzielenie praw użytkowania częstotliwości radiowych w pasmach 5G zobowiązanie do przestrzegania wymogów w zakresie bezpieczeństwa sieci na podstawie dyrektywy 2002/20/WE;
d) stosować inne środki zapobiegawcze mające na celu ograniczenie potencjalnych zagrożeń dla cyberbezpieczeństwa.

Środki te powinny obejmować obowiązki nakładane na dostawców oraz operatorów celem zapewnienia bezpieczeństwa sieci 5G[74].

W wyniku powyższych zaleceń powstały unijna skoordynowana ocena ryzyka cyberbezpieczeństwa sieci 5G[75] oraz Unijny zestaw środków dla cyberbezpieczeństwa sieci 5G – tzw. 5G Toolbox[76]. W dokumentach tych wskazano na ryzyka związane z sieciami 5G, także te związane z dostawcami sprzętu i oprogramowania dla tej sieci. Wśród wskazanych ryzyk jedno dotyczy dostawców, którzy znajdują się pod wpływem państw prowadzących agresywne działania

[74] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 79–80.

[75] *Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks* https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049, zwana *Unijną oceną cyberbezpieczeństwa sieci 5G*.

[76] *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures* https://digitalstrategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures [dostęp: 8.02.2024 r.].

w cyberprzestrzeni. Państwo takie może wpływać na dostawcę, aby wykorzystał ukryte podatności w sprzęcie lub oprogramowaniu dostarczonemu innemu państwu, aby uzyskać dostęp do wrażliwych danych przesyłanych przez ten sprzęt czy też wpływać na dostępność usług świadczonych poprzez ten sprzęt. Dostawca taki będzie działał na rzecz interesów państwa, pod którego wpływem się znajduje. Prawdopodobieństwo zaistnienia tej sytuacji zależy od stopnia, w jakim dostawca ma dostęp do sieci, w szczególności jej krytycznych funkcji[77]. Natomiast ryzyka dotyczą również aspektów technicznych, np. tego, czy dostawca jest w stanie zapewnić bezpieczeństwo swoich produktów, jak reaguje na incydenty związane z tymi produktami, jak zarządza podatnościami własnych produktów. Niska jakość sprzętu i oprogramowania dostarczanego przez dostawcę, w tym ukryte podatności, może umożliwić cyberatak na sieć dokonywany przez inne państwa w cyberprzestrzeni, grupy *Advanced Persistent Threat* czy grupy przestępcze[78]. Z wyżej wskazanych dokumentów wynika więc, że mogą istnieć dostawcy sprzętu lub oprogramowania, którzy poprzez dostarczany sprzęt lub oprogramowanie mogą zagrażać państwom członkowskim UE. Przyjęło się określać takich dostawców jako „dostawców wysokiego ryzyka" (ang. *high risk vendors*). 5G Toolbox wskazuje środki strategiczne, które będą w stanie zmitygować ryzyka wskazane w Unijnej ocenie cyberbezpieczeństwa sieci 5G. Przede wszystkim Toolbox 5G zaleca środki strategiczne:

- SM01 – wzmocnienie roli władz krajowych – środek ten polega m.in. na wyposażeniu władz krajowych w kompetencje do zakazu, ograniczenia lub wprowadzenia wymagań odnośnie do produktów dla sieci 5G, biorąc pod uwagę m.in. bezpieczeństwo krytycznych (ang. *critical and sensitive*) części sieci 5G, ryzyka związane z wpływem państw trzecich na łańcuchy dostaw 5G czy ryzyka dla bezpieczeństwa narodowego;
- SM03 – ocena ryzyka dostawców – przeprowadzenie rygorystycznej oceny ryzyka dostawców, a następnie wprowadzenie niezbędnych wyłączeń w krytycznych zasobach[79].

W swoim komunikacie z 29 stycznia 2020 r. Komisja Europejska wskazała, że „państwa członkowskie zgodziły się co do konieczności oceny profilu ryzyka poszczególnych dostawców i w konsekwencji stosowania odpowiednich ograniczeń wobec dostawców uznanych za stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń, aby skutecznie łagodzić ryzyko w odniesieniu

[77] Zob. Unijna ocena cyberbezpieczeństwa sieci 5G s. 22, przypis 14 i 15, s. 27; 5G Toolbox, s. 43 i 44.

[78] Zob. Unijna ocena cyberbezpieczeństwa sieci 5G pkt 2.51, 5G Toolbox, s. 43.

[79] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 81.

do kluczowych aktywów, jak wskazano w zestawie narzędzi"[80]. W uzasadnieniu projektu z 3 lipca 2023 r. wskazuje się, że zmiany do u.k.s.c. są elementem działań na rzecz wdrożenia postanowień 5G Toolbox. Należy więc zauważyć, że postanowienia 5G Toolbox zostały już uwzględnione co najmniej w znacznej części w polskich przepisach prawa. W Dz.U. z dnia 29 czerwca 2020 r., poz. 1130 zostało opublikowane rozporządzenie Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług. Rozporządzenie to zostało wydane na podstawie art. 175d p.t. W szczególności uwzględnione zostały wymagania Toolbox sformułowane w ramach strategicznych środków w punkcie SM05 – *Ensuring the diveristy of suppliers for individual MNOs through multivendor strategies*, czyli zapewnienia różnorodności w zakresie dostawców infrastruktury dla komórkowych operatorów telekomunikacyjnych. Wymagania te realizują postanowienia § 3 ust. 1 pkt 2 rozporządzenia z 22 czerwca 2020 r. Zgodnie z tym przepisem przedsiębiorca telekomunikacyjny dostarczający sieć piątej generacji (5G) „stosuje strategię skutkującą brakiem uzależnienia się od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług".

W art. 66a projektu z dnia 3 lipca 2023 r. została dodana kompetencja ministra właściwego do spraw informatyzacji do przeprowadzenia postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. W uzasadnieniu projektu wyjaśniono, że postępowanie to będzie prowadzone w celu ochrony ważnych interesów państwowych w postaci bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego. Wspomniano już, że kwestia cyberbezpieczeństwa sieci 5G jest kwestią ważną dla Unii Europejskiej z uwagi na współzależności pomiędzy sieciami telekomunikacyjnymi państw członkowskich UE. Ze względu na potencjalne szkody, które może przynieść zakłócenie funkcjonowania tych sieci, jest to również materia dotycząca bezpieczeństwa państwa. Przepis ten nie ogranicza się wyłącznie do sieci 5G. Postępowaniu będzie mógł być poddany dostawca produktów, usług i procesów ICT nie tylko dla sieci 5G, ale również dla innych systemów informacyjnych, jeżeli zostanie spełniona przesłanka zapewnienia ochrony bezpieczeństwa państwa[81].

W rozumieniu art. 66a ust. 1 projektu z dnia 3 lipca 203 r. dostawcą sprzętu lub oprogramowania jest dostawca produktów ICT, usług ICT lub procesów

[80] https://eur-lex.europa.eu/legalcontent/PL/TXT/?uri=COM:2020:0050:FIN&_sm_au_=iVVZRW54FHZ10n2PVkFHNKt0jRsMJ [dostęp: 8.02.2024 r.].

[81] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 82.

ICT[82]. Zgodnie z tą definicją dostawcy może to być producent, importer, dystrybutor. Postępowaniem będą mogły być objęte wszystkie podmioty kluczowe w łańcuchu dostaw. Postępowanie nie będzie dotyczyło wszystkich produktów, usług i procesów ICT pochodzących od konkretnego dostawcy sprzętu lub oprogramowania, lecz tylko tych, które są wykorzystywane przez:

1) podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorów usług kluczowych, dostawców usług cyfrowych, czy podmiotów publicznych:
   a) operatorów usług kluczowych świadczących usługi kluczowe, które mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej,
   b) dostawców usług cyfrowych świadczących usługi cyfrowe (internetowe platformy handlowe, usługi przetwarzania w chmurze, wyszukiwarki internetowe), które są niezbędne dla zapewnienia funkcjonowania współczesnego społeczeństwa informacyjnego,
   c) podmioty publiczne realizujące, za pomocą systemów informacyjnych, zadania publiczne na rzecz obywateli;
2) przedsiębiorców telekomunikacyjnych obowiązanych posiadać aktualne i uzgodnione plany działań w sytuacji szczególnego zagrożenia (obecnie, na gruncie prawa telekomunikacyjnego, jest to 69 podmiotów). Przedsiębiorcy ci mają za zadanie m.in. współpracę z podmiotami i służbami wykonującymi zadania w zakresie: ratownictwa, niesienia pomocy ludności, obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego;
3) właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 u.z.k. (w uzasadnieniu projektu z dnia 3 lipca 2023 r. zwani operatorami infrastruktury krytycznej – grupa 100–200 podmiotów). Operatorzy infrastruktury krytycznej zarządzają infrastrukturą krytyczną, którą stanowią systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców[83].

---

[82] Produktem ICT jest element lub grupa elementów systemu informacyjnego. Usługą ICT jest usługa polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem systemów informacyjnych. Procesem ICT jest zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT. Definicja systemu informacyjnego obejmuje także sieć telekomunikacyjną, por. Sejm RP VIII kadencji, druk nr 2505, *Rządowy projekt ustawy o krajowym systemie cyberbezpieczeństwa*, uzasadnienie, s. 18–19, https://sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=2505 [dostęp: 8.02.2024 r.].

[83] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 82–83.

W uzasadnieniu projektu z 3 lipca 2023 r. wyjaśnia się, że podmioty te są szczególnie ważne dla zapewnienia bezpieczeństwa państwa, dlatego konieczne jest, żeby korzystały z bezpiecznego sprzętu lub oprogramowania w trakcie świadczenia usług na rzecz państwa i obywateli. Wskazuje się, że choć niniejszą nowelizacją dodaje się do podmiotów krajowego systemu cyberbezpieczeństwa przedsiębiorców komunikacji elektronicznej, to niniejsze postępowanie ma dotyczyć sprzętu lub oprogramowania wykorzystywanego przez przedsiębiorców komunikacji elektronicznej sporządzających plany działań w sytuacjach szczególnych zagrożeń[84].

Projekt z dnia 3 lipca 2023 r. określa podmioty, których może dotyczyć postępowanie w sprawie dostawcy. Nie jest natomiast precyzyjnie określone, co będzie przedmiotem tego postępowania. Z postanowień art. 66a ust. 1 projektu wynika tylko, że postępowanie jest prowadzone w sprawie uznania dostawcy produktów ICT, usług ICT lub procesów ICT, za dostawcę wysokiego ryzyka. Nie jest natomiast wskazane, jakich produktów czy usług ma dotyczyć postępowanie. W przypadku, gdyby ocenie miały podlegać urządzenia lub oprogramowanie dla sieci telekomunikacyjnych, należałoby wyraźnie wskazać, że ocenie podlega dostawca w zakresie oferowanych urządzeń lub oprogramowania dla sieci 5G, a nie np. dla sieci 4G, sieci stacjonarnej lub terminali abonenckich. Wszczęcie z urzędu albo na wniosek przewodniczącego Kolegium postępowania w sprawie uznania dostawcy za dostawcę wysokiego ryzyka powinno zawierać uzasadnienie. Projektowany system oceny będzie miał zastosowanie uniwersalne, nie tylko do obszaru sieci 5G, ale także wobec wszelkich innych zastosowań u podmiotów krajowego systemu cyberbezpieczeństwa, w tym operatorów usług kluczowych, tj. m.in.: sektora energetyki, finansowego, ochrony zdrowia czy transportu. W związku z tym brak precyzji w zakresie kreślenia przedmiotu postępowania może skutkować tym, że np. wykluczenie dokonane wobec danego dostawcy będzie potencjalnie uzasadnione wobec jednego sektora, ale w drugim spowoduje istotne i nieoczekiwane konsekwencje, które trudno będzie naprawić.

Wniosek przewodniczącego Kolegium o wszczęcie postępowania w sprawie uznania dostawcy za dostawcę wysokiego ryzyka powinien zawierać:

– identyfikację urządzeń lub oprogramowania dostawcy, które mają podlegać ocenie ryzyka, a w przypadku dokonywania oceny w zakresie sieci lub usług komunikacji elektronicznej wskazanie konkretnych typów sieci i jej warstw lub usług, których ocena ryzyka i jej konsekwencje mają dotyczyć. Podobnie jak w przypadku procedur certyfikacji należy wyraźnie określać, co jest

[84] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 83.

oceniane. Inne ryzyko rodzi wykorzystywanie radiolinii, a inne elementy pasywne anteny danego producenta;
- identyfikację podmiotów, które wykorzystują lub mogą wykorzystywać urządzenia lub oprogramowanie dostawcy, które mają podlegać ocenie ryzyka, w tym wskazanie, czy są to podmioty krajowego systemu cyberbezpieczeństwa czy przedsiębiorcy komunikacji elektronicznej;
- identyfikację poziomu wykorzystania sprzętu lub oprogramowania w realizacji przez przedsiębiorców telekomunikacyjnych obowiązków wynikających ze stanów nadzwyczajnych i stanu wojny;
- identyfikację poziomu zobowiązań przedsiębiorców telekomunikacyjnych i użytkowników końcowych wobec dostawcy;
- identyfikację innych podmiotów działających na tym samym rynku co oceniany dostawca, w zakresie urządzeń i oprogramowania, w którego zakresie ma zostać dokonana ocena;
- określenie, jakiego zakresu dotyczy ocena, tj. czy np. powszechnego użycia (usługa masowa) czy np. użycia w określonych systemach czy usługach (np. rejestry państwowe, określone kategorie przemysłu, określone strategiczne lokalizacje);
- identyfikację skali działań mających zostać podjętych przez przedsiębiorstwa telekomunikacyjne, podmioty publiczne i użytkowników końcowych, w tym kosztów;
- identyfikację rozwiązań alternatywnych działań w stosunku do sprzętu lub oprogramowania danego dostawcy;.
- uzasadnienie wniosku, w tym przedstawienie potencjalnych ryzyk związanych z wykorzystaniem urządzeń lub oprogramowania danego dostawcy.

Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka stosuje się, jeżeli ustawa nie stanowi inaczej, przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, z wyłączeniem art. 28, art. 31, art. 51, art. 66a i art. 79 tej ustawy (art. 66a ust. 2 projektu z dnia 3 lipca 2023 r.). W uzasadnieniu projektu wyjaśniono[85], że dzięki temu dostawca sprzętu lub oprogramowania będzie brał udział w postępowaniu na prawach strony, z odmiennościami wynikającymi ze szczególnych regulacji wynikających z przepisów nowelizacji. W postępowaniu nie będą stosowane przepisy następujących artykułów k.p.a.:
- art. 28 – projekt wprowadza wyjątek, że w tym szczególnym postępowaniu stroną postępowania jest każdy, wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka;

[85] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 83–84.

