NR 1 - STYCZEŃ 2021

NEWSLETTER

IT-TECH

W NUMERZE:

Traple Konarski Podrecki & Wspólnicy

TKP

Nowelizacja prawa telekomunikacyjnego – częściowe wdrożenie EKŁE

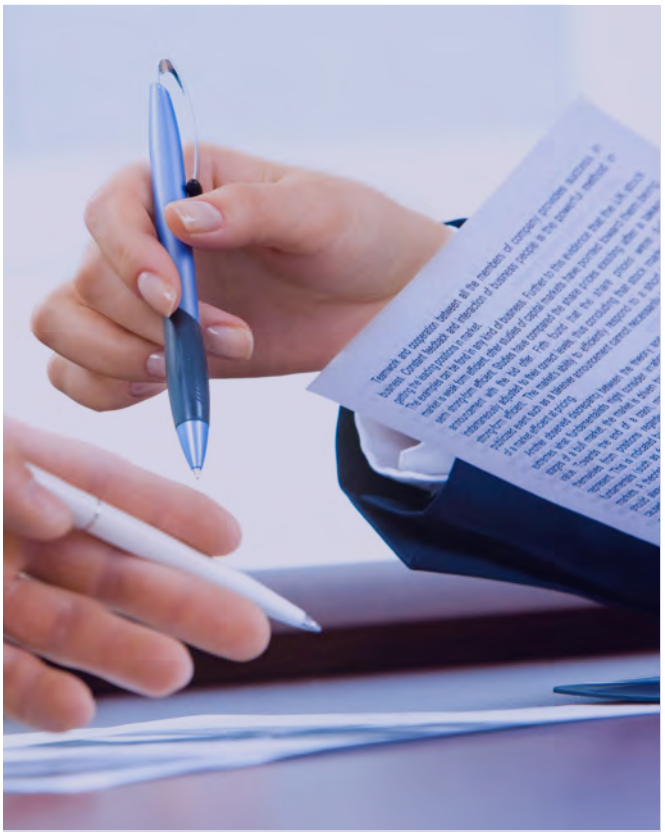
r.pr. Magdalena Gąsowska-Paprota

Z dniem 21 grudnia 2020 r. weszła w życie nowelizacja ustawy Prawo telekomunikacyjne (PT)[1], wprowadzona ustawą z dnia 14 maja 2020 r. o zmianie niektórych ustaw w zakresie działań osłonowych w związku z rozprzestrzenianiem się wirusa SARS-CoV-2[2], czyli tzw. tarczą 3.0. Ta nowelizacja PT stanowi pierwszy etap wdrożenia w polskim prawie zmian wymaganych Europejskim Kodeksem Łączności Elektronicznej (EKŁE)[3].

To „kadłubowe" wdrożenie EKŁE dotyczy obszaru umów zawieranych z abonentami, a także usług dostępu do Internetu, w tym ich ciągłości przy zmianie dostawcy – czyli ogranicza się do wybranych zagadnień z tytułu III EKŁE, który dotyczy praw użytkowników końcowych (w szczególności art. 102, 105, 106 EKŁE).

Główne zmiany związane są z ułatwieniem rozwiązania umowy o świadczenie usług telekomunikacyjnych przez abonenta – teraz dostawca usług telekomunikacyjnych musi umożliwić abonamentowi złożenie wypowiedzenia również w formie dokumentowej, jeżeli w takiej formie umożliwia zawarcie umowy. Dla zachowania formy dokumentowej, zgodnie z art. 77(2) i 77(3) kodeksu cywilnego[4], wystarczy złożenie oświadczenia właściwie w jakikolwiek utrwalony sposób umożliwiający zidentyfikowanie nadawcy. Może to być m.in. zwykły email. Tak złożone oświadczenie abonenta o wypowiedzeniu, przedsiębiorca ma obecnie obowiązek niezwłocznie potwierdzić (w ciągu 1 dnia roboczego) poprzez wiadomość SMS (lub połączenie głosowe w przypadku usług stacjonarnych), a następnie na trwałym nośniku w ciągu 14 dni.

Co więcej, nowości wiążą się z automatycznym przedłużaniem umowy o świadczenie usług telekomunikacyjnych zawartej na czas określony w umowę na czas nieokreślony. Po pierwsze, dostawca usług ma obowiązek poinformować abonenta o takim przedłużeniu z 30-dniowym wyprzedzeniem, jednocześnie informując o sposobach rozwiązania umowy i swoich najkorzystniejszych pakietach taryfowych. Po drugie, abonent będzie miał prawo rozwiązać taką przedłużoną umowę w każdym czasie z zachowaniem 1-miesięcznego okresu wypowiedzenia. Abonentowi, który wyraził zgodę na otrzymywanie wiadomości marketingowych, dostawca usług musi zresztą rokrocznie przesyłać informację o swoich najkorzystniejszych pakietach taryfowych.



[1] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2019 r. poz. 2460 z późn. zm.).
[2] Dz. U. poz. 875 z późn. zm.
[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona)Tekst mający znaczenie dla EOG (Dz. U. UE. L. z 2018 r. Nr 321, str. 36 z późn. zm.).
[4] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2020 r. poz. 1740 z późn. zm.).

Wprowadzono ponadto obowiązek umożliwienia abonentowi, będącemu konsumentem, monitorowania stopnia wykorzystania usług rozliczanych w oparciu o czas lub ilość wykorzystanych danych/jednostek oraz informowania o wykorzystaniu limitu.

Jeżeli chodzi o przenoszenie numerów do innego dostawcy usług, dotychczas abonent mógł zdecydować się na przeniesienie do 1-miesiąca po rozwiązaniu umowy.

Nowe przepisy o ciągłości usług dostępu do internetu w przypadku zmiany dostawcy przewidują m.in., że nowy usługodawca ma obowiązek aktywować usługę przeniesionego klienta najpóźniej w ciągu 1 dnia roboczego, a do tego czasu dotychczasowy dostawca ma obowiązek świadczyć usługę. UKE będzie zaś miał za zadanie zapewnić system teleinformatyczny do wymiany informacji między dostawcami usług, mający umożliwiać realizację ich obowiązków związanych z zapewnieniem ciągłością dostępu do internetu.

Nowelizacja zapewnia jedynie fragmentaryczne wdrożenie przepisów EKŁE, a w obszarze praw użytkowników końcowych czekają nas dalsze zmiany, m.in. dotyczące ograniczenia odszkodowań za wcześniejsze rozwiązanie umowy przez abonenta, nakazujące przyznanie części uprawnień mikro-, małym przedsiębiorcom i organizacjom non-profit na równi z konsumentami, i inne. Na wdrożenie EKŁE w całości, pomimo upływu terminu 21 grudnia 2020 r. wyznaczonego tą dyrektywą, będziemy musieli poczekać, gdyż obecnie projekt ustawy Prawo komunikacji elektronicznej, która ma zastąpić PT, i ustawy ją wprowadzającej jest na etapie konsultacji i opiniowania i nie został jak na razie w ogóle podany do wiadomości finalny projekt, który zostanie przekazany do Sejmu.

Jak uzyskać zezwolenie na umieszczenie infrastruktury telekomunikacyjnej na nieruchomości prywatnej?

r.pr. Magdalena Gąsowska-Paprota, apl. radc. Aleksander Elmerych

Dynamiczny rozwój nowych technologii ma niewątpliwie ogromny wpływ na nasze codzienne życie prywatne i zawodowe – rozwiązania *smart home* umożliwiają nam zdalną obsługę wszystkich domowych urządzeń, chmura obliczeniowa sprawia, że możemy pracować zdalnie tak, jakbyśmy byli w biurze, a narzędzia wideokonferencyjne dają nam możliwość udziału w spotkaniach online z poziomu laptopa lub smartfona, niezależnie od tego, gdzie się w danej chwili znajdujemy. Wszystkie wymienione wyżej technologie łączy to, że do funkcjonowania wymagają szybkiego, stałego i stabilnego łącza internetowego, z którym – poza obszarami dużych miast i miejscowości – nadal występują spore trudności.

Rozwój infrastruktury telekomunikacyjnej podstawą rozwoju gospodarczego

Szybki Internet stanowi element niezbędny dla zapewnienia wzrostu gospodarczego, tworzenia miejsc pracy oraz umożliwienia obywatelom i przedsiębiorstwom dostępu do treści i usług. W związku z tym wspieranie rozwoju łączności internetowej wysokiej przepustowości jest jednym z głównych założeń unijnej, a także polskiej polityki rozwoju gospodarczego i społecznego, co znalazło odzwierciedlenie m.in. w komunikatach Komisji Europejskiej (np. Europejska agenda cyfrowa[1], W kierunku europejskiego społeczeństwa gigabitowego[2]) oraz w polskim Narodowym Planie Szerokopasmowym[3], który zakłada m.in. zapewnienie do 2025 r. wszystkim gospodarstwom domowym dostępu do Internetu o przepustowości dla łącza „w dół" wynoszącej co najmniej 100 Mb/s. Inwestycje mające prowadzić do spełnienia założeń wynikających z tych strategicznych aktów prawnych realizowane są m.in. w ramach działania 1.1 Programu Operacyjnego Polska Cyfrowa, którego celem jest wyeliminowanie terytorialnych różnic w możliwości dostępu do szerokopasmowego Internetu o wysokich przepustowościach. Realizacja tego rodzaju inwestycji wymaga fizycznej instalacji określonego rodzaju urządzeń i obiektów infrastruktury telekomunikacyjnej, np. rurociągów światłowodowych, studzienek telekomunikacyjnych, słupów czy masztów na działkach należących nie do inwestora, lecz m.in. do prywatnych właścicieli, co wiąże się z koniecznością uzyskania ich zgody.

Umowne uregulowanie zlokalizowania infrastruktury telekomunikacyjnej na nieruchomości

Inwestorzy realizujący inwestycje telekomunikacyjne powinni w pierwszej kolejności dążyć do osiągnięcia porozumienia z właścicielami nieruchomości i spróbować uregulować kwestię umieszczenia na nieruchomości infrastruktury telekomunikacyjnej w umowie. Można wskazać na dwa rodzaje umów, które pozwalają osiągnąć ten cel:

- umowa o ustanowienie służebności przesyłu, uregulowana w art. 305(1) i następnych Kodeksu cywilnego[4] (dalej: „k.c.");
- umowa o korzystanie z nieruchomości, uregulowana w art. 33 ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych[5] (dalej: „megaustawa").

[1] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Europejska agenda cyfrowa, KOM(2010) 245 wersja ostateczna/2.
[2] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Łączność dla konkurencyjnego jednolitego rynku cyfrowego: w kierunku europejskiego społeczeństwa gigabitowego, COM/2016/0587 final.
[3] Uchwała nr 2/2014 Rady Ministrów z dnia 8 stycznia 2014 r. w sprawie przyjęcia programu rozwoju „Narodowy Plan Szerokopasmowy".
[4] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2020 r., poz. 1740).
[5] Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (t.j. Dz. U. z 2019 r., poz. 2410, z późn. zm.).

Służebność przesyłu uregulowana w k.c. jest instytucją pozwalającą każdemu przedsiębiorcy, który zamierza wybudować na cudzej nieruchomości urządzenia przesyłowe lub który jest właścicielem takich urządzeń (a więc zgodnie z art. 49 § 1 k.c. urządzeń służących do doprowadzania lub odprowadzania płynów, pary, gazu, energii elektrycznej lub innych podobnych urządzeń, np. urządzeń telekomunikacyjnych), na uregulowanie zasad korzystania z nieruchomości w związku z obsługą tych urządzeń. Służebność przesyłu może zatem obejmować w szczególności prawo polegające na dostępie do oznaczonej części nieruchomości, możliwość wykonywania naprawy i konserwacji urządzeń czy zapewnienie do nich drogi dojazdowej. Zgodnie z art. 305(4) k.c. do służebności przesyłu stosuje się odpowiednio przepisy o służebnościach gruntowych, a więc m.in. powinny one zostać oznaczone według zasad współżycia społecznego i przy uwzględnieniu zwyczajów miejscowych (art. 287 k.c.), a także powinny być wykonywane w sposób jak najmniej utrudniający korzystanie z nieruchomości obciążonej (art. 288 k.c.).

