Uwaga! Artykuł został opublikowany w dwóch wersjach językowych – podstawą do cytowań jest wersja angielska

Jacek Kudła
Polskie Towarzystwo Kryminalistyczne Oddział Warmińsko-Mazurski
ORCID: 0000-0002-4077-3900
jkjacekudla@gmail.com

Alfred Staszak
Uniwersytet Zielonogórski
ORCID: 0000-0003-1318-6513
alfredstaszak@wp.pl

Kontrola operacyjna w systemie informatycznym (postulaty *de lege ferenda*)

ABSTRAKT

W artykule przedstawiono propozycję zmian w przepisach dotyczących szeroko rozumianego podsłuchu. Dynamika rozwoju przestępczości posługującej się nowymi technologiami, a w szczególności przestępczości cybernetycznej, stawia przed wymiarem sprawiedliwości, organami ścigania i służbami specjalnymi coraz większe wyzwania, którym można sprostać, jedynie wprowadzając nowe rozwiązania prawne pozwalające na stosowanie najnowszych osiągnięć technicznych. Jednocześnie orzecznictwo sądowe nakłada na ustawodawcę obowiązek poszukiwania i tworzenia nowych rozwiązań prawnych, które potrafiłyby pogodzić interesy i prawa jednostki z dobrem ogólnospołecznym. Powstaje zatem pytanie, czy konieczna jest kolejna nowelizacja przepisów w tym zakresie czy też niezbędne jest całkowicie nowe spojrzenie na sposób unormowań prawnych dotyczących zagadnień związanych z podsłuchem procesowym i operacyjnym. W niniejszym artykule podjęto próbę przedstawienia tej problematyki, biorąc pod uwagę przede wszystkim zmiany przepisów inwigilacyjnych w związku z ciągłym i progresywnym rozwojem sieci 5G i planowaniem stopniowego wdrażania sieci 6G. Przedstawione konstruktywne uwagi *de lege ferenda* w ocenie autorów powinny stać się pomocne do ustanowienia nowego prawa dotyczącego kontroli operacyjnej. Prawa, które czyniłoby zadość normom gwarantowanym konstytucyjnie w zakresie praw obywatelskich i jednocześnie wyposażałoby państwo i jego organy ścigania oraz służby specjalne w skuteczne narzędzia walki z nowymi formami i przejawami przestępczości. Intencją autorów jest przedstawienie problematyki dotyczącej podsłuchu *sensu largo* na tle współczesnych technologii i nowych propozycji rozwiązań prawnych przy jednoczesnym poszanowaniu zasad polskiego procesu karnego oraz oczekiwań praktyki w skutecznym zwalczaniu najpoważniejszych przestępstw.

Słowa kluczowe: system informacyjny; przestępczość cybernetyczna; kontrola operacyjna; przepisy inwigilacyjne; prawa obywatelskie; współczesne technologie; podsłuch procesowy i operacyjny

WPROWADZENIE

Współczesny sposób pozyskiwania danych od providerów IAP[1] w celu zwalczania przestępczości[2] oraz związany z tym progresywny rozwój sieci 5G z perspektywami 6G wymaga od ustawodawcy stopniowego i racjonalnego dostosowywania przepisów prawa do

[1] Internet Access Provider (IAP) lub Internet Service Provider (ISP) to pojęcia oznaczające dostawcę usług internetowych. Do zakresu usług świadczonych przez dostawców należy: przygotowanie domeny, zapewnienie przestrzeni i pamięci dla poszczególnych serwerów, tworzenie bazy danych, adresów e-mail i wielu dodatkowych usług (jak np. sklepy internetowe, blogi). Dostawcy najczęściej dopasowują swoją ofertę do indywidualnych potrzeb klientów, oferując za odpowiednią opłatą kompletne pakiety domen.
[2] W. Filipkowski, *The use of data mining technology for fighting cyber crimes – selected forensic aspects*, [w:] *Current Problems of the Penal Law and Criminology*, eds. E. Guzik-Makaruk, E.W. Pływaczewski, vol. 7, Warszawa 2017, s. 386–395.

rozwoju technologicznego[3]. Obecnie, biorąc pod uwagę ścisłe kryteria prawne, nie można już mówić wyłącznie o systemie teleinformatycznym. Należy dzisiaj odnosić się do kontroli operacyjnej w systemie informatycznym[4] czy nawet – używając liczby mnogiej – w systemach informatycznych. W art. 2 pkt 14 ustawy o krajowym systemie cyberbezpieczeństwa „system informacyjny" został wstępnie zdefiniowany jako system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne wraz z przetwarzanymi w nim danymi w postaci elektronicznej[5]. Jednak proces przetwarzania danych w postaci elektronicznej sprawia, że do zakresu systemu informacyjnego należy zaliczyć: system teleinformatyczny, w tym dane z chmury[6] internetowej, dane informatyczne dotyczące przekazu telekomunikacyjnego oraz dane telekomunikacyjne. Obszar danych związanych z przekazem, na które składają się dane techniczne, metadane oraz to, co stanowi „istotę" przekazu, czyli treść informacji, należy kategorycznie od siebie oddzielić dla potrzeb rzetelnego stosowania przepisów prawa[7]. Właściwa charakterystyka systemu informacyjnego została określona w Europejskim kodeksie łączności elektronicznej, którego implementacja do prawa krajowego musiała nastąpić do dnia 21 grudnia 2020 r.[8] Zgodnie z wyżej wymienionym kodeksem za podstawową usługę w systemie informacyjnym należy uznać tzw. usługę łączności elektronicznej[9] (dalej odpowiednio: usługę łączności interpersonalnej).

W tym kontekście rodzi się pytanie, czy nie nadszedł już czas na gruntowne przemodelowanie systemu kontroli procesowej i operacyjnej, tak aby przepisy mogły być stosowane w rozwijających się systemach informatycznych, w których wymiana informacji następuje jednocześnie pomiędzy wieloma uczestnikami procesu komunikacji. Proces komunikacji bowiem to złożony proces wzajemnej wymiany informacji, a kontrola tego procesu nie może być oparta na fikcji, że podsłuch dotyczy tylko i wyłącznie jednej osoby w tym procesie uczestniczącej.

[3] Por. K. Ożóg-Wróbel, *Katalog metod prowadzenia czynności operacyjno-rozpoznawczych*, „Roczniki Nauk Prawnych" 2012, vol. 4, s. 122.
[4] Na system informacyjny i konieczność jego wyróżnienia wskazał już w 2015 r. B. Hołyst (*Podsłuchiwanie i inwigilacja użytkowników mediów elektronicznych w kontekście bezpieczeństwa informacyjnego*, „Prokuratura i Prawo" 2015, nr 3, s. 7).
[5] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2020, poz. 1369 z późn. zm.) wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 194/1, 2016).
[6] A. Krasuski, *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018, s. 75–80.
[7] Zob. J. Kudła, A. Staszak, *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, „Prokuratura i Prawo" 2017, nr 7–8, s. 31–57.
[8] Art. 124 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (wersja przekształcona), tekst mający znaczenie dla EOG (Dz.Urz. UE L 321/36, 2018).
[9] Por. E. Patkowski, *Big Data w służbie służb – sięganie po owoc zakazany (?)*, [w:] *Przestępczość teleinformatyczna 2017*, red. J. Kosiński, Szczytno 2018, s. 144.

Uwaga! Artykuł został opublikowany w dwóch wersjach językowych – podstawą do cytowań jest wersja angielska

OBECNY STAN PRAWNY I STOSOWANE METODY KONTROLI OPERACYJNEJ W SYSTEMACH INFORMATYCZNYCH

Usługi łączności interpersonalnej umożliwiają interpersonalną i interaktywną wymianę informacji i obejmują takie usługi, jak tradycyjne połączenia głosowe między dwiema osobami czy też wszystkie rodzaje poczty elektronicznej, usługi przekazywania wiadomości lub czatów grupowych[10]. Usługi łączności interpersonalnej obejmują tylko łączność między „skończoną", czyli określoną liczbą osób fizycznych, którą wskazuje osoba wysyłająca komunikat.

Łączność między osobami prawnymi powinna być objęta zakresem tej definicji w sytuacjach, gdy osoby fizyczne działają w imieniu tych osób prawnych lub stanowią przynajmniej jedną stronę procesu komunikacji. Łączność interaktywna oznacza, że usługa umożliwia odbiorcy informacji udzielenie odpowiedzi. Usługi, które nie spełniają tych wymogów, takie jak: linearne usługi medialne, wideo na żądanie, strony internetowe, sieci internetowe, serwisy społecznościowe, blogi lub wymiana informacji między urządzeniami, nie powinny być uznawane za usługi łączności interpersonalnej. W wyjątkowych okolicznościach usługi nie należy uznać za usługę łączności interpersonalnej, jeżeli narzędzie do komunikacji interpersonalnej i interaktywnej stanowi wyłącznie nieznaczny dodatek do innej usługi oraz z obiektywnych przyczyn technicznych nie może być użytkowane bez tej usługi głównej, a jego integracja z usługą nie służy obejściu zasad regulujących usługi łączności elektronicznej.

