#KWKR E-BOOK

ZMIANY W PRZEPISACH DOTYCZĄCYCH DZIAŁALNOŚCI TELEKOMUNIKACYJNEJ 2023

Jarosław Straś
Radca prawny
Associate

KONIECZNY WIERZBICKI
KANCELARIA RADCÓW PRAWNYCH

Spis treści

Wprowadzenie

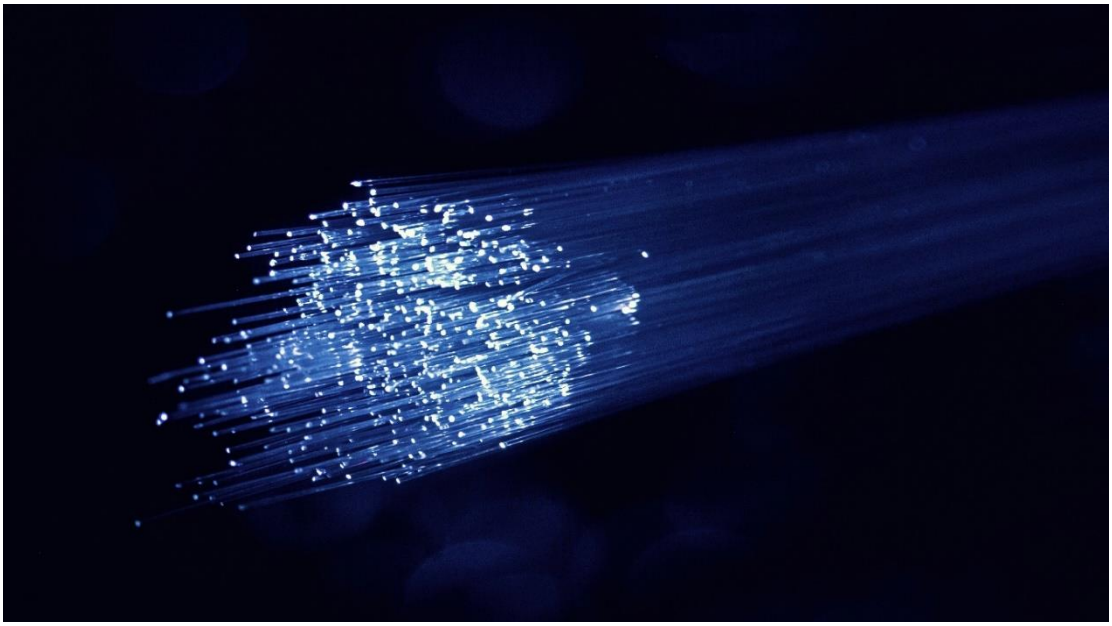
Kiedy w grudniu 2022 roku został wniesiony do Sejmu projekt ustawy Prawo komunikacji elektronicznej, wydawało się, że w kolejnym roku doczekamy się wejścia w życie przepisów, które zastąpią ustawę z dnia 16 lipca 2004 r. Prawo telekomunikacyjne i tym samym nastąpi implementacja Europejskiego kodeksu łączności elektronicznej (EKŁE). Niestety niedługo po tym, jak nad projektem zaczęła pracować komisja sejmowa, został on wycofany z Sejmu i do tej pory tam nie powrócił.

Zahamowanie prac nad projektem Prawo komunikacji elektronicznej nie oznacza wcale, że w przepisach regulujących działalność telekomunikacyjną, w trakcie ostatnich kilku miesięcy, nie działo się zbyt wiele. Wręcz przeciwnie. Do szerszego omówienia obecnego stanu prac nad przepisami, które mają zastąpić ustawę Prawo telekomunikacyjne jeszcze w tym opracowaniu wrócimy, natomiast wśród zagadnień, które powinny stanowić obszar zainteresowania przedsiębiorców telekomunikacyjnych, a wokół których toczyły się prace legislacyjne, możemy wyróżnić:

- ochronę przed skutkami nadużyć wynikającymi z kradzieży tożsamości i obowiązkami przedsiębiorców telekomunikacyjnych, które zapobiegać mają tzw. *SIM-swapping*;
- nowe obowiązki przedsiębiorców telekomunikacyjnych w zakresie zwalczania nadużyć w komunikacji elektronicznej,
- prace nad regulacjami zwiększającymi ochronę małoletnich przed dostępem do treści nieodpowiednich w internecie.