– art. 31 – wyłącza się udział organizacji społecznej w postępowaniu;
– art. 51 – wyłącza się przepis, który zawęża osobiste stawiennictwo do obrębu gminy lub miasta, w którym zamieszkuje albo przebywa osoba, jak również sąsiedniej gminy albo miasta;
– art. 66a – wyłącza się przepis dotyczący prowadzenia metryki sprawy;
– art. 79 – wyłącza się przepis o udziale strony w przeprowadzeniu dowodu.

W uzasadnieniu projektu wyjaśniono, że wyłączenia tych przepisów k.p.a. są niezbędne ze względu na szczególny charakter tego postępowania, które ma na celu zapewnienie bezpieczeństwa narodowego. W celu usprawnienia przebiegu postępowania i wzmocnienia trwałości rozstrzygnięć konieczne jest zawężenie przymiotu strony oraz udziału organizacji społecznej, mając na względzie, że do każdego takiego postępowania według zasad ogólnych mogłoby przystąpić na prawach strony nawet setki podmiotów korzystających z konkretnych produktów pochodzących od konkretnego dostawcy sprzętu lub oprogramowania. Wyłączenie art. 28 k.p.a. jest konieczne, ponieważ postępowanie jest wszczynane z urzędu przez ministra albo na wniosek przewodniczącego Kolegium – co za tym idzie – stroną jest każdy, wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Wskazano, że podobne rozwiązanie znajduje się w art. 88 ust. 1 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów. Z kolei wyłączenie art. 31 k.p.a. wynika ze szczególnego związku tego postępowania z kwestiami bezpieczeństwa narodowego. Ze względu na ogólnopolski zasięg decyzji, jaka ma zostać wydana w tym postępowaniu, został także wyłączony art. 51 k.p.a. W uzasadnieniu wyjaśniono także, że kwestia metryki sprawy przy tego typu postępowaniu jest złożona. Obowiązkowo w ramach postępowania o uznaniu dostawcy za dostawcę wysokiego ryzyka będą przeprowadzane szerokie analizy podmiotu, którego dotyczy postępowanie, oraz jego produktów. Ujawnienie nazwisk osób, które przeprowadzały te analizy, mogłoby narazić je na działania ze strony podmiotów zainteresowanych konkretnym wynikiem sprawy. Ponadto wiele osób to funkcjonariusze, których tożsamość, ze względu na wykonywane zadania, musi być chroniona. Z powyższych względów wyłączony został również art. 66a k.p.a. W związku z wrażliwym charakterem informacji, jakie będą wykorzystywane w ramach tego postępowania, konieczne jest wyłączenie udziału strony z przeprowadzanych dowodów[86].

Zgodnie z art. 66a ust. 3 projektu z dnia 3 lipca 2023 r. stroną postępowania w sprawie uznania za dostawcę wysokiego ryzyka jest każdy, wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka.

[86] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 84.

Projekt wyłącza więc stosowanie art. 28 k.p.a., który definiuje stronę postępowania administracyjnego, a w to miejsce wprowadza węższą definicję strony, którą miałby być ten, wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Wydana w wyniku takiego postępowania decyzja spowoduje jednak powstanie, z mocy prawa, obowiązków po stronie podmiotów wskazanych w art. 66a ust. 1 pkt 1–3 projektu z dnia 3 lipa 2023 r. (niewprowadzanie lub wycofanie z użytkowania danych produktów, usług lub procesów dostarczanych przez dostawcę, którego dotyczy decyzja). Projekt pozbawia więc statusu strony podmioty, które na podstawie k.p.a. przymiot ten posiadałyby, co wpływa na ocenę interesu prawnego na gruncie p.p.s.a., a w konsekwencji możliwości wniesienia skargi do sądu (istnienie prawa do sądu)[87].

Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka może przystąpić, na wniosek na prawach strony, przedsiębiorca komunikacji elektronicznej, który w poprzednim roku obrotowym uzyskał przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych[88]. Przepisy art. 31 § 2 i 3 k.p.a. stosuje się odpowiednio (art. 66a ust. 4 projektu z dnia 3 lipca 2023 r.). Za poprzedni rok obrotowy uznaje się rok, przed którym postępowanie zostało wszczęte. Za ostatni komunikat Prezesa Głównego Urzędu Statystycznego uznaje się ostatni komunikat Prezesa Głównego Urzędu Statystycznego przed wszczęciem postępowania (art. 66a ust. 5 projektu z dnia 3 lipca 2023 r.). W uzasadnieniu projektu wyjaśniono, że umożliwiono w ten sposób przystąpienie do postępowania na prawach strony kilkunastu największych przedsiębiorców komunikacji elektronicznej. Będą to tacy przedsiębiorcy komunikacji elektronicznej, którzy w poprzednim roku obrotowym uzyskali przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej, wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych. Aby przystąpić do postępowania, taki przedsiębiorca będzie obowiązany złożyć stosowny wniosek. Zmiana

[87] Zob. H. Mądrzak, *Prawo do sądu jako gwarancja ochrony praw człowieka*, w: L. Wiśniewski (red.), *Podstawowe prawa jednostki i ich sądowa ochrona*, Warszawa 1997, s. 197; B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2012, Nb 4 do art. 45.

[88] Dz.U. z 2022 r. poz. 504, 1504 i 2461.

odpowiada na postulaty strony społecznej, jednocześnie zapewniając sprawny przebieg postępowania[89].

Zgodnie z art. 66a ust. 6 projektu z dnia 3 lipca 2023 r. minister właściwy do spraw informatyzacji zawiadamia o wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Zawiadomienie udostępnia się także w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji niezwłocznie po doręczeniu tego zawiadomienia. Według art. 66a ust. 7 projektu z dnia 3 lipca 2023 r., jeżeli dostawcą sprzętu lub oprogramowania jest strona niemająca siedziby na terytorium państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej albo państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu – stronie umowy o Europejskim Obszarze Gospodarczym zawiadomienie, o którym mowa w ust. 6, udostępnia się w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji. Udostępnienie ma skutek doręczenia po upływie 14 dni od dnia jego dokonania. W uzasadnieniu wyjaśniono, że przepis ten stanowi szczególną regulację w stosunku do zasad doręczeń określonych w k.p.a. Zawiadomienie o wszczęciu postępowania wobec dostawcy, który ma siedzibę na terytorium Unii Europejskiej, Konfederacji Szwajcarskiej czy państwa członkowskiego EFTA będzie doręczane na zasadach ogólnych wynikających z k.p.a. Natomiast po otrzymaniu potwierdzenia doręczenia informacja o tym będzie publikowana na stronie Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, aby uprawnieni przedsiębiorcy telekomunikacyjni mogli złożyć wniosek o dopuszczenie do postępowania na prawach strony[90].

Zgodnie z art. 66a ust. 8 projektu z dnia 3 lipca 2023 r. przed rozstrzygnięciem sprawy minister właściwy do spraw informatyzacji zasięga opinii Kolegium. Kolegium przekazuje opinię w terminie trzech miesięcy od dnia wystąpienia o opinię. Okresu od dnia wystąpienia o opinię do dnia otrzymania opinii nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 k.p.a. nie stosuje się. Przepis ten stanowi, że zajęcie stanowiska przez organ następuje w drodze postanowienia, na które służy stronie zażalenie. W uzasadnieniu projektu wyjaśniono, że postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek przewodniczącego Kolegium. Minister właściwy do spraw informatyzacji jest odpowiedzialny za bezpieczeństwo cyberprzestrzeni w wymiarze cywilnym, stąd też zasadne jest, aby to on prowadził tego rodzaju postępowanie. Przed wydaniem decyzji minister właściwy ds. informatyzacji będzie obowiązany zwrócić się

[89] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 85.

[90] *Ibidem*.

do Kolegium o wydanie opinii w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Kolegium będzie miało trzy miesiące, licząc od dnia wystąpienia o opinię, na przekazanie jej do ministra. Termin od dnia wystąpienia o opinię do dnia otrzymania opinii nie będzie wliczał się do terminu załatwienia sprawy[91].

Powstaje pytanie, czy można zaskarżyć opinie Kolegium na podstawie p.p.s.a. w trybie zaskarżania aktów z zakresu administracji publicznej. Opinie Kolegium można bowiem zaliczyć do kategorii spraw, o których mówi art. 3 § 2 pkt 4 p.p.s.a. Zgodnie z tym przepisem kontrola działalności administracji publicznej przez sądy administracyjne obejmuje orzekanie w sprawach skarg na inne niż określone w pkt 1–3 akty lub czynności z zakresu administracji publicznej dotyczące uprawnień lub obowiązków wynikających z przepisów prawa, z wyłączeniem aktów lub czynności podjętych w ramach postępowania administracyjnego określonego w k.p.a., postępowań określonych w działach IV, V i VI ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa, postępowań, o których mowa w dziale V w rozdziale 1 ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej oraz postępowań, do których mają zastosowanie przepisy powołanych ustaw. Przedmiotem skargi do sądu administracyjnego mogą więc być akty lub czynności, które:

1) nie mają charakteru decyzji lub postanowienia, gdyż te są zaskarżalne na podstawie art. 3 § 2 pkt 1–3 p.p.s.a.[92];
2) są podejmowane w sprawach indywidualnych, ponieważ akty o charakterze ogólnym zostały wymienione w art. 3 § 2 pkt 5 i 6 p.p.s.a.;
3) muszą mieć charakter publicznoprawny[93];
4) dotyczą uprawnień lub obowiązków wynikających z przepisu prawa[94];
5) nie mogą być podjęte w ramach postępowania administracyjnego określonego w k.p.a. lub w Ordynacji podatkowej bądź ustawy o Krajowej Administracji Skarbowej.

Wskazane elementy są określane jako konstytuujące pojęcie aktu lub czynności z art. 3 § 2 pkt 4 p.p.s.a.[95] Analogiczne stanowisko jest także prezentowane

---

[91] *Ibidem*.

[92] Zob. szerzej M. Bogusz, *Pojęcie aktów lub czynności z zakresu administracji publicznej dotyczących stwierdzenia lub uznania uprawnienia lub obowiązku wynikających z przepisów prawa w rozumieniu art. 16 ust. 1 pkt 4 ustawy o NSA*, „Samorząd Terytorialny" 2000, nr 1–2, s. 180.

[93] B. Dauter, B. Gruszczyński, A. Kabat, M. Niezgódka-Medek, *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, Warszawa 2009, s. 30.

[94] Zob. postanowienie NSA z 28.11.2005 r., I OSK 1756/06, LEX nr 2207747.

[95] Zob. B. Adamiak, *Z problematyki właściwości sądów administracyjnych (art. 3 § 2 pkt 4 p.p.s.a.)*, „Zeszyty Naukowe Sądownictwa Administracyjnego" 2006, nr 2, s. 9.

w orzecznictwie sądów administracyjnych[96]. Wymienione w art. 3 § 2 pkt 4 p.p.s.a. akty mają bardziej sformalizowany charakter niż czynności, które są działaniami faktycznymi, wywołującymi następstwa w zakresie uprawnień lub obowiązków[97]. W praktyce to na sądach administracyjnych będzie spoczywać obowiązek każdorazowego ustalenia, czy wskazany w skardze do sądu akt lub czynność spełnia przesłanki warunkujące uznanie za potencjalny przedmiot kontroli sądu na podstawie art. 3 § 2 pkt 4 p.p.s.a.[98] Ocena taka powinna być zawsze dokonywana z uwzględnieniem konstytucyjnej gwarancji prawa do sądu[99]. Należy przyjąć, że opinia Kolegium nie ma charakteru decyzji lub postanowienia, o których mowa w art. 3 § 2 pkt 1–3 p.p.s.a. Opinia Kolegium jest podejmowana w sprawie indywidualnej, ponieważ akty o charakterze ogólnym zostały wymienione w art. 3 § 2 pkt 5–7 p.p.s.a. Prezentowany jest także pogląd, że akty lub czynności o charakterze indywidualnym (art. 3 § 2 pkt 4 p.p.s.a) nie muszą być podejmowane w sytuacjach konkretnych ani w stosunku do konkretnego adresata, co pozwala na przyjęcie szerszej interpretacji zakresu kognicji sądownictwa administracyjnego w zakresie stosowania art. 3 § 2 pkt 4 p.p.s.a.[100] Opinia Kolegium ma charakter indywidualny, gdyż będzie skierowana do określonych dostawców infrastruktury telekomunikacyjnej. W przypadku dostawców infrastruktury telekomunikacyjnej, także ze względu na ograniczony krąg takich podmiotów w Polsce, łatwo jest ich zidentyfikować. Opinia Kolegium ma także charakter publicznoprawny, gdyż jest aktem z zakresu administracji publicznej, wydawanym przez Kolegium, czyli organ administracji publicznej, realizujący kompetencje w obszarze prawa publicznoprawnego. Opinia Kolegium dotyczy uprawnień lub obowiązków wynikających z przepisów materialnego prawa administracyjnego. W przypadku opinii Kolegium uprawnienia i obowiązki wynikają z przepisów u.k.s.c. Wszystko to uzasadnia przyjęcie, że każdemu, kto ma w tym interes prawny, przysługuje

---

96 Zob. wyrok WSA w Olsztynie z 20.09.2006 r., II SA/Ol 456/06, LEX nr 193384.

97 Zob. M. Jaśkowska, *Akty i czynności z zakresu administracji publicznej w rozumieniu art. 16 ust. 1 pkt 4 ustawy o Naczelnym Sądzie Administracyjnym jako przedmiot kontroli*, w: J. Stelmasiak, J. Niczyporuk, S. Fundowicz (red.), *Polski model sądownictwa administracyjnego*, Lublin 2003, s. 168.

98 Zob. J.P. Tarno, *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, Warszawa 2008, s. 33.

99 Zob. R. Hauser (red.), *System prawa administracyjnego*, t. 10: *Postępowanie przed sądami administracyjnymi*, Warszawa 2016, s. 179.