Będące elementami definicji terminy „nieznaczny" i „czysto pomocniczy" należy interpretować wąsko i z perspektywy użytkownika końcowego. Funkcję łączności interpersonalnej można uznać za nieznaczną w przypadku, gdy jej obiektywna przydatność dla użytkownika końcowego jest bardzo ograniczona i gdy w rzeczywistości jest ona wykorzystywana zaledwie przez użytkowników końcowych. Przykładem funkcji, która mogłaby zostać uznana za nieobjętą zakresem stosowania definicji usługi łączności interpersonalnej, może być zasadniczo kanał komunikacyjny w grach internetowych, w zależności od funkcji narzędzia do komunikacji wykorzystywanego w usłudze. Przy czym usługi łączności interpersonalnej, co jest bardzo istotne dla potrzeb stosowania kontroli operacyjnej, należy podzielić zarówno na te, które wykorzystują numery z krajowego lub międzynarodowego planu numeracji, jak i na te, które takich numerów nie wykorzystują. Istotna jest w tym przypadku rzeczywista kontrola danego dostawcy nad transmisją sygnału.

Stąd należy wyraźnie odróżnić usługę łączności interpersonalnej od usługi łączności elektronicznej. Usługa łączności elektronicznej jest pojęciem szerszym i oznacza usługę zazwyczaj świadczoną za wynagrodzeniem za pośrednictwem sieci łączności elektronicznej, która obejmuje (z wyjątkiem usług związanych z zapewnianiem albo wykonywaniem kontroli treści przekazywanych przy wykorzystaniu sieci lub usług łączności elektronicznej) następujące rodzaje usług:

[10] Por. K. Ożóg-Wróbel, *Przestępstwo kradzieży sygnału telewizyjnego w świetle ustawy o ochronie niektórych usług świadczonych drogą elektroniczną, opartych lub polegających na dostępie warunkowym. Sharing internetowy*, [w:] *Własność intelektualna w sieci*, red. D. Żak, Lublin 2014, s. 183–196.

- usługę dostępu do Internetu zdefiniowaną w art. 2 pkt 2 rozporządzenia (UE) 2015/2120[11],
- usługę łączności interpersonalnej (jak wyżej),
- usługi polegające całkowicie lub częściowo na przekazywaniu sygnałów, takie jak usługi transmisyjne, stosowane na potrzeby świadczenia usług łączności maszyna–maszyna oraz na potrzeby nadawania (tzw. internet rzeczy; Internet of Things, IoT[12]).

Wszystkie te obszary podlegają w przypadku zaistnienia i spełnienia warunków dopuszczalności odpowiednio kontroli operacyjnej stosowanej przez uprawnione służby. Ponadto nowego ustawowego kształtu wymagają przepisy dotyczące kontroli operacyjnej w związku z progresywnym rozwojem wielkich zbiorów danych (Big Data), np. w tak koniecznych obszarach rozdziału danych, dla potrzeb właściwego stosowania przepisów prawa (w tym kontroli operacyjnej czy też zabezpieczenia danych na podstawie art. 218a Kodeksu postępowania karnego[13]), jak „przenoszenie usługi połączeń głosowych do domeny transmisji danych". Jest to czynność legislacyjna, która prędzej lub później nastąpi ze względu na dostosowanie przepisów prawa dotyczących kontroli operacyjnej do współczesnego rozwoju technologicznego. Powinno to jednak nastąpić przy przestrzeganiu wszystkich zasad bezpieczeństwa informacji w cyberprzestrzeni.

Sceptykom należy przypomnieć, że zapewnienie bezpieczeństwa w sieci nie stanowi żadnej przeszkody we właściwym unormowaniu nowej kontroli operacyjnej w ustawach wszystkich służb. Wręcz odwrotnie, zwraca uwagę na obszary systemu, które powinny zostać poddane szczególnym zabezpieczeniom w celu zapobieżenia dostępu przez osoby nieuprawnione. Problem ten autorzy sygnalizowali wielokrotnie w mediach, przeznaczonych przede wszystkim dla środowisk prawniczych.

[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiające środki dotyczące dostępu do otwartego internetu i dotyczące opłat detalicznych za regulowane usługi łączności wewnątrzunijnej oraz zmieniające dyrektywę 2002/22/WE, a także rozporządzenie (UE) nr 531/2012 (Dz.Urz. UE L 310/1, 2015).

[12] Jacek Kudła był ekspertem Grupy Roboczej ds. IoT powołanej przez Ministra Cyfryzacji w 2018 r. Wynikiem pracy Grupy Roboczej ds. IoT był raport dla rządu oraz materiały edukacyjne pozwalające m.in. na przyszłą poprawną legislację tej problematyki w polskim systemie prawa. Na pierwszym posiedzeniu Grupy Roboczej zaproponował temat „Pozyskiwanie danych od IAP i ISP dla potrzeb rzetelnego stanowienia przepisów prawa, w tym rozwoju internetu rzeczy (IoT)" wraz z uzasadnieniem o treści: „W celu uniknięcia przyszłych barier prawnych ograniczających rozwój internetu rzeczy, a przede wszystkim w celu wprowadzenia standardów i regulacji dla tej części rynku – warto zwrócić uwagę na wyraźne rozróżnienie danych w chmurze obliczeniowej, dalej w systemach teleinformatycznych – dla potrzeb stanowienia i stosowania przepisów prawa. To od rzetelnego i prawnego rozróżnienia danych będzie następnie zależało dalsze postępowanie odpowiednich organów. Zatem po pierwsze, należy ustalić, z jakim rodzajem usługi mamy do czynienia, a następnie o jakie konkretnie dane chodzi. Ustawa o krajowym systemie cyberbezpieczeństwa pozwala na wyodrębnienie operatora usług kluczowych i odpowiednio dostawcy usług cyfrowych, co stanowi ułatwienie nie tylko w zakresie cyberbezpieczeństwa, ale także w aspektach technicznych pozyskiwania danych informatycznych. Ustawa ta też pozwala, przy właściwej interpretacji przepisów, w pewnym stopniu na zapobieganie tworzeniu nieuzasadnionych barier prawnych ograniczających rozwój IoT (np. w zakresie ochrony danych osobowych). Jednak w dalszym ciągu istnieje potrzeba określenia w aktach normatywnych lub przepisach wykonawczych – o jakie dane chodzi. W mojej ocenie podstawowe kryterium rozróżnienia danych powinien stanowić ich podział we wszystkich aktach normatywnych, w tym branży IoT – na dane techniczne i informacje. Z których można odpowiednio odczytać treść informacji, odtworzyć dźwięk i obraz, a następnie odróżnić je od tych, z których można uzyskać tylko dane techniczne – także w chmurze obliczeniowej, co we współczesnej teleinformatyce i procesie stanowienia prawa jest jak najbardziej możliwe".

[13] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz.U. 2021, poz. 534), dalej: k.p.k.

Do środków technicznych najnowszych technologii, które powinny zostać określone w nowych przepisach dotyczących kontroli operacyjnej, należy zaliczyć te wymienione w Europejskim kodeksie łączności elektronicznej. Są to m.in.: nowe formy zarządzania siecią[14] (sieci emulowane programowo lub sieci programowalne), technologia protokołu internetowego IP, usługa łączności głosowej (jej dwukierunkowość), szeroko rozumiany IoT[15], telefonia internetowa (Voice over Internet Protocol, VoIP), usługi przekazywania wiadomości i obsługa poczty elektronicznej przez Internet, usługa łączności interpersonalnej oraz usługi polegające wyłącznie lub głównie na przekazywaniu sygnałów (tj. widmo radiowe), usługi polegające całkowicie lub częściowo na przekazywaniu sygnałów (takie jak usługi transmisyjne stosowane na potrzeby świadczenia usług łączności maszyna–maszyna; IoT) oraz na potrzeby nadawania, a także usługa dostępu do Internetu, femtokomórki, pikokomórki, metrokomórki lub mikrokomórki itd.

Przepisy ustawy Prawo telekomunikacyjne[16] i inne obejmują wykorzystanie widma radiowego przez wszystkie sieci łączności elektronicznej, w tym nowy typ wykorzystania widma radiowego[17], na tzw. potrzeby własne przez nowe rodzaje sieci, składające się wyłącznie z autonomicznych systemów ruchomych urządzeń radiowych, które są połączone za pomocą łączy bezprzewodowych, bez zarządzania centralnego ani operatora sieci scentralizowanej i nie zawsze w ramach wykonywania określonej działalności gospodarczej[18]. W powstającym obecnie środowisku łączności bezprzewodowej 5G takie sieci powstają, poza budynkami przy drogach, na potrzeby transportu (samochodów podłączonych do sieci)[19], energetyki, badań naukowych, e-zdrowia, ochrony publicznej i organizacji systemu ratownictwa w przypadku katastrof, internetu rzeczy, łączności maszyna–maszyna. W związku z tym stosowanie przez państwa członkowskie na podstawie art. 7 dyrektywy 2014/53/UE[20] dodatkowych wymogów krajowych w odniesieniu do oddawania do użytku lub eksploatacji takich urządzeń radiowych w celu efektywnego i wydajnego wykorzystania widma radiowego oraz zapobiegania szkodliwym zakłóceniom powinno być zgodne z zasadami rynku wewnętrznego, zasadami bezpieczeństwa oraz odpowiednio z potrzebami służb.

---

[14] E. Guzik-Makaruk, K. Laskowska, *Poczucie bezpieczeństwa oraz zagrożenie cyberterroryzmem w świetle wyników badań empirycznych*, [w:] *Przestępczość w XXI wieku – zapobieganie i zwalczanie. Problemy technologiczno-informatyczne*, red. E.W. Pływaczewski, W. Filipkowski, Z. Rau, Warszawa 2015, s. 646.