Umowa o korzystanie z nieruchomości z art. 33 megaustawy jest z kolei specjalnym typem umowy, wprowadzonym na potrzeby realizowania inwestycji telekomunikacyjnych polegających np. na budowie linii kablowych, rurociągów światłowodowych, studni telekomunikacyjnych czy słupów telekomunikacyjnych. Właściciel, użytkownik wieczysty lub zarządca nieruchomości powinien zawrzeć umowę o korzystanie z nieruchomości, jeżeli z wnioskiem o jej zawarcie wystąpi jeden z podmiotów wskazanych w art. 33 megaustawy, a więc:

- operator w rozumieniu art. 2 pkt 27 lit. b pr. tel.[6], czyli przedsiębiorca telekomunikacyjny uprawniony do dostarczania publicznych sieci telekomunikacyjnych lub świadczenia usług towarzyszących lub
- podmiot, o którym mowa w art. 4 pkt 1, 2, 4, 5 i 8 pr. tel. (np. jednostki podległe Ministrowi Obrony Narodowej lub ministrowi właściwemu do spraw administracji publicznej, jednostki organizacyjne Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu i Centralnego Biura Antykorupcyjnego czy Krajowej Administracji Skarbowej i in.) lub
- jednostka samorządu terytorialnego wykonująca działalność w zakresie telekomunikacji, o której mowa w art. 3 ust. 1 megaustawy.

Zakres podmiotów mogących skorzystać z umowy o korzystanie z nieruchomości na potrzeby zalegalizowania umieszczenia na niej infrastruktury telekomunikacyjnej został zatem znacząco ograniczony, przy jednoczesnym rozszerzeniu katalogu podmiotów zobowiązanych do zawarcia takiej umowy – oprócz właścicieli nieruchomości zobowiązani są również użytkownicy wieczyści i zarządcy nieruchomości. Mają oni obowiązek umożliwienia podmiotom wskazanym w pkt. 1–3 powyżej umieszczenia na nieruchomości obiektów i urządzeń infrastruktury telekomunikacyjnej, jeżeli:

- nie jest to związane wyłącznie z zapewnieniem telekomunikacji w budynku znajdującym się na tej nieruchomości oraz
- nie uniemożliwia to racjonalnego korzystania z nieruchomości, w szczególności nie prowadzi do istotnego zmniejszenia wartości nieruchomości.
- Umowa o korzystanie z nieruchomości jest co do zasady odpłatna i powinna zostać zawarta na piśmie w terminie 30 dni od dnia wystąpienia do właściciela ze stosownym wnioskiem.

Brak zgody właściciela nieruchomości na zawarcie umowy

W praktyce jednak część właścicieli nieruchomości może odmówić zawarcia umowy – w takiej sytuacji, w zależności od obranego wcześniej trybu postępowania:

- 1inwestor może na podstawie art. 305(2) § 1 k.c. wystąpić do sądu z wnioskiem o ustanowienie na jego rzecz służebności przesyłu;
- inwestor może na podstawie art. 33 ust. 7 megaustawy wszcząć postępowanie administracyjne w sprawie wydania decyzji ograniczającej korzystanie z nieruchomości przez udzielenie zezwolenia na umieszczenie na tej nieruchomości infrastruktury telekomunikacyjnej (dalej: „decyzja ograniczająca korzystanie z nieruchomości").

[6] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2019 r., poz. 2460, z późn. zm.).

Warto pamiętać przy tym, że przesłanką sądowego ustanowienia służebności przesyłu jest odmowa zawarcia umowy o ustanowienie służebności przesyłu, a przesłanką wydania decyzji ograniczającej korzystanie z nieruchomości jest bezskuteczny upływ 30 dni od dnia wystąpienia z wnioskiem o zawarcie umowy ograniczającej korzystanie z nieruchomości – dlatego już przystępując do rozmów z właścicielem, inwestor powinien prowadzić je w taki sposób, by w razie odmowy właściciela możliwe było skorzystanie przez inwestora z wybranej dalszej drogi postępowania albo sądowego, albo administracyjnego. Omawiane tryby postępowania, choć w praktyce prowadzą do osiągnięcia podobnego skutku, są bowiem trybami całkowicie rozłącznymi i prowadzonymi na podstawie odrębnych przepisów materialnych i proceduralnych. Zdecydowawszy się na uregulowanie kwestii umieszczenia infrastruktury telekomunikacyjnej na nieruchomości w drodze służebności przesyłu, należy skorzystać z postępowania sądowego, natomiast kwestia korzystania z nieruchomości na potrzeby umieszczenia na niej infrastruktury telekomunikacyjnej może zostać uregulowana w drodze decyzji administracyjnej.

Postępowanie sądowe w sprawie ustanowienia służebności przesyłu jest prowadzone na wniosek w postępowaniu nieprocesowym. W jego trakcie często zachodzi konieczność powołania biegłych, np. na okoliczność wyznaczenia obszaru korzystania z nieruchomości czy ustalenia wartości służebności przesyłu. Prowadzi to do wydłużenia czasu rozpatrywania sprawy oraz wiąże się często z koniecznością ponoszenia kosztów opinii biegłych, które niekiedy wielokrotnie przewyższają wartość samej służebności. Warto również pamiętać o tym, że w przypadku wyznaczenia przez sąd rozprawy inwestor powinien zapewnić sobie odpowiednią reprezentację, co z uwagi na miejscową właściwość sądu położenia nieruchomości może napotkać trudności praktyczne związane z dojazdami.

Z kolei postępowania administracyjne o wydanie decyzji ograniczającej korzystanie z nieruchomości prowadzone są przez starostę właściwego ze względu na położenie nieruchomości, na podstawie art. 33 megaustawy w zw. z art. 124 i 124a u.g.n.[7], w trybie określonym przepisami Kodeksu postępowania administracyjnego[8] (dalej: „k.p.a.”). W praktyce wątpliwości budzi „odpowiednie stosowanie” przepisów art. 124 i 124a u.g.n. do postępowania administracyjnego w sprawie wydania decyzji ograniczającej korzystanie z nieruchomości, w szczególności w zakresie różnic pomiędzy wnioskiem o zawarcie umowy o korzystanie z nieruchomości a podjęciem rokowań, o których mowa w art. 124 ust. 3 u.g.n., jak również w zakresie stosowania pozostałych przepisów rozdziału 4 u.g.n., które regulują zasady wywłaszczenia nieruchomości. Powoduje to szereg trudności praktycznych, które zostały zauważone m.in. przez Urząd Komunikacji Elektronicznej – w odpowiedzi na nie opublikowano specjalny przewodnik dla starostów dotyczący decyzji ograniczających korzystanie z nieruchomości, w którego przygotowaniu brali udział prawnicy naszej kancelarii (link do przewodnika znajduje się na końcu artykułu). Poza przesłankami z art. 33 megaustawy, omówionymi w poprzedniej części artykułu, do wydania decyzji ograniczającej korzystanie z nieruchomości konieczne jest m.in. przeprowadzenie rokowań z właścicielem oraz zapewnienie zgodności z planem miejscowym lub decyzją o lokalizacji inwestycji celu publicznego (z wyjątkiem sytuacji, które dotyczą głównie urządzeń łączności publicznej stanowiących jednocześnie infrastrukturę telekomunikacyjną o nieznacznym oddziaływaniu), a w zakresie urządzeń łączności publicznej decyzja powinna zostać również uzgodniona z Prezesem Urzędu Komunikacji Elektronicznej. Pewne odrębności zostały także przewidziane w przypadku postępowania, którego przedmiotem jest nieruchomość o nieuregulowanym stanie prawnym, a więc taka, której właściciela nie można ustalić lub której właściciel nie żyje i nie zostało zakończone po nim postępowanie spadkowe (zob. art. 124a u.g.n.). Decyzja ograniczająca korzystanie z nieruchomości wydawana jest na podstawie przepisów postępowania administracyjnego, zatem co do zasady postępowanie nie powinno trwać dłużej niż dwa miesiące w przypadku spraw szczególnie skomplikowanych (art. 35 § 3 k.p.a.). W praktyce jednak realny termin załatwienia sprawy jest dłuższy – organy administracji publicznej mają możliwość wydłużenia terminu wynikającego z art. 35 k.p.a., a dodatkowo w postępowaniach najczęściej zachodzi konieczność uzgodnienia treści decyzji z Prezesem Urzędu Komunikacji Elektronicznej. W odróżnieniu od postępowania sądowego w sprawie ustanowienia służebności decyzja ograniczająca korzystanie z nieruchomości nie określa odszkodowania należnego właścicielowi – takie odszkodowanie może zostać mu przyznane w drodze osobnej decyzji administracyjnej, wydawanej dopiero po umieszczeniu infrastruktury telekomunikacyjnej na nieruchomości[9].

[7] Ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami (t.j. Dz. U. z 2020 r., poz. 1990).
[8] Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2020 r., poz. 256, z późn. zm.).
[9] Zob. wyrok Naczelnego Sądu Administracyjnego z dnia 5 października 2007 r., sygn. I OSK 1389/06

Który tryb postępowania wybrać?

Kwestia umieszczenia infrastruktury telekomunikacyjnej na nieruchomości może zostać uregulowana albo w drodze ustanowienia służebności przesyłu (poprzez zawarcie umowy, a w razie niepowodzenia – w trybie postępowania sądowego), albo w drodze uzyskania zezwolenia na umieszczenie infrastruktury telekomunikacyjnej na nieruchomości (poprzez zawarcie umowy, a w razie niepowodzenia – w trybie postępowania administracyjnego).

Ustanowienie służebności przesyłu na drodze postępowania sądowego z jednej strony będzie pociągało za sobą z reguły wyższe koszty (obejmujące m.in. koszty opinii biegłych oraz koszty zastępstwa procesowego, w tym dojazdów na rozprawy) i – jak pokazuje praktyka – co do zasady będzie trwało dłużej. W postanowieniu ustanawiającym służebność przesyłu sąd przyzna również właścicielowi odpowiednie wynagrodzenie. Z drugiej jednak strony zasady ustanawiania służebności przesyłu zostały uregulowane w Kodeksie cywilnym i Kodeksie postępowania cywilnego[10], dzięki czemu wątpliwości dotyczące sposobu stosowania przepisów są znacząco ograniczone.

Z kolei w przypadku decyzji ograniczającej korzystanie z nieruchomości istnieją wątpliwości dotyczące kumulatywnego stosowania przesłanek z art. 33 megaustawy oraz z art. 124 u.g.n., a także dotyczące odpowiedniego stosowania przepisów art. 124 i 124a u.g.n. do postępowania administracyjnego prowadzącego do wydania tej decyzji. Należy również pamiętać, że zakres podmiotów mogących skorzystać z trybu administracyjnego został znacząco ograniczony w art. 33 ust. 1 megaustawy. Niemniej wszczęcie i prowadzenie postępowania administracyjnego przez inwestora wiąże się ze znacząco niższymi kosztami z uwagi na brak rozpraw i kosztów opinii biegłych, a także co do zasady powinno zostać zakończone szybciej niż postępowanie sądowe. Dodatkowo przyznanie właścicielowi odszkodowania za umieszczenie infrastruktury telekomunikacyjnej na nieruchomości następuje w drodze osobnej decyzji administracyjnej, wydawanej na wniosek inwestora lub właściciela po zrealizowaniu inwestycji na nieruchomości. Powstanie obowiązku zapłaty odszkodowania na rzecz właściciela zależy zatem od tego, czy zostanie w tej sprawie wszczęte postępowanie administracyjne, a w razie przyznania właścicielowi odszkodowania – obowiązek zapłaty powstanie później niż w przypadku sądowego ustanowienia służebności przesyłu.