100 Zob. M. Jaśkowska, *Właściwość sądów administracyjnych [zagadnienia wybrane]*, w: J. Zimmermann (red.), *Koncepcja systemu prawa administracyjnego. Zjazd Katedr Prawa Administracyjnego i Postępowania Administracyjnego, Zakopane, 24–27 września 2006 r.*, Warszawa 2007, s. 587 i n.

skarga do Wojewódzkiego Sądu Administracyjnego na akt z zakresu administracji publicznej (art. 3 § 2 pkt 4 p.p.s.a.) w postaci opinii Kolegium[101].

W projekcie z dnia 3 lipca 2023 r. powinny być jednak wskazane wprost środki odwoławcze, które pozwalałyby na ich wniesienie przez podmiot niezadowolony z dokonanej oceny ryzyka dostawcy (opinii Kolegium) do organów sprawujących wymiar sprawiedliwości. Wymiar sprawiedliwości polega na wyrokowaniu poprzez podejmowanie konkretnych decyzji władczych o prawach i obowiązkach podmiotów indywidualnych, na podstawie norm generalnych i abstrakcyjnych, zgodnie z odpowiednimi przepisami proceduralnymi i normami kompetencji (właściwości) decyzyjnej. Wymiar sprawiedliwości sprawują, zgodnie z art. 175 Konstytucji RP, w szczególności sądy administracyjne. W sposób oczywisty Kolegium nie posiada cech sądu. Od rozstrzygnięcia opinii Kolegium powinny więc być wyraźnie określone środki odwoławcze do sądu.

Zgodnie z art. 66a ust. 9 projektu z dnia 3 lipca 2023 r. opinia Kolegium powinna zawierać analizę:

1) zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania, z uwzględnieniem informacji o zagrożeniach uzyskanych od państw członkowskich lub organów Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego;
2) prawdopodobieństwa, z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem:
   a) przepisów prawa regulujących stosunki między dostawcą sprzętu lub oprogramowania a tym państwem oraz praktyki stosowania prawa w tym zakresie,
   b) prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, w szczególności w przypadku, gdy nie ma porozumień w zakresie ochrony tych danych między Unią Europejską i tym państwem,
   c) struktury własnościowej dostawcy sprzętu lub oprogramowania,
   d) zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania;
3) trybu, zakresu i rodzaju powiązań dostawcy sprzętu lub oprogramowania z podmiotami określonymi w załączniku do rozporządzenia Rady (UE)

[101] Zob. M. Rogalski, *Środki zaskarżenia w aukcji prowadzonej na podstawie przepisów Prawa telekomunikacyjnego w celu rozdysponowania częstotliwości*, „Przegląd Ustawodawstwa Gospodarczego" 2021, nr 10, s. 22–24.

2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim[102];

4) liczby i rodzajów wykrytych podatności i incydentów dotyczących typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;
5) trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w art. 66a ust. 1 pkt 1–3 projektu z dnia 3 lipca 2023 r., oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;
6) treści wydanych rekomendacji, o których mowa w art. 33 ust. 4 u.k.s.c., dotyczących sprzętu lub oprogramowania danego dostawcy.

W uzasadnieniu projektu wyjaśniono, że art. 66a ust. 9 projektu z dnia 3 lipca 2023 r. posiada wskazanie elementów analizy, która ma być zawarta w opinii Kolegium. Nawiązują one do pkt. 2.37 raportu Unii Europejskiej dotyczącego unijnej oceny ryzyka cyberbezpieczeństwa sieci 5G[103]. Celem opinii Kolegium jest kompleksowa analiza działalności dostawcy sprzętu lub oprogramowania. W skład Kolegium wchodzą ministrowie kluczowi dla bezpieczeństwa państwa, a także szefowie służb specjalnych. Będą więc w stanie pozyskać niezbędne informacje do oceny dostawcy od swoich jednostek podległych lub nadzorowanych. Zasadne jest, aby opinia podejmowała kwestie zagrożeń, które stwarza dostawca. Nie są to jednak zwykłe zagrożenia, lecz takie, które wpływają na bezpieczeństwo narodowe. Przepis art. 66a ust. 9 pkt 1 projektu z dnia 3 lipca 2023 r. precyzuje, że chodzi o zagrożenia w wymiarze ekonomicznym, wywiadowczym oraz terrorystycznym. Ponadto konieczna będzie analiza zagrożeń, które stwarza dostawca dla zobowiązań sojuszniczych (np. w ramach NATO czy innych umów międzynarodowych), a także europejskich. Niewątpliwie zobowiązaniem europejskim jest zapewnienie na poziomie unijnym wysokiego poziomu bezpieczeństwa systemów informacyjnych (co wynika z dyrektywy NIS/NIS 2) oraz bezpieczeństwa sieci i usług komunikacji elektronicznej (co wynika z EKŁE). Uzasadnienie dalej wyjaśnia, że kolejnym aspektem opinii powinna być analiza prawdopodobieństwa, z jakim dostawca znajduje się pod wpływem państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu

[102] Dz.Urz. UE L 129I z 17.05.2019, s. 1, ze zm.

[103] *Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks*, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049 [dostęp: 15.10.2023 r.].

Północnoatlantyckiego (at.t. 66a ust. 9 pkt 2 projektu z dnia 3 lipca 2023 r.). Ta część opinii skupiać się ma na powiązaniach dostawcy sprzętu lub oprogramowania z państwem spoza Unii Europejskiej oraz NATO. Wpływ ten może obejmować prawodawstwo danego państwa, które reguluje stosunki między państwem a dostawcą (np. w zakresie swobody działalności gospodarczej czy bezpieczeństwa przetwarzanych danych). W uzasadnieniu wskazuje się, że Kolegium powinno uwzględnić także praktykę stosowania tych przepisów, aby sprawdzić, jak one funkcjonują – np. czy gwarancje zawarte w tych przepisach rzeczywiście są respektowane przez dane państwo. Z uwagi na to, że współcześnie coraz więcej danych osobowych jest przesyłanych poza Unię Europejską, ważna jest także kwestia ochrony danych osobowych w danym państwie i kwestia faktycznego stosowania tych przepisów. Opinia będzie także zawierała analizę struktury własnościowej dostawcy sprzętu lub oprogramowania. Chodzi tutaj o ustalenie, kto faktycznie sprawuje kontrolę własnościową nad dostawcą. Ostatecznie powinny być sprawdzone możliwości wpływu danego państwa na dostawcę. Opinia będzie więc dotyczyła otoczenia regulacyjnego dostawcy, faktycznego stosowania prawa, struktury własnościowej aż po realny wpływ państwa na dostawcę. Po dokonaniu analiz uzyskany zostanie całościowy obraz relacji między dostawcą a państwem[104].

W uzasadnieniu projektu wyjaśniono także, że rozporządzeniem wykonawczym Rady (UE) 2020/1125 z dnia 30 lipca 2020 r. wykonującym rozporządzenie (UE) 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim Unia Europejska wskazała podmioty, które dokonują cyberataków na Unię lub jej państwa członkowskie. Wskazane jest, aby opinia Kolegium dotyczyła również informację, jakie są relacje pomiędzy tymi podmiotami a dostawcą sprzętu lub oprogramowania. Jak już wyżej wspomniano, ryzyka dotyczą również aspektów technicznych produktów, usług i procesów ICT dostarczanych przez dostawcę. Dlatego do technicznych aspektów opinii należy analiza:

1) liczby i rodzajów wykrytych podatności i incydentów dotyczących zakresu typów produktów ICT lub rodzajów usług ICT, lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;
2) trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w art. 66a ust. 1 pkt 1–4 projektu z 3 lipca 2023 r., oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;

[104] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 85–86.

3) treści wydanych wcześniej rekomendacji, o których mowa w art. 33 ust. 4 u.k.s.c., dotyczących sprzętu lub oprogramowania danego dostawcy. Jest to związane z potencjalnymi ryzykami, które wiążą się z niską jakością sprzętu lub oprogramowania[105].

Przepis art. 66a ust. 9 projektu z dnia 3 lipca 2023 r. jest bardzo ważny, gdyż kluczowym zagadnieniem jest to, według jakich kryteriów ocena zostanie przeprowadzona. Ocena musi być bowiem dokonywana przy pomocy precyzyjnie określonych, jasnych, niebudzących wątpliwości i weryfikowalnych kryteriów. Nie mogą to być kryteria posługujące się pojęciami niezdefiniowanymi, pozwalającymi na wieloznaczne oceny. W przeciwnym razie nie będzie to ocena obiektywna, ale uznaniowa, pozbawiona merytorycznych podstaw, prowadząca do błędnych wniosków. Przykładowo wiele wątpliwości może budzić kryterium sformułowane w art. 66a ust. 9 pkt 2 projektu z dnia 3 lipca 2023 r., dotyczące „prawdopodobieństwa, z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego". Kryterium to jest niejasne i rodzi następujące pytania: o jaki stopień prawdopodobieństwa chodzi w tym przepisie; co to znaczy być pod kontrolą państwa; czy chodzi o politykę, ekonomię itp.; czy wpływ państwa powinien zawsze być oceniany negatywnie? Ocena na podstawie kraju pochodzenia niesie ze sobą ryzyko dyskryminacyjnego traktowania innego państwa.

Przewidziane w art. 66a ust. 9 projektu z dnia 3 lipca 2023 r. kryteria oraz związany z nim mechanizm oceny przez Kolegium może budzić wątpliwości także co do zgodności z wymaganiami określonymi w 5G Toolbox w zakresie środków strategicznych (s. 12 5G Toolbox). Chodzi o środek określony jako SM03, zgodnie z którym ocena profilu ryzyka dostawców i zastosowanie ograniczeń do dostawców uznanych za wysokiego ryzyka powinna następować w odniesieniu do kluczowych aktywów. Mechanizm oceny przewidziany w projekcie oraz związane z nim kryteria oceny nie uwzględniają natomiast wpływu dostawcy na *key assets* (aktywa kluczowe)[106]. Zaproponowany mechanizm oceny dostawcy w projekcie nie uwzględnia kategorii aktywów z punktu widzenia bezpieczeństwa, wraz z ich poziomem wrażliwości oraz wykazem kluczowych elementów (kategorie elementów i funkcji). Niewłaściwe jest nałożenie takich samych zobowiązań na wszystkie aktywa, gdyż wpływ części aktywów na bezpieczeństwo infrastruktury telekomunikacyjnej jest znikomy. W tym więc zakresie projekt nie uwzględnia wymagań SM03 5G Toolbox, a ściśle zalecenia w zakresie oceny wpływu kluczowych aktywów (*key assets*).

---

[105] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 87.

[106] Pojęcie *key assets* (aktywa kluczowe) jest wyjaśnione na s. 21 5G Toolbox.

Postanowienia art. 66a ust. 9 pkt 2 lit. a i c–d projektu z 3 lipca 2023 r., określające kryteria przeprowadzania oceny, mogą zostać uznane za sprzeczne z przepisami § 6 z.t.p. Zgodnie z tym paragrafem przepisy ustawy redaguje się tak, aby dokładnie i w sposób zrozumiały dla adresatów zawartych w nich norm wyrażały intencje prawodawcy. Wskazane postanowienia art. 66a ust. 9 pkt 2 lit. a i c–d projektu, naruszają przepis § 6 z.t.p., gdyż są niezrozumiałe i nie jest możliwe na podstawie tych postanowień projektu ustalenie ich treści przy zastosowaniu dostępnych wykładni. Postanowienie art. 66a ust. 9 pkt 2 lit. a i c–d projektu z 3 lipca 2023 r. mogą także zostać uznane za sprzeczne z § 11 z.t.p., zgodnie z którym w ustawie nie zamieszcza się wypowiedzi, które nie służą wyrażaniu norm prawnych, a w szczególności postulatów czy zaleceń. Wskazane postanowienia projektu mają bardziej charakter zaleceń czy wytycznych niż konkretnych, precyzyjnych norm prawnych. Postanowienia art. 66a ust. 9 pkt 2 lit. a i c–d projektu z 3 lipca 2023 r. mogą także zostać uznane za sprzeczne z § 3 ust. 2 z.t.p. Zgodnie z tym przepisem z.t.p. w ustawie nie można zamieszczać przepisów, które regulowałyby sprawy wykraczające poza wyznaczony przez nią zakres przedmiotowy (stosunki, które reguluje) oraz podmiotowy (krąg podmiotów, do których się odnosi). Przepisy art. 66a ust. 9 pkt 2 projektu stanowią podstawę do wykluczenia z rynku konkretnego przedsiębiorcy telekomunikacyjnego poprzez uniemożliwienie mu sprzedaży określonych produktów i usług. Uregulowanie to może zostać uznane za wykraczające poza zakres przedmiotowy oraz podmiotowy ustawy o Krajowym systemie cyberbezpieczeństwa. Zakres przedmiotowy ustawy o Krajowym systemie cyberbezpieczeństwa wyznacza art. 1 ust. 1 tej ustawy. Zgodnie z tym przepisem u.k.s.c. określa:

1) organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;
2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy;
3) zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Zakres przedmiotowy i podmiotowy u.k.s.c. nie dotyczy więc problematyki związanej z wykluczeniem z rynku określonego dostawcy sprzętu telekomunikacyjnego lub oprogramowania. Przepis art. 66a ust. 9 pkt 2 projektu z 3 lipca 2023 r. może wreszcie naruszać postanowienia § 4 ust. 2 z.t.p. Zgodnie z § 4 ust. 2 z.t.p. w ustawie nie powtarza się dających się bezpośrednio stosować postanowień aktów normatywnych ustanowionych przez organizacje międzynarodowe lub organy międzynarodowe. Postanowienia art. 66a ust. 4 pkt 2 Projektu powtarzają natomiast postanowienia *EU coordinated risk assessment of the cybersecurity of 5G networks* z 9 października 2019 r. przygotowanej przez Network and Information Security Cooperation Group (s. 22).

Sformułowane w art. 66a ust. 9 projektu z dnia 3 lipca 2023 r. kryteria oceny dostawcy wskazują, że ocena będzie dokonywana nie pod kątem technicznych zagrożeń związanych z wykorzystaniem sprzętu lub oprogramowania ocenianego dostawcy, ale z perspektywy czynników ogólnych o charakterze potencjalnym i geopolitycznym. Tymczasem, w zakresie kryteriów oceny dostawców główną rolę powinny odgrywać kryteria o charakterze technicznym, które pozwalałyby na badanie pod względem technicznym bezpieczeństwa infrastruktury, czyli weryfikacji za pomocą mierzalnych technicznych kryteriów, bezpieczeństwa tej infrastruktury. Techniczne kryteria oceny powinny być ze sobą powiązane i tworzyć spójny model ochrony bezpieczeństwa infrastruktury. Model ten powinien charakteryzować się obiektywnością weryfikacji kryteriów i dużym stopniem profesjonalizacji weryfikacji, gwarantującej poprawność wyników stosowanych kryteriów oceny. Kryteria pozatechnologiczne bardzo często są niedefiniowalne i posługują się niedookreślonymi pojęciami, które są trudne do zweryfikowania i dokonania oceny. Nie powinny one odgrywać kluczowej roli, gdyż mogą prowadzić do błędnych wniosków.