[15] Zob. A. Krasuski, *op. cit.*, s. 221.

[16] Art. 111 ust. 3 pkt 2, art. 112 ust. 4 pkt 8 oraz art. 189 ust. 2 pkt 2 lit. e ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. 2019, poz. 2460).

[17] Załącznik nr 1, 2 i 3 do decyzji wykonawczej Komisji (UE) 2020/167 z dnia 5 lutego 2020 r. w sprawie norm zharmonizowanych dotyczących urządzeń radiowych, opracowanych na potrzeby dyrektywy Parlamentu Europejskiego i Rady 2014/53/UE (Dz.Urz. UE L 34/46, 2020).

[18] Por. m.in. określenie wymogów prawnych związanych z wykonywaniem działalności gospodarczej przez brokera w chmurze obliczeniowej w: A. Krasuski, *op. cit.*, s. 524 i n.

[19] Por. odpowiednio art. 3 pkt 1 rozporządzenia wykonawczego Komisji (UE) 2020/911 z dnia 30 czerwca 2020 r. określające cechy punktów dostępu bezprzewodowego o bliskim zasięgu zgodnie z art. 57 ust. 2 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 ustanawiającej Europejski kodeks łączności elektronicznej (Dz.Urz. UE L 208/48, 2020).

[20] Dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE (Dz.Urz. UE L 153/62, 2014).

W celu zapewnienia większej skoordynowanej dostępności widma radiowego, aby uzyskać bardzo szybkie sieci stacjonarne i bezprzewodowe, w kontekście 5G, Zespół ds. Polityki Spektrum Radiowego uznał zakresy częstotliwości 3,4–3,8 GHz i 24,25–27,5 GHz za priorytetowe pasma odpowiednie do realizacji celów planu działania w zakresie sieci 5G. Zakresy częstotliwości 40,5–43,5 GHz i 66–71 GHz wskazano do dalszej analizy pod kątem ich ewentualnego wykorzystania w przyszłości. Konieczne było zatem zapewnienie, by do dnia 31 grudnia 2020 r. całość lub część zakresów 3,4–3,8 GHz oraz 24,25–27,5 GHz była dostępna dla systemów naziemnych, umożliwiających dostarczanie usług bezprzewodowej szerokopasmowej łączności elektronicznej, zgodnie ze zharmonizowanymi warunkami ustanowionymi za pomocą technicznych środków wykonawczych przyjętych zgodnie z art. 4 decyzji nr 676/2002/WE[21] (w uzupełnieniu decyzji Parlamentu Europejskiego i Rady 2017/899[22]) z uwagi na to, że te zakresy mają szczególne właściwości pod względem zasięgu i przepustowości danych, dzięki którym można je odpowiednio połączyć, aby spełnić wymogi 5G. Państwa członkowskie mogłyby jednak być narażone na zakłócenia, które mogą pochodzić z państw trzecich, które zgodnie z Regulaminem Radiokomunikacyjnym ITU[23] przeznaczyły te zakresy na usługi inne niż międzynarodowa ruchoma łączność telekomunikacyjna. Może to mieć wpływ na obowiązek realizacji wspólnego terminu wdrożenia. Najprawdopodobniej przyszłe stosowanie pasma 26 GHz dla usług bezprzewodowych sieci naziemnych 5G będzie koncentrować się m.in. na obszarach miejskich i podmiejskich oraz obszarach zawierających hotspoty. Można przewidzieć realizację pewnej ich części wzdłuż głównych dróg i torów kolejowych na obszarach wiejskich. Daje to możliwość wykorzystywania pasma 26 GHz do innych usług niż sieci bezprzewodowe 5G poza tymi obszarami geograficznymi, np. do celów komunikacji biznesowej lub zastosowań w pomieszczeniach. Państwa członkowskie będą tym samym miały możliwość wyznaczenia i udostępniania tego pasma na zasadzie niewyłączności.

Dostępność sieci o bardzo dużej przepustowości będzie widoczna w takich obszarach zasięgu 5G i 6G, jak: szkoły, węzły transportowe, główni dostawcy usług publicznych i przedsiębiorstwa zaawansowane cyfrowo. Zapewni to dostępność niezakłóconego zasięgu 5G na obszarach miejskich i na głównych liniach transportu naziemnego, a także dostępność sieci łączności elektronicznej zdolnych do zapewnienia prędkości co najmniej 100 Mb/s, z możliwością zwiększenia do prędkości gigabitowych, dla wszystkich gospodarstw domowych. Rozwój nowych technologii następuje tak gwałtownie, że konieczne staje się dostosowanie do niego przepisów dotyczących m.in. kontroli operacyjnej.

Należy podkreślić, że w ramach kolejnego programu „Horyzont Europa" Komisja podjęła działania w sprawie sieci 6G (inteligentne sieci i usługi). Jak wynika z komunikatu Komisji do Parlamentu Europejskiego i Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 29 stycznia 2020 r. (zob. również załącznik doty-

[21] Decyzja nr 676/2002/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie ram regulacyjnych dotyczących polityki spektrum radiowego we Wspólnocie Europejskiej (decyzja o spektrum radiowym) (Dz.Urz. UE L 108/1, 2002).

[22] Decyzja Parlamentu Europejskiego i Rady (UE) 2017/899 z dnia 17 maja 2017 r. w sprawie wykorzystywania zakresu częstotliwości 470–790 MHz w Unii (Dz.Urz. UE L 138/131, 2017).

[23] Regulamin Radiokomunikacyjny. Artykuły, 2016, www.il-pib.pl/images/stories/rozne/Regulamin_Radiokomunikacyjny/pdf/Regulamin_Radiokomunikacyjny_2016-2019-Tom1.pdf [dostęp: 10.02.2021].

czący kategorii ryzyka)[24], Komisja zamierza ukończyć wdrażanie sieci 5G i rozpocząć przygotowania w zakresie sieci 6G, tj. technologii mobilnej nowej generacji. Wszystkie argumenty, o których wyżej była mowa, niejako wymagają nowego unormowania przepisów[25], nie tylko dla potrzeb gwarancyjnych, lecz także dla potrzeb nowych możliwości działalności operacyjnej służb.

KONTROLA OPERACYJNA W SYSTEMIE INFORMACYJNYM – KONSTRUKTYWNE UWAGI *DE LEGE FERENDA* JAKO GŁOS W DYSKUSJI O PRAWNYCH GRANICACH KONTROLI OPERACYJNEJ

Pragniemy rozpocząć nie tyle od kontroli operacyjnej, ile od kodeksowej kontroli i utrwalania rozmów, a przede wszystkim od pytania: Czy kontrola i utrwalanie rozmów, o których jest mowa w art. 237 k.p.k., są przydatne w praktyce? Praktycy (głównie prokuratorzy) twierdzą, że są to rzadko stosowane tzw. martwe normy prawne[26].

Co do zasady należałoby się zgodzić z tak postawioną tezą, biorąc pod uwagę statystyki oraz wyniki podsłuchu procesowego w postępowaniach przygotowawczych. Co zatem może stanowić przyczynę takiego stanu faktycznego? Należy dodać, że z wykładni prawa wynika, iż w momencie gdy jest prowadzone postępowanie przygotowawcze, powinien być stosowany co do zasady podsłuch procesowy[27]. Zapewnia on bowiem gwarancje, których z kolei nie można się doszukać w podsłuchu operacyjnym. Podstawowymi przesłankami, które w praktyce przemawiają za korzystaniem z kontroli operacyjnej, a nie z procesowych kontroli i utrwalania rozmów, są właśnie kwestie określonych gwarancji. Praktyka wymusza więc, aby odnieść się do tego kontrowersyjnego zagadnienia prawnego.

Podsłuch procesowy może zostać rozpoczęty po wszczęciu postępowania i zarządza go sąd na wniosek prokuratora. Jest on niedopuszczalny w ramach czynności operacyjno-rozpoznawczych. To problem, który występuje podczas podsłuchu procesowego, determinujący jego rzadkie stosowanie. Wyłączenie tzw. trybu operacyjnego w jego wnioskowaniu w konsekwencji w praktyce wywołuje niezliczoną ilość przeszkód związanych m.in. z obiegiem dokumentacji z podsłuchu procesowego, do której pracownicy operacyjni mają utrudniony dostęp lub takiego dostępu nie mają. Wiąże się to dalej z brakiem analizy informacji z podsłuchu, którą co do zasady wykonuje prokurator lub wyznaczony funkcjonariusz prowadzący postępowanie przygotowawcze. Powoduje to, że podsłuch ten jest tak wysoce sformalizowany procesowo, że w konsekwencji staje się nie przydatny (nie wchodząc w dalsze szczegóły).

---

[24] Komunikat Komisji do Parlamentu Europejskiego i Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Bezpieczne wprowadzenie sieci 5G w UE – wdrażanie unijnego zestawu narzędzi, Bruksela, 29.01.2020, COM(2020) 50 final.

[25] Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Nowa strategia przemysłowa dla Europy – Bruksela, 10.03.2020, COM(2020) 102 final.