Podsumowując powyższe, należałoby stwierdzić, że mimo ryzyka związanego z niepewnym stanem prawnym dla podmiotów wymienionych w art. 33 ust. 1 megaustawy uzyskanie zezwolenia na umieszczenie na nieruchomości infrastruktury telekomunikacyjnej w drodze decyzji ograniczającej korzystanie z nieruchomości może okazać się pod wieloma względami korzystniejsze od prowadzenia postępowania sądowego o ustanowienie służebności przesyłu. Za wyborem trybu administracyjnego przemawiają przede wszystkim znacząco niższe koszty, szybkość postępowania, obowiązek wypłaty odszkodowania dopiero po jego ustaleniu w drodze osobnej decyzji administracyjnej wydawanej po umieszczeniu infrastruktury telekomunikacyjnej na nieruchomości, a także związanie organu administracji publicznej przepisami k.p.a., które co do zasady są korzystniejsze dla wnioskodawcy niż przepisy postępowania cywilnego.

Kompleksowe omówienie przesłanek wydania decyzji ograniczającej korzystanie z nieruchomości, trybu postępowania i odrębności związanych z nieruchomościami o nieuregulowanym stanie prawnym znajduje się w specjalnym przewodniku dla starostów, który został przygotowany przez prawników naszej kancelarii. Przewodnik został objęty patronatem Urzędu Komunikacji Elektronicznej, Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji, Polskiej Izby Komunikacji Elektronicznej oraz Polskiej Izby Informatyki i Telekomunikacji.

[10] Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (t.j. Dz. U. z 2020 r., poz. 1575, z późn. zm.).

Stosowanie art. 55 pr. aut. do umów wdrożeniowych

r.pr. Agnieszka Wachowska, apl. radc. Aleksander Elmerych

Na gruncie umów na stworzenie i wdrożenie systemów IT dochodzi często do sporów pomiędzy zamawiającym a wykonawcą w momencie odbioru programu komputerowego, z uwagi na ujawnione w nim wady. Pojawiają się wtedy wątpliwości dotyczące tego, jakie przepisy znajdują zastosowanie do umów wdrożeniowych oraz z jakich uprawnień mogą skorzystać strony.

Kwalifikacja prawna umów wdrożeniowych

Umowy na wdrożenie systemów IT należą do umów nienazwanych, zatem – co do zasady – to od woli stron i sposobu sformułowania postanowień umownych będzie zależał ich charakter[1]. Dziś większych wątpliwości nie budzi to, że umowy wdrożeniowe mogą być konstruowane w modelu zarówno umowy o świadczeniu usług, jak i umowy o dzieło[2], a także w modelu mieszanym, zawierającym elementy i umowy o dzieło, i umowy o świadczenie usług – wtedy o charakterze umowy rozstrzygają przeważające elementy świadczenia wykonawcy[3]. W kwestii elementów charakterystycznych dla umowy o dzieło wypowiedział się Sąd Najwyższy w wyroku z dnia 31 stycznia 2017 r.[4], wskazując, że: „różnica z umową o dzieło wyraża się w tym, że jej przedmiotem jest wykonanie dzieła, z reguły jednostkowego, indywidualnego, na odpowiedzialność i ryzyko wykonawcy, czyli przy spełnieniu parametrów i wymagań określonych lub właściwych dla przedmiotu zamówienia". Odnosząc się natomiast do umowy o świadczenie usług, w tym samym wyroku Sąd Najwyższy stwierdził, że jej cechą istotną jest staranność w wykonywaniu czynności oraz że będzie ona „tam, gdzie zleceniobiorca ma pracować, najczęściej wykonując powtarzalne, podobne i takie same, z reguły proste czynności". Pomimo wciąż rosnącego znaczenia wdrożeń realizowanych z zastosowaniem zwinnego podejścia, w ramach których umowy wdrożeniowe tworzone są jako umowy o świadczenie usług, obecnie nadal znaczna część zawieranych umów wdrożeniowych konstruowana jest z uwzględnieniem podejścia kaskadowego, w modelu umowy o dzieło, gdzie szczegółowy zakres wdrożenia oraz wymagania funkcjonalno-techniczne dotyczące systemu definiowane są przed rozpoczęciem prac implementacyjnych – najczęściej w analizie przedwdrożeniowej lub w projekcie technicznym, które wyznaczają wykonawcy z góry określone cele.

Umowa wdrożeniowa jako umowa o dostarczenie utworu

Jednocześnie nie należy zapominać o tym, że w zasadzie w ramach każdej umowy wdrożeniowej jednym ze świadczeń wykonawcy jest wykonanie i dostarczenie utworu w postaci programu komputerowego, a czasem także innych, pobocznych utworów, takich jak dokumentacja techniczna czy instrukcja użytkownika. Konsekwencją powyższego może być to, że w tym zakresie umowa wdrożeniowa może być traktowana jako umowa o dostarczenie utworu w rozumieniu przepisów Ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[5] (dalej: „pr. aut.").

[1] Na temat kwalifikacji prawnej umów wdrożeniowych pisze również B. Widła, Wdrożenia systemów informatycznych w orzecznictwie Sądu Najwyższego, „Czas Informacji" 2012, nr 2–3, s. 121–125.
[2] Tak wyrok Sądu Okręgowego w Łodzi z dnia 10 czerwca 2016 r., sygn. XIII Ga 442/16.
[3] Zob. wyrok Sądu Rejonowego dla Łodzi-Śródmieścia w Łodzi z dnia 27 listopada 2017 r., sygn. XIII GC 1603/17 (nieprawomocny).
[4] Sygn. I UK 488/15.
[5] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2019 r,. poz. 1231, z późn. zm.).

W związku z tym pojawia się pytanie, czy w razie zidentyfikowania wad w systemie dostarczonym przez zamawiającego należy stosować przepisy odnoszące się do umowy o dzieło (art. 638 Kodeksu cywilnego[6], dalej jako: „k.c.”), czy też przepisy regulujące kwestię wad utworu dostarczanego przez twórcę (art. 55 pr. aut.).

Konsekwencje stosowania art. 55 pr. aut. do odpowiedzialności wykonawcy za wady przedmiotu wdrożenia

Przepisy pr. aut. w znacznym stopniu ograniczają uprawnienia zamawiającego w razie stwierdzenia wad w systemie dostarczonym w ramach wdrożenia. W pierwszej kolejności warto zaznaczyć, że stosowanie art. 55 pr. aut. wyłączałoby możliwość skorzystania przez zamawiającego z uprawnień z tytułu rękojmi za wady dzieła na podstawie art. 638 k.c. W doktrynie wskazuje się bowiem, że nawet w przypadku, gdy dostarczenie utworu było elementem umowy o dzieło, art. 55 pr. aut. wyłącza na zasadzie *lex specialis* stosowanie przepisu art. 638 k.c.[7]. Gdyby przyjąć zatem, że do wdrażanego oprogramowania, w zakresie usuwania wad systemu, znajdują zastosowanie przepisy prawa autorskiego, błędy oprogramowania powinny być wtedy naprawiane w trybie przewidzianym przez art. 55 ust. 1 pr. aut., który po pierwsze posługuje się pojęciem „usterki”, a nie „wady”, a po drugie konstruuje odpowiedzialność twórcy na zasadzie winy, a nie na zasadzie ryzyka jak w przypadku przepisów o rękojmi przy sprzedaży[8]. Wykonawca systemu IT mógłby zatem, co do zasady, zwolnić się z odpowiedzialności za usterki w razie wykazania, że są one wynikiem okoliczności, za które nie ponosi on odpowiedzialności. Ponadto, zgodnie z art. 55 ust. 3 pr. aut., uprawnienie zamawiającego do żądania naprawienia usterek wygasałoby z chwilą przyjęcia utworu. Oznaczałoby to, że wykonawca nie odpowiada w zasadzie za wszelkie błędy systemu, które nie zostały wykryte na etapie testów i odbiorów, przed rozpoczęciem korzystania z oprogramowania. Praktyka pokazuje natomiast, że nie wszystkie błędy można zidentyfikować od razu – problemy związane z niestabilnością systemu, zawieszaniem się, czy w szczególności dotyczące jego wydajności, ujawniają się dopiero przy pełnym produkcyjnym wykorzystaniu systemu. Kwestia ta jest tym bardziej istotna, że stosownie do treści art. 55 ust. 4 pr. aut. – w przypadku braku odmiennych postanowień umownych – jeżeli zamawiający nie zawiadomi twórcy o przyjęciu utworu, nieprzyjęciu lub uzależnieniu przyjęcia od dokonania określonych zmian w terminie 6 miesięcy, zastosowanie znajduje fikcja prawna przyjęcia utworu przez zamawiającego bez zastrzeżeń[9]. W takiej sytuacji, nawet gdyby dostarczony system miał bardzo poważne usterki, dochodzi do przyjęcia utworu i zamawiający nie ma już żadnej możliwości domagania się ich naprawienia od wykonawcy. Skutek zastosowania fikcji prawnej z art. 55 ust. 4 pr. aut. jest zatem dla zamawiającego bardzo poważny.

W doktrynie funkcjonuje natomiast pogląd, prezentowany m.in. przez E. Traple, zgodnie z którym przepis art. 55 pr. aut. ma charakter jedynie względnie obowiązujący i nie wyłącza możliwości umownej modyfikacji zasad odpowiedzialności za wady utworu[10]. Przyjęcie takiego stanowiska oznaczałoby, iż nawet w przypadku uznania, że do umowy wdrożeniowej i jej rezultatów będących utworami znajduje zastosowanie art. 55 pr. aut., wypierając przepisy k.c. w tym zakresie, strony mogłyby w treści umowy zmienić zakres odpowiedzialności twórcy za wady utworu, np. poprzez wskazanie konkretnych błędów traktowanych jako usterki systemu, czy ustalić inne terminy lub sposoby ich naprawienia, korzystniejsze dla zamawiającego. Takie rozwiązanie umożliwiałoby częściowe zniwelowanie negatywnych dla zamawiającego skutków zastosowania art. 55 pr. aut.

[6] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2020 r., poz. 1740).
[7] Tak P. Wasilewski, *Przejście autorskich praw majątkowych i dozwolony użytek chronionych utworów. Komentarz do wybranych przepisów*, kom. do art. 55, Warszawa 2012, Lex/el 2020, Nb 4.
[8] Zob. A. Gołaszewska [w:] W. Machała, R. Sarbiński (red.), *Prawo autorskie i prawa pokrewne. Komentarz*, kom. do art. 55, Warszawa 2019, Lex/el 2020, Nb 6.
[9] Ibidem, Nb 17.
[10] E. Traple, *Umowy o eksploatację utworów w prawie polskim*, Warszawa 2010, s. 285.

Czy „usterka” w rozumieniu art. 55 pr. aut. oznacza to samo, co „wada” na gruncie art. 638 k.c.?