Przewidziane w art. 66a ust. 9 projektu z dnia 3 lipca 2023 r. kryteria oceny dostawcy powinny być uzupełnione o następujące elementy:

- weryfikację techniczną w odpowiednim laboratorium. Taka ocena byłaby niezbędna dla określenia poziomu ryzyka oraz możliwości wdrożenia odpowiednich środków technicznych i organizacyjnych;
- wpływ na konkurencję i konsumentów, a także możliwość utrzymania ciągłości usług, systemów i produktów, w których stosowane jest dane oprogramowanie lub urządzenie. Ocenie należałoby poddać, czy wydanie opinii nie będzie skutkowało ograniczeniem możliwości świadczenia usług oraz faktycznym powstaniem na krajowym rynku monopoli lub duopoli oraz związanym z tym realnym ryzykiem dla przedsiębiorstw i konsumentów;
- zidentyfikowanie podmiotów, których ocena ryzyka będzie dotyczyła (posiadających lub mogących planować zakup urządzeń lub oprogramowania ocenianego dostawcy) oraz zapoznanie się z ich opinią w sprawie dokonywanej oceny.

Istotną częścią systemu zapewnienia bezpieczeństwa jest nałożenie na przedsiębiorców obowiązku identyfikacji krytycznych obszarów swojej architektury sieciowej. W przypadku bowiem tych elementów infrastruktury należy zastosować wyższy poziom bezpieczeństwa. Składniki są krytyczne w szczególności wtedy, gdy techniczne nieprawidłowości prowadzić mogą do istotnych naruszeń bezpieczeństwa lub naruszeń ochrony danych w znacznym stopniu. Krytyczność danego składnika jest uzasadniona przez te jego funkcje, które mogą doprowadzić do nieprawidłowości technicznych w przypadku awarii.

Przedsiębiorca powinien porównać wszystkie składniki infrastruktury telekomunikacyjnej przed ich zastosowaniem z listą składników krytycznych. Bezpieczna eksploatacja może być zagwarantowana tylko przez zgodność z wymogami opisanymi w certyfikacie. W przypadku, gdy odpowiednie systemy certyfikacji nie są dostępne, operatorzy sieci powinni wprowadzić tymczasowo inne odpowiednie środki techniczne oraz środki bezpieczeństwa w czasie korzystania z elementów krytycznych.

Istotną kwestią jest zapewnienie wiarygodności producenta lub dostawcy infrastruktury telekomunikacyjnej. Używanie bowiem krytycznych składników infrastruktury telekomunikacyjnej z nieznanych lub niewiarygodnych źródeł może stworzyć zagrożenia dla bezpieczeństwa. Przedsiębiorcy są zobowiązani do właściwego wyboru producentów i dostawców krytycznych składników infrastruktury telekomunikacyjnej. Częścią właściwego wyboru jest odpowiednie zbadanie wiarygodności źródła zaopatrzenia. W celu stwierdzenia wiarygodności źródła zaopatrzenia przedsiębiorstwo powinno uzyskać deklarację, która powinna odnosić się do wszystkich kwestii istotnych z punktu widzenia zapewnienia bezpieczeństwa. Konkretna treść deklaracji powinna być ustalana pomiędzy przedsiębiorcą telekomunikacyjnym a dostawcą lub producentem w każdym indywidualnym przypadku. Przedsiębiorca powinien mieć możliwość weryfikacji integralności nabytych składników krytycznych w każdym czasie, począwszy od ich odbioru, a skończywszy na uruchomieniu. Obszary niezabezpieczone podczas dostawy do chwili uruchomienia powinny być wyraźnie i osobno udokumentowane w koncepcji bezpieczeństwa przez przedsiębiorcę przy wsparciu producenta lub dostawcy. Na tym etapie zagrożenia dostarczone krytyczne składniki powinny być zabezpieczone przed ewentualną manipulacją lub innymi wpływami. Może to być zapewnione przez mechanizmy specyficzne dla danego produktu lub mechanizmy zewnętrzne. W przypadku odbioru przedsiębiorca powinien sprawdzić, czy dane komponenty nie zostały podczas dostawy zmanipulowane, naruszone lub w inny sposób zmienione. Również w przypadku przechowywania przedsiębiorca powinien zapewnić integralność składników.

Przedsiębiorca powinien wdrożyć i prowadzić monitoring bezpieczeństwa infrastruktury w celu ciągłego identyfikowania zagrożeń i zapobiegania im. Monitoring bezpieczeństwa infrastruktury powinien obejmować wszystkie krytyczne składniki infrastruktury telekomunikacyjnej, a w szczególności te składniki, które przekazują dane osobowe zewnętrznym kontrahentom, np. w związku z roamingiem. Powinny być przygotowane odpowiednie procedury monitoringu bezpieczeństwa. Powinien być zatrudniony odpowiedni personel techniczny, posiadający stosowne kompetencje z uwagi na postępowanie z krytycznymi składnikami infrastruktury. W celu prawidłowego wykonania tych obowiązków

sama znajomość procesów technicznych nie jest wystarczająca. Wszyscy pracownicy pracujący w obszarach istotnych z punktu widzenia bezpieczeństwa powinni być odpowiednio co do zakresu swej odpowiedzialności przeszkoleni w ramach regularnych działań szkoleniowych. Przedsiębiorca powinien także zapewnić w odpowiednim zakresie redundancję krytycznych składników infrastruktury. Dotyczy to w szczególności sytuacji, gdy składniki krytyczne muszą spełniać bardzo wysokie wymagania w zakresie dyspozycyjności. Powinny być dostępne odpowiednie techniczne rozwiązania alternatywne na wypadek awarii. Zakres redundancji powinien określić przedsiębiorca w przygotowanej przez niego procedurze bezpieczeństwa.

Należy także zauważyć, że zarówno projektowane przepisy, jak i uzasadnienie nie odnoszą się do potencjalnej sytuacji, w której ocena ryzyka musiałaby zostać wydana, np. wobec dostawcy z kraju UE lub NATO. Należałoby więc doprecyzować, jakie skutki i jakie reguły kolizyjne będą stosowane w przypadku wpływu wydanej negatywnej oceny, która spowodowałaby faktyczne zablokowanie wymiany handlowej z kraju, w którym ma siedzibę dostawca uznany za dostawcę wysokiego ryzyka, na prawo międzynarodowe i zawarte umowy.

Zgodnie z art. 66a ust. 10 projektu z dnia 3 lipca 2023 r., sporządzając opinię Kolegium, uwzględnia:

1) certyfikaty wydane dla produktów ICT, usług ICT lub procesów ICT, wydane lub uznawane w państwach członkowskich Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego;
2) analizy, o których mowa w art. 64a ust. 1 i 2 projektu z dnia 3 lipca 2023 r.

Szczególnie istotna jest kwestia certyfikacji, która powinna dotyczyć składników infrastruktury uznanych za krytyczne. Podstawowym celem certyfikacji bezpieczeństwa jest niezależna i obiektywna weryfikacja gwarancji bezpieczeństwa. Dotrzymanie takiej gwarancji jest oceniane przez neutralną jednostkę kontrolną w ramach procedury certyfikacyjnej. Wraz z wejściem w życie rozporządzenia 2019/881 wprowadzono jednolite europejskie ramy certyfikacji w zakresie bezpieczeństwa w cyberprzestrzeni, które regulują uznawanie europejskich systemów certyfikacji w zakresie bezpieczeństwa cybernetycznego. Wskazane rozporządzenie obowiązuje także w Polsce, co oznacza, że certyfikat przyznany w innym kraju UE obowiązuje w Polsce i odwrotnie. W ten sposób unika się wielokrotnej certyfikacji danego produktu w różnych państwach. Składniki infrastruktury telekomunikacyjnej służące realizacji funkcji krytycznych mogą być wykorzystywane przez operatorów publicznych sieci telekomunikacyjnych wtedy, gdy zostały sprawdzone pod kątem bezpieczeństwa informatycznego przez uznaną jednostkę kontrolną zgodnie z rozporządzeniem 2019/881, i posiadają certyfikat uznanej jednostki certyfikującej.

Zgodnie z art. 66a ust. 11 projektu z dnia 3 lipca 2023 r. procedura sporządzenia opinii przebiega w następujący sposób:

1) przewodniczący Kolegium powołuje zespół w celu opracowania projektu opinii w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, zwany dalej „zespołem opiniującym", w skład którego wchodzą przedstawiciele członków Kolegium wskazani przez przewodniczącego Kolegium;
2) każdy członek zespołu opiniującego przygotowuje stanowisko w zakresie swojej właściwości, które następnie przekazuje zespołowi opiniującemu. W przypadku wystąpienia negatywnego sporu co do zakresu właściwości spór rozstrzyga przewodniczący Kolegium, wskazując właściwego członka zespołu opiniującego;
3) jeżeli nie zostały wykonane analizy, o których mowa w art. 64a ust. 1 i 2 projektu z dnia 3 lipca 2023 r., przewodniczący Kolegium zleca ich wykonanie;
4) zespół opiniujący przedstawia przewodniczącemu Kolegium projekt opinii;
5) uzgodnienie opinii następuje na posiedzeniu Kolegium;
6) uzgodnioną opinię przewodniczący Kolegium przekazuje ministrowi właściwemu do spraw informatyzacji.

W uzasadnieniu projektu z 3 lipca 2023 r. wyjaśniono, że opinia zostanie przygotowana przez zespół opiniujący, w skład którego wchodzą przedstawiciele członków Kolegium. Każdy członek zespołu opiniującego przygotowuje stanowisko w zakresie swojej właściwości. Przewodniczący Kolegium będzie miał kompetencje do rozstrzygnięcia ewentualnego negatywnego sporu co do zakresu tej właściwości poprzez wskazanie właściwego członka zespołu opiniującego[107].

Zgodnie więc z projektem organem uprawnionym do dokonywania oceny byłoby Kolegium, które jest działającym przy Radzie Ministrów organem opiniodawczo-doradczym. W jego skład wchodzą przedstawiciele administracji publicznej, tj. Pełnomocnik Rządu ds. Cyberbezpieczeństwa, określeni ministrowie, szef BBN, minister koordynator służb specjalnych. Oznacza to, że Kolegium jest głównie gremium polityczno-administracyjnym. W jego składzie brakuje natomiast organów lub jednostek posiadających pogłębioną wiedzę techniczną oraz doświadczenie w certyfikacji i ocenie urządzeń i oprogramowania. Osoby takie znajdują w jednostkach i organach podległych lub nadzorowanych przez podmioty tworzące skład kolegium, których udział w Kolegium nie jest przewidziany. Postulować więc należy, aby skład Kolegium, przynajmniej na potrzeby dokonywania oceny dostawców, uzupełniany był o jednostki *stricte* techniczne, w tym certyfikacyjne, które na podstawie przyjętych międzynarodowych standardów mogłyby przedstawiać ocenę techniczno-inżynierską ocenianych dostawców. Jednostki te

[107] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 88.

mogłyby być zarówno laboratoriami publicznymi, jak i prywatnymi, niekoniecznie mającymi siedzibę na terytorium Polski. Udział takich jednostek w procesie oceny byłby korzystny również dla trwałości decyzji w sprawie dostawców, która mając uzasadnienie techniczne, miałaby mocniejsze podstawy merytoryczne. Powinna być przewidziana także możliwość zgłoszenia wniosku przez kilku członków Kolegium wspólnie. Zagadnienia w zakresie cyberbezpieczeństwa mają charakter międzysektorowy, dlatego należałoby dopuścić możliwość składania wniosku, którego inicjatorem byłoby więcej podmiotów niż jeden.

W zakresie dokonywanych ocen należy uwzględniać także zagrożenia związane z aplikacjami. Projekt z 3 lipca 2023 r. nakłada na dostawców sprzętu i operatorów telekomunikacyjnych bardzo wygórowane wymagania i środki kontroli, ale pomija kwestie aplikacji, które mają fundamentalne znaczenie dla cyberbezpieczeństwa. Aplikacje mogą mieć dostęp do wiadomości czy plików. Na rynku są dostępne aplikacje, które umożliwiają np. stosowanie podsłuchu. Umożliwiają rejestrowanie nie tylko treści rozmów telefonicznych, ale i otoczenia, w tym śledzenie użytkownika za pomocą GPS. Wskazane zagrożenie dla cyberbezpieczeństwa powinno być uwzględnione w szerszym nawet zakresie niż tylko ryzyka związane z samą siecią telekomunikacyjną.

Zgodnie z art. 66a ust. 12 projektu z dnia 3 lipca 2023 r. minister właściwy do spraw informatyzacji, w drodze decyzji, uznaje dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi. W uzasadnieniu projektu z 3 lipca 2023 r. wyjaśniono, że nie chodzi więc o zwykłe zagrożenie, tylko o jego kwalifikowaną postać. Postępowanie w sprawie uznania za dostawcę wysokiego ryzyka będzie postępowaniem administracyjnym. Dostawca będzie mógł przedstawić swoje racje w postępowaniu, zanim zostanie uznany za dostawcę wysokiego ryzyka. Decyzja będzie mogła być zaskarżona do sądu administracyjnego, co zapewni dostawcy możliwość obrony swoich praw. Dostawca będzie mógł być uznany za dostawcę wysokiego ryzyka, jeżeli będzie spełniał szczególnego rodzaju przesłanki – będzie stwarzał poważne zagrożenie dla obronności, bezpieczeństwa państwa. Zanim dostawca zostanie uznany za dostawcę wysokiego ryzyka, jego sprawa zostanie wszechstronnie wyjaśniona. Nastąpi to poprzez opinię Kolegium oraz czynności przeprowadzone przez ministra właściwego do spraw informatyzacji. Dostawca będzie mógł przedstawić swoje stanowisko, a w przypadku uznania za dostawcę wysokiego ryzyka, kwestionować to przed sądem administracyjnym[108]. Prawo do wniesienia odwołania powinno przysługiwać jednak nie tylko dostawcy, w stosunku

[108] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 88, 92.

do którego będzie wydana decyzja, ale także podmiotowi, którego dotyczą jej postanowienia, w tym przedsiębiorcy telekomunikacyjnemu, w szczególności, że skutki tej oceny będą go dotyczyły bezpośrednio.

