

RETENCJA DANYCH I DOSTĘP DO DANYCH RETENCYJNYCH 2 LATA PÓŹNIEJ: RAPORT RPO W KWESTII WYKONANIA WYROKU ETPC PIETRZAK, BYCHAWSKA-SINIARSKA I INNI P. POLSCE

Cyfrowa rzeczywistość, analogowe przepisy.

O niedostosowaniu procedur do współczesnych form pozyskiwania informacji
w związku z zapobieganiem i zwalczaniem przestępczości i gwarancji praw jednostki

Warszawa, 19 czerwca 2026 r.

r. pr. dr Piotr Zakrzewski
Naczelnik Wydziału ds. Legislacyjnych i Ustrojowych Zespołu Prawa Karnego Biura RPO
Adiunkt w Katedrze Prawa Karnego, WPiA, Uniwersytet Kardynała Stefana Wyszyńskiego w
Warszawie



Jakie dane stanowią dane objęte retencją? (1)

- Ostatecznie przecież organy państwa nie dysponują treścią komunikatów przesyłanych drogą elektroniczną, a „jedynie” danymi o lokalizacji (gdzie znajdował się użytkownik sieci telekomunikacyjnej), danymi o połączeniach wychodzących i przychodzących (dane z billingów), itp. Informacje o subskrypcjach (np. gazet, podcastów) czy o danych używanych do logowania również nie wydają się czynnością nadmiernie ingerującą w przestrzeń prywatności jednostki. Tymczasem zakres informacji analizowany łącznie dostarcza organom państwa precyzyjnych informacji o życiu danej osoby – o tym, gdzie i jak długo przebywa, z kim się kontaktuje, jakie ma zainteresowania, itp. Informacje te mogą być przechowywane, a następnie – w dogodnym momencie – użyte przeciwko jednostce.
- Podśluch – pozyskanie danych dotyczących treści obejmujących treść komunikatów, rozmów, smsów, maili, itp. – jest swoistą „opcją atomową” i najbardziej agresywnym wkroczeniem w sferę prywatności jednostki. Dane o lokalizacji, dane transmisyjne (dane o ruchu), dane IP czy dane abonenckie, to swego rodzaju „*soft inwigilacja*”. Patrząc całościowo owa „*soft inwigilacja*” może być równie dolegliwa dla jednostki, co „klasyczna” niejawna inwigilacja – czyli obejmująca dostęp do komunikatów, rozmów, itp.

Jakie dane stanowią dane objęte retencją? (2)

- Podsumowując, dane podlegające retencji można podzielić na trzy kategorie:
 - dane dotyczące abonenta (dane abonenckie), tj. dane identyfikujące użytkownika sieci/usługi telekomunikacyjnej lub internetowej,
 - dane transmisyjne/dane o ruchu (*traffic data*), odnoszące się do połączeń, jakie zostały wykonywane (godziny, rodzaju połączenia, odbiorcy połączenia),
 - a także dane o lokalizacji (umiejscawiające połączenie, jaki i użytkownika w określonym obszarze).
- Na podstawie przepisów krajowych podział na te trzy kategorie danych ma charakter porządkujący, ponieważ prawodawca nie wprowadza żadnego rozróżnienia w zakresie ich zatrzymywania – dane mniej ingerujące w prywatność jednostki, jak dane abonenckie, podlegają takim samym zasadom zatrzymywania jak dane o lokalizacji, czy dane o ruchu. **W krajowym porządku prawnym retencja danych ma charakter uogólniony i niezróżnicowany.**

W czym jest problem? (1)

- Zasadniczym problemem – z perspektywy zgodności krajowych rozwiązań ustawowych z normami prawnymi wyższego rzędu – jest zaprojektowanie całego systemu retencji danych niejako „na wzór” standardu dopuszczalnego wyłącznie dla ochrony bezpieczeństwa narodowego.
- Kwestie dotyczące danych retencyjnych – zatrzymywania i dostępu do nich – mają znaczenie także z uwagi na fakt, że w dniu 16 sierpnia 2026 r. wejdzie w życie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz. U. UE. L. z 2023 r. Nr 191, str. 118.).

W czym jest problem? (2)

- Problematyczne jest także uregulowanie zasad dostępu do danych retencyjnych (pozyskanie danych w formie „stałego łącza”, bez zaangażowania pracowników dostawców usług łączności, możliwość dostępu do danych dotyczących osób, które nie są w żaden sposób zaangażowane w jakąkolwiek działalność przestępczą), brak realnego nadzoru zewnętrznego nad dostępem do danych o ruchu, danych o lokalizacji, itp.: w formie kontroli sądowej następczej, w formie „społecznej” kontroli czy też w formie skarg indywidualnych, jeśli pozyskano dane konkretnej osoby. W konsekwencji nie jest dalekie od prawdy stwierdzenie, że każdy może zostać poddany „soft” inwigilacji, niezależnie od jakiegokolwiek związku z działalnością przestępczą, a system został zaprojektowany tak, by jednostka nie dowiedziała się o pozyskaniu jej danych telekomunikacyjnych.