Na gruncie art. 55 ust. 1 pr. aut. zamawiający może domagać się od wykonawcy usunięcia usterek obecnych w dostarczonym przez niego utworze. Z uwagi na to, że przepisy pr. aut. nie definiują pojęcia usterki, należy rozważyć, czy zakres usterki jest pojęciem tożsamym z pojęciem wady na gruncie art. 638 k.c., który w tym zakresie odsyła do przepisów o rękojmi rzeczy sprzedanej (art. 556 k.c. i n.). W doktrynie wskazuje się, że pojęcie usterki należy interpretować w sposób zbliżony do pojęcia wady fizycznej rzeczy[11]. P. Wasilewski dokonuje nawet rozróżnienia tych pojęć[12], wskazując, że jeżeli mamy do czynienia z wadą nośnika, na którym utwór utrwalono, to należy ją traktować jako wadę fizyczną, natomiast jeżeli wada dotyczy samej istoty utworu jako dobra niematerialnego, to wtedy należy ją traktować jako usterkę w rozumieniu art. 55 ust. 1 pr. aut. Jak wskazuje T. Targosz, usterka może mieć charakter ilościowy, merytoryczny lub polegać na niedopasowaniu do szczególnych wymogów nabywcy[13]. Z kolei A. Gołaszewska zauważa, że usterka powinna też istnieć obiektywnie, choć szczególne znaczenie przy rozstrzyganiu, czy dany błąd można traktować jako usterkę, będzie miała wykładnia woli stron wyrażonej w umowie[14] – w szczególności w przypadku usterek polegających na niedopasowaniu utworu do wymogów nabywcy.

W odróżnieniu od wad na gruncie k.c. w przypadku usterek na gruncie art. 55 pr. aut. nie wprowadzono podziału na usterki istotne i nieistotne – w braku odrębnych regulacji prawnych wszelkie błędy utworu należy traktować jednolicie, jako usterki podlegające naprawieniu przed przyjęciem przez zamawiającego, w trybie przewidzianym w art. 55 pr. aut. Wśród mogących występować w systemie informatycznym błędów, które będą miały charakter usterki w rozumieniu art. 55 ust. 1 pr. aut., wskazuje się m.in.: brak określonych modułów czy funkcjonalności[15], zawieszanie się, brak możliwości wykonania określonych funkcji[16], brak cech określonych wcześniej w dokumentacji technicznej będącej podstawą przystąpienia do wdrożenia, niska prędkość przetwarzania danych czy niekompatybilność z wymaganiami sprzętowymi podanymi w specyfikacji sprzętowej[17]. Zatem w przypadku systemów informatycznych zakres pojęcia usterki będzie bardzo zbliżony do pojęcia wady na gruncie przepisów k.c.

Co na to orzecznictwo?

Orzecznictwo sądowe poruszające problematykę stosowania art. 55 pr. aut. do umów wdrożeniowych jest dosyć ubogie. W sporach sądy bowiem często pomijają fakt występowania art. 55 pr. aut., przechodząc do rozpoznania sporu z automatycznym stosowaniem przepisów Kodeksu cywilnego i zwykle przepisów umowy o dzieło. W orzecznictwie wyrażony został pogląd, zgodnie z którym do umów wdrożeniowych, konstruowanych w modelu umowy o dzieło, należy stosować przepisy art. 627 k.c. i n., a nie przepisy pr. aut.[18] Pogląd ten został również potwierdzony w wyroku, który zapadł 19 lutego 2020 r. przed Sądem Apelacyjnym w Warszawie[19]. Sąd potwierdził w nim stanowisko sądu okręgowego, zgodnie z którym do umowy wdrożeniowej, w której jako wykonawca nie występuje osoba fizyczna będąca twórcą, tylko podmiot profesjonalny zatrudniający programistów, nie należy stosować przepisów ustawy pr. aut., tylko przepisy Kodeksu cywilnego dotyczące umowy o dzieło. W uzasadnieniu do wyroku sąd wskazał, że w przepisach pr. aut. mowa jest bowiem o twórcach, a więc o osobach fizycznych będących autorami utworu. Jeśli chodzi o możliwość stosowania przepisów prawa autorskiego do umów wdrożeniowych, odmienne stanowisko zaprezentował Sąd Apelacyjny w Warszawie w wyroku z dnia 10 lipca 2017 r. [20], stwierdzając, że do skutków odstąpienia od umowy wdrożeniowej należy stosować art. 59 pr. aut. jako przepis szczególny w stosunku do art. 494 k.c. Orzecznictwo sądowe jest zatem w tej kwestii niekonsekwentne i niejednolite.

[11] Tak A. Gołaszewska [w:] *Prawo autorskie…*, op. cit., Nb 3 oraz T. Targosz [w:] D. Flisak (red.), *Prawo autorskie i prawa pokrewne. Komentarz*, kom. do art. 55, Warszawa 2015, Lex/el 2020, Nb 9.
[12] Zob. P. Wasilewski, *Przejście autorskich praw…*, op. cit., Nb 3.
[13] Zob. T. Targosz [w:] P*rawo autorskie…*, op. cit., Nb 12.
[14] Tak A. Gołaszewska [w:] *Prawo autorskie…*, op. cit., Nb 4.
[15] Tak ibidem.
[16] Tak T. Targosz [w:] *Prawo autorskie…*, op. cit., Nb 12.
[17] Podobnie E. Traple, op. cit., s. 285.
[18] Podobnie E. Traple, op. cit., s. 285.
[19] Zob. wyrok Sądu Apelacyjnego we Wrocławiu z dnia 28 sierpnia 2013 r., sygn. I ACa 796/13, w którym sąd opiera swoje rozstrzygnięcie na przepisach k.c.
[20] Sygn. VII AGa 599/19, niepubl.

Podsumowanie

Dokonując zbiorczej oceny wszystkich konsekwencji, które wynikają z zastosowania art. 55 pr. aut. do umów wdrożeniowych, bezsprzecznie należy ocenić, że są one znacznie względniejsze dla wykonawcy (twórcy oprogramowania). Przepisy te stawiają wykonawcę na uprzywilejowanej pozycji w stosunku do regulacji zawartych w Kodeksie cywilnym, ograniczając w znacznym zakresie jego odpowiedzialność za wady dostarczonego systemu.

Jednocześnie wydaje się, że głównym *ratio legis* wprowadzenia szczególnej regulacji dotyczącej odpowiedzialności za wady utworu w przepisach prawa autorskiego była ochrona słabszej strony stosunku prawnego[21], którą – co do zasady – w przypadku dostarczenia klasycznych utworów, takich jak obrazy czy utwory muzyczne, jest indywidualny twórca – artysta, osoba fizyczna nieznająca się często na realiach obrotu gospodarczego. Natomiast w obecnych realiach obrotu, w przypadku umów wdrożeniowych, po stronie wykonawcy występuje zazwyczaj przedsiębiorca z branży IT, zatrudniający niekiedy setki, a nawet tysiące pracowników, działający jako profesjonalista w dziedzinie produkcji złożonych programów komputerowych. Jednocześnie jego doświadczenie i wiedza w zakresie przebiegu wdrożenia, procesu powstawania oprogramowania oraz aspektów technicznych funkcjonowania systemu, w tym również możliwych błędów systemu, stawiają takiego przedsiębiorcę częstokroć na znacznie silniejszej pozycji negocjacyjnej od zamawiającego.

Natomiast ewentualne opóźnienia w realizacji wdrożenia czy błędy dostarczonego systemu mogą powodować poważne konsekwencje po stronie zamawiających – zarówno finansowe, jak i wizerunkowe. Dlatego też w praktyce to zamawiającym często bardziej zależy na doprowadzeniu realizacji umowy wdrożeniowej do końca, nawet kosztem wielu ustępstw w stosunku do wykonawców.

Z powyższych względów, mając na uwadze obecne realia rynkowe, wydaje się, że w przypadku wdrożeń systemów IT szczególna ochrona zapewniana wykonawcom na gruncie art. 55 pr. aut. nie znajduje żadnego racjonalnego uzasadnienia – nie ma bowiem podstaw do twierdzenia, że to wykonawca jest słabszą stroną stosunku prawnego. Na problem ten zwróciła uwagę również prof. E. Traple, wskazując przy rozważaniach dotyczących stosowania art. 55 pr. aut. do umów na stworzenie i wdrożenie programu komputerowego, że w przypadku takich umów będziemy mieli do czynienia z osobami prawnymi jako stronami i przepisy pełniące szczególną funkcję ochronną w stosunku do twórców nie znajdą zastosowania[22].

Wobec powyższego wydaje się, że można przyjąć dwa odmienne podejścia do stosowania przepisów pr. aut. do umów wdrożeniowych:

- Pierwsze z nich zakłada stosowanie regulacji pr. aut. jako *lex specialis* w stosunku do kodeksowych przepisów odnoszących się do umowy o dzieło, traktując je jednocześnie jako przepisy względnie obowiązujące oraz dopuszczając ich umowną modyfikację przez strony.
- Drugie podejście zakłada natomiast dopuszczenie możliwości odstąpienia od stosowania przepisów pr. aut. regulujących kwestie uprawnień stron w przypadku wad w utworze lub niedostarczenia utworu do umów wdrożeniowych w sytuacjach, w których nie znajduje to jakiegokolwiek uzasadnienia z uwagi na brak występowania po stronie wykonawcy indywidualnego twórcy – artysty będącego słabszą stroną stosunku prawnego.

Zaproponowane podejścia zostały szerzej omówione w artykule pt. *Konsekwencje istnienia wad oprogramowania przy odbiorach wdrożenia systemu IT* autorstwa Agnieszki Wachowskiej oraz Aleksandra Elmerycha. Artykuł ukazał się w dodatku specjalnym „Prawo nowych technologii" do „Monitora Prawniczego" nr 20/2020.

[21]Zob. J. Barta, R. Markiewicz, *Prawo autorskie*, Rozdział I Uwagi wstępne, Warszawa 2016, Lex/el 2020.
[22]Zob. E. Traple, op. cit., s. 285.

Przekazanie sądowi dowodu drogą elektroniczną nie jest publicznym udostępnieniem utworu

r.pr. Joanna Dworak

Wyrokiem z dnia 28 października 2020 r., w postępowaniu BY przeciwko CX (C-637/19), TSUE dokonał wykładni art. 3 ust. 1 Dyrektywy 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (dalej: „Dyrektywa"). Celem tej Dyrektywy jest zapewnienie równorzędnego poziomu ochrony praw własności intelektualnej we wszystkich państwach członkowskich. Na gruncie sprawy rozpatrywanej przez sąd szwedzki do Trybunału wpłynął wniosek o wydanie orzeczenia w trybie prejudycjalnym w przedmiocie m.in.:

- czy pojęcie „publiczny", użyte w art. 3 ust. 1 i art. 4 ust. 1 Dyrektywy, ma jednolite znaczenie;
- czy na ocenę kwestii tego, czy przedłożenie chronionego utworu sądowi stanowi „publiczne udostępnianie" lub „publiczne rozpowszechnianie", ma wpływ fakt, że prawo krajowe przewiduje ogólną zasadę dostępu do dokumentów publicznych, zgodnie z którą każdy może na wniosek uzyskać dostęp do dokumentów procesowych przedłożonych sądowi, chyba że zawierają one informacje poufne.

W rozstrzyganej sprawie skarżący i pozwany w postępowaniu głównym są dwiema osobami fizycznymi, z których każda prowadzi witrynę internetową. W ramach sporu toczącego się przed szwedzkimi sądami cywilnymi pozwany w postępowaniu głównym przekazał sądowi rozpoznającemu sprawę jako dowód w postępowaniu kopię strony tekstu zawierającą fotografię, która to strona pochodziła z witryny internetowej skarżącego w postępowaniu głównym. Skarżący podniósł, że jemu przysługują prawa autorskie do tej fotografii, i zażądał zasądzenia od pozwanego w postępowaniu głównym wypłaty odszkodowania za naruszenie praw autorskich oraz za naruszenie szczególnej ochrony przyznanej utworom fotograficznym.

Sąd rozpatrujący sprawę w pierwszej instancji stwierdził, że ponieważ fotografia ta została przekazana sądowi w ramach czynności procesowej, każda osoba mogła zażądać jej udostępnienia na podstawie obowiązujących przepisów prawnych. Sąd ten wywnioskował z tego, że pozwany w postępowaniu głównym dokonał publicznego rozpowszechnienia tej fotografii. Na takie rozstrzygnięcie skarżący w postępowaniu głównym wniósł apelację.