W niniejszym opracowaniu przedstawiamy omówienie zapowiadanych zmian dla podmiotów z branży telekomunikacyjnej.

Zachęcamy do lektury!



Zwiększona ochrona przed skutkami kradzieży tożsamości, a nowe obowiązki dostawców usług telekomunikacyjnych

Zwiększenie skali zjawiska nieuprawnionego wejścia w posiadanie numeru PESEL, w wyniku np. kradzieży dokumentów tożsamości lub wycieku danych, skłoniło ustawodawcę do podjęcia działań zmierzających do ochrony osób dotkniętych skutkami takich zdarzeń.

Działania mają być ukierunkowane na zapobieganie zaciąganiu zobowiązań o charakterze majątkowym na szkodę osób, których kradzież tożsamości dotyczy. Wśród przypadków, które wymienia się najczęściej przy okazji posłużenia się cudzymi danymi są zawarcie umów kredytu i pożyczki, sprzedaż nieruchomości oraz otwieranie rachunków rozliczeniowych. Wraz ze zwiększeniem wachlarza możliwości dostępu użytkowników do usług np. bankowości elektronicznej z poziomu telefonu komórkowego doszło także do wykreowania nowego zagrożenia, które określa się jako *SIM-swapping*, czyli wyrobienia duplikatu karty SIM, która może później zostać użyta do autoryzowania transakcji wykonywanych przez przestępców w instytucjach płatniczych.

Przepisami ustawy z dnia 7 lipca 2023 r. *o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości* (dalej: „**Ustawa**"), bo taką pełną nazwę nosi akt prawny, o którym jest tutaj mowa, objęta została zatem grupa podmiotów i instytucji, do których należą banki, instytucje kredytowe, notariusze, a także przedsiębiorcy telekomunikacyjni.

Jeśli mielibyśmy mówić o wspólnym charakterze obowiązków ww. podmiotów, na podstawie Ustawy, z pewnością należy wymienić obowiązek weryfikowania w tzw. **rejestrze zastrzeżeń numerów PESEL**, przed dokonaniem określonej czynności, czy w przypadku osoby, której ta czynność ma dotyczyć, nie doszło do zastrzeżenia jej numeru PESEL.

Obecnie kwestia weryfikacji tożsamości osoby żądającej wyrobienia duplikatu karty SIM regulowana jest wewnętrznymi procedurami danego operatora. Najczęściej odbywa się to w salonie dostawcy, gdzie pracownik weryfikuje tożsamość na podstawie okazanego dokumentu tożsamości.

Przypominajmy, że Prezes Urzędu Komunikacji Elektronicznej już w 2018 roku występował do dostawców mobilnych usług telekomunikacyjnych i Związku Banków Polskich z wnioskiem o podjęcie działań skierowanych przeciwko coraz częstszemu występowaniu zjawiska SIM-swap-fraud[1].

W tym miejscu należy doprecyzować, że omawiany obowiązek nie będzie mógł być zrealizowany w przypadku wszystkich abonentów. Klientami przedsiębiorców telekomunikacyjnych są również obcokrajowcy nieposiadający numeru PESEL. Posiadanie numeru PESEL nie jest obecnie obligatoryjne w przypadku zawarcia umowy o świadczenie usług telekomunikacyjnych. Zgodnie z art. 60b ust. 1 pkt 1) b) ustawy *Prawo telekomunikacyjne*, w celu weryfikacji tożsamości osoby fizycznej, która chce zawrzeć umowę o świadczenie usług telekomunikacyjnych, cudzoziemiec, który nie posiada numeru PESEL, podaje dostawcy usług nazwę, serię i numer dokumentu potwierdzającego tożsamość, a w przypadku cudzoziemców, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej – numer paszportu lub karty pobytu.