[26] A. Staszak, *Ewolucja przepisów dotyczących podsłuchu procesowego – niewielkie zmiany o istotnym znaczeniu,* [w:] *Zmiany w prawie karnym materialnym i procesowym w latach 2013–2017. Zagadnienia wybrane,* red. H. Paluszkiewicz, „Acta Iuridica Lebusana" 2017, nr 7, s. 113.

[27] Por. P. Hofmański, S. Zabłocki, *Elementy metodyki pracy sędziego w sprawach karnych*, Warszawa 2011, s. 453–456.

Wytłumaczeniem tej sytuacji jest jednak to, że zgodnie z art. 239 § 2 k.p.k. ogłoszenie postanowienia o kontroli i utrwalaniu rozmów telefonicznych osobie w postępowaniu przygotowawczym może być odroczone nie później niż do czasu zakończenia tego postępowania. Jeżeli chodzi o gwarancje procesowe, jest to rzetelne rozwiązanie, ale jeżeli chodzi o praktyczne przesłanki efektywności stosowania podsłuchu, to sprowadza się do „powiadomienia" osoby, wobec której podsłuch procesowy był stosowany dosyć szybko, bo już w momencie zakończenia postępowania. Jeden z autorów, zarówno stosujący w praktyce podsłuchy operacyjne, jak i przyglądający się podsłuchom procesowym, spotkał się w przypadku tych ostatnich z sytuacją, w której zarządzono podsłuch procesowy i zaledwie po trzech tygodniach osobie, wobec której go stosowano, ogłoszono postanowienie o kontroli i utrwalaniu rozmów (gdyż zakończono postępowanie przygotowawcze).

Jest tak także dzisiaj, a wynika to nie tyle z niekompetencji organu procesowego, ile z restrykcyjnego stosowania przez ten organ norm prawnych kodeksu postępowania karnego i innych przepisów gwarancyjnych, w tym przepisów Unii Europejskiej. Niestety, dodatkową przeszkodą jest konieczność „wymuszonego" znajdowania prawdziwych przesłanek faktycznych przez funkcjonariuszy pionów operacyjno-rozpoznawczych służb, stanowiących podstawy do stosowania kontroli operacyjnej, gdy jest już prowadzone postępowanie przygotowawcze. Należy o tym powiedzieć *expressis verbis*, ponieważ obecna konstrukcja przepisów często zmusza ich do poszukiwania wciąż nowych ustaleń faktycznych, pozwalających na zarządzenie kontroli operacyjnej w przypadku, gdy jest już prowadzone postępowanie przygotowawcze. Podczas kontroli operacyjnej funkcjonariusze mają również większe możliwości wykrywcze (tzw. kuchnia operacyjna), których w przypadku podsłuchu procesowego brakuje (tzw. zupełny brak pracy operacyjnej). To dalej wpływa na jego efektywność, dlatego należy zastanowić się nad całkowitą zmianą przepisów w tym zakresie, żeby zapobiec funkcjonowaniu w polskim systemie prawa nieefektywnej i niepotrzebnej kontroli i utrwalania rozmów. Jak wielokrotnie podkreślał Z. Brodzisz, „uzasadniona w tej sytuacji jest zatem inkorporacja do KPK tzw. dowodów niekonwencjonalnych, pozyskiwanych obecnie w celu zwalczania przestępstw w ramach czynności operacyjno-rozpoznawczych, na podstawie przepisów policyjnych i innych"[28].

Trzeba jeszcze dodać, że postanowienie o kontroli i utrwalaniu rozmów powinno być doręczone osobie, której podsłuch dotyczy[29], co wywołuje kolejne skutki procesowe. *A contrario* w przypadku kontroli operacyjnej, zgodnie z art. 19 ust. 16 ustawy z dnia 6 kwietnia 1990 r. o Policji[30], osobie, wobec której kontrola operacyjna była stosowana, nie udostępnia się materiałów zgromadzonych podczas trwania tej kontroli[31]. Przepis nie narusza uprawnień wynikających z art. 321 k.p.k. Nie oznacza to jednak, że osoba, wobec której stosowana była kontrola operacyjna, nie może zapoznać się z materiałami z tej kontroli. Następuje to odpowiednio na danym etapie postępowania karnego. Mówiąc w pewnym uproszczeniu, nie należy konstruować norm prawnych przepisów w taki sposób, aby doprowadzać do przypadków niemalże niezwłocznego „powiadamiania" osoby, wobec której stosowano podsłuchy. Takie

[28] Zob. J. Skorupka, *Kodeks postępowania karnego*. *Komentarz*, Warszawa 2020, s. 858.
[29] *Ibidem*, s. 587.
[30] T.j. Dz.U. 2020, poz. 360, dalej: u.P.
[31] *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne*, red. M. Kusak, P. Wiliński, Warszawa 2020, s. 116.

czynności dochodzeniowo-śledcze i odpowiednio (*de lege ferenda*) operacyjno-rozpoznawcze byłyby nieefektywne i w konsekwencji nieprzydatne. Stąd konieczne jest dostosowanie przepisów do nowych wymogów kontroli operacyjnej w systemie informacyjnym z jednoczesnym i proporcjonalnym zachowaniem norm gwarancyjnych. Normy te nie powinny wpływać negatywnie na efektywność czynności operacyjno-rozpoznawczych i jednocześnie powinny stanowić odpowiednio gwarancje procesowe i dalej konstytucyjne. Zachowanie proporcji pomiędzy wartościami, o których mowa, jest w przypadku podsłuchu operacyjnego szczególnie pożądane[32]. Jak stwierdził A. Staszak, „dopóki prokurator i sąd nie będą w wystarczającym stopniu odpowiedzialni za wynik postępowania (nie będą odpowiedzialni za ustalenie sprawcy przestępstwa, jego osądzenie i skazanie), dopóty nie będą miały one praktycznego zastosowania”[33]. Także dzisiaj aktualne wydają się być uwagi krytyczne dotyczące art. 239 k.p.k. przedstawiane w doktrynie[34]. To one stanowią odpowiedź na pytanie, dlaczego kontrola i utrwalanie rozmów są rzadko lub nie są wcale stosowane w praktyce[35].

Kolejnym problemem we współczesnej praktyce stosowania kontroli operacyjnej jest kwestia zapoznawania się z materiałami uzasadniającymi zastosowanie podsłuchu przez miejscowo właściwego prokuratora okręgowego w przypadku, gdy o podsłuch operacyjny wnioskuje komendant wojewódzki Policji, ale komórką policji wnioskującą jest np. komisariat Policji (czyli jednostka organizacyjna Policji najniższego szczebla). Pojawia się w związku z tym kilka pytań związanych z właściwością i możliwością zapoznania się przez prokuratora okręgowego z materiałami pozwalającymi podjąć decyzję co do wstępnej ich akceptacji w postaci zgody i dalej przekazania do sądu bądź niewyrażenia zgody na dalszy bieg czynności w sprawie stosowania kontroli operacyjnej.

Po pierwsze, należy podkreślić, że ustawa o policji nie ogranicza wnioskowania o podsłuch operacyjny tylko i wyłącznie do zakresu właściwości komendy wojewódzkiej Policji (KWP). To, że z wnioskiem występuje komendant wojewódzki Policji, nie oznacza, że pochodzi on np. z wydziału kryminalnego KWP. Może on pochodzić z komendy powiatowej Policji czy nawet w uzasadnionych przypadkach z komisariatu, choć w ocenie autorów niniejszego opracowania niewielkie komórki operacyjne w komisariatach nie są właściwie przygotowane do tzw. obsługi stosowania kontroli operacyjnej. W przypadku konieczności jej stosowania przez małe jednostki, tj. o niewielkiej obsadzie etatowej, sprawę operacyjną powinna przejąć jednostka nadrzędna. Zatem jeżeli wniosek o kontrolę operacyjną został sporządzony przez funkcjonariusza z komórki operacyjno-rozpoznawczej komisariatu Policji, to proces ten powinien być dalej monitorowany przez wyznaczoną osobę z jednostki nadrzędnej, aż do momentu rzetelnego zapoznania się przez prokuratora okręgowego z materiałami uzasadniającymi kontrolę operacyjną bądź sprawa taka powinna zostać przejęta np. przez komendę wojewódzką Policji lub odpowiednio inne wyższego stopnia jednostki, np. Centralne Biuro Śledcze Policji (CBŚP) lub Biuro Spraw Wewnętrznych Policji (BSWP). W naszej ocenie problem ten dzisiaj powinien zostać rozwiązany poprzez odpowiednie wykorzystanie koordyna-

[32] A. Grzelak, *Data Retention Saga Continues: Decision of the Polish Constitutional Tribunal of 30 July 2014 in Case K 23/11*, “European Public Law” 2016, vol. 22(3), s. 475–488.
[33] A. Staszak, *Ewolucja przepisów…*, s. 125.
[34] K. Ponikwia, *Uwagi krytyczne do art. 239 k.p.k.*, „Prokuratura i Prawo” 2002, nr 10, s. 142.
[35] Por. P. Kosmaty, *Podsłuch procesowy – zamierająca instytucja walki z przestępczością*, „Prokurator” 2009, nr 2, s. 9–21.

torów kontroli operacyjnej, o których mowa w przepisach instrukcyjnych[36]. Niestety, przepisy instrukcyjne również należy zmienić, a nawet wprowadzić pewne unormowania do ustaw służb. Otóż obecnie komendanci wojewódzcy Policji wyznaczają wojewódzkich koordynatorów kontroli operacyjnej, do zadań których należy:

- monitorowanie problemów utrudniających sprawną i skuteczną kontrolę operacyjną oraz udzielanie jednostkom organizacyjnym Policji na obszarze województwa pomocy doradczej w zakresie wykonywania czynności związanych z kontrolą operacyjną,
- zapewnianie należytej znajomości przepisów regulujących wykonywanie kontroli operacyjnej i umiejętności ich praktycznego stosowania przez prowadzących pracę operacyjną policjantów jednostek organizacyjnych Policji z obszaru województwa.