Sąd apelacyjny z kolei wskazał, że w szczególności powinna być rozstrzygnięta kwestia, czy przekazanie kopii tej fotografii sądowi, w ramach czynności procesowej, może stanowić niedozwolone udostępnienie utworu w rozumieniu prawa autorskiego, jako publiczne rozpowszechnianie lub publiczne udostępnianie, mając na względzie fakt, iż strony wyjaśniły, że rozpatrywana fotografia została przekazana sądowi pocztą elektroniczną w postaci kopii elektronicznej. Sąd wskazał również na konieczność ustalenia, czy można uznać, że przekazanie utworu sądowi podlega zakresowi pojęcia „publicznego" udostępniania lub rozpowszechniania.

Pochylając się nad rozstrzygnięciem przedmiotowego pytania, TSUE uznał, iż z dotychczasowego orzecznictwa wynika, że publiczne udostępnianie utworu, inne niż rozpowszechnianie kopii fizycznych tego utworu, jest objęte nie pojęciem „publicznego rozpowszechniania" zawartym w art. 4 ust. 1 Dyrektywy, lecz pojęciem „publicznego udostępniania" w rozumieniu art. 3 ust. 1 Dyrektywy (por. wyrok TSUE z dnia 19 grudnia 2019 r., Nederlands Uitgeversverbond i Groep Algemene Uitgevers, C-263/18). Kolejno z dotychczasowego orzecznictwa wynika również, że wszelkie działanie, poprzez które użytkownik, z pełną świadomością skutków swojego zachowania, udziela dostępu do utworów chronionych, może stanowić czynność udostępniania w rozumieniu art. 3 ust. 1 Dyrektywy (wyrok TSUE z dnia 14 czerwca 2017 r., Stichting Brein, C-610/15). Tak też będzie zatem w przypadku przekazania sądowi drogą elektroniczną chronionego utworu w charakterze dowodu w ramach toczącego się między jednostkami postępowania sądowego.

Następnie jednak TSUE stwierdził, że aby wchodzić w zakres pojęcia „publicznego udostępniania" w rozumieniu art. 3 ust. 1 Dyrektywy, chronione utwory powinny zostać faktycznie udostępnione publiczności (por. wyrok TSUE z dnia 14 czerwca 2017 r., Stichting Brein, C-610/15). W tym względzie pojęcie „publiczności" odnosi się do nieokreślonej liczby potencjalnych odbiorców i zakłada ponadto dość znaczną liczbę osób. W przedmiotowej sprawie zaś należy uznać, że takie udostępnianie, jakie miało miejsce w postępowaniu sądowym, w którego toku zostało zadane pytanie prejudycjalne, dotyczy jasno określonej i zamkniętej grupy osób, którym powierzono wykonywanie w sądzie zadań z zakresu usług publicznych, a nie nieokreślonej liczby potencjalnych odbiorców. Udostępnianie nie zostało skierowane do osób ogólnie, lecz do indywidualnych i określonych profesjonalistów. W tych okolicznościach należy stwierdzić, że przekazanie sądowi drogą elektroniczną chronionego utworu w charakterze dowodu w ramach toczącego się między jednostkami postępowania sądowego nie może zostać uznane za „publiczne udostępnianie" w rozumieniu art. 3 ust. 1 Dyrektywy.

Tym samym Trybunał zapewnił ochronę autorom utworów przekazywanych jako materiał dowodowy w procesie, orzekając, że krąg osób mogących zapoznać się z takim utworem nie jest nieograniczony. Na gruncie powyższego warto dostrzec, że taki sam walor, a mianowicie braku publicznego udostępnienia, będzie dotyczył np. oprogramowania przedkładanego jako dowód w sprawie.

Kolejny krok w kierunku regulacji sztucznej inteligencji – rezolucje Parlamentu Europejskiego

adw. Karolina Grochecka Goljan

Uwagi wstępne

W dniu 20 października 2020 r. Parlament Europejski przyjął trzy nowe i znaczące rezolucje odnoszące się do sztucznej inteligencji. Rezolucje dotyczą następujących obszarów:

- etyki AI – Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. zawierająca zalecenia dla Komisji w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii (2020/2012(INL))[1],
- odpowiedzialności cywilnej za AI – Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. z zaleceniami dla Komisji w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję (2020/2014(INL))[2] oraz
- aspektów praw własności intelektualnej w stosunku do AI – Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie praw własności intelektualnej w dziedzinie rozwoju technologii sztucznej inteligencji (2020/2015(INI))[3].
- Rezolucje nie odnoszą się konkretnie do jednego podmiotu czy też ich wyodrębnionej grupy. Przepisy w nich zawarte przeznaczone są dla szerokiego grona odbiorców, gdyż dotyczą różnych obszarów funkcjonowania.

Rezolucje nie odnoszą się konkretnie do jednego podmiotu czy też ich wyodrębnionej grupy. Przepisy w nich zawarte przeznaczone są dla szerokiego grona odbiorców, gdyż dotyczą różnych obszarów funkcjonowania.

Ważnym postulatem Parlamentu Europejskiego w odniesieniu do wszystkich rezolucji jest zastrzeżenie, że przy stosowaniu AI należy kierować się zasadą „ograniczonego zaufania". Nie powinno się pozostawiać jej pełnej decyzyjności czy też dawać zbyt dużo swobody. Przede wszystkim Parlament Europejski podkreślił, że nie należy przekazywać systemom opartym na AI prawa do wydawania autonomicznych decyzji w momencie, gdy dotyczy to istotnych aspektów prawa i obowiązków obywateli. Chodzi tu o minimalizację ryzyka związanego z funkcjonowaniem AI oraz zbudowanie zaufania do pracy systemów przy zachowaniu racjonalności oraz odpowiedzialności.

Na rynku podnosi się, że ze względu na naciski ze strony Parlamentu Europejskiego na harmonizację przepisów dotyczących AI – spodziewać się w ich wyniku należy wydania rozporządzenia, a nie dyrektywy Unii. Sam Parlament Europejski zaznacza to w rezolucjach. Widoczne jest to np. w rezolucji dotyczącej aspektów praw własności intelektualnej w stosunku do AI, gdzie wskazano, że regulacje z zakresu AI powinny mieć formę rozporządzenia, a nie dyrektywy, aby ustanowić jednakowe standardy w całej Unii oraz uniknąć rozdrobnienia europejskiego jednolitego rynku cyfrowego i promować innowacje.

Rezolucja nr 1 – dotycząca etyki AI

Za inicjatywą ustawodawczą w tym zakresie kryje się wezwanie Komisji Europejskiej do przedstawienia nowych ram prawnych określających zasady etyczne i zobowiązania prawne, których należy przestrzegać przy opracowywaniu, wdrażaniu i wykorzystywaniu AI, robotyki i pokrewnych technologii w UE, w tym oprogramowania, algorytmy i dane. W szczególności, chodzi o zbudowanie zaufania obywateli Unii do AI w oparciu o szeroko rozumiane zasady etyki.

W tekście jednolitym przyjętym przez Parlament Europejski wskazano, że ramy prawne dla etyki AI powinny być oparte na prawie UE, Karcie praw podstawowych i międzynarodowym prawie praw człowieka oraz mieć zastosowanie w szczególności do technologii wysokiego ryzyka w celu ustanowienia równych standardów w całej UE.

[1] Tekst rezolucji dostępny tutaj: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_PL.html,
[2] Tekst rezolucji dostępny tutaj: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_PL.html.

Podkreślono, że przyszłe przepisy powinny być tworzone zgodnie z kilkoma zasadami przewodnimi: sztuczną inteligencją ukierunkowaną na człowieka i stworzoną przez człowieka („*a human – centric and human – made AI*"), bezpieczeństwem, przejrzystością i odpowiedzialnością, zabezpieczeniem przed uprzedzeniami i dyskryminacją, prawem do zadośćuczynienia, odpowiedzialnością społeczną i środowiskową oraz poszanowaniem prywatności i ochrony danych.

Parlament Europejski w swojej rezolucji podkreśla wielokrotnie cel nadrzędny AI, jakim jest dążenie do zwiększenia dobrostanu, dobrobytu i wolności jednostki (tzw. „*human – centric approach*").

Ocena ryzyka

Parlament Europejski podkreśla, że w celu zapewnienia jednolitego wdrażania systemu oceny ryzyka oraz zgodności z powiązanymi zobowiązaniami prawnymi, należy stworzyć wyczerpujący i łączny wykaz sektorów wysokiego ryzyka oraz zastosowań lub celów wysokiego ryzyka.

Parlament wskazuje, że ocena tego czy sztuczna inteligencja, robotyka czy powiązane z nimi technologie należy uznać za obarczone wysokim ryzykiem, a tym samym podlegające rygorowi zobowiązań prawnych i zasad etycznych dotyczących AI powinna zawsze wynikać z bezstronnej, regulowanej i zewnętrznej oceny *ex ante* opartej na konkretnych i określonych kryteriach. W tym względzie, sztuczną inteligencję, robotykę i powiązane z nimi technologie należy uznać za obarczone wysokim ryzykiem, jeżeli ich rozwój, wdrażanie i wykorzystywanie wiąże się ze znacznym ryzykiem spowodowania obrażeń ciała lub szkody dla osób fizycznych lub społeczeństwa, z naruszeniem praw podstawowych i zasad bezpieczeństwa określonych w prawie Unii. Do celów oceny, czy technologie AI wiążą się z takim ryzykiem, należy wziąć pod uwagę sektor, w którym są opracowywane, wdrażane lub wykorzystywane, ich konkretne zastosowanie lub cel oraz stopień obrażenia lub szkody, których wystąpienia można się spodziewać. Pierwsze i drugie kryterium, tj. sektor i konkretne zastosowanie lub cel, należy rozpatrywać łącznie.

Europejska certyfikacja zgodności z zasadami etycznymi

Elementem rezolucji jest również opracowanie, skoordynowanych na szczeblu UE, wspólnych kryteriów i procedury składania wniosków w odniesieniu do wydawania europejskiego certyfikatu zgodności z zasadami etycznymi, w tym na wniosek dowolnego podmiotu opracowującego, wdrażającego lub wykorzystującego technologie nieuznawane za charakteryzujące się wysokim ryzykiem, który chciałby uzyskać poświadczenie pozytywnej oceny zgodności przeprowadzonej przez odpowiedni krajowy organ nadzoru.

Zgodnie ze stanowiskiem Parlamentu Europejskiego, taki europejski certyfikat zgodności z zasadami etycznymi zachęcałby do uwzględniania etyki na etapie projektowania w całym łańcuchu dostaw ekosystemów sztucznej inteligencji. Wskazuje się, że w przypadku technologii wysokiego ryzyka certyfikacja ta stanowiłaby obowiązkowy warunek wstępny kwalifikacji do uczestnictwa w procedurach udzielania zamówień publicznych w zakresie systemów sztucznej inteligencji, robotyki i powiązanych z nimi technologii.

Ochrona prywatności

W rezolucji wyraźnie wskazano również, że jest ona skonstruowana w oparciu o przeświadczenie, że wytwarzanie i wykorzystywanie danych, w tym danych osobowych, takich jak dane biometryczne, wynikające z rozwoju, wdrażania i wykorzystywania AI, robotyki i powiązanych technologii szybko wzrasta, co podkreśla potrzebę poszanowania i egzekwowania prawa obywateli do prywatności i ochrony danych osobowych zgodnie z prawem Unii.

Tak więc, ochrona danych osobowych (w tym oczywiście przestrzeganie RODO) jest kluczowe dla prawidłowego wdrażania i funkcjonowania systemów w oparciu o AI, szczególnie tych dotyczących profilowania.

Rezolucja zakłada również, że wykorzystanie AI przez organy publiczne do celów istotnego interesu publicznego powinno zawsze być ujawniane, proporcjonalne, ukierunkowane do konkretnych celów, ograniczone w czasie i przeprowadzane zgodnie z prawem Unii, z należytym poszanowaniem ludzkiej godności i autonomii oraz praw podstawowych określonych w Karcie praw podstawowych.