Ustawa będzie wymagała od przedsiębiorców telekomunikacyjnych podjęcia stosownych działań w przypadku osoby, która żąda wydania jej kopii lub wtórnika karty SIM.

[1] https://www.uke.gov.pl/akt/prezes-uke-ostrzega-przed-naduzyciami-z-podmiana-kart-sim,114.html

Przykładowe obowiązki dostawców usług:

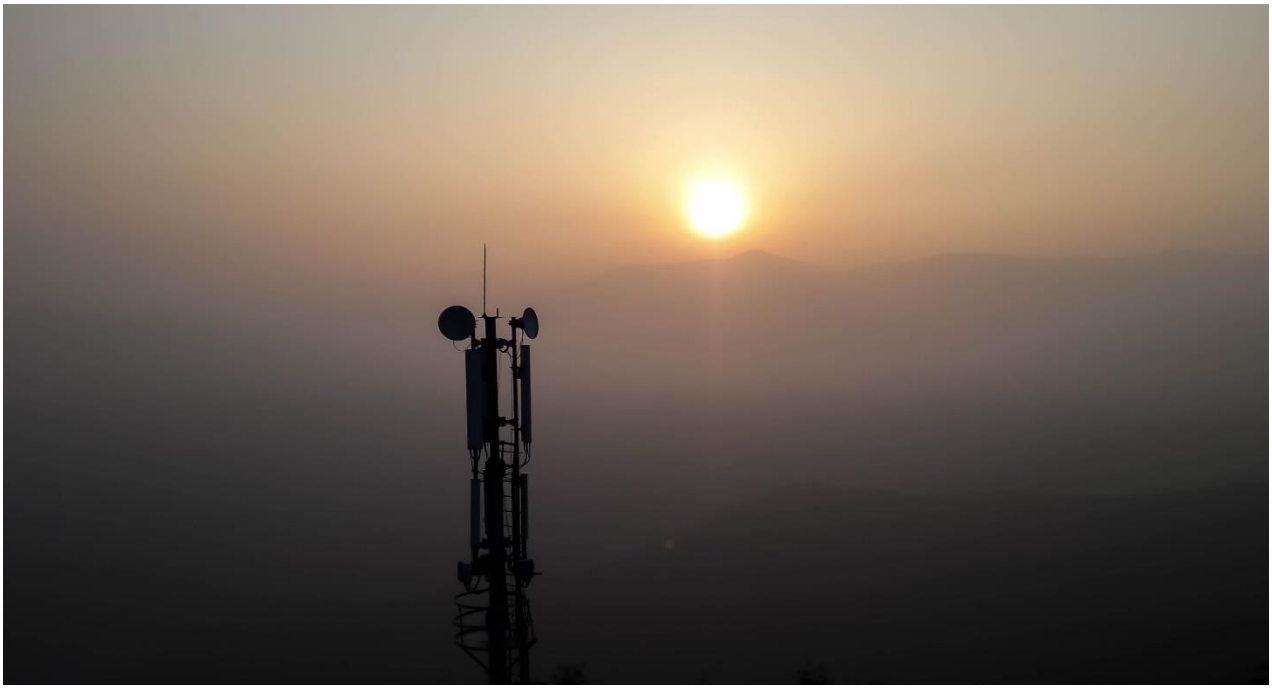
- dokonanie weryfikacji czy numer PESEL, podany przez abonenta żądającego wydania kopii lub wtórnika kary lub innego urządzenia służących do identyfikacji abonenta, jest zastrzeżony w rejestrze zastrzeżeń numerów PESEL;
- odmowa dokonania czynności, jeśli numer PESEL jest zastrzeżony lub w chwili weryfikacji system informatyczny rejestru zastrzeżeń numerów PESEL jest niedostępny;
- po ponownej nieudanej próbie dokonania weryfikacji - odmowa wydania kopii lub wtórnika karty lub ich wydanie, z zachowaniem należytej staranności przy weryfikacji tożsamości abonenta;
- udokumentowanie weryfikacji abonenta, w przypadku wydania mu kopii lub wtórnika karty pomimo niedostępności rejestru zastrzeżeń numerów PESEL.

Rozpoczęcie realizacji nowych obowiązków:

Obowiązek weryfikacji danych zastrzeżonych w rejestrze będzie spoczywał na przedsiębiorcach telekomunikacyjnych począwszy od **1 czerwca 2024 r.**

Treść nowych przepisów:

https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20230001394/T/D20231394L.pdf



Dostawcy usług w służbie zwalczania nadużyć w komunikacji elektronicznej

Obszar komunikacji elektronicznej, bo właśnie w ten sposób Europejski kodeks łączności elektronicznej (EKŁE) określa to, co do tej pory nazywaliśmy telekomunikacją (o szerszym wpływie EKŁE na prace legislacyjne w naszym kraju, w dalszej części opracowania), narażony jest na coraz powszechniejsze zjawiska świadczenia lub korzystania z usług telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa.

Takim zagrożeniom zapobiegać ma ustawa z dnia 28 lipca 2023 r. *o zwalczaniu nadużyć w komunikacji elektronicznej* (dalej: „**Ustawa**").

Wśród rodzajów nadużyć pojawiających się w toku prac legislacyjnych nad Ustawą wymieniono takie niepożądane zjawiska, jak:

- **generowanie sztucznego ruchu telekomunikacyjnego**, które stanowi zagrożenie zarówno dla przedsiębiorców telekomunikacyjnych, jak również dla użytkowników końcowych. Dochodzi bowiem do inicjowania wielogodzinnych połączeń, które nie zawierają żadnej treści i nie służą komunikowaniu się. Sztuczny ruch powoduje zmniejszenie przepustowości sieci telekomunikacyjnych, a poprzez włamanie do urządzeń klienckich również straty finansowe po ich stronie wskutek np. wykonywania połączeń na kierunki egzotyczne czy o podwyższonej opłacie;
- **smishing**, polegający na dokonywaniu nadużyć przy użyciu wiadomości SMS. Za ich pośrednictwem odbiorca może przypadkowo zainstalować złośliwe oprogramowanie na swoim telefonie komórkowym (np. klikając w link zamieszczony w treści takiej wiadomości) lub wprost wskazać dane lub informacje służące następnie do dokonywania niekorzystnego rozporządzania mieniem odbiorcy;
- **CLI spoofing**, czyli podszywanie się pod numer zaufanej osoby lub instytucji i wykonywanie połączeń z rzekomo prawdziwego numeru tych podmiotów. Odbiorca jest wtedy najczęściej nakłaniany do podjęcia określonych działań związanych z niekorzystnym rozporządzaniem swoim mieniem;
- **nieuprawniona zmiana informacji adresowej**, z którą mamy do czynienia w sytuacji niedozwolonego oddziaływania na urządzenia telekomunikacyjne. Wskutek zmiany danych rejestrowych i zgubienia źródła ruchu może dojść do wprowadzenia w błąd systemów dostawcy usług. W takiej sytuacji operatorzy telekomunikacyjni nie są w stanie zapewnić tzw. uprawnionym podmiotom (np. Policji lub Agencji Bezpieczeństwa Wewnętrznego) danych pozwalających na ustalenie sprawcy fałszywych alarmów bombowych.

Przykładowe obowiązki przedsiębiorców telekomunikacyjnych:

- blokowanie wiadomości SMS, zawierających treści uznane za smishing, według wzorca wiadomości wyczerpującej znamiona tego zagrożenia. Wzorzec takiej wiadomości będzie tworzony przez i publikowany przez CSIRT NASK,
- zapewnienie swoim użytkownikom końcowym oraz CSIRT NASK możliwość bezpłatnego korzystania z numeru skróconego 8080, w celu przekazywania informacji do CSIRT NASK oraz wysyłania z tego numeru wiadomości zwrotnych przez CSIRT NASK w sprawie podejrzenia, że treści wiadomości SMS wyczerpują znamiona smishingu,

- blokowanie połączeń głosowych lub ukrywanie identyfikacji numeru wywołującego dla użytkownika końcowego w przypadku występowania CLI spoofingu oraz stosowanie środków organizacyjnych i technicznych służących monitorowaniu, wykrywaniu oraz wymianie informacji o CLI spoofing (np. w oparciu o rekomendacje wydane przez Prezesa UKE),
- wykonanie decyzji Prezesa UKE nakazującej zablokowanie dostępu do numeru lub usługi w terminie nie krótszym niż 6 godzin od ogłoszenia decyzji oraz wstrzymanie pobierania opłat za połączenia lub usługi realizowane po upływie ww. terminu.

Rozpoczęcie realizacji nowych obowiązków:

Przedsiębiorcy telekomunikacyjni są zobowiązani do wdrożenia proporcjonalnych środków o charakterze organizacyjnym i technicznym mających na celu zapobieganie:

- generowaniu sztucznego ruchu i smishingu w terminie **6 miesięcy** od dnia wejścia w życie Ustawy, tj. do dnia **26 marca 2024 r.**,
- CLI spoofingu i nieuprawnionej zmianie informacji adresowej w terminie **12 miesięcy** od dnia wejścia w życie Ustawy, tj. do dnia **26 września 2024 r.**

Treść nowych przepisów:

https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20230001703/T/D20231703L.pdf

Ochrona małoletnich w internecie przy udziale przedsiębiorców telekomunikacyjnych

Do tego, aby na przedsiębiorcach telekomunikacyjnych ciążyły nowe obowiązki w zakresie ochrony małoletnich w internecie było bardzo blisko. Wszystko za sprawą projektu *ustawy o ochronie małoletnich przed dostępem do treści nieodpowiednich w Internecie* (dalej: „**Projekt**"), którego początki sięgają prac Rządowego Centrum Legislacji z jesieni zeszłego roku. Wnioskodawcą tego Projektu było Ministerstwo Cyfryzacji.

Przypomnijmy, że celem Projektu było nałożenie na dostawców usług dostępu do Internetu obowiązku zapewnienia abonentowi możliwości skorzystania z usługi ograniczenia dostępu do treści pornograficznych w internecie. Projekt pozostawiał jednak wedle uznania dostawców usług dobór narzędzi, którymi będą się posługiwali w celu zapewnienia świadczenia tej usługi.

Projekt zakładał możliwość zwrócenia w każdym momencie przez abonenta o rozpoczęcie świadczenia usługi ograniczenia dostępu do treści pornograficznych w internecie. Docelowo rozpoczęcie świadczenia takiego ograniczenia nie powinno przekraczać 1 dnia roboczego od momentu złożenia żądania. Usługa ograniczenia dostępu miała być opisana w regulaminie, który nie miał być jednak tożsamy z regulaminem świadczenia usług telekomunikacyjnych. Powstałby zatem obowiązek przygotowania kolejnego dokumentu abonenckiego.

Za świadczoną usługę ograniczenia dostępu użytkownicy końcowi mieli nie ponosić kosztów.

Przykładowe obowiązki dostawców usług, które przewidywał Projekt:

- obowiązek proponowania użytkownikowi końcowemu możliwości skorzystania z usługi przed zawarciem umowy o świadczenie usług telekomunikacyjnych i obowiązek niezwłocznego uruchomienia usługi w przypadku takiego żądania przez abonenta w trakcie obowiązywania umowy;
- obowiązek sporządzenia regulaminu usługi ograniczenia dostępu do treści pornograficznych w internecie;
- podejmowanie działań promujących korzystanie przez abonentów z rozwiązań ograniczających dostęp małoletnich do treści nieodpowiednich;
- obowiązek raportowy (coroczny) w zakresie realizacji usługi ograniczającej dostęp do treści nieodpowiednich;

Treść projektu zmian w przepisach:

Projekt został wniesiony do Sejmu, jednak zaprzestano tam dalszych prac nad jego uchwaleniem. Z treścią proponowanych zmian można zapoznać się pod adresem:

https://orka.sejm.gov.pl/Druki9ka.nsf/0/DFD0223E5B48AABAC12589B9003AA2D3/%24File/3282-ustawa.docx

Kolejny rok bez Prawa komunikacji elektronicznej

Tak jak pisaliśmy na wstępie niniejszego opracowania, wydawało się, że rok 2023 przyniesienie zastąpienie obecnie obowiązującej ustawy Prawo telekomunikacyjne, zupełnie nowym aktem prawnym, tj. Prawo komunikacji elektronicznej (dalej: „**PKE**"), który miał w szczególności implementować przepisy Europejskiego kodeksu łączności elektronicznej (dalej: „**EKŁE**"). EKŁE weszło w życie 17 grudnia 2018 r., a termin transpozycji jego przepisów do prawa krajowego państw członkowskich został wyznaczony na dzień 21 grudnia 2020 r.

Jeszcze w czerwcu bieżącego roku Polska i Irlandia były jedynymi państwami w Unii Europejskiej, które nie zdołały zaimplementować przepisów EKŁE. Irlandia zdążyła sobie już z tym problemem poradzić i tak oto obecnie Polska pozostała jedynym krajem członkowskim, który nie wdrożył w całości przepisów EKŁE.

Przypomnijmy, że pierwszy projekt PKE został ogłoszony w lipcu 2020 r. Ministerstwo Cyfryzacji zapraszając do konsultacji „reklamowało" go jako ustawę, która regulować ma działanie całego polskiego sektora łączności elektronicznej. Zakres podmiotowy nowego aktu prawnego zakładał bowiem objecie nim nie tylko dostawców usług telekomunikacyjnych, ale także podmioty świadczące usługi „komunikacji interpersonalnej niewykorzystującej numerów". PKE dotyczyłoby zatem komunikatorów internetowych i poczty elektronicznej. Po pierwszym projekcie PKE doczekaliśmy się jeszcze trzech kolejnych, aż w końcu, 9 grudnia 2022 r., ostateczny projekt PKE wpłynął do Sejmu.

Przykładowe obowiązki dostawców usług, które przewidywał projekt PKE:

- koniecznym stałby się obowiązek dostosowania dokumentów abonenckich. Zniknąć miała możliwość używania wielu wzorców umownych, w tym regulaminów (np. regulaminu ogólnego, regulaminu usług dodatkowych, regulaminu promocji itp.), a nawet cennika. Wszystkie informacje wymagane przez ustawę miały zostać przekazane abonentom w ramach trzech dokumentów: umowy, informacji przedumownych i podsumowania warunków umowy;
- obowiązek retencji danych telekomunikacyjnych przez okres 12 miesięcy i przekazywania tych danych tzw. uprawnionym podmiotom (np. Policji) oraz sądowi i prokuratorowi. Obowiązek ten znany jest już dostawcom usług na podstawie ustawy Prawo telekomunikacyjne jednakże w projekcie PKE został on dodatkowo rozszerzony;
- realizacja obowiązku zatrzymania świadczenia usług w przeciągu zaledwie 6 godzin, w przypadku zagrożenia bezpieczeństwa państwa lub porządku publicznego;
- realizacja zmian w zakresie uzyskiwania zgody użytkowników na przesyłanie informacji marketingowych (wprowadzenie jednej zgody marketingowej zamiast budzącego obecnie kontrowersje zbierania dwóch oddzielnych zgód – na podstawie PT i ustawy o świadczeniu usług drogą elektroniczną lub łączenia tych zgód w jednym oświadczeniu odbiorcy);

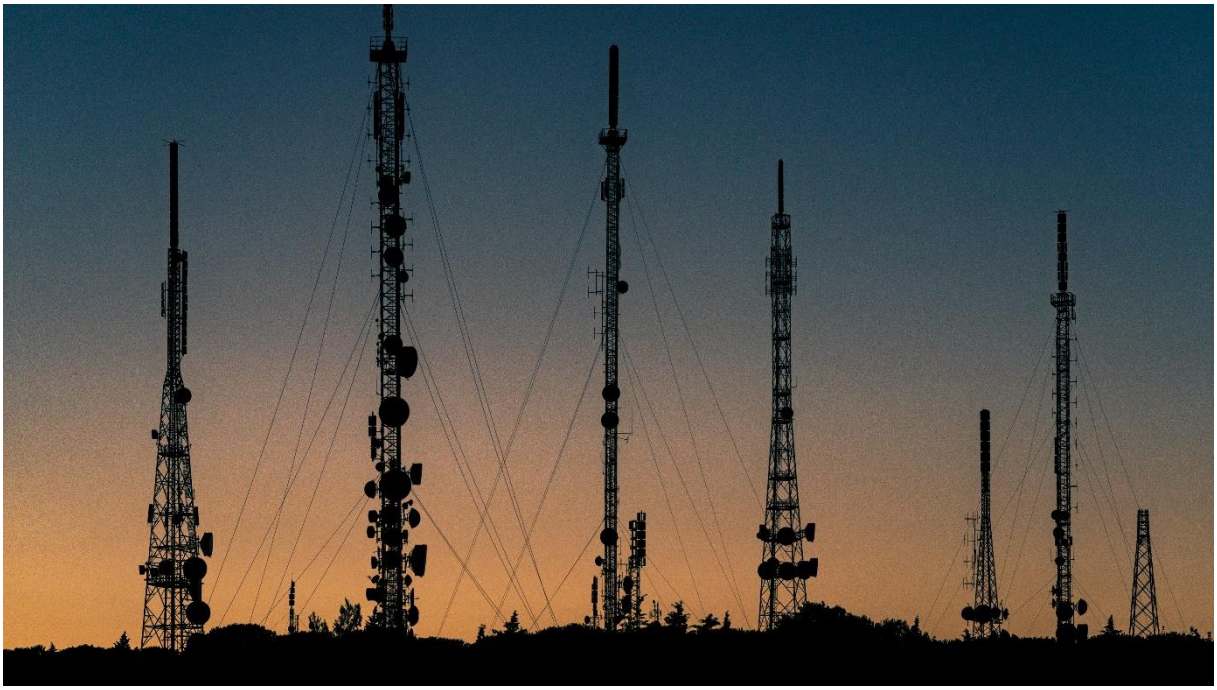
Projekt PKE, po wysłuchaniu publicznym w ramach posiedzenia Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii z dnia 6 marca 2023 r., został jednak z prac sejmowych wycofany w kwietniu 2023 roku. Taki sam los spotkał procedowaną równolegle z PKE ustawę Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej (druk nr 2862) – dalej: „**Przepisy wprowadzające PKE**").

Główne zarzuty kierowane pod adresem projektu PKE to:

- obecność w projekcie PKE oraz Przepisach wprowadzających PKE tzw. ***lex pilot***, które odnoszą się do *ustawy o radiofonii i telewizji* w zakresie rozpowszechniania programów telewizyjnych objętych zasadą *must carry must offer* (MCMO). Proponowane zmiany miały ograniczać listę programów objętych ww. zasadą do programów nadawcy publicznego oraz rozszerzać listę o dalsze programy publiczne, co naruszałoby przepisy m.in. EKŁE;
- wątpliwe pod względem ich zgodności z konstytucyjnymi oraz unijnymi zasadami, przepisy dotyczące obowiązku **retencji danych telekomunikacyjnych**. Przypomnijmy, że projekt PKE w tej kwestii w dużej mierze pokrywa się z przepisami ustawy Prawo telekomunikacyjne, a biorąc pod uwagę katalog danych, które podlegają obowiązkowi retencji, dodatkowo nawet rozszerza go o *dane jednoznacznie identyfikujące użytkownika sieci*. Problem w tej kwestii sięga jeszcze przepisów ustawy Prawo telekomunikacyjne, których odpowiedniki w ustawodawstwach innych państw członkowskich były kwestionowane w licznych orzeczeniach Trybunału Sprawiedliwości Unii Europejskiej, natomiast w polskim porządku prawnym pozostały w gruncie rzeczy niezmienione (poza skutkami wyroku Trybunału Konstytucyjnego z 2014 r.).

Treść projektu zmian w przepisach:

Termin transpozycji przepisów EKŁE minął **21 grudnia 2021 roku**. Obecnie trudno jest przewidzieć kiedy kolejny projekt PKE zostanie wniesiony do Sejmu i jak długo potrwają prace legislacyjne.



KONIECZNY WIERZBICKI
KANCELARIA RADCÓW PRAWNYCH

Obszar TMT w ramach Kancelarii KWKR

Wsparcie prawne dla Klientów działających w sektorze nowych technologii to jedna z naszych głównych specjalizacji. Obsługujemy wiele podmiotów, które opracowują i komercjalizują nowoczesne rozwiązania czy produkty, pomagając w realizacji strategii biznesowej przy jednoczesnej dbałości dbając o to zabezpieczenie efektów ich pracy.

Projektujemy i przygotowujemy regulacje umów dotyczące przenoszenia praw do produktów, systemów licencyjnych o różnym zakresie, a także innych możliwości korzystania z produktów takich jak SaaS.

Mamy szerokie doświadczenie w przygotowywaniu, opiniowaniu i negocjowaniu różnych umów handlowych z dostawcami i klientami naszych klientów, działających zarówno w Polsce. jak i środowisku międzynarodowym. Naszą specjalizacją są kontrakty IT.

Przygotowujemy rozwiązania w zakresie przenoszenia i korzystania z praw własności intelektualnej: znaków towarowych, wzorów przemysłowych, wzorów użytkowych, patentów.

O B S Ł U G U J E M Y

Klientów, którzy oferują usługi chmurowe lub usługi IT dostarczane w chmurze. Pomagamy zidentyfikować rodzaj chmury, sklasyfikować informacje przetwarzane na środowisku chmurowym a także zweryfikować zakres regulacji koniecznych do implementacji w celu zapewnienia zgodności z wymogami regulacyjnymi.

Postępowania w zakresie przekształceń, połączeń i podziałów podmiotów z sektora usług IT i telekomunikacji.

O P R A C O W U J E M Y

umowy w przedmiocie rozwiązań IT, dotyczące każdego etapu tworzenia i korzystania z oprogramowania; począwszy od analiz, poprzez wdrożenie, po utrzymanie i rozwój oprogramowania, w każdym modelu wykonywania prac (agile, body leasing, etc) lub rozliczania ich realizacji (fixed price, time & material, etc).

opinie prawne i procedury wewnętrzne dla przedsiębiorców telekomunikacyjnych.

R E P R E Z E N T U J E M Y

Klientów w sprawach w toku negocjacji, w postępowaniach sądowych, administracyjnych, mediacyjnych oraz arbitrażowych, związanych z ochroną danych osobowych, własności intelektualnej oraz IT.

KONIECZNY WIERZBICKI
KANCELARIA RADCÓW PRAWNYCH

Kontakt

Jarosław Straś

Associate

jaroslaw.stras@kwkr.pl