W naszej ocenie pozycja koordynatora ds. kontroli operacyjnej powinna zostać unormowana w przepisach ustawowych. Jego obowiązki nie mogą się sprowadzać tylko do tych określonych w § 16 Decyzji nr 290[37]. Wśród zadań wymienionych w przepisie instrukcyjnym brakuje zadania najważniejszego, mianowicie nakładającego obowiązek na koordynatora kontroli operacyjnej obowiązkowego uczestnictwa w przedstawieniu i odpowiednio omówieniu podstawowych materiałów uzasadniających kontrolę operacyjną.

Nowe przepisy powinny stworzyć możliwości, aby prokurator – oprócz wniosku o kontrolę operacyjną wraz z uzasadnieniem – mógł również uzyskać co najmniej najważniejsze (podstawowe) materiały ze sprawy operacyjnej uzasadniające późniejsze zarządzenie kontroli operacyjnej. Naturalnie w żadnym razie nie chodzi tutaj o ujawnienie tzw. kuchni operacyjnej[38]. W rozmowie z prokuratorem oraz podczas przedstawiania wyłączonych materiałów ze sprawy operacyjnej nie należy ujawniać zasad stosowania techniki operacyjnej czy techniki specjalnej, w tym szeroko rozumianego maskowania. Mówiąc o materiałach stanowiących podstawę wnioskowania o podsłuch, policjant powinien przedstawić np. rzetelnie sporządzoną „analityczną" notatkę służbową czy też wyniki niektórych metod pracy operacyjnej bez ujawniania szczegółów tych metod. Ponadto powinien wskazać przesłanki spełnienia przez Policję zasady subsydiarności oraz inne materiały, które wypełniałyby oczekiwania ustawodawcy, stanowiące warunki dopuszczalności stosowania kontroli operacyjnej, które zostały wymienione w ustawie. To właśnie wymienione argumenty przekonają prokuratora, a następnie sąd o zasadności zastosowania kontroli operacyjnej. Marzeniem autorów niniejszej publikacji jest, aby funkcjonariusze wnioskujący o kontrolę operacyjną potrafili wiedzę zdobytą podczas czynności operacyjno-rozpoznawczych uargumentować w języku ustawowym, zrozumiałym dla prokuratora i sędziego. Taką rolę miałby *de lege ferenda* odgrywać wymieniony w ustawie koordynator do spraw kontroli operacyjnej. Dodajmy, że nie tylko wojewódzki koordynator, lecz także koordynator ds. kontroli operacyjnej w CBŚP i BSWP.

W tym miejscu powstaje pytanie o kwestie organizacyjne. Należy je pozostawić wewnętrznemu uregulowaniu przez poszczególne służby, gdyż nie ma potrzeby tworzenia sekcji koordynatorów ds. kontroli operacyjnej w jednostkach organizacyjnych np. Policji. Chodzi tylko o wyznaczenie osoby, która by się zajmowała, w obszarze województwa, pomocą

[36] Decyzja nr 290 Komendanta Głównego Policji z dnia 13 sierpnia 2014 r. w sprawie określenia podziału zadań służbowych policjantów wykonujących czynności w zakresie sporządzania i przekazywania dokumentacji kontroli operacyjnej (Dz.Urz. KGP, poz. 53).
[37] *Ibidem*.
[38] Zob. J. Kudła, *Glosa do wyroku SA w Warszawie z 29.01.2020 r., sygn. akt II AKa 219/19*, LEX/el. 2020.

w przygotowaniu materiałów uzasadniających stosowanie kontroli operacyjnej dla sądu lub prokuratora, a następnie potrafiła o nich merytorycznie porozmawiać z prokuratorem i odpowiednio przedstawić je sądowi, czyli przekazać organom przesłanki ustawowe pozwalające na podjęcie pozytywnej lub negatywnej decyzji. Koordynator ds. kontroli operacyjnej powinien być neutralny. Jeżeli podczas przedstawienia materiałów i rozmowy (merytorycznej) np. z prokuratorem doszłoby do nowych ustaleń i ocen mających wpływ na stan faktyczny, koordynator powinien zrozumieć również negatywną decyzję organu. Dalej powinien umieć ją przekazać i merytorycznie uzasadnić komendantowi wojewódzkiemu Policji. Pełniłby on zatem rolę osoby niezależnej, neutralnej. Należy się w pełni zgodzić z Sądem Apelacyjnym w Białymstoku, że „decyzja sądu w przedmiocie wyrażenia zgody na przeprowadzenie kontroli operacyjnej może mieć charakter blankietowy, odwołujący się do treści zawartych we wniosku o przeprowadzenie takiej kontroli. Dopuszczalność takiej formy postanowienia sądowego wynika z regulacji szczególnych, przez co nie narusza ona wymogów wynikających z przepisu art. 94 § 1 k.p.k.”[39]. Materiały, które uzasadniają jej przeprowadzenie, nie mogą już jednak mieć charakteru blankietowego, co wynika *expressis verbis* z wykładni prawa.

Na tle powyższego stanowiska zajętego przez Sąd Apelacyjny w Białymstoku pojawia się kolejne zagadnienie prawne, dotyczące stosowania nowej kontroli operacyjnej w systemie informacyjnym. W tym przypadku nie dotyczy ono bezpośrednio służb, lecz organu, który ostatecznie zarządza kontrolę operacyjną w trybie art. 19 ust. 1 u.P. oraz odpowiednio wyraża na nią zgodę w trybie art. 19 ust. 3 u.P., czyli sądu okręgowego.

Jak wynika z obecnego stanu prawnego, sąd okręgowy po rozpoznaniu wniosku Policji (odpowiednio pozostałych służb) może wydać dwa rodzaje decyzji. Po pierwsze, może w formie postanowienia wyrazić zgodę na zastosowanie kontroli operacyjnej. W decyzji o wyrażeniu zgody istnieje obowiązek podania okresu, na jaki może zostać zastosowana kontrola operacyjna oraz godziny, od której może być rozpoczęta. Po drugie, sąd może nie uwzględnić wniosku Policji, tj. Komendanta Głównego Policji, Komendanta CBŚP, Komendanta BSWP albo komendanta wojewódzkiego Policji (i odpowiednich podmiotów w przypadku pozostałych służb). Należy zaznaczyć, że w przypadku zarządzenia lub wyrażenia przez sąd okręgowy zgody na zastosowanie kontroli operacyjnej, nie musi on sporządzać uzasadnienia wydanego postanowienia (art. 98 § 3 k.p.k. stosuje się odpowiednio). Natomiast obligatoryjnie jest do tego zobowiązany w przypadku niezarządzenia lub niewyrażenia zgody na podsłuch operacyjny. Jeśli sąd nie zarządza lub nie wyraża zgody na przedmiotową czynność, wtedy jest związany terminem siedmiu dni, o którym mowa w art. 98 § 2 k.p.k. Mianowicie w sprawie zawiłej lub z innych ważnych przyczyn można odroczyć sporządzenie uzasadnienia postanowienia na czas do siedmiu dni. Termin ten ma charakter instrukcyjny, zatem jego przekroczenie nie wywołuje skutków procesowych. Tak jest w przypadku, gdy orzeczenie podlega zaskarżeniu (art. 98 § 3 zdanie ostatnie k.p.k.)[40].

Wydaje się, w dalszym ciągu analizując normę prawną z art. 98 § 3 k.p.k. i przy uwzględnieniu gwarancyjności całej procedury, że niezwykle istotna pozostaje rola prokura-

[39] Wyrok SA w Białymstoku z dnia 16 stycznia 2014 r., II AKa 260/13, LEX nr 1422328.
[40] Na podstawie art. 19 ust. 20 u.P. na postanowienia sądu, o których mowa w art. 19 ust. 1, 3, 8 i 9 u.P., przysługuje zażalenie organowi Policji, który złożył wniosek o wydanie tego postanowienia. Na postanowienie sądu, o którym mowa w art. 19 ust. 3 u.P., zażalenie przysługuje właściwemu prokuratorowi, o którym mowa w art. 19 ust. 1 u.P. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

tora biorącego udział w niejawnym posiedzeniu, który zachowując zasadę kontradyktoryjności, pozostaje niezależny i w pełni obiektywny, również biorąc pod uwagę kryteria wcześniej wyrażonej przez siebie zgody.

De lege ferenda autorzy niniejszego opracowania proponują, aby sąd okręgowy sporządzał uzasadnienie postanowienia, o którym mowa, bez względu na to, czy zarządził lub wyraził zgodę na zastosowanie kontroli operacyjnej czy też tych czynności odmówił. Uzasadnienie przez sąd okręgowy wszystkich postanowień wydawanych w sprawie kontroli operacyjnej oprócz spełnienia podstawowych gwarancji procesowych dodatkowo pozwoliłoby na uzasadnienie ostatecznej i rzetelnej oceny merytorycznej otrzymanych materiałów. Ponadto ułatwiłoby służbom analizę prawną wszystkich wydanych orzeczeń. To w konsekwencji wpłynęłoby na jakość czynności policyjnych w prowadzonych sprawach operacyjnych.