Zgodnie z projektem decyzja zawiera w szczególności wskazanie typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka (art. 66a ust. 13 projektu z dnia 3 lipca 2023 r.). Decyzja powinna także precyzyjnie wskazywać, kiedy zaczyna obowiązywać, w szczególności w zakresie nakładanych obowiązków na dostawcę lub inne podmioty. Okres, w którym zaczną być wymagane obowiązki, powinien być odpowiednio długi, umożliwiając dostosowanie się do nich podmiotom zobowiązanym.

W uzasadnieniu projektu wyjaśniono, że dzięki prawnemu zidentyfikowaniu dostawcy wysokiego ryzyka będzie możliwe wprowadzenie dodatkowych środków mitygujących zagrożenie, jakie stwarza sprzęt lub oprogramowanie dostarczane przez dostawcę wysokiego ryzyka[109]. Minister właściwy do spraw informatyzacji ogłasza decyzję w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski" oraz udostępnia w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji, a także na stronie internetowej urzędu obsługującego tego ministra (art. 66a ust. 14 projektu z dnia 3 lipca 2023 r.).

Projekt z dnia 3 lipca 2023 r. nie przewiduje możliwości przedstawienia środków zaradczych. Tymczasem podmiot, który został uznany za dostawcę wysokiego ryzyka, powinien mieć zapewnioną możliwość przedstawienia środków zaradczych i planu naprawczego albo wniesienia odwołania.

Od decyzji nie przysługuje wniosek o ponowne rozpatrzenie sprawy (art. 66a ust. 16 projektu z dnia 3 lipca 2023 r.). W uzasadnieniu projektu wyjaśniono, że ze względu na charakter sprawy – stwierdzenie poważnego zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi – decyzja ta będzie podlegała natychmiastowej wykonalności. Od decyzji w sprawie uznania za dostawcę wysokiego ryzyka nie będzie przysługiwał wniosek o ponowne rozpatrzenie sprawy, gdyż jak wyjaśniono w uzasadnieniu projektu, prawa strony postępowania będą zagwarantowane poprzez możliwość złożenia skargi do sądu administracyjnego. W przypadku, gdy w trakcie postępowania zostanie stwierdzone, że dostawca nie stanowi poważnego zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi, to zgodnie z zasadami ogólnymi k.p.a. zostanie wydana decyzja o umorzeniu postępowania[110].

---

109 Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 88.

110 Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 88.

Zgodnie z brzmieniem art. 66a ust. 15 projektu z dnia 3 lipca 2023 r. decyzja podlega natychmiastowemu wykonaniu, co oznacza, że ewentualne wniesienie odwołania nie wstrzymuje działań określonych w art. 66b projektu. W praktyce oznacza to więc, że odwołanie będzie miało ograniczone, praktyczne znaczenie, skoro pomimo jego wniesienia będą podejmowane nieodwracalne w swoich skutkach decyzje w zakresie np. wycofania sprzętu z sieci operatora czy utraty kontraktu na sprzedaż infrastruktury telekomunikacyjnej. W doktrynie prawa i orzecznictwie sądowym zwraca się uwagę na konieczność zachowania „daleko idącej ostrożności" przy wykonywaniu decyzji ostatecznych przed upływem terminu do ich zaskarżenia, ponieważ może to doprowadzić do powstania stanów nieodwracalnych[111].

Zgodnie z art. 66b ust. 1 projektu z dnia 3 lipca 2023 r. w przypadku wydania decyzji, o której mowa w art. 66a ust. 12 projektu z dnia 3 lipca 2023 r., podmioty, o których mowa w art. 66a ust. 1 pkt 1–3 projektu z dnia 3 lipca 2023 r.:

1) nie wprowadzają do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka;
2) wycofują z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 66a ust. 12 projektu z dnia 3 lipca 2023 r.

Przedsiębiorcy komunikacji elektronicznej obowiązani posiadać aktualne i uzgodnione plany działań oraz wprowadzone do stosowania w sytuacji szczególnego zagrożenia, wycofują w ciągu 5 lat typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy (art. 66b ust. 2 projektu z dnia 3 lipca 2023 r.).

W uzasadnieniu projektu z dnia 3 lipca 2023 r. wyjaśniono, że następstwem prawnego zidentyfikowania dostawcy wysokiego ryzyka powinno być zmitygowanie ryzyka, które on stwarza. Art. 66b projektu z dnia 3 lipca 2023 r. wprowadza więc niezbędne wymogi bezpieczeństwa dla podmiotów krajowego systemu cyberbezpieczeństwa, operatorów infrastruktury krytycznej czy 69 przedsiębiorców komunikacji elektronicznej w związku z wykorzystywaniem sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka. Podmioty krajowego systemu cyberbezpieczeństwa, operatorzy infrastruktury krytycznej, przedsiębiorcy komunikacji elektronicznej sporządzający plany działań w sytuacji szczególnego

[111] T. Woś (red.), *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, LEX 2016, komentarz do art. 61 i przywołane tam orzecznictwo.

zagrożenia nie będą mogli wprowadzać do użytkowania zakresów typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka. Dotyczyć to będzie zarówno nowych produktów, usług i procesów, jak i używanych. W tym przypadku chodzi o sytuację, w której w chwili wydania decyzji dany podmiot nie ma danego produktu, usługi lub procesu ICT. Nie będzie mógł więc ich używać lub z nich korzystać. Celem jest, aby nie wprowadzać kolejnych produktów, usług, procesów ICT, żeby nie zwiększać już i tak wysokiego ryzyka związanego z nimi. Innym obowiązkiem będzie wycofanie z użytkowania zakresów typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, jednak nie później niż 7 lat od dnia opublikowania informacji o decyzji. Chodzi tutaj o sytuację, w której w chwili wydania decyzji o uznaniu za dostawcę wysokiego ryzyka dany podmiot już używa lub korzysta z produktów, usług i procesów ICT uwzględnionych w decyzji o uznaniu za dostawcę wysokiego ryzyka. Będzie więc musiał wycofać go w terminie 7 lat. Jest to związane z tym, że natychmiastowe wycofanie produktów, usług i procesów ICT mogłoby być niemożliwe w praktyce, gdyż mogłoby spowodować zaprzestanie świadczenia usług. Natomiast przedsiębiorcy komunikacji elektronicznej, posiadający lub korzystający z typów produktów ICT, rodzajów usług ICT, konkretnych procesów ICT wskazanych w decyzji i określonych w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy będą musieli wycofać je w ciągu 5 lat od ogłoszenia decyzji. Takie skrócenie okresu na wycofanie jest spowodowane szczególnym znaczeniem dla bezpieczeństwa państwa usług telekomunikacyjnych, szczególnie sprzętu lub oprogramowania wykorzystywanych do realizowania funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku nr 3[112].

Do czasu wycofania sprzętu lub oprogramowania, o którym mowa w art. 66b ust. 1 pkt 2 projektu z dnia 3 lipca 2023 r., dopuszcza się użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, w zakresie naprawy, modernizacji, wymiany elementu lub aktualizacji, jeżeli jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług, w szczególności dokonywania niezbędnych napraw awarii lub uszkodzeń (art. 66b ust. 3 projektu z dnia 3 lipca 2023 r.).

W uzasadnieniu projektu wyjaśniono, że jednocześnie wprowadzono przepis umożliwiający użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym

[112] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 88–89.

decyzją w sprawie uznania za dostawcę wysokiego ryzyka, dostarczanych przez dostawcę wysokiego ryzyka, w zakresie naprawy, modernizacji, wymiany elementu lub aktualizacji. Będzie to możliwe wyłącznie, jeśli jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług, w szczególności dokonywania niezbędnych napraw awarii lub uszkodzeń. Te same przepisy zostały zastosowane do podmiotów publicznych, które już zakupiły określony sprzęt w drodze zamówienia publicznego. Jest to niezbędne rozwiązanie zarówno dla zapewnienia ciągłości świadczenia usług, jak i ochrony dyscypliny finansów publicznych. Wyżej zaproponowana interwencja prawodawcy jest konieczna ze względu na istotność dla bezpieczeństwa państwa usług świadczonych przez podmioty obowiązane do wycofania sprzętu lub oprogramowania. Podmioty te mogą być związane wieloletnimi umowami z dostawcą wysokiego ryzyka na dostarczanie sprzętu lub oprogramowania czy świadczenie usług serwisowych. Bez prawnego obowiązku stopniowego wycofania sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka podmioty te nie wycofają sprzętu lub oprogramowania, m.in. z uwagi na ryzyko odpowiedzialności kontraktowej wobec dostawcy. W konsekwencji ryzyko związane ze sprzętem lub oprogramowaniem pochodzącym od dostawcy wysokiego ryzyka nie zostanie skutecznie zmitygowane. Podkreślić należy, że jest to wyjątek od podstawowej reguły zakazu wprowadzania do użytkowania i obowiązku wycofania wskazanego wyżej sprzętu lub oprogramowania w ciągu 5–7 lat. Wyjątek ten nie może być interpretowany rozszerzająco. Wyjaśnienia wymaga termin „użytkowania" użyty w tym przepisie. Nie należy go utożsamiać z użytkowaniem z Kodeksu cywilnego, które jest ograniczonym prawem rzeczowym. „Użytkowanie" w rozumieniu art. 66b projektu z 3 lipca 2023 r. oznacza każdy przypadek używania czy korzystania z produktu, usługi, procesu ICT do świadczenia usług przez dany podmiot. Według projektodawców w zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W proponowanych przepisach jest mowa o 5–7 latach. Termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia[113].

Przewidziany w projekcie okres na wycofanie sprzętu powinien być dłuższy i wynieść 9–10 lat, gdyż tyle wynoszą realne okresy amortyzacji urządzeń.

[113] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 89–90.

Na marginesie okresy te nie odpowiadają technicznej użyteczności, która co do zasady jest dłuższa niż czas amortyzacji. Wymiana sprzętu powinna odnosić się do określonego sprzętu i oprogramowania zamiast do dostawcy. Konstrukcja wycofywania sprzętu z użytkowania wywołuje poważne wątpliwości z uwagi na obowiązywanie jednej z kardynalnych zasad prawa, tj. zasady „niedziałania prawa wstecz". Przepis nakazujący wycofywanie sprzętu zakupionego wiele lat wcześniej stanowi objęcie regulacją zdarzeń wcześniejszych, sprzed kilku lat, które dotyczyły zawierania umów o zakup sprzętu na podstawie obowiązujących wówczas przepisów. Tym bardziej więc powinien być uwzględniony postulat zapewnienia odpowiednio długiego okresu na wycofywanie sprzętu z użytkowania. Z wycofaniem używanego sprzętu i wprowadzeniem nowego sprzętu wiąże się szereg konsekwencji dla przedsiębiorcy telekomunikacyjnego:

- konieczność wykonania prac analitycznych oraz planistycznych w zakresie przygotowania procedury wyboru nowego dostawcy i wdrożenia nowych elementów sieciowych lub oprogramowania;
- przeprowadzenie procedury przetargowej i dodatkowych negocjacji przeprowadzenia wyboru nowego dostawcy sprzętu lub oprogramowania;
- realizacja procesu wdrożenia sprzętu lub oprogramowania oraz przeprowadzenia procesu odtwarzania dodatkowych funkcjonalności, w tym dodatkowych szkoleń pracowników;
- ryzyko kumulacji przetargów wynikających ze zmiany dostawcy sprzętu lub oprogramowania po stronie wielu przedsiębiorców telekomunikacyjnych (w kraju i za granicą), przekraczających możliwości dostawców w danym okresie i w konsekwencji opóźnienia;
- ryzyko kumulacji działań po stronie dostawców przedsiębiorców telekomunikacyjnych w zakresie integracji nowego sprzętu lub oprogramowania, co będzie powodować opóźnienia;
- poniesienie dodatkowych opłat administracyjnych, np. kosztów pozwoleń radiowych;
- poniesienie dodatkowej marży dla dostawców nowego sprzętu i oprogramowania, którzy będą tworzyć i wykorzystywać presję czasową na przedsiębiorców telekomunikacyjnych;
- poniesienie dodatkowej marży dla dostawców starego sprzętu lub oprogramowania, którzy będą wykorzystywać wszelkie nieprzewidziane działania po stronie przedsiębiorców telekomunikacyjnych;
- kumulacja dodatkowych kosztów przez przedsiębiorców telekomunikacyjnych związanych z utrzymywaniem sprzętu lub oprogramowania starego i nowego dostawcy w okresie przejściowym;

– w przypadku złożonych usług telekomunikacyjnych na rynku B2B zmiana dostawcy sprzętu lub oprogramowania oznaczać będzie przeprowadzenie dodatkowych ustaleń z klientami B2B w zakresie integracji;
– ryzyko pogorszenia jakości usług telekomunikacyjnych w okresie przejściowym, co może powodować dodatkowe finansowe reperkusje w stosunku do użytkowników końcowych.

Zmiana dostawcy sprzętu lub oprogramowania spowoduje kumulację zamówień do dostawców nowego sprzętu, co w konsekwencji może prowadzić do opóźnień. Z reguły rynek telekomunikacyjny w Polsce w okresie 2–3 lat osiąga zdolność techniczną porównywalną do najbardziej wartościowych rynków telekomunikacyjnych (USA, Korea, Niemcy, Wielka Brytania). Czynnik ten powinien być brany pod uwagę przy określaniu okresu na wycofanie sprzętu, w porównaniu do innych bogatszych rynków. Decyzja w sprawie dostawcy wysokiego ryzyka może mieć wpływ na konkurencyjność rynku telekomunikacyjnego, ponieważ przedsiębiorcy telekomunikacyjni w różnym stopniu będą posiadać sprzęt lub oprogramowanie określonego dostawcy. W celu uniknięcia tak dalece idących konsekwencji decyzji niezbędne jest zastosowanie odpowiednio wydłużonego czasu na jej realizację.