Rezolucja nr 2 – dotycząca odpowiedzialności cywilnej za AI

O propozycji przepisów regulujących zasady odpowiedzialności za szkody wyrządzone przez sztuczną inteligencję przedstawionych w dniu 4 maja 2020 r. przez komitet ds. prawnych Parlamentu Europejskiego pisaliśmy na naszym blogu tutaj.

W rezolucji nie znajdziemy nowych rozwiązań w zakresie odpowiedzialności za szkodę, a jedynie nakierowanie wskazujące, że obecne regulacje powinny być na bieżąco monitorowane i doprecyzowywane. Podkreśla się jednak, że w każdym wypadku użytkownik musi mieć pewność, że potencjalne szkody spowodowane przez systemy wykorzystujące AI są objęte odpowiednim ubezpieczeniem oraz że istnieje określona droga prawna dochodzenia roszczeń.

Parlament Europejski w swojej rezolucji wskazuje, że bezpośrednią lub pośrednią przyczyną szkody mogą być zarówno fizyczne jak i wirtualne działania systemów AI, same zaś szkody są niemal zawsze wynikiem tego, że ktoś skonstruował lub wdrożył taki system albo ingerował w niego.

Parlament Europejski wyraża opinię, że nieprzejrzystość, zdolność do łączenia się i autonomiczność systemów może sprawić, że w praktyce będzie bardzo trudno powiązać konkretne szkodliwe działania systemów AI z konkretnymi danymi wprowadzonymi przez człowieka lub jego decyzjami na etapie projektowania systemu, a nawet będzie to niemożliwe. Przypomniał jednocześnie, że zgodnie z szeroko stosowanymi koncepcjami odpowiedzialności można mimo wszystko obejść tę przeszkodę, czyniąc odpowiedzialnymi poszczególne osoby w całym łańcuchu wartości, które tworzą, utrzymują lub kontrolują ryzyko związane z systemem AI. Wobec powyższego, Parlament Europejski zauważył, że nie ma konieczności nadawania systemom AI osobowości prawnej.

Odpowiedzialność zależna od rodzaju ryzyka i odpowiedzialność operatora

W rezolucji wskazuje się, że istotnym czynnikiem determinującym odpowiedzialność powinien być rodzaj systemu AI, nad którym sprawuje kontrolę dany operator. Im większe ryzyko jakie niesie ze sobą system AI, tym większe zagrożenie dla chronionych wartości takich jak życie, zdrowie, własność. Z tego względu postuluje się w rezolucji stworzenie powszechnego, surowego systemu odpowiedzialności dla autonomicznych systemów AI obarczonych wysokim ryzykiem (odpowiedzialność na zasadzie ryzyka). Operator systemu AI, który nie jest systemem obarczonym wysokim ryzykiem może być natomiast pociągnięty do odpowiedzialności na zasadzie winy.

Parlament Europejski uważa, że przy ustalaniu, czy system AI stanowi wysokie ryzyko, należy wziąć pod uwagę sektor, oraz charakter podejmowanych działań. Zaznacza ponadto, że znaczenie tego potencjału zależy od wzajemnego oddziaływania między dotkliwością ewentualnych szkód, prawdopodobieństwem, że ryzyko spowoduje szkodę lub uszkodzenie, oraz sposobem wykorzystania systemu AI.

Parlament zaleca też, aby wszystkie systemy AI wysokiego ryzyka zostały wyczerpująco wymienione w załączniku (aneksie) do proponowanego rozporządzenia (które ma powstać w oparciu o rezolucje). Uważa, że można stworzyć także specjalny komitet, który zajmowałby się monitorowaniem systemów AI wysokiego ryzyka.

Pojęcie operatora należy rozumieć szeroko, jako obejmujące zarówno operatora front-end, jak i back – end. Operator front-end to osoba fizyczna lub prawna, która do pewnego stopnia kontroluje ryzyko związane z obsługą i funkcjonowaniem systemu AI i korzysta z jego działania. Z kolei operator back – end to osoba fizyczna lub prawna, która w sposób ciągły określa cechy technologii, dostarcza dane i podstawowe usługi wsparcia, a zatem sprawuje również pewną kontrolę nad ryzykiem związanym z obsługą i funkcjonowaniem systemu AI.

Parlament uważa ponadto, że ze względu na złożoność i łączność systemu AI operator będzie w wielu przypadkach pierwszym widocznym punktem kontaktowym dla osoby poszkodowanej.

Parlament Europejski zauważa też, że mogą zaistnieć sytuacje, w których występuje więcej niż jeden operator, na przykład operator typu back – end i front – end. W takim przypadku wszyscy operatorzy powinni ponosić solidarną odpowiedzialność, mając jednocześnie prawo do roszczeń między sobą. Jest to odpowiedzialność solidarna i proporcjonalna.

Ubezpieczenie

Parlament Europejski jest zdania, że wszyscy operatorzy systemów AI wysokiego ryzyka wymienionych w załączniku (aneksie) do proponowanego rozporządzenia powinni posiadać ubezpieczenie od odpowiedzialności cywilnej.

PE stoi na stanowisku, że w zakresie odpowiedzialności cywilnej za AI, Komisja powinna rozważyć przyjęcie rozporządzenia. W zakresie regulacji dotyczących ubezpieczenia, proponowane rozporządzenie powinno obejmować naruszenia istotnych chronionych przepisami praw: do życia, zdrowia, nienaruszalności cielesnej i własności oraz powinno wskazywać kwoty i zakres odszkodowania, a także termin przedawnienia roszczeń. Proponowane rozporządzenie powinno również obejmować istotne szkody niematerialne, jeśli dana osoba podniosła zauważalną, tj. możliwą do zweryfikowania szkodę ekonomiczna.

Rezolucja nr 3 – dotycząca aspektów praw własności intelektualnej w stosunku do AI

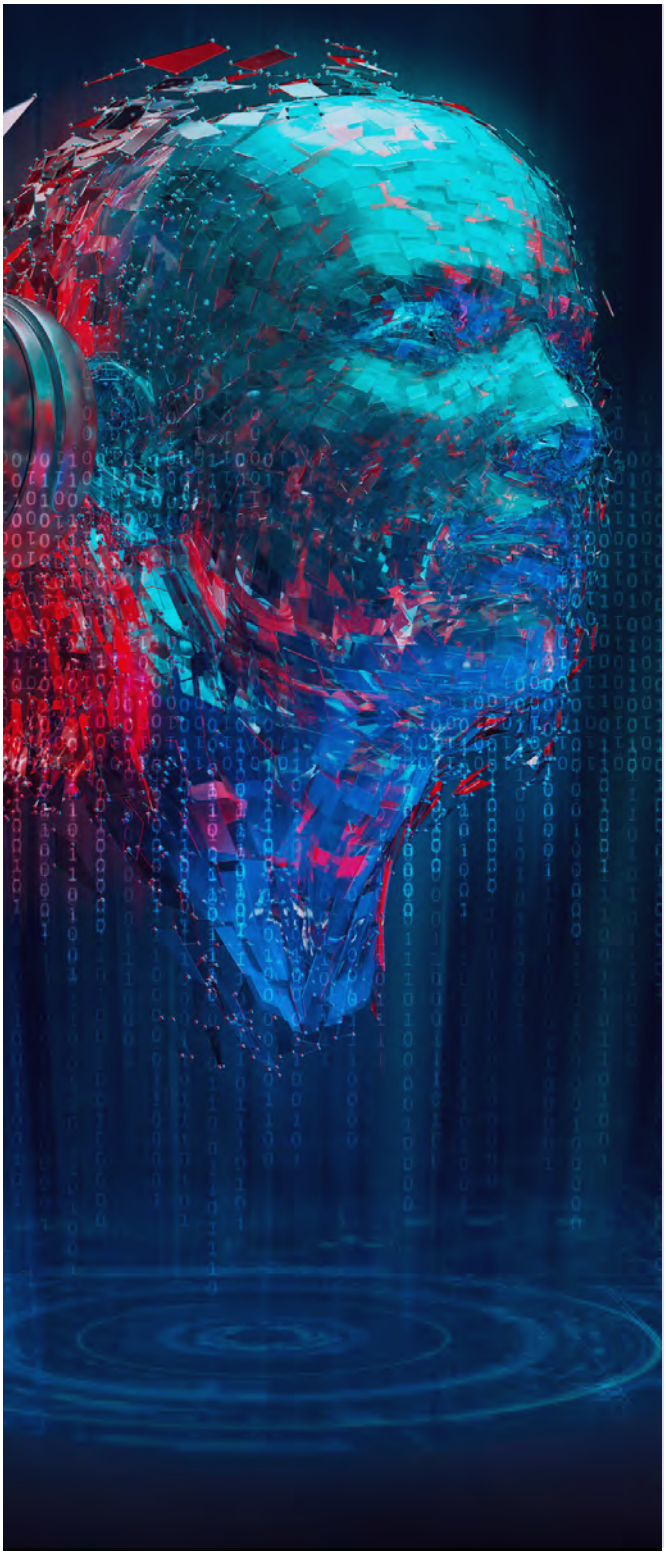
Zgodnie z najkrótszą rezolucją przedstawioną przez Parlament, w zakresie praw własności intelektualnej w odniesieniu do AI, ważne jest aby odróżnić twórczość człowieka wspomaganą przez AI od twórczości autonomicznie generowanej przez AI. Twórczość generowana przez AI autonomicznie wiąże się z koniecznością wdrożenia regulacji w zakresie ochrony praw własności intelektualnej, takimi jak kwestie własności, wynalazczości i odpowiedniego wynagrodzenia, a także kwestie związane z potencjalną koncentracją na rynku.

Wskazuje jednocześnie, że prawa własności intelektualnej na rzecz rozwoju technologii AI należy odróżnić od wszelkich praw własności intelektualnej przyznawanych w odniesieniu do twórczości wytworzonej przez AI oraz podkreśla, że w przypadku gdy AI jest wykorzystywana wyłącznie jako narzędzie wspomagające autora w procesie tworzenia, nadal zastosowanie mają obecne ramy własności intelektualnej.

Parlament podkreśla, że twórczość technologiczna tworzona przez technologie AI musi być chroniona w ramach praw własności intelektualnej, aby zachęcić do inwestowania w tę formę twórczości i zwiększyć pewność prawa dla obywateli, przedsiębiorstw i wynalazców, którzy obecnie należą do najczęstszych użytkowników technologii AI. Wskazuje się jednocześnie, że dzieła wyprodukowane samodzielnie przez sztuczne podmioty i roboty mogą nie kwalifikować się do ochrony na podstawie prawa autorskiego w celu poszanowania zasady oryginalności związanej z osobą fizyczną, ponieważ pojęcie „twórczości intelektualnej" odnosi się do osobowości autora. Jednocześnie jednak, jeżeli zostanie ustalone, że takie utwory mogą być chronione prawem autorskim zaleca, aby wszelkie prawa własności przysługiwały wyłącznie osobom fizycznym lub prawnym, które stworzyły utwór zgodnie z prawem, i wyłącznie za zgodą podmiotu praw autorskich, jeżeli wykorzystywane są materiały chronione prawem autorskim, chyba że mają zastosowanie wyjątki lub ograniczenia dotyczące praw autorskich.

Co dalej?

Omówione pokrótce rezolucje Parlamentu Europejskiego stanowią wytyczne dla Komisji Europejskiej. Po analizie wyników konsultacji, w pierwszym kwartale 2021 r. Komisja powinna zaproponować horyzontalny wniosek regulacyjny. Będziemy zatem na bieżąco monitorować prace nad przedmiotowymi regulacjami – które jak się wydaje – będą miały znaczący wpływ na rynek.