Podobnie *de lege ferenda* należałoby postępować w przypadku zastosowania art. 168b k.p.k. Obecnie decyzję w przedmiocie wykorzystania tego dowodu, na określonym etapie postępowania karnego, ustawodawca zastrzegł dla prokuratora z tego powodu, że wyłącznie prokurator na etapie formułowania oskarżenia decyduje o tym, jakie dowody na jego poparcie przedstawi sądowi. „Zgoda następcza" prokuratora na podstawie art. 168b k.p.k. nie zamyka dalszej oceny sądowej przedmiotowych dowodów, chyba że prokurator nie wyrazi „quasi-zgody następczej"[41]. Jak podkreślono, w obecnym stanie prawnym decyzję procesową o wyrażeniu „quasi-zgody następczej", o której mowa w art. 168b k.p.k., lub decyzję o niewyrażeniu takiej zgody podejmuje prokurator[42]. Decyzja ta nie jest określona w ustawie jako forma decyzji zastrzeżonej tylko dla sądu. Jest to decyzja procesowa, która na podstawie kodeksu postępowania karnego powinna przybrać formę postanowienia.

Prokurator co do zasady[43] wydaje postanowienie na podstawie art. 93 § 3 k.p.k. Prawo do złożenia zażalenia na decyzję prokuratora dotyczącą zgody następczej z art. 168b k.p.k. nie zostało w przypadku kontroli operacyjnej wyraźnie przewidziane w ustawie. W związku z tym art. 465 § 2 k.p.k. stanowi jedynie przepis pozwalający na określenie właściwości do rozpoznania zażalenia, gdyby taka możliwość *de lege ferenda* została uwzględniona w ustawie. Odrębnie, w przypadku podsłuchu procesowego, tj. kontroli i utrwalania rozmów, zaskarżenie decyzji prokuratora do sądu jest możliwe na podstawie art. 240 k.p.k. *De lege ferenda* możliwość zaskarżenia decyzji prokuratora w zakresie tzw. zgody następczej, o której mowa w art. 168b k.p.k., zapewniłaby zatem pełną gwarancyjność przepisów oraz pozwoliłaby Policji na złożenie zażalenia również w tym zakresie.

Kolejne zagadnienie prawne ściśle dotyczące kontroli operacyjnej stosowanej w systemie informacyjnym to tzw. katalog przestępstw, o którym mowa w art. 19 ust. 1 u.P. Od lat ustawodawca oraz doktryna uzasadniają potrzeby jego zmian, które jednak polegają na ciągłym rozszerzaniu o nowe przestępstwa. Do najtrudniejszych, w ocenie autorów niniejszego opracowania, należy odpowiedź na pytanie, czy dokonać całkowitego zniesienia obecnego katalogu na rzecz katalogu bardziej ogólnego, tj. nieodsyłającego do poszczególnych prze-

[41] S. Hoc, J. Kudła, *Zgoda następcza z art. 168b Kodeksu postępowania karnego. Komentarz praktyczny*, LEX/el. 2016.
[42] D. Szumiło-Kulczycka, *Dalsze wykorzystywanie materiałów z kontroli operacyjnej (uwagi na tle art. 168b k.p.k.)*, „Państwo i Prawo" 2018, z. 10, s. 107–120.
[43] Na podstawie art. 93 § 3 k.p.k. prokurator może wydać zarządzenie co do materiałów otrzymanych od policji wymagających tzw. zgody następczej.

stępstw *expressis verbis* wskazanych w enumeratywnym systemie. Uzależnienie stosowania podsłuchu procesowego np. mogłoby być wówczas związane z umyślnym przestępstwem zagrożonym karą pozbawienia wolności od jednego roku (chodzi naturalnie o ustawowy wymiar kary), przestępstwem na tle seksualnym oraz przestępstwem, którego skutkiem jest śmierć człowieka (w tym przypadku także przestępstwem nieumyślnym).

W związku z konfliktem wielu stanowisk dotyczących tego zagadnienia prawnego należy przedstawić argumenty przemawiające zarówno za zmianą katalogu, jak i te, które pozwalają na zachowanie jego obecnego kształtu normatywnego. Na pewno za określonymi zmianami ustawowymi przemawia ciągła zmiana katalogu. Zatem jak wiele razy należy go zmieniać, uwzględniając gwarancyjność prawa obowiązującą w tym przedmiocie. Jedną z propozycji jest taka zmiana katalogu, która polegałaby na wskazaniu, że dopuszczalne jest stosowanie kontroli operacyjnej jedynie w przypadku umyślnych przestępstw zagrożonych karą pozbawienia wolności, których dolna granica ustawowego zagrożenia jest nie niższa niż rok pozbawienia wolności, natomiast w przypadku przestępstw skarbowych narażających państwo na uszczuplenie należności publicznoskarbowych w określonej wysokości – na wskazaniu jej wysokości albo kwotowo, albo poprzez odniesienie jej do wielokrotności wynagrodzenia[44]. Progi te muszą być dobrane adekwatnie, aby nie pozostały poza nimi przestępstwa o dużym ciężarze społecznej szkodliwości, tak jak jest obecnie z przestępstwem zgwałcenia z art. 197 § 1 Kodeksu karnego (k.k.). Przy tej okazji warto byłoby się zastanowić nad granicami ustawowego zagrożenia niektórych przestępstw o szczególnie dużym stopniu społecznej szkodliwości (np. przestępstwa wymuszonej aborcji z art. 152 k.k., zanieczyszczania środowiska w znacznych rozmiarach z art. 182 k.k., nieodpowiedniego postępowania z odpadami z art. 183 k.k. itd.), a także coraz bardziej nagminnych przestępstw skarbowych. Podobne rozwiązanie wskazał ustawodawca odpowiednio w art. 607b k.p.k., tj. w przypadku Europejskiego Nakazu Aresztowania. Tak określone ramy katalogu przestępstw mogłyby być uzupełnione o przestępstwa na tle seksualnym oraz o te, których skutkiem jest śmierć człowieka, niezależnie od zamiaru sprawcy i ostatecznej kwalifikacji przyjętego czynu[45].

Za pozostawieniem obecnego kształtu normatywnego tzw. katalogu przestępstw przemawia dotychczasowa wykładnia prawa. Chodzi o zasadę życzliwej interpretacji wszystkich praw i wolności obywatelskich. Prawa te mogą być interpretowane rozszerzająco, a ich wszelkie ograniczenia – ściśle lub nawet zawężająco. Właśnie z takim przypadkiem możemy mieć do czynienia w katalogu przestępstw z art. 19 ust. 1 u.P. Wszystkie ograniczenia, z którymi mamy do czynienia przede wszystkim podczas stosowania norm prawnych dotyczących kontroli operacyjnej, „muszą być traktowane jako wyjątek i w związku z tym interpretowane ściśle lub zawężająco”[46].

Unormowanie katalogu przestępstw przez pryzmat zagrożenia karą wywołuje pewne wątpliwości. Dotyczą one szczególnie jeszcze większych niż obecnie możliwości jego rozszerzenia w sposób „pokrętny”, tzn. poprzez ciągłe zmiany Kodeksu karnego, a także „manipu-

[44] A. Staszak, *Refleksje na temat procesowego wykorzystania materiałów zgromadzonych podczas stosowania kontroli operacyjnej (w świetle uchwały SN z 28 czerwca 2018r., I KZP 4/18)*, [w:] *Zmiany w prawie karnym materialnym i procesowym w latach 2013–2017. Zagadnienia wybrane*, red. H. Paluszkiewicz, „Acta Iuridica Lebusana” 2019, nr 11, s. 117.
[45] *Ibidem*, s. 118.
[46] L. Morawski, *Zasady wykładni prawa*, Toruń 2010, s. 199.

lowania" przy dolnej granicy ustawowego zagrożenia karą pozbawienia wolności za przestępstwa umyślne. Argumentem, który przemawia za uzasadnieniem tej tezy, jest wielość zmian ustawy Kodeks karny – począwszy od jej wielkiej reformy i ogłoszenia ustawy z dniem 2 sierpnia 1997 r. aż do dnia dzisiejszego[47]. Katalog ten powinien być jasny i czytelny nie tylko dla prawników, lecz także dla wszystkich, a zwłaszcza dla policjantów (odpowiednio funkcjonariuszy pozostałych służb) stosujących kontrolę operacyjną. Należy pamiętać, że zmieniając katalog w art. 19 ust. 1 u.P., *ex officio* zostają zmienione katalogi przestępstw, o których mowa w art. 19a i 19b u.P. Stąd należy wrócić do przypadku, w którym niejasność interpretacji przepisów, nawet enumeratywnie wymienionych, w obecnym katalogu przestępstw doprowadziła funkcjonariuszy do niezamierzonych błędów[48].