W uzasadnieniu projektu wskazano także, że proponowane rozwiązania mają wpływ na swobodę działalności gospodarczej podmiotów zobowiązanych do wycofania sprzętu. Wpływają bowiem na wolność podejmowania decyzji gospodarczych. Mają także wpływ na wykonywanie niektórych atrybutów prawa własności, tj. prawa do używania produktów. Wskazać należy, że przepisy te mają na celu mitygację ryzyk związanych ze sprzętem lub oprogramowaniem pochodzącym od dostawcy wysokiego ryzyka. Tak jak wyżej wspomniano, korzystanie z takiego sprzętu mogłoby doprowadzić do poważnych ryzyk naruszenia poufności danych oraz naruszenia dostępności usługi. Co za tym idzie, doprowadziłoby to do poważnego utrudnienia funkcjonowania obywateli, współczesnego społeczeństwa informacyjnego, a także do ryzyka przejęcia kontroli nad infrastrukturą krytyczną państwa. Wycofanie sprzętu lub oprogramowania pochodzących od dostawcy wysokiego ryzyka jest zatem konieczne do zapewnienia funkcjonowania demokratycznego państwa prawnego. Proponowane rozwiązania nie naruszają istoty swobody prowadzenia działalności gospodarczej. Ogranicza się wykorzystywanie przez przedsiębiorców konkretnego sprzętu lub oprogramowania do świadczenia usług. W pozostałym zakresie przedsiębiorcy będą mogli swobodnie podejmować decyzje biznesowe. Przepisy te nie naruszają również istoty prawa własności. Tak jak wyżej wspomniano, nie ma mechanizmu natychmiastowego wycofania sprzętu lub oprogramowania, przez czas wycofywania z użytkowania podmioty te będą mogły w pełni wykonywać prawo własności.

Ponadto w czasie wycofywania będzie można wprowadzić dotychczas posiadany sprzęt lub oprogramowanie, pochodzący od dostawcy wysokiego ryzyka, aby dokonać niezbędnych napraw usterek czy awarii, aby zapewnić ciągłość świadczenia usługi. W uzasadnieniu dalej wskazuje się, że sprzęt lub oprogramowanie pochodzące od dostawcy wysokiego ryzyka i tak podlegałyby stopniowej wymianie ze względu na zużycie czy postęp technologiczny. Proponowane rozwiązanie wpisuje się więc w mechanizm stopniowej wymiany sprzętu. Rozwiązanie to wpłynie na swobodę prowadzenia działalności gospodarczej przez dostawcę wysokiego ryzyka. W uzasadnieniu podkreśla się jednak, że będzie to związane z poważnym zagrożeniem dla państwa, które stwarza ten dostawca. Jednakże istota prowadzenia działalności gospodarczej przez dostawcę wysokiego ryzyka nie zostanie naruszona. Taki dostawca nadal będzie mógł prowadzić działalność gospodarczą[114].

W dalszej części uzasadnienia wskazano, że wartością konstytucyjną, która w tej sytuacji powinna być bardziej chroniona od swobody prowadzenia działalności gospodarczej czy prawa własności, jest bezpieczeństwo państwa. Państwo powinno odpowiednio zaadresować problem dostawcy wysokiego ryzyka, który może, dzięki podatnościom w sprzęcie lub oprogramowaniu, które dostarczył, doprowadzić do ataku na infrastrukturę krytyczną państwa (np. inteligentne sieci energetyczne, sieci telekomunikacyjne), zakłócać funkcjonowanie organów państwa (np. poprzez ataki *man in the middle*, kradzież danych) czy zakłócić działanie kluczowych dla społeczeństwa usług (np. poprzez atak na systemy i urządzenia szpitalne, bez których znacznie utrudnione jest wykonywanie operacji ratujących życie). Może to się odbyć poprzez celowo zaprojektowane ukryte podatności lub również ukryte podatności powstałe w wyniku aktualizacji oprogramowania dostarczonego przez dostawcę wysokiego ryzyka. Wykorzystanie podatności w infrastrukturze telekomunikacyjnej, której elementy dostarczył taki dostawca, mogłoby utrudnić lub uniemożliwić funkcjonowanie usług komunikacji elektronicznej na danym obszarze. Demokratyczne państwo prawne nie może być bezbronne i musi zawczasu identyfikować poważne zagrożenia dla jego funkcjonowania oraz skutecznie je mitygować. W uzasadnieniu dalej się wskazuje, że zagrożenia stwarzanego przez dostawcę wysokiego ryzyka (który działa pod wpływem obcych służb wywiadowczych lub grup przestępczych) oraz jego sprzęt lub oprogramowanie nie da się inaczej zmitygować, jak tylko poprzez stopniowe wycofanie takiego sprzętu. Podmioty korzystające z tych produktów, usług, procesów nie będą w stanie zidentyfikować ukrytych podatności, poprzez które

[114] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 90–91.

dostawca wysokiego ryzyka będzie mógł dokonywać ataków. W związku z tym nie jest możliwe zmitygowanie ryzyka stwarzanego przez dostawcę wysokiego ryzyka poprzez wprowadzenie dodatkowych środków bezpieczeństwa, innych niż wycofanie sprzętu lub oprogramowania, ponieważ będą one nieskuteczne wobec ukrytych podatności pozwalających np. nagle wyłączyć sprzęt czy zakłócić telekomunikację między podmiotami[115].

Podmioty, o których mowa w art. 66a ust. 1 pkt 1–3 projektu z dnia 3 lipca 2023 r., do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. z 2022 r. poz. 1710, 1812, 1933 i 2185 oraz z 2023 r. poz. 412 i 825), nie mogą nabywać sprzętu, oprogramowania i usług określonych w decyzji, o której mowa w art. 66a ust. 12. projektu z dnia 3 lipca 2023 r. (art. 66b ust. 4 projektu z dnia 3 lipca 2023 r.). W przypadku, gdy podmioty, o których mowa w art. 66a ust. 1 pkt 1–3 projektu z dnia 3 lipca 2023 r., do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych, nabyły w drodze zamówienia publicznego przed dniem ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 66a ust. 12 projektu z dnia 3 lipca 2023 r., produkt ICT, usługę ICT lub proces ICT określone w tej decyzji, mogą korzystać z tych produktów, usług lub procesów nie dłużej niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 66a ust. 12 projektu z dnia 3 lipca 2023 r., a w przypadku produktów ICT, usług ICT lub procesów ICT wykorzystywanych do wykonywania funkcji krytycznych określonych w załączniku nr 3 do ustawy, nie dłużej niż 5 lat (art. 66b ust. 5 projektu z dnia 3 lipca 2023 r.).

Zgodnie z art. 66c ust. 1 projektu z dnia 3 lipca 2023 r. podmioty, o których mowa w art. 66a ust. 1 pkt 1–3 projektu z dnia 3 lipca 2023 r., są zobowiązane przekazać informacje na wniosek uprawnionych organów, o których mowa w art. 66a ust. 2 projektu z dnia 3 lipca 2023 r., o wycofywanych typach produktów ICT, rodzajach usług ICT i konkretnych procesach ICT w zakresie objętym decyzją, o której mowa w art. 66a ust. 12 projektu z dnia 3 lipca 2023 r. W uzasadnieniu projektu wyjaśniono, że organy właściwe do spraw cyberbezpieczeństwa będą mogły zwracać się do podmiotów krajowego systemu cyberbezpieczeństwa o udzielenie informacji w sprawie wycofywanych produktów ICT, usług ICT i procesów ICT. Podobne kompetencje będzie miał w stosunku do przedsiębiorców telekomunikacyjnych Prezes UKE. Przepis wzmocni kompetencje organów i zapewni im możliwość monitorowania procesu wycofywania produktów ICT, usług ICT i procesów ICT[116].

---

[115] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 91–92.

[116] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 92.

Według art. 66c ust. 2 projektu z dnia 3 lipca 2023 r. uprawnionymi organami do uzyskania informacji, o których mowa w art. 66c ust. 1 projektu z dnia 3 lipca 2023 r., są wobec:

1) operatorów usług kluczowych i dostawców usług cyfrowych – organy właściwe do spraw cyberbezpieczeństwa;
2) SOC zewnętrznych – minister właściwy do spraw informatyzacji;
3) przedsiębiorców komunikacji elektronicznej – Prezes UKE;
4) podmiotów publicznych – właściwe organy nadzoru lub minister właściwy do spraw informatyzacji;
5) właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym – ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych odpowiedzialni za systemy, o których mowa w art. 3 pkt 2 tej ustawy.

Według art. 66c ust. 3 projektu z dnia 3 lipca 2023 r. wniosek powinien zawierać:

1) wskazanie podmiotu obowiązanego do przekazania informacji;
2) datę wydania decyzji, o której mowa w art. 66a ust. 13 projektu z dnia 3 lipca 2023 r.;
3) wskazanie zakresu żądanych informacji;
4) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni;
5) uzasadnienie;
6) pouczenie o zagrożeniu karą, o której mowa w art. 73 ust. 2d projektu z dnia 3 lipca 2023 r.

Według art. 66c ust. 4 projektu z dnia 3 lipca 2023 r. minister właściwy do spraw informatyzacji może zwrócić się do uprawnionych organów, o których mowa w ust. 2 pkt 1 lub ust. 2 pkt 3–5 projektu z dnia 3 lipca 2023 r., aby uzyskały informacje, o których mowa w art. 66c ust. 1 projektu z dnia 3 lipca 2023 r. Na wniosek ministra właściwego do spraw informatyzacji uprawniony organ, o którym mowa w art. 66c ust. 2 pkt 1 lub ust. 2 pkt 3–5 projektu z dnia 3 lipca 2023 r., przekazuje uzyskane informacje, o których mowa w art. 66c ust. 1 projektu z dnia 3 lipca 2023 r., temu ministrowi (art. 66c ust. 5 projektu z dnia 3 lipca 2023 r.).

Zgodnie z art. 66d ust. 1 projektu z dnia 3 lipca 2023 r. sąd administracyjny rozpatruje skargę na decyzję, o której mowa w art. 66a ust. 12 projektu z dnia 3 lipca 2023 r. na posiedzeniu niejawnym w składzie trzech sędziów. Odpis sentencji wyroku z uzasadnieniem doręcza się wyłącznie ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią

uzasadnienia, która nie zawiera informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych (art. 66d ust. 2 projektu z dnia 3 lipca 2023 r.).

W uzasadnieniu projektu wyjaśniono, że w artykule 66d projektu z dnia 3 lipca 2023 r. wprowadzono przepisy dotyczące procedury przed sądem administracyjnym, jest to więc przepis o charakterze *lex specialis* do ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi. Był on wzorowany na art. 38 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[117], która dotyczy rozpoznania skargi na decyzję o odmowie wydania poświadczenia bezpieczeństwa. Przepis ma za zadanie pogodzić dwie wartości prawne – prawo do złożenia skargi na decyzję administracyjną oraz ochronę informacji niejawnych, których ujawnienie mogłoby narazić państwo na niepowetowane szkody. Sąd administracyjny będzie rozpatrywał skargę na decyzję o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka na posiedzeniu niejawnym. Z kolei sentencja wyroku z uzasadnieniem zostanie doręczona tylko ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią uzasadnienia, która nie wymaga utajnienia ze względu na ochronę informacji niejawnych. Według projektodawców takie sformułowanie przepisu będzie zgodne z wyrokiem Trybunału Konstytucyjnego, który za niekonstytucyjne uznał brak doręczenia jawnych elementów wyroku sądu administracyjnego[118]. Przepis stanowi niezbędne odstąpienie od zasady ustności i jawności, jednakże strona będzie miała możliwość składania pism procesowych, jak w każdym innym postępowaniu przed sądem administracyjnym. W dalszej części uzasadnienia projektu wyjaśniono, że rozwiązanie to jest konieczne dla zapewnienia bezpieczeństwa demokratycznego państwa prawnego – ujawnienie informacji niejawnych wykorzystanych w postępowaniu o uznaniu za dostawcę wysokiego ryzyka mogłoby narazić Rzeczpospolitą na niepowetowane szkody. Nie została naruszona istota prawa do sądu, ponieważ w zakresie, w jakim uzasadnienie nie zawiera informacji niejawnych (uzasadnienie prawne, kwestia wykładni, ustalenia organu niepodlegające utajnieniu), zostanie doręczone skarżącemu, dzięki czemu będzie mógł złożyć skargę kasacyjną. Rozwiązanie jest też proporcjonalne *sensu stricto*, bowiem sędziowie mają z urzędu dostęp do wszystkich materiałów niejawnych, które będą zgromadzone w sprawie. Będą więc mogli skrupulatnie zbadać legalność postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Na poparcie tego rozwiązania projektodawcy odwołali się do wyroku Naczelnego Sądu Administracyjnego z 8 marca 2017 r. sygn. akt I OSK 1312/15: „strona skarżąca – z istoty

[117] Dz.U. z 2023 r. poz. 756.

[118] Wyrok Trybunału Konstytucyjnego z dnia 23 maja 2018 r. sygn. akt SK 8/14, Legalis.

sprawy mająca ograniczony dostęp do szeregu informacji z nią związanych – powinna móc działać w zaufaniu, że zasadniczo pełny dostęp do informacji posiada sąd, do którego zwraca się ona o kontrolę działania organu administracji publicznej, i że tę kontrolę sąd ten dokona w sposób niezależny i niezawisły w oparciu o pełną wiedzę wynikającą z ustaleń organu, w tym także niejawnych"[119].

Proponowane jednak w art. 66d ust. 1–2 projektu z dnia 3 lipca 2023 r. rozwiązania, a w szczególności rozpatrywanie przez sąd administracyjny skargi na posiedzeniu niejawnym oraz doręczenie skarżącemu odpisu wyroku z tą częścią uzasadnienia, która nie zawiera informacji niejawnych, może oznaczać w praktyce prowadzenie postępowania z naruszeniem zasady efektywnej ochrony sądowej, stanowiącej jeden z fundamentów zasady prawa do sądu wyrażonej zarówno w art. 45 Konstytucji RP, jak i art. 6 EKPC[120].

Zgodnie z art. 66e projektu z dnia 3 lipca 2023 r. minister właściwy do spraw informatyzacji prowadzi i udostępnia przy użyciu systemu teleinformatycznego listę produktów ICT, usług ICT i konkretnych procesów ICT objętych decyzjami, o których mowa w art. 66a ust. 12 projektu z dnia 3 lipca 2023 r.

## 3. Certyfikacja

Ministerstwo Cyfryzacji na początku lutego 2020 r. przeprowadziło konsultacje *Założeń dostosowania polskiego prawa do wymogów Aktu o cyberbezpieczeństwie* („Założenia"), czyli rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 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"). Akt o cyberbezpieczeństwie to rozporządzenie UE, które jest automatycznie obowiązujące we wszystkich krajach UE. Nie jest więc konieczna jego implementacja, jak w przypadku dyrektyw, do krajowego porządku prawnego. Tytuł III Aktu o cyberbezpieczeństwie brzmi *Ramy certyfikacji cyberbezpieczeństwa* (art. 46–65) i reguluje zgodnie z tym tytułem kwestie związane z certyfikacją. Zgodnie z art. 46 ust. 1 Aktu o cyberbezpieczeństwie celem stworzenia europejskich ram certyfikacji cyberbezpieczeństwa

[119] Uzasadnienie projektu z dnia 3 lipca 2023 r., s. 92–93.