Dyrektywa NIS2 – propozycja nowej regulacji w zakresie cyberbezpieczeństwa

r.pr. Joanna Jastrząb

Pod koniec 2020 r. Komisja Europejska zakończyła proces rewizji dyrektywy NIS i przedstawiła propozycję nowej, kompleksowej regulacji, która została nazwana „dyrektywą NIS2". Przepisy te mają całkowicie zastąpić dyrektywę NIS, eliminując jej słabości i znaczące różnice w implementacji pomiędzy poszczególnymi państwami członkowskimi. Komisja nie zdecydowała się przy tym na propozycję rozporządzenia, bezpośrednio stosowanego w krajach UE, choć była to jedna z rozważanych dróg, o czym pisaliśmy w poprzednich wydaniach newslettera (por. artykuł dostępny pod linkiem: klik).

Podmioty objęte regulacją

Najważniejszą zmianą w stosunku do obecnie obowiązującej dyrektywy wydaje się wprowadzenie jasnego kryterium określenia, które podmioty są tą dyrektywą objęte. Na gruncie obecnie obowiązującej dyrektywy NIS tymi podmiotami byli m.in. operatorzy usług kluczowych czy dostawcy usług cyfrowych. W przypadku tej pierwszej kategorii to państwa członkowskie w regulacjach krajowych miały stworzyć system identyfikacji operatorów usług kluczowych – skutkiem tego był brak jednolitości podejścia i znaczne zróżnicowanie np. w liczbie wyznaczonych operatorów.

Biorąc pod uwagę powyższe, zdecydowano, że to sama dyrektywa NIS2 będzie określać krąg podmiotów, które będą podlegać jej regulacjom. Szukając prostego i jednolitego kryterium, uznano, że pomocne będzie oparcie się na kryterium wielkości podmiotu – spod dyrektywy wyłączono więc mikroprzedsiębiorców i małych przedsiębiorców (z pewnymi wyjątkami) i stwierdzono, że każdy średni i duży przedsiębiorca, który prowadzi działalność wskazaną w załączniku do propozycji dyrektywy, powinien być objęty jej regulacją. Powierzono również ENISA (unijnej agencji ds. cyberbezpieczeństwa) prowadzenie rejestru podmiotów objętych dyrektywą, do którego te podmioty powinny same się zgłosić.

Kluczowe i istotne podmioty

W zakresie podmiotów objętych regulacją przebudowano również podział na operatorów usług kluczowych i dostawców usług cyfrowych – zastąpiono go w dyrektywie NIS2 podziałem na kluczowe podmioty (*essential entities*) i istotne podmioty (*important entities*) oraz rozszerzono sektory i rodzaje usług, w których te podmioty działają.

Za kluczowe podmioty (*essential entities*) dyrektywa NIS2 uznaje m.in. wskazane podmioty z sektora energii, transportu, bankowości, zdrowia, zaopatrzenia w wodę i infrastruktury cyfrowej, jak również podmioty publiczne. W tej ostatniej kategorii wskazano także dostawców usług chmurowych (dotąd podlegali ograniczonej regulacji jako dostawcy usług cyfrowych), dostawców centrów danych, dostawców CDN (*content delivery network*), dostawców usług zaufania (dotychczas byli wyłączeni spod regulacji) czy dostawców publicznych sieci łączności elektronicznej i dostawców usług łączności elektronicznej, jeśli są one powszechnie dostępne.

Pewnego rodzaju ciekawostką, pokazującą jednak dążenie do stworzenia regulacji odpowiedniej na najbliższe lata, jest wskazanie w ramach tej kategorii również sektora przestrzeni kosmicznej (*space*), a w jego ramach operatorów infrastruktury naziemnej – która jest własnością państw członkowskich lub podmiotów prywatnych, jest przez nie zarządzana i eksploatowana – wspierających świadczenie usług kosmicznych. Podmioty te na gruncie dyrektywy NIS2 będą uznawane za kluczowe podmioty.

Druga kategoria podmiotów (*important entities*) obejmuje niektóre podmioty sektora pocztowego, zarządzania odpadami, produkcji i dystrybucji chemikaliów, żywności i innych wskazanych produktów, a także wskazanych dostawców usług cyfrowych, tj. dostawców:

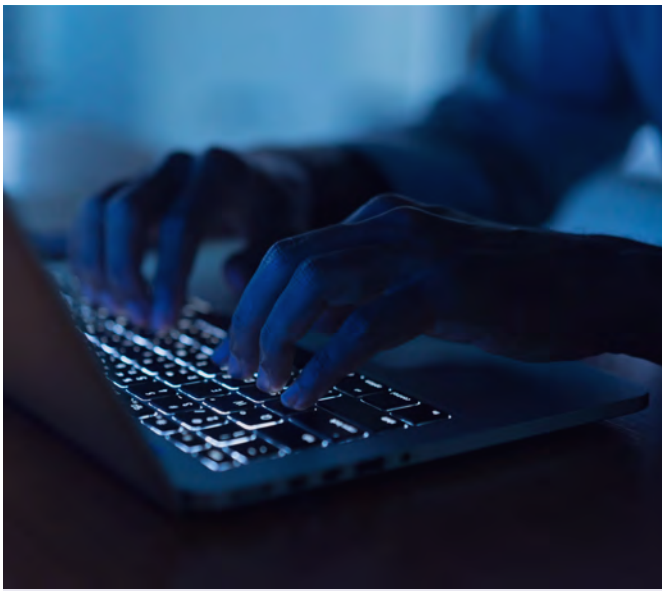
- internetowych platform handlowych (*providers of online marketplaces*);
- wyszukiwarek internetowych (*providers of online search engines*);
- serwisów społecznościowych (*providers of social networking services platform*) – warto zwrócić uwagę, że ci dostawcy nie byli dotąd objęci dyrektywą NIS.

Podejście oparte na ryzyku i kary administracyjne

Zarówno kluczowe, jak i istotne podmioty zgodnie z dyrektywą NIS2 powinny podlegać takim samym wymogom w zakresie zarządzania ryzykiem i obowiązkom sprawozdawczym. Takie same wymogi nie oznaczają jednak, że zrezygnowano z podejścia opartego na ryzyku – wręcz przeciwnie. W praktyce oznacza to, że ustawa implementująca dyrektywę NIS2 nie powinna zawierać rozróżnienia obowiązków kluczowych i istotnych podmiotów – jak obecna ustawa o krajowym systemie cyberbezpieczeństwa różnicuje obowiązki operatorów usług kluczowych i dostawców usług cyfrowych.

Odnośnie do podejścia opartego na ryzyku kraje członkowskie powinny zgodnie z projektem dyrektywy NIS2 zapewnić, że podmioty objęte regulacją podejmą odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych, które podmioty te wykorzystują przy świadczeniu swoich usług. Projekt dyrektywy NIS2 przewiduje przy tym, że systemy nadzoru i sankcji pomiędzy podmiotami kluczowymi i istotnymi powinny być zróżnicowane, co będzie się bezpośrednio przekładać na wysokość kar za naruszenie przepisów.

W tym zakresie projekt dyrektywy NIS2 jasno odnosi się do wysokości kar administracyjnych, które mogą zostać nałożone na kluczowe lub istotne podmioty, określając ich górną granicę – 10 milionów euro lub 2% przychodu, w zależności od tego, która kwota będzie wyższa. Taka propozycja jest o tyle istotna, że maksymalne kwoty kar administracyjnych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa (implementującej dyrektywę NIS) były znacząco niższe, a w porównaniu z karami, które mogły zostać nałożone na gruncie RODO – nieznaczne. Jednocześnie doświadczenia wdrożenia RODO pokazują, że zagrożenie niewykonania obowiązków wysokimi karami jest pewnego rodzaju motywacją dla podmiotów zobowiązanych.



Dyrektywa NIS2 – rewolucja w dziedzinie cyberbezpieczeństwa?

Opisane wyżej propozycje zmian jasno pokazują, że wyciągnięto wnioski z często niedoskonałej, ale przede wszystkim niejednolitej implementacji dyrektywy NIS. Nie zdecydowawszy się na wprowadzenie rozporządzenia unijnego, Komisja podjęła próbę wyeliminowania rozbieżności podejścia krajów członkowskich w poszczególnych krajowych regulacjach, przynajmniej w najistotniejszych kwestiach. Trzeba przy tym pamiętać, że opisywana dyrektywa NIS2 jest dopiero projektem, a ostateczny kształt regulacji będzie jeszcze podlegać uzgodnieniom.

Niezależnie jednak od tego wdrożenie dyrektywy NIS2 wymagać będzie w dalszej perspektywie zmian w polskim krajowym systemie cyberbezpieczeństwa, w którego skład wejdzie więcej podmiotów niż dotychczas. Oznaczać to będzie także rezygnację z procedury wyznaczania podmiotów decyzją administracyjną. Odciążenie organów właściwych w tym zakresie może pozwolić na przekierowanie sił i środków nie tylko na nadzór nad podmiotami zobowiązanymi (czyli w praktyce weryfikację spełnienia przez nich ustawowych obowiązków), lecz także na tworzenie inicjatyw wspierających wymianę informacji w zakresie cyberbezpieczeństwa.

Propozycja dyrektywy NIS2 jest dostępna pod linkiem: klik.

Objęcie ISAC krajowym systemem cyberbezpieczeństwa – nowelizacja ustawy o KSC

r.pr. Joanna Jastrząb, apl. adw. Dominika Duda

Na początku września zeszłego roku jednym z ważniejszych tematów dotyczących cyberbezpieczeństwa stał się projekt nowelizacji Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej: „ustawa o KSC"). Trafił on wtedy do publicznych konsultacji i zakładano, że nowelizacja zostanie wprowadzona w grudniu. Pod koniec 2020 r. okazało się jednak, że zostanie to opóźnione. Zgłoszono do niej szereg uwag, głównie przez przedstawicieli sektora prywatnego, organizacje pozarządowe, a także przez niektóre instytucje państwowe[1]. Na razie nie jest jeszcze do końca pewne, kiedy i w jakim ostatecznym brzmieniu nowelizacja zostanie wprowadzona. „Projekt ustawy jest w ostatniej fazie po etapie uzgodnień międzyresortowych i konsultacji publicznych i mamy nadzieję, że zostanie skierowany pod obrady komitetów Rady Ministrów na początku roku" – taką informację podał podczas posiedzenia sejmowej Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (CNT) Marek Zagórski, sekretarz stanu w Kancelarii Prezesa Rady Ministrów (KPRM), pełnomocnik ds. cyberbezpieczeństwa[2].

O nowelizacji pisaliśmy już w poprzednich wydaniach newslettera (por. wydanie październikowe dostępne tutaj). Wśród zaproponowanych zmian jest objęcie krajowym systemem cyberbezpieczeństwa ISAC (ang. *information sharing and analysis centre*), a więc specjalistycznych organizacji mających zwykle formę partnerstwa publiczno-prywatnego (PPP), do których zadań należy w szczególności wymiana informacji, dobrych praktyk i doświadczeń dotyczących zagrożeń cyberbezpieczeństwa, podatności oraz incydentów.

W dzisiejszym świecie, w którym informacja jest kluczowa i może być przekazywana w kilka sekund, jest to fundamentalne dla światowych i krajowych systemów cyberbezpieczeństwa. Umożliwia to bowiem szybkie i sprawne reagowanie na a zagrożenia, wspólną edukację, przekazywanie ciekawych pomysłów oraz znacznie zmniejsza wszelkie związane z tym koszty. Zauważył to polski ustawodawca i włączył ISAC do krajowego systemu cyberbezpieczeństwa, podkreślając przez to ich rolę w tym zakresie. Możliwość tworzenia ISAC wprowadzona została do projektu nowelizacji ustawy o KSC w art. 4a. Warto dodać, że regulacja ta nie wskazuje wprost zasad czy też norm ich szczegółowego funkcjonowania, a więc ustawodawca postanowił pozostawić na tym polu dowolność podmiotom, które chciałyby je założyć.

W powyższej nowelizacji znalazł się również przepis, zgodnie z którym minister właściwy ds. informatyzacji ma prowadzić i nadzorować wykaz ISAC. Ma on zawierać m.in. nazwę (firmę) ISAC, imię i nazwisko osoby reprezentującej ISAC wraz z danymi kontaktowymi czy też datę wpisania ISAC do wykazu. Sam wykaz będzie dostępny publicznie – będzie publikowany na stronie podmiotowej Biuletynu Informacji Publicznej (BIP). Warto także wspomnieć, że w ramach powyższego nadzoru minister ds. informatyzacji będzie mógł zwrócić się do ISAC z żądaniem usunięcia nieprawidłowości (działalności niezgodnej z prawem lub naruszania zasad współpracy w ramach krajowego systemu cyberbezpieczeństwa) albo wykreślić ten podmiot z wykazu.

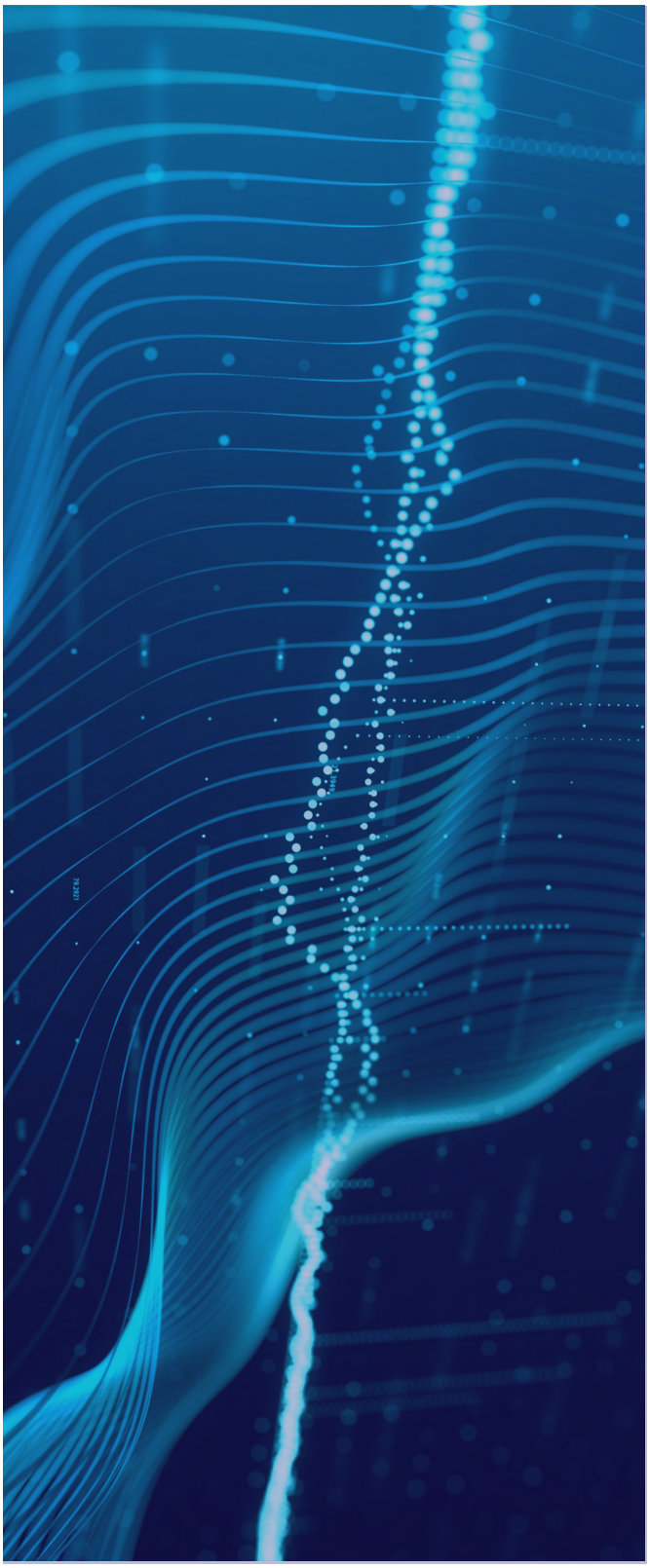
[1] Uwagi do projektu nowelizacji ustawy dostępne są na oficjalnej stronie Rządowego Centrum Legislacji : https://legislacja.rcl.gov.pl/projekt/12337950/katalog/12716614#12716614 (dostęp: 13.01.2020).
[2] Źródło informacji prasowej: https://itreseller.com.pl/ustawa-o-krajowym-systemie-cyberbezpieczenstwa-ksc-ma-trafic-pod-obrady-komitetow-rady-ministrow-na-poczatku-2021-roku-poinformowal-marek-zagorski/ (dostęp: 13.01.2020).

ISAC od dłuższego czasu z powodzeniem działają zarówno na świecie, jak i w Europie, a od niedawna także w Polsce. Zdecydowana większość centrów ma charakter sektorowy (obejmujący całość danej branży, np. bankowej czy energetycznej) o zasięgu krajowym lub międzynarodowym. Pierwsza polska organizacja ISAC została powołana dla sektora transportu kolejowego i nazywa się Centrum Wymiany i Analizy Informacji ISAC-Kolej, a zawiązały ją spółki kolejowe i NASK – PIB.

Do tej pory sposób funkcjonowania ISAC nie został jednak w Polsce prawnie uregulowany (w zakresie choćby ich struktury czy sposobów finansowania – uzgodnienie tych kwestii należy jak na razie do podmiotów założycielskich). Jak zostało już wspomniane wyżej, nowelizacja ustawy o KSC zaznacza co prawda rolę ISAC, ale pomija powyższe kwestie, nie określając również sposobu ich powołania. Chociaż to rozwiązanie można różnie ocenić, z pewnością pozostaje elastyczne dla podmiotów, które planują ISAC założyć. Bez wątpienia jednak wyraźne objęcie ISAC krajowym systemem cyberbezpieczeństwa może przyczynić się do wzrostu ich roli, a w konsekwencji doprowadzić do szybkiej i sprawnej wymiany informacji pomiędzy podmiotami zarówno prywatnymi, jak i publicznymi.

Podsumowanie

Nowelizacja ustawy o KSC w kontekście ISAC to dobra wiadomość dla podmiotów krajowego systemu cyberbezpieczeństwa. Świadczy to o tym, że polski ustawodawca zauważył, jak ważną rolę mogą odegrać ISAC w tym systemie. Pozostawił też pewną dowolność podmiotom chcącym utworzyć Centra Wymiany i Analizy Informacji w zakresie ich struktury, funkcjonowania oraz organizacji, z czego wnioskować można, że w ten sposób chce zachęcić i zmotywować do ich tworzenia, nie zaś trzymać się sztywnych ram i formalnych wymogów, które mogłyby zdemotywować chcących zakładać ISAC. Takie podejście, zakładające pewną elastyczność i swobodę, będzie zresztą sprzyjać procesowi wymiany informacji, co jest głównym celem tworzenia ISAC. Podmioty członkowskie będą mogły wybrać optymalne rozwiązania, które pozwolą im to zapewnić. Pozostaje więc czekać na skierowanie projektu nowelizacji do dalszych prac, co ma nastąpić w I kwartale 2021 r.



Inwestycje poniesione na wdrożenie dyrektywy NIS – raport ENISA

W przeddzień publikacji propozycji nowej dyrektywy dotyczącej cyberbezpieczeństwa (NIS2) ENISA opublikowała raport na temat kosztów poniesionych na wdrożenie dyrektywy NIS. Jego podstawą są badania przeprowadzone wśród 251 organizacji sektora prywatnego: operatorów usług kluczowych i dostawców usług cyfrowych z Francji, Niemiec, Włoch, Hiszpanii i Polski. Przedsiębiorcy odpowiadali na pytania dotyczące tego, jak dysponują budżetem w zakresie bezpieczeństwa informacji oraz jak na te wydatki wpłynęła dyrektywa NIS.

Co wynika z raportu?

82% badanych przedsiębiorców pozytywnie ocenia wpływ dyrektywy NIS na bezpieczeństwo informacji w ich organizacji.

58% ankietowanych organizacji zadeklarowało, że implementacja wymogów dyrektywy NIS została zakończona. Co ciekawe, wśród polskich przedsiębiorców ten odsetek był najniższy – tylko **42,9%** z nich zakończyło implementację. Najwyższy odsetek w tym zakresie dotyczy Niemiec (**70,6%**).

14–18 miesięcy trwa zwykle wdrażanie przepisów dyrektywy NIS, jak deklarują badani. Większość z nich zaczęła ją wdrażać w 2018 i 2019 r.

Ponad połowa organizacji (**50,7%**) przeprowadziła wdrożenie NIS samodzielnie, podczas gdy **28,9%** zatrudniło nowy personel, a **20,4%** skorzystało z usług zewnętrznych doradców.

Aż **38,5%** badanych organizacji wskazało niejasne oczekiwania odnośnie do nałożonych wymogów jako wyzwanie we wdrożeniu dyrektywy NIS. Taki sam odsetek ankietowanych uznał, że wyzwaniem w tym zakresie była konieczność nadania priorytetu innym aktom prawnym (jak RODO).

Pełny raport dostępny jest pod linkiem: klik.

NADCHODZĄCE WYDARZENIA

26.01.2021
SZKOLENIE

Zwinne wdrożenie w umowach IT (AGILE, PRINCE2 AGILE) - przygotowanie i negocjowanie umów w projektach IT przy zwinnym podejściu

r. pr. Agnieszka Wachowska

Więcej informacji >>

16.02.2021
SZKOLENIE

Umowy na utrzymanie, serwis i rozwój systemów IT - najlepsze praktyki i sporne kwestie

r. pr. Agnieszka Wachowska

Więcej informacji >>

25.02.2021
SZKOLENIE

Prawne aspekty cyberbezpieczeństwa

r. pr. Agnieszka Wachowska, r.pr. Joanna Jastrząb

Więcej informacji >>

09.03.2021
SZKOLENIE

Niewykonanie lub nienależyte wykonanie umowy IT - co zrobić aby uniknąć sporu i jak się zachować w sytuacjach kolizyjnych pomiędzy Wykonawcą i Zamawiającym?

adw. Xawery Konarski, r. pr. Agnieszka Wachowska

Więcej informacji >>

NR 1 - STYCZEŃ 2021

PUBLIKACJE

Nr 1/2021 IT Professional:

- **r.pr. Magdalena Gąsowska** – Oprogramowanie jako produkt podwójnego zastosowania

ZESPÓŁ IT-TELCO

Xawery Konarski
Adwokat, Senior Partner
xawery.konarski@traple.pl

Agnieszka Wachowska
Radca prawny, Partner
agnieszka.wachowska@traple.pl

Piotr Nepelski
Radca prawny, Senior Associate
piotr.nepelski@traple.pl

Tomasz Krzyżanowski
Radca prawny, Senior Associate
tomasz.krzyżanowski@traple.pl

Joanna Dworak
Radca prawny, Senior Associate
joanna.dworak@traple.pl

Joanna Jastrząb
Radca prawny, Senior Associate
joanna.jastrzab@traple.pl

Magdalena Gąsowska-Paprota
Radca prawny, Senior Associate
magdalena.gasowska@traple.pl

Karolina Grochecka-Goljan
Adwokat, Senior Associate
karolina.grochecka@traple.pl

Małgorzata Kotwica
Associate
malgorzata.kotwica@traple.pl

Aleksander Elmerych
Aplikant radcowski, Junior Associate
aleksander.elmerych@traple.pl

Pytania prosimy kierować na adres:
it-telco@traple.pl

Redaktor newslettera:
r.pr. Joanna Jastrząb