Opinia Komisji Weneckiej

- W zaleceniach, jakie zostały sformułowane w opinii Komisji Weneckiej, zwrócono uwagę na:
 - konieczność wzmocnienia zasady proporcjonalności w pozyskiwaniu danych na podstawie art. 20c ustawy o Policji;
 - zobowiązanie Policji do prowadzenia rzetelnej dokumentacji (ewidencji), umożliwiającej skuteczną kontrolę następczą (ex post) operacji polegających na dostępie do danych nie dotyczących treści, w szczególności realizowanych poprzez „stałe łącze”;
 - zagwarantowanie skutecznego mechanizmu nadzoru nad konkretnymi operacjami pozyskania danych nie dotyczących treści, sprawowanego przez niezależny organ; organ ten powinien dysponować niezbędnymi uprawnieniami śledczymi i wiedzą ekspercką oraz mieć możliwość korzystania z adekwatnych środków prawnych.

Wyrok ETPC z dnia 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, skargi nr 72038/17 i 25237/18. (1)

- W wyroku w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, ETPC stwierdził naruszenie art. 8 EKPC także w odniesieniu do przepisów o retencji danych. W orzeczeniu tym Trybunał strasburski wskazał, że „**przepisy krajowe, zgodnie z którymi dostawcy usług łączności są zobowiązani do przechowywania danych dotyczących komunikacji w sposób ogólny i niezróżnicowany do celów ewentualnego dostępu przez właściwe organy krajowe, są niewystarczające, aby ograniczyć ingerencję w korzystanie przez skarżących z ich prawa do poszanowania życia prywatnego do tego, co jest niezbędne w demokratycznym społeczeństwie**”.

Wyrok ETPC z dnia 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, skargi nr 72038/17 i 25237/18. (2)

- Trybunał przypominał, że obecne możliwości technologiczne, komunikowanie się za pośrednictwem telefonów, Internetu i innych usług łączności, może ujawniać dane osobowe jednostki, a także dostarczać precyzyjnych informacji na temat życia prywatnego określonej osoby. Monitorowanie aktywności danej osoby w sieciach społecznościowych, monitorowanie schematów przemieszczania się, nawyków komunikacyjnych pozwala na stworzenie jej intymnego portretu. Problem ten jest zwielokrotniony, jeśli przepisy pozwalają na masowe przechwytywanie, przechowywanie i udostępnianie danych o abonentach usług telekomunikacyjnych, danych o ruchu/danych transmisyjnych oraz danych o lokalizacji.

Wyrok ETPC z dnia 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, skargi nr 72038/17 i 25237/18. (3)

- Ze względu na możliwość powiązania różnych kategorii danych oraz zakres możliwych do uzyskania informacji o jednostce „**pozyskiwanie powiązanych danych dotyczących komunikacji w kontekście masowego przechwytywania może być tak samo inwazyjne jak pozyskiwanie treści komunikatów, a zatem przechwytywanie i zatrzymywanie takich danych oraz przeprowadzane na nich wyszukiwania muszą być analizowane w świetle tych samych zabezpieczeń, które mają zastosowanie do treści komunikatów, bez konieczności, aby przepisy prawne regulujące przetwarzanie takich danych były identyczne pod każdym względem z przepisami regulującymi przetwarzanie treści komunikatów**”.

Aktualnie prawo dostępu do danych telekomunikacyjnych/danych o łączności w trybie pozaprocesowym mają:

- **Policja**, w tym także m.in. Centralne Biuro Zwalczania Cyberprzestępczości (art. 5d ustawy o Policji), Centralne Biuro Śledcze Policji (art. 5a ustawy o Policji), Biuro Spraw Wewnętrznych Policji (art. 5b ustawy o Policji)
 - na podstawie art. 20c ustawy o Policji - możliwe jest pozyskanie danych wskazanych w art. 45 ust. 1 i art. 49 p.k.e. w celu zapobiegania lub wykrywania przestępstw, przestępstw skarbowych albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych; pozyskiwanie danych podlega kontroli właściwego miejscowo sądu okręgowego na podstawie art. 20ca ustawy o Policji;
 - na podstawie art. 20cb ustawy o Policji możliwe jest pozyskanie danych wskazanych w art. 43 ust. 1 tiret drugi i art. 389 p.k.e. w celu zapobiegania lub wykrywania przestępstw, przestępstw skarbowych albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych. Dane o abonencie, dane o lokalizacji i dane transmisyjne pozyskane w trybie art. 20cb nie podlegają kontroli sądowej;

Aktualnie prawo dostępu do danych telekomunikacyjnych/danych o łączności w trybie pozaprocesowym mają ponadto:

- Agencja Bezpieczeństwa Wewnętrznego
- Straż Graniczna
- Krajowa Administracja Skarbowa
- Służba Ochrony Państwa
- Centralne Biuro Antykorupcyjne
- Żandarmeria Wojskowa
- Służba Kontrwywiadu Wojskowego
- Generalny Inspektor Informacji Finansowej Ministerstwa Finansów



Aktualnie prawo dostępu do danych telekomunikacyjnych/danych o łączności w trybie procesowym mają:

- organem właściwym do wystąpienia z wnioskiem do operatorów/