[120] Por. P. Daniel, *Ochrona tymczasowa w przepisach p.p.s.a. w świetle prawa unijnego*, „Zeszyty Naukowe Sądownictwa Administracyjnego" 2011, nr 5, s. 28. Zob. także A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, Warszawa 2019, komentarz do art. 47.

jest poprawa warunków funkcjonowania rynku wewnętrznego poprzez zwiększenie poziomu cyberbezpieczeństwa w Unii.

W założeniach powinna być wyraźnie określona relacja pomiędzy krajowym (polskim) programem certyfikacji bezpieczeństwa a europejskim programem certyfikacji bezpieczeństwa. Relacje te określa art. 57 Aktu o cyberbezpieczeństwie, wskazując, że certyfikaty wystawione przez akredytowane jednostki certyfikujące w ramach europejskich programów certyfikacji będą honorowane na terenie wspólnego rynku. W założeniach powinno więc być stwierdzone, że po pierwsze, krajowy program certyfikacji bezpieczeństwa będzie zgodny z europejskim programem certyfikacji bezpieczeństwa. Po drugie, że certyfikat bezpieczeństwa wydany zgodnie z europejskim programem certyfikacji bezpieczeństwa w jednym kraju UE będzie respektowany w Polsce. Co więcej, zgodnie z art. 57 ust. 2 Aktu o cyberbezpieczeństwie, kraje UE nie mogą wprowadzać nowych krajowych programów certyfikacji cyberbezpieczeństwa dotyczących produktów ICT, usług ICT i procesów ICT, które są już objęte obowiązującym europejskim programem certyfikacji cyberbezpieczeństwa.

Przede wszystkim należałoby najpierw określić, jak będą wdrażane poszczególne przepisy Aktu o cyberbezpieczeństwie, a nie przedstawiać model certyfikacji. Uporządkowałoby to dyskusje w zakresie wdrażania poszczególnych postanowień Aktu o cyberbezpieczeństwie, gdyż byłoby w ten sposób wiadomo, jakie kwestie i w jaki sposób będą wdrażane. Innymi słowy, najpierw należałoby zidentyfikować te sprawy w oparciu Akt o cyberbezpieczeństwie, a później dostosowywać do tego opisywany model certyfikacji. Efektem tego podejścia jest to, że nie do końca wiadomo, jak będzie wyglądało ostatecznie wdrożenie postanowień Aktu o cyberbezpieczeństwie albo według autorów opracowania jak będzie wyglądał model certyfikacji w Polsce. To szczególnie ważne, gdyż opis tego modelu jest bardzo ogólny. Innymi słowy, opis wdrożenia postanowień Aktu o cyberbezpieczeństwie czy inaczej modelu certyfikacji jest niepełny. W związku z tym, że będą stosowane (wdrażane) postanowienia Aktu o cyberbezpieczeństwie, należałoby wyjaśnić, czy są, a jeżeli tak, jakie przepisy UE, z których wynikałby obowiązek certyfikacji. Jeżeli natomiast takich przepisów nie ma, należałoby to także wyraźnie wskazać. Należałoby także wskazać, jakie ustawy sektorowe mogą przewidywać obowiązek certyfikacji. Analogicznie precyzyjnie powinno zostać określone, na czym będzie polegać i w jakim akcie prawnym będzie uregulowany ewentualny obowiązek użytkowania produktów certyfikowanych. Brak takich informacji powoduje, że nie jest znany ostateczny kształt certyfikacji. Utrudnia to ocenę przyszłego modelu certyfikacji, ponieważ obecnie z jednej strony wskazuje się, że certyfikacja będzie nieobowiązkowa, ale z drugiej – że będą wyjątki od tej zasady

przewidujące certyfikację obowiązkową. Wyjątki te powinny być wskazane i opisane.

Założenia dotyczące wdrażania rozporządzenia w zakresie certyfikacji w Polsce to zaledwie dwuipółstronicowy dokument. Założenia przewidują więc certyfikację obowiązkową i nieobowiązkową. Przy określeniu podmiotów zobowiązanych do obowiązkowej certyfikacji należy odnieść się do rodzaju świadczonych usług oraz wielkości samych operatorów. Dla większości operatorów, szczególnie mniejszych, powinna wystarczyć deklaracja zgodności. Będzie to tańsze rozwiązanie. Rozważany jest także obowiązek nadania certyfikatu o wyższym stopniu w przypadku operatorów infrastruktury krytycznej o bardzo wysokim znaczeniu (rurociągi, energetyka, obsługa organów centralnych administracji publicznej, łączność).

Proponowany w założeniach model dla Polski to model mieszany. Zakłada współpracę sektora publicznego i prywatnego w celu zapewnienia łatwej dostępności certyfikacji oraz jej promocji wśród przedsiębiorców. Model ten ma nie naruszać innych przepisów o certyfikacji. Podkreśla się konieczność określenia modelu certyfikacji cyberbezpieczeństwa w Polsce przede wszystkim w zakresie sposobu tworzenia programów certyfikacji.

Zgodnie z założeniami laboratoria w tym systemie certyfikacji powinny działać na zasadach rynkowych. Ponieważ koszt oceny jest trudny do oszacowania i zależny od wielu czynników, powinien być kształtowany przez rynek. Regulacja w tym zakresie powinna być minimalna. Zgodnie z założeniami możliwe jest utworzenie jednej lub wielu jednostek certyfikujących. Mogą być one publiczne lub prywatne. W polskim prawie znane są oba modele. W założeniach zwraca się uwagę, że przy jednej jednostce certyfikującej państwo ma większą kontrolę nad tym, kto jest certyfikowany. Niemniej jednak model ten jest niewydolny, kiedy dużo podmiotów jest zainteresowanych uzyskaniem certyfikatu.

Zgodnie z założeniami publiczne jednostki certyfikujące można przyporządkować do jednostek, w których obecnie funkcjonują zespoły CSIRT. Wymaga to jednak dalszych uzgodnień z tymi jednostkami. Według założeń pozwoliłoby to na zachowanie spójności systemu z krajowym systemem cyberbezpieczeństwa, ale oznacza to także konieczność ustalenia odgórnie kosztów uzyskania certyfikatu. W przypadku prywatnych jednostek certyfikujących można określić sposoby ich funkcjonowania na podstawie modelu stosowanego dla wyrobów przeznaczonych na potrzeby obronności i bezpieczeństwa państwa. Koszty certyfikacji powinny być ustalane przez jednostkę na zasadach rynkowych. Według założeń dopuszcza się istnienie wielu krajowych organów ds. certyfikacji cyberbezpieczeństwa (organu nadzoru), ale celem zachowania spójności działań i jednolitego nadzoru sugerowane jest ustanowienie jednego organu nadzoru.

Proponowanym krajowym organem jest minister cyfryzacji. Do jego obowiązków należałoby m.in.: monitorowanie przestrzegania ustawy, monitorowanie wykonywania obowiązków wytwórców lub dostawców w zakresie samooceny, rozpatrywanie skarg. W założeniach są określone zasady nadzoru i kontroli, w tym produktów i usług, co do których zachodzi podejrzenie, że zostały niewłaściwie oznaczone certyfikatem. Podejrzenie może też wynikać z uzyskania informacji z innego kraju UE. W założeniach podkreśla się, że pomimo iż będzie tylko jeden organ nadzoru, to może być wielu właścicieli programów certyfikacji, którzy będą mieli własne uprawnienia, niewynikające z ustawy. Według założeń polecany model kontroli powinien zostać opracowany na podstawie kryteriów zawartych w ustawie – Prawo przedsiębiorców (w stosunku do prywatnych jednostek certyfikujących) i w ustawie o kontroli w administracji rządowej (w stosunku do publicznych jednostek certyfikujących). Powinny być określone sankcje, jakie mogą stosować organy kontroli w przypadku niezastosowania się do zaleceń przez podmiot kontrolowany – np. cofnięcie certyfikatu, ale także nakładanie kar finansowych z tytułu nieodpowiedniego użytkowania certyfikatu.

W założeniach powinna być także wyraźnie sformułowana zasada, że dotychczas uzyskane certyfikaty bezpieczeństwa pozostają nadal ważne do okresu upływu ich ważności, niezależnie od tego, czy był to certyfikat wydany przez instytucję publiczną, czy prywatną oraz czy wydany został przez podmiot z UE czy spoza UE (istnieją instytucje międzynarodowe, które tego rodzaju certyfikaty wydają). Zasada ta powinna obowiązywać niezależnie od tego, w jakiej procedurze certyfikat bezpieczeństwa został otrzymany, pod warunkiem, że jest to instytucja i procedura międzynarodowo akceptowana, np. normy ISO. Okres przejściowy wprowadzania nowych rozwiązań powinien być odpowiednio długi, liczony nawet w latach, aby zapewnić sprawne wdrożenie nowych zasad certyfikacji.

# Zakończenie

1. Zagadnienia dotyczące bezpieczeństwa sieci i usług łączności elektronicznej są uregulowane zarówno w przepisach unijnych, jak i krajowych. Podstawowe akty unijne w tym zakresie obowiązują w Polsce bezpośrednio, gdyż są rozporządzeniami lub wymagają jako dyrektywy implementacji do polskiego porządku prawnego. W zakresie cyberbezpieczeństwa obowiązuje obecnie NIS 2. Przed przyjęciem NIS 2 w UE w Polsce były prowadzone od 2020 r. prace nad nowelą k.s.c., której projekt z dnia 3 lipca 2023 r. został skierowany do Sejmu, a następnie wycofany z niego przez rząd. W obecnej sytuacji należy postulować dokonanie implementacji nowej dyrektywy NIS 2 i zaniechać dalszych prac nad nowelą ustawy o krajowym systemie cyberbezpieczeństwa. Kontynuowanie prac nad projektem z dnia 3 lipca 2023 r. oznaczać może przyjęcie rozwiązań niespójnych z dyrektywą NIS 2. Brak uzasadnienia dla prowadzenia dalszych prac legislacyjnych nad dwoma nowelami u.k.s.c. w tym samym czasie, tj. jednej wynikającej z konieczności implementacji przepisów unijnych (NIS 2), a drugiej, stanowiącej kontynuację trwających prac nad nowelą u.k.s.c. Przyjmowanie przepisów w drodze kolejnej noweli u.k.s.c. mogło zagrozić terminowej transpozycji NIS 2. Prowadzenie prac zarówno nad wdrożeniem NIS 2, jak i nowelą u.k.s.c. mogłoby spowodować także dla przedsiębiorców, zwłaszcza mniejszych i średnich, dodatkowe koszty związane najpierw z wprowadzeniem obowiązków z noweli u.k.s.c., a następnie analogicznych lub zmodyfikowanych obowiązków wynikających z wdrożenia NIS 2.

2. Po raz pierwszy w obszarze bezpieczeństwa sieci i usług telekomunikacyjnych pojawiła się kwestia bezpieczeństwa sprzętu i usług dostarczanych przez dostawców z innych krajów do budowy sieci nowej generacji 5G. W projekcie z dnia 3 lipca 2023 r. przygotowane zostały w tym zakresie nowe uregulowania, dotychczas niewystępujące w polskim systemie prawnym, a dotyczące oceny dostawców sprzętu, usług i oprogramowania ICT (art. 1 pkt 58 i n. projektu z dnia 3 lipca 2023 r.). Przewidziane w art. 66a projektu z dnia 3 lipca 2023 r. postępowanie w sprawie uznania dostawcy produktów ICT, usług ICT lub procesów ICT, za dostawcę wysokiego ryzyka, kończy się wydaniem decyzji, która jest w znaczeniu faktycznym i prawnym rozstrzygnięciem o istotnych prawach i obowiązkach podmiotów gospodarczych działających na rynku telekomunikacyjnym w Polsce. Stanowi ona ograniczenie praw podmiotów gospodarczych. Przepis art. 22 Konstytucji RP dopuszcza ograniczenie wolności działalności gospodarczej, ale to ograniczenie jest dopuszczalne tylko w drodze ustawy

i tylko ze względu na ważny interes publiczny. Musi więc być wykazany „ważny interes publiczny" uzasadniający tworzenie tego rodzaju ograniczeń. Ponadto należy podkreślić, że aby ustanawiane przez organy władzy publicznej ograniczenia wolności działalności gospodarczej były ograniczeniami usprawiedliwionymi (a tym samym by były one konstytucyjnie legalne), muszą być one nie tylko ukierunkowane na realizację ważnego interesu publicznego, ale równocześnie muszą też być względem tego ważnego interesu publicznego proporcjonalne. Proporcjonalność ustanawianych ograniczeń jest (obligatoryjną) materialną przesłanką usprawiedliwiającą te ograniczenia, przy czym obowiązek spełniania tej przesłanki przez organy władzy publicznej (kreujące ograniczenia wolności działalności gospodarczej) wynika z art. 31 ust. 3 Konstytucji RP, mówiącego o wymogu „konieczności" ustanawianych ograniczeń.

3. Projekt z dnia 3 lipca 2023 r. określa podmioty, których może dotyczyć postępowanie w sprawie dostawcy. Nie jest natomiast precyzyjnie określone, co będzie przedmiotem tego postępowania. Z postanowień art. 66a ust. 1 projektu wynika tylko, że postępowanie jest prowadzone w sprawie uznania dostawcy produktów ICT, usług ICT lub procesów ICT za dostawcę wysokiego ryzyka. Nie jest natomiast wskazane, jakich produktów czy usług ma ono dotyczyć. W przypadku więc, gdyby ocenie miały podlegać urządzenia lub oprogramowanie dla sieci telekomunikacyjnych, należałoby wyraźnie wskazać, jakich urządzeń lub oprogramowania dotyczy to postępowanie. Projektowany system oceny będzie miał zastosowanie, nie tylko do przedsiębiorców łączności elektronicznej w zakresie sieci 5G, ale także wobec innych podmiotów krajowego systemu cyberbezpieczeństwa, w tym operatorów usług kluczowych, tj. m.in. sektora energetyki, finansowego, ochrony zdrowia czy transportu. W związku z tym brak precyzji w zakresie określenia przedmiotu postępowania może skutkować tym, że np. wykluczenie dokonane wobec danego dostawcy będzie potencjalnie uzasadnione wobec jednego sektora, ale w drugim spowoduje istotne i nieoczekiwane konsekwencje.