Do bardzo oczekiwanych zmian należy zaliczyć konieczność unormowania przepisów dotyczących kontroli operacyjnej w ten sposób, aby nie dotyczyły, tak jak jest obecnie, jednej osoby i prowadzonej przez nią rozmowy. Zmiana ta jest związana z rozwojem technologicznym i dla poprawnego, rzetelnego stosowania przepisów prawa jest potrzebna. Dotyczy ona bezpośrednio: 1) samego procesu komunikacji; 2) możliwości prowadzenia rozmów, a także utrwalania obrazu i dźwięku, jakie współcześnie istnieją w systemie informacyjnym, w tym w chmurze, czyli w wielkich zbiorach danych (Big Data). Interlokutor, czyli osoba prowadząca z kimś rozmowę, wykonuje zawsze ten proces z innym podmiotem. Mamy tu do czynienia, zgodnie z procesem komunikacji, z wymianą informacji pomiędzy co najmniej dwiema osobami. Obecne unormowania prawne są sprzeczne z podstawowym procesem komunikacji odbywającym się w relacji: nadawca – przekaz – odbiorca[49]. Z kolei odnosząc się do wielkich zbiorów danych, należy zaznaczyć, że współczesne środowisko systemu informacyjnego daje tyle możliwości komunikacji pomiędzy wieloma osobami, w tym osobami przypadkowymi, że nie sposób je wszystkie wymienić[50]. Dostęp służb do tych danych jest ograniczony[51], nie zmienia to jednak faktu prowadzenia rozmów pomiędzy co najmniej dwiema osobami, innymi osobami oraz osobami przypadkowymi, np. wyjątkowo z trzeciego kręgu zainteresowań potencjalnego figuranta, które dołączyły do dyskusji czy rozmowy.

Taki stan rzeczy nie wymaga rewolucji w przepisach, a po prostu zmiany kilku z nich. Mamy tu na myśli zmianę odpowiednio: art. 19 ust. 1, art. 19 ust. 7 pkt 4 i art. 19 ust. 15 u.P. We wniosku o zastosowanie kontroli operacyjnej nie mogą być, jak ma to miejsce obecnie, wymienione tylko dane osoby lub inne dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie kontrola operacyjna, ze wskazaniem miejsca lub sposobu jej stosowania. Powinny być tam na pewno dane osoby, wobec której będzie stosowana kontrola operacyjna, jak również powinno zostać użyte w przedmiotowym wniosku pojęcie innych danych, ale uzupełnione o wielu rozmówców i rozmowy. Norma

[47] Zob. wszystkie zmiany od 2 sierpnia 1997 r. ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. 2019, poz. 1950).
[48] Wyrok SA w Katowicach z dnia 11 października 2012 r., II AKa 368/12, LEX nr 1236427 wraz z glosą J. Kudły.
[49] A. Staszak, *Refleksje na temat procesowego wykorzystania materiałów…*, s. 117.
[50] Por. W. Filipkowski, *Wybrane obszary zastosowania technologii data mining w kryminalistyce*, [w:] *Meandry prawa karnego i kryminalistyki. Księga jubileuszowa Prof. zw. dra hab. Stanisława Pikulskiego*, red. W. Cieślak, J. Kasprzak, I. Nowicka, Szczytno 2015, s. 513–523.
[51] Służby mają ograniczony dostęp do wielu danych ze względu na to, że serwery z danymi umieszczone są w różnych częściach świata.

prawna art. 19 ust. 7 pkt 4 u.P. mogłaby więc brzmieć następująco: „Wniosek organu Policji, o którym mowa w ust. 1, o zarządzenie przez sąd okręgowy kontroli operacyjnej powinien zawierać, w szczególności: dane rozmów i rozmówców osoby lub inne dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie kontrola operacyjna, ze wskazaniem miejsca lub sposobu jej stosowania”[52]. Imię i nazwisko osoby, wobec której byłaby stosowana kontrola operacyjna, co do zasady powinny się znaleźć na wniosku. Warto dodać, że już dzisiaj autorzy zachęcają, aby dokonywać we wnioskach stosownych uzupełnień, np.: „…kontrola operacyjna będzie stosowana wobec: Jana Kowalskiego, jego rozmów i rozmówców…”. Pierwsza część zdania we wniosku ma charakter szczegółowy, wymienia się tu bowiem daną osobę z imienia i nazwiska, a druga jego część ma znaczenie ogólne i polega na wprowadzeniu takich pojęć, jak: „…jego rozmów i rozmówców…”. Zapewnia to prawną możliwość stosowania kontroli operacyjnej we współczesnym systemie informacyjnym bez naruszenia norm gwarancyjnych.

Wniosek o zastosowanie kontroli operacyjnej zawiera uzasadnienie oraz załączane są do niego załączniki w postaci materiałów uzasadniających potrzebę stosowania kontroli operacyjnej. Szczegóły i inne dane ze sprawy operacyjnej, niemające znaczenia dla uzasadnienia stosowania kontroli operacyjnej (jak wcześniej stwierdzono), nie powinny być przedstawiane prokuratorowi i sądowi. Nie chodzi zatem o to, aby prokurator i sąd wspólnie z Policją prowadzili sprawę operacyjną, z którą się w całości zapoznali. Jak wynika z przepisów prawa, organy te posiadają odrębną właściwość i kompetencje ustawowe w tym zakresie. Istotą jest stworzenie realnych możliwości prawnych zapoznania się przez prokuratora z takimi materiałami w zakresie uzasadniającym dopuszczalność zastosowania podsłuchu operacyjnego.

Innym ważnym zagadnieniem prawnym wymagającym odniesienia się jest kwestia zapoznania się przez prokuratora ze wszystkimi materiałami z kontroli operacyjnej, a na późniejszym etapie zapoznanie się przez sąd orzekający i odpowiednio sąd kontrolujący[53] z materiałami ze stosowanych metod pracy operacyjnej, czyli wynikami niektórych czynności operacyjno-rozpoznawczych, z których został przeprowadzony dowód. W przypadku prokuratora obecnie nie może się on zapoznać ze wszystkimi materiałami z kontroli operacyjnej. Chodzi przede wszystkim o te, o których jest mowa w art. 19 ust. 15f pkt 1 u.P., czyli zawierające informacje z zakresu tajemnicy spowiedzi i tajemnicy obrończej. Materiały te zgodnie z art. 19 ust. 15f *in fine* u.P. są po zarządzeniu Komendanta Głównego Policji, Komendanta CBŚP, Komendanta BSWP albo komendanta wojewódzkiego Policji niezwłocznie, komisyjnie i protokolarnie niszczone. Są one całkowicie pozbawione kontroli prokuratorskiej i sądowej. Tajemnica spowiedzi oraz tajemnica obrończa stanowią bezwzględny zakaz dowodowy, polegający na tym, iż nie wolno przesłuchiwać jako świadków: obrońcy albo adwokata lub radcy prawnego działającego na podstawie art. 245 § 1 k.p.k., co do faktów, o których dowiedział się, udzielając porady prawnej lub prowadząc sprawę, oraz duchownego co do faktów, o których dowiedział się przy spowiedzi. Ustawodawca zdecydował się na takie unormowanie, uwzględniając w procesie legislacyjnym rację Naczelnej Rady Adwokackiej dotyczącą natychmiastowego zniszczenia takich materiałów zgromadzonych podczas kontroli operacyjnej. Zapoznanie się z takimi materiałami przez sąd nie jest możliwe nawet na podstawie art. 19

[52] Propozycja autorów nowej normy prawnej z art. 19 ust. 7 pkt 4 u.P.
[53] D. Świecki, *Konstrukcja apelacji jako środka odwoławczego w procesie karnym*, Warszawa 2018, s. 229.

ust. 15h u.P., ponieważ w przepisie jest mowa wyłącznie o materiałach z art. 19 ust. 15g pkt 2 u.P. Stąd słusznie materiały, o których mowa w art. 19 ust. 15f pkt 1 u.P., są całkowicie wyłączone spod kontroli prokuratorskiej i sądowej. Pozostaje w związku z tym wymagać od Policji rzetelnej oceny takich materiałów. W pozostałym zakresie *de lege ferenda* po zakończonej kontroli operacyjnej wszystkie materiały powinny trafiać do oceny „na biurko" prokuratora, zarówno te, które zdaniem policji stanowią dowody pozwalające na wszczęcie postępowania karnego lub mające znaczenie dla toczącego się postępowania, jak i te, które takich dowodów nie zawierają (oprócz tych natychmiast zniszczonych w trybie art. 19 ust. 15f pkt 1 u.P.). Przemawia za tym konieczność ich rzetelnej oceny, która dzisiaj spoczywa co do zasady wyłącznie na Policji (chodzi o materiały, które nie zawierają dowodów i są przez policję niszczone). Należy jednak pamiętać, że w przypadku kontroli operacyjnej stosowanej w systemie informacyjnym powstanie o wiele więcej materiałów niezawierających dowodów dotyczących informacji co do tzw. osób przypadkowych, czyli tych z odległych kręgów powiązań figuranta. Wydaje się więc, że ostatecznie o zniszczeniu takich materiałów powinien decydować prokurator, a nie – jak dotychczas – Policja. Obecnie ustawodawca określił w art. 19 ust. 17 u.P., że zgromadzone podczas stosowania kontroli operacyjnej materiały, niezawierające dowodów pozwalających na wszczęcie postępowania karnego lub dowodów mających znaczenie dla toczącego się postępowania karnego, podlegają niezwłocznemu, protokolarnemu i komisyjnemu zniszczeniu. Zniszczenie materiałów zarządza organ Policji, który wnioskował o zarządzenie kontroli operacyjnej[54].