4. Wszczęcie z urzędu albo na wniosek przewodniczącego Kolegium postępowania w sprawie uznania dostawcy za dostawcę wysokiego ryzyka powinno zawierać uzasadnienie. Wniosek przewodniczącego Kolegium o wszczęcie postępowania w sprawie uznania dostawcy za dostawcę wysokiego ryzyka powinien w szczególności zawierać: ustalenie urządzeń lub oprogramowania dostawcy, które mają podlegać ocenie ryzyka; określenie podmiotów, które wykorzystują lub mogą wykorzystywać urządzenia lub oprogramowanie dostawcy, które mają podlegać ocenie ryzyka; identyfikację poziomu wykorzystania sprzętu lub oprogramowania w realizacji przez przedsiębiorców telekomunikacyjnych obowiązków wynikających ze stanów nadzwyczajnych i stanu wojny; ustalenie poziomu

zobowiązań przedsiębiorców telekomunikacyjnych i użytkowników końcowych wobec dostawcy; ustalenie innych podmiotów działających na tym samym rynku co oceniany dostawca w zakresie urządzeń i oprogramowania, w którego zakresie ma zostać dokonana ocena; określenie, jakiego zakresu dotyczy ocena; stwierdzenie skali działań mających zostać podjętych przez przedsiębiorstwa telekomunikacyjne, podmioty publiczne i użytkowników końcowych, w tym kosztów; propozycje alternatywnych działań w stosunku do sprzętu lub oprogramowania danego dostawcy.

5. Zgodnie z art. 66a ust. 3 projektu z dnia 3 lipca 2023 r. stroną postępowania w sprawie uznania za dostawcę wysokiego ryzyka jest każdy, wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Projekt wyłącza więc stosowanie art. 28 k.p.a., który definiuje stronę postępowania administracyjnego, a w to miejsce wprowadza węższą definicję strony, którą miałby być ten, wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Wydana w wyniku takiego postępowania decyzja spowoduje jednak powstanie z mocy prawa obowiązków po stronie podmiotów wskazanych w art. 66a ust. 1 pkt 1–3 projektu z dnia 3 lipa 2023 r. (niewprowadzanie lub wycofanie z użytkowania danych produktów, usług lub procesów dostarczanych przez dostawcę, którego dotyczy decyzja). Projekt pozbawia więc statusu strony podmiotów, które na podstawie k.p.a. przymiot ten posiadałyby, co wpływa na ocenę interesu prawnego na gruncie p.p.s.a., a w konsekwencji możliwości wniesienia skargi do sądu (istnienie prawa do sądu).

6. Przepis art. 66a ust. 9 projektu z dnia 3 lipca 2023 r. jest szczególnie ważny, gdyż kluczowym zagadnieniem jest to, według jakich kryteriów ocena zostanie przeprowadzona. Ocena musi być bowiem dokonywana według precyzyjnie określonych, jasnych, niebudzących wątpliwości i weryfikowalnych kryteriów. Nie mogą to być kryteria posługujące się pojęciami niezdefiniowanymi, pozwalającymi na wieloznaczne oceny. W przeciwnym razie nie będzie to ocena obiektywna, ale uznaniowa, pozbawiona merytorycznych podstaw, prowadząca do błędnych wniosków. W zakresie kryteriów oceny dostawców główną rolę powinny odgrywać kryteria o charakterze technicznym, które pozwalałyby na badanie pod względem technicznym bezpieczeństwa infrastruktury, czyli weryfikację za pomocą mierzalnych technicznych kryteriów bezpieczeństwa tej infrastruktury. Techniczne kryteria oceny powinny być ze sobą powiązane i tworzyć spójny model ochrony bezpieczeństwa infrastruktury. Model ten powinien charakteryzować się obiektywnością weryfikacji kryteriów i dużym stopniem profesjonalizacji weryfikacji, gwarantującej poprawność wyników stosowanych kryteriów oceny. Kryteria pozatechnologiczne bardzo często są niedefiniowalne i posługują się niedookreślonymi pojęciami, które są trudne do zweryfikowania i dokonania oceny. Przewidziane w art. 66a ust. 9 projektu z dnia 3 lipca 2023 r.

kryteria oceny dostawcy powinny być uzupełnione o następujące elementy: weryfikację techniczną w odpowiednim laboratorium; wpływ na konkurencję i konsumentów, a także możliwość utrzymania ciągłości usług, systemów i produktów, w których stosowane jest dane oprogramowanie lub urządzenie; zidentyfikowanie podmiotów, których ocena ryzyka będzie dotyczyła.

7. Zgodnie z projektem organem uprawnionym do dokonywania oceny jest Kolegium, które jest działającym przy Radzie Ministrów organem opiniodawczo-doradczym. W jego skład wchodzą przedstawiciele administracji publicznej, tj. Pełnomocnik Rządu ds. Cyberbezpieczeństwa, określeni ministrowie, szef BBN, minister koordynator służb specjalnych. Oznacza to, że Kolegium jest głównie gremium polityczno-administracyjnym. W jego składzie brakuje natomiast organów lub jednostek posiadających pogłębioną wiedzę techniczną oraz doświadczenie w certyfikacji i ocenie urządzeń i oprogramowania. Osoby takie znajdują w jednostkach i organach podległych lub nadzorowanych przez podmioty tworzące skład kolegium, których udział w Kolegium nie jest przewidziany. Postulować więc należy, aby skład Kolegium, przynajmniej na potrzeby dokonywania oceny dostawców, uzupełniany był o jednostki *stricte* techniczne, w tym certyfikacyjne, które na podstawie przyjętych międzynarodowych standardów mogłyby przedstawiać analizę techniczno-inżynierską ocenianych dostawców. Jednostki te mogłyby być zarówno laboratoriami publicznymi, jak i prywatnymi, niekoniecznie mającymi siedzibę na terytorium Polski. Udział takich jednostek w procesie oceny byłby korzystny również dla trwałości decyzji w sprawie dostawców, która posiadając uzasadnienie techniczne, miałaby mocniejsze podstawy merytoryczne.

8. Projekt z dnia 3 lipca 2023 r. nie przewiduje możliwości przedstawienia środków zaradczych. Tymczasem podmiot, który został uznany za dostawcę wysokiego ryzyka, powinien mieć zapewnioną możliwość przedstawienia środków zaradczych i planu naprawczego albo wniesienia odwołania.

9. Przewidziany w projekcie okres na wycofanie sprzętu powinien być dłuższy i wynieść okres 9–10 lat, gdyż tyle wynoszą realne okresy amortyzacji urządzeń. Wymiana sprzętu powinna odnosić się do określonego sprzętu i oprogramowania zamiast do dostawcy. Konstrukcja wycofywania sprzętu z użytkowania wywołuje poważne wątpliwości z uwagi na obowiązywanie jednej z kardynalnych zasad prawa, tj. zasady niedziałania prawa wstecz. Przepis nakazujący wycofywanie sprzętu zakupionego wiele lat wcześniej stanowi objęcie regulacją zdarzeń wcześniejszych, sprzed kilku lat, które dotyczyły zawierania umów o zakup sprzętu na podstawie obowiązujących wówczas przepisów. Tym bardziej więc powinien być uwzględniony postulat zapewnienia odpowiednio długiego okresu na wycofywanie sprzętu z użytkowania.

10. Proponowane w art. 66d ust. 1–2 projektu z dnia 3 lipca 2023 r. rozwiązania, a w szczególności rozpatrywanie przez sąd administracyjny skargi na posiedzeniu niejawnym oraz doręczenie skarżącemu odpisu wyroku z tą częścią uzasadnienia, która nie zawiera informacji niejawnych, może oznaczać w praktyce prowadzenie postępowania z naruszeniem zasady efektywnej ochrony sądowej, stanowiącej jeden z fundamentów zasady prawa do sądu wyrażonej zarówno w art. 45 Konstytucji RP, jak i art. 6 EKPC.

# Bibliografia


Adamiak B., *Z problematyki właściwości sądów administracyjnych (art. 3 § 2 pkt 4 p.p.s.a.)*, „Zeszyty Naukowe Sądownictwa Administracyjnego" 2006, nr 2.

Banasiński C., Nowak W., *Europejski i krajowy system cyberbezpieczeństwa*, w: C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018.

Banasiński C., *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, w: *idem*, (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018.

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2012.

Besiekierska A. (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.

Betkier M., Górski J., *Ochrona sieci przed zagrożeniami*, „Prawo i Regulacje Świata Telekomunikacji i Mediów" 2010, nr 2.

Bogusz M., *Pojęcie aktów lub czynności z zakresu administracji publicznej dotyczących stwierdzenia lub uznania uprawnienia lub obowiązku wynikających z przepisów prawa w rozumieniu art. 16 ust. 1 pkt 4 ustawy o NSA*, „Samorząd Terytorialny" 2000, nr 1–2.

Ciapała J., *Konstytucyjna wolność działalności gospodarczej w Rzeczypospolitej Polskiej*, Szczecin 2009.

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

Dauter B., Gruszczyński B., Kabat A., Niezgódka-Medek M., *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, Warszawa 2009.

Garlicki L., *Polskie prawo konstytucyjne*, Warszawa 2002.

Gronkiewicz A., Ziółkowska A., *Sankcja administracyjna w korporacjach zawodowych w odniesieniu do samorządów zaufania publicznego*, w: M. Lewicki, R. Lewicka, G. Stahl (red.), *Sankcje administracyjne. Blaski i cienie*, Warszawa 2011.

Hauser R. (red.), *System prawa administracyjnego*, t. 10: *Postępowanie przed sądami administracyjnymi*, Warszawa 2016.

Hauser R., Wierzbowski M. (red.), *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, Warszawa 2023.

Jaśkowska M., *Akty i czynności z zakresu administracji publicznej w rozumieniu art. 16 ust. 1 pkt 4 ustawy o Naczelnym Sądzie Administracyjnym jako przedmiot kontroli*, w: J. Stelmasiak, J. Niczyporuk, S. Fundowicz (red.), *Polski model sądownictwa administracyjnego*, Lublin 2003.

Jaśkowska M., *Właściwość sądów administracyjnych (zagadnienia wybrane)*, w: J. Zimmermann (red.), *Koncepcja systemu prawa administracyjnego. Zjazd Katedr Prawa Administracyjnego i Postępowania Administracyjnego, Zakopane, 24–27 września 2006 r.*, Warszawa 2007.

Kitler W., Taczkowska-Olszewska J., Radoniewicz F. (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.

Koselski M., *Sporządzenie planów działań operatorów publicznych w sytuacjach szczególnych zagrożeń*, „Biuletyn Urzędu Regulacji Telekomunikacji i Poczty" 2003, nr 2.

Litwiński P. (red.), P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018.

Lubasz D., w: E. Bielak-Jomaa, D. Lubasz, *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.

Mądrzak H., *Prawo do sądu jako gwarancja ochrony praw człowieka*, w: L. Wiśniewski (red.), *Podstawowe prawa jednostki i ich sądowa ochrona*, Warszawa 1997.

Piątek S., *Prawo telekomunikacyjne. Komentarz*, Warszawa 2019.

*Prokop K., Stany nadzwyczajne w Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.*, Białystok 2005.

Rogalski M., *Projekt ustawy Prawo komunikacji elektronicznej – zagadnienia wybrane*, „Krytyka Prawa" 2021, nr 2.

Rogalski M., *Specobowiązki przedsiębiorców telekomunikacyjnych*, „Prawo Teleinformatyczne" 2007, nr 1.

Rogalski M., *Środki zaskarżenia w aukcji prowadzonej na podstawie przepisów Prawa telekomunikacyjnego w celu rozdysponowania częstotliwości*, „Przegląd Ustawodawstwa Gospodarczego" 2021, nr 10.

Safjan M., Bosek L., *Konstytucja RP. Tom I. Komentarz do art. 1–86*, Warszawa 2016.

Sibiga G., *Wystąpienie – nowa kompetencja Generalnego Inspektora Ochrony Danych Osobowych*, dodatek do „Monitor Prawniczy" 2011, nr 3.

Tarno J.P., *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, Warszawa 2008.

Trąbiński P., *Podział kompetencji* w zapewnianiu cyberbezpieczeństwa, w: G. Szpor, A. Gryszczyńska (red.), *Internet. Strategie bezpieczeństwa. Internet: security strategy*, Warszawa 2017.

Vytogianni E., Dekker M., *Security Supervision under the EECC*, https://www.enisa.europa.eu/publications/supporting-the-implementation-of-theeuropean-electronic--commmunications-code-eecc [dostęp: 12.02.2023 r.].

Wincenciak M., *Sankcje w prawie administracyjnym i procedura ich wymierzania*, Warszawa 2008.

Wiśniewski L., *Stany nadzwyczajne w projekcie nowej Konstytucji RP* w: T. Jasudowicz (red.), *Prawa człowieka w sytuacjach nadzwyczajnych ze szczególnym uwzględnieniem prawa i praktyki polskiej*, Toruń 1997.

Woś T. (red.), *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, LEX 2016.

Wróbel A. (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, Warszawa 2019.

W monografii podjęto wybrane problemy polityki bezpieczeństwa w obszarze sieci i usług łączności elektronicznej, ze szczególnym uwzględnieniem obowiązujących regulacji międzynarodowych i krajowych w tym zakresie. Jest to materia, która, z roku na rok, zyskuje coraz większą uwagę, ze względu na obejmowanie usługami łączności elektronicznej coraz większej ilości kontaktów osobistych, zwłaszcza w obszarze administracji i dziedzin związanych z infrastrukturą wrażliwą, w tym krytyczną.

Dr hab. Andrzej Zapałowski, prof. UR

Autor monografii podjął się wyzwania sprowadzającego się nie tylko do analizy obowiązujących przepisów prawa Unii Europejskiej i prawa polskiego w zakresie bezpieczeństwa sieci i usług łączności elektronicznej, ale również przybliżenia projektów aktów normatywnych. Istotnym atutem monografii są krytyczne i konstruktywne uwagi *de lege lata* i *de lege ferenda* w sferze prawa cyberbezpieczeństwa. Stąd też opracowanie może i powinno stanowić istotną pomoc zarówno dla podmiotów stosujących, jak i tworzących prawo cyberbezpieczeństwa.

Dr hab. Mariusz Wieczorek, prof. URad

ISBN 978-83-66723-71-9
9 788366 723719

DOI 10.26399/978-83-66723-71-9