W przypadku postępowania sądowego, w wyniku którego z czynności operacyjno-rozpoznawczych został przeprowadzony dowód, sąd zobowiązany jest do jego oceny na podstawie przepisów karnoprocesowych. Natomiast w uzasadnionych przypadkach powinien dokonać kontroli w zakresie ich gromadzenia na podstawie przepisów z ustaw policyjnych[55].

PODSUMOWANIE

Wyrażamy przekonanie, że wszystkie powyżej przedstawione argumenty będą stanowić ważne wskazówki wytyczające kierunek przyszłych zmian, które wydają się konieczne, a wręcz niezbędne. Gruntowna przebudowa systemu stosowania kontroli rozmów i ich utrwalania w krótszej lub dłuższej perspektywie wydaje się konieczna i niezbędna. Musi być ona oparta na gruntownym rozeznaniu w nowoczesnych komunikatorach internetowych, na technologicznych rozwiązaniach stanowiących bazę ich funkcjonowania, a przede wszystkim na zmianie podejścia do modelu, że w złożonym procesie komunikacji podsłuchiwana jest tylko jedna osoba. Z tych względów jesteśmy przekonani, że wspomniane zmiany są konieczne, a nowe spojrzenie na proces komunikacji z użyciem systemów informatycznych pozwoli na oderwanie się od archaicznego systemu prawnego w tym zakresie z jednoczesnym zapewnieniem gwarancji praw procesowych wszystkim uczestnikom procesu komunikacji.

[54] Por. wyrok TK z dnia 30 lipca 2014 r., K 23/11, LEX nr 1491305.
[55] Por. J. Kudła, *Glosa do wyroku Sądu Apelacyjnego w Warszawie z dnia 29.01.2020 r., sygn. akt 219/19*, LEX nr 2834474.

BIBLIOGRAFIA

LITERATURA

Filipkowski W., *The use of data mining technology for fighting cyber crimes – selected forensic aspects,* [w:] *Current Problems of the Penal Law and Criminology,* eds. E. Guzik-Makaruk, E.W. Pływaczewski, vol. 7, Warszawa 2017.

Filipkowski W., *Wybrane obszary zastosowania technologii data mining w kryminalistyce,* [w:] *Meandry prawa karnego i kryminalistyki. Księga jubileuszowa Prof. zw. dra hab. Stanisława Pikulskiego*, red. W. Cieślak, J. Kasprzak, I. Nowicka, Szczytno 2015.

Grzelak A., *Data Retention Saga Continues: Decision of the Polish Constitutional Tribunal of 30 July 2014 in Case K 23/11*, "European Public Law" 2016, vol. 22(3).

Guzik-Makaruk E., Laskowska K., *Poczucie bezpieczeństwa oraz zagrożenie cyberterroryzmem w świetle wyników badań empirycznych,* [w:] *Przestępczość w XXI wieku – zapobieganie i zwalczanie. Problemy technologiczno-informatyczne*, red. E.W. Pływaczewski, W. Filipkowski, Z. Rau, Warszawa 2015.

Hoc S., Kudła J., *Zgoda następcza z art. 168b Kodeksu postępowania karnego. Komentarz praktyczny*, LEX/el. 2016.

Hofmański P., Zabłocki S., *Elementy metodyki pracy sędziego w sprawach karnych,* Warszawa 2011.

Hołyst B., *Podsłuchiwanie i inwigilacja użytkowników mediów elektronicznych w kontekście bezpieczeństwa informacyjnego*, „Prokuratura i Prawo" 2015, nr 3.

Kosmaty P., *Podsłuch procesowy – zamierająca instytucja walki z przestępczością*, „Prokurator" 2009, nr 2.

Krasuski A., *Chmura obliczeniowa. Prawne aspekty zastosowania,* Warszawa 2018.

Kudła J., *Glosa do wyroku SA w Warszawie z 29.01.2020 r., sygn. akt II AKa 219/19,* LEX/el. 2020.

Kudła J., *Glosa do wyroku Sądu Apelacyjnego w Warszawie z dnia 29.01.2020 r., sygn. akt 219/19*, LEX nr 2834474.

Kudła J., Staszak A., *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, „Prokuratura i Prawo" 2017, nr 7–8.

Morawski L., *Zasady wykładni prawa*, Toruń 2010.

Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne, red. M. Kusak, P. Wiliński, Warszawa 2020.

Ożóg-Wróbel K., *Katalog metod prowadzenia czynności operacyjno-rozpoznawczych*, „Roczniki Nauk Prawnych" 2012, vol. 4.

Ożóg-Wróbel K., *Przestępstwo kradzieży sygnału telewizyjnego w świetle ustawy o ochronie niektórych usług świadczonych drogą elektroniczną, opartych lub polegających na dostępie warunkowym. Sharing internetowy,* [w:] *Własność intelektualna w sieci*, red. D. Żak, Lublin 2014.

Patkowski E., *Big Data w służbie służb – sięganie po owoc zakazany (?),* [w:] *Przestępczość teleinformatyczna 2017*, red. J. Kosiński, Szczytno 2018.

Ponikwia K., *Uwagi krytyczne do art. 239 k.p.k.*, „Prokuratura i Prawo" 2002, nr 10.

Skorupka J., *Kodeks postępowania karnego. Komentarz,* Warszawa 2020.

Staszak A., *Ewolucja przepisów dotyczących podsłuchu procesowego – niewielkie zmiany o istotnym znaczeniu,* [w:] *Zmiany w prawie karnym materialnym i procesowym w latach 2013–2017. Zagadnienia wybrane*, red. H. Paluszkiewicz, „Acta Iuridica Lebusana" 2017, nr 7.

Staszak A., *Refleksje na temat procesowego wykorzystania materiałów zgromadzonych podczas stosowania kontroli operacyjnej (w świetle uchwały SN z 28 czerwca 2018r., I KZP 4/18),* [w:] *Zmiany w prawie karnym materialnym i procesowym w latach 2013–2017. Zagadnienia wybrane*, red. H. Paluszkiewicz, „Acta Iuridica Lebusana" 2019, nr 11.

Szumiło-Kulczycka D., *Dalsze wykorzystywanie materiałów z kontroli operacyjnej (uwagi na tle art. 168b k.p.k.)*, „Państwo i Prawo" 2018, z. 10.

Świecki D., *Konstrukcja apelacji jako środka odwoławczego w procesie karnym*, Warszawa 2018.

NETOGRAFIA

Regulamin Radiokomunikacyjny. Artykuły, 2016, www.il-pib.pl/images/stories/rozne/Regulamin_Radiokomunikacyjny/pdf/Regulamin_Radiokomunikacyjny_2016-2019-Tom1.pdf [dostęp: 10.02.2021].

AKTY PRAWNE

Decyzja nr 676/2002/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie ram regulacyjnych dotyczących polityki spektrum radiowego we Wspólnocie Europejskiej (decyzja o spektrum radiowym) (Dz.Urz. UE L 108/1, 2002).

Decyzja Parlamentu Europejskiego i Rady (UE) 2017/899 z dnia 17 maja 2017 r. w sprawie wykorzystywania zakresu częstotliwości 470–790 MHz w Unii (Dz.Urz. UE L 138/131, 2017).

Decyzja wykonawcza Komisji (UE) 2020/167 z dnia 5 lutego 2020 r. w sprawie norm zharmonizowanych dotyczących urządzeń radiowych, opracowanych na potrzeby dyrektywy Parlamentu Europejskiego i Rady 2014/53/UE (Dz.Urz. UE L 34/46, 2020).

Dyrektywa Parlamentu Europejskiego i Rady 2014/53/UE z dnia 16 kwietnia 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich dotyczących udostępniania na rynku urządzeń radiowych i uchylająca dyrektywę 1999/5/WE (Dz.Urz. UE L 153/62, 2014).

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

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.Urz. UE L 321/36, 2018).

Komunikat Komisji do Parlamentu Europejskiego i Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Bezpieczne wprowadzenie sieci 5G w UE – wdrażanie unijnego zestawu narzędzi, Bruksela, 29.01.2020, COM(2020) 50 final.

Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów – Nowa strategia przemysłowa dla Europy – Bruksela, 10.03.2020, COM(2020) 102 final.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiające środki dotyczące dostępu do otwartego internetu i dotyczące opłat detalicznych za regulowane usługi łączności wewnątrzunijnej oraz zmieniające dyrektywę 2002/22/WE, a także rozporządzenie (UE) nr 531/2012 (Dz.Urz. UE L 310/1, 2015).

Rozporządzenie wykonawcze Komisji (UE) 2020/911 z dnia 30 czerwca 2020 r. określające cechy punktów dostępu bezprzewodowego o bliskim zasięgu zgodnie z art. 57 ust. 2 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 ustanawiającej Europejski kodeks łączności elektronicznej (Dz.Urz. UE L 208/48, 2020).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz.U. 2020, poz. 360).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. 2019, poz. 1950).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz.U. 2021, poz. 534).

Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. 2019, poz. 2460).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2020, poz. 1369 z późn. zm.).

ORZECZNICTWO

Wyrok SA w Katowicach z dnia 11 października 2012 r., II AKa 368/12, LEX nr 1236427.

Wyrok SA w Białymstoku z dnia 16 stycznia 2014 r., II AKa 260/13, LEX nr 1422328.

Wyrok TK z dnia 30 lipca 2014 r., K 23/11, LEX nr 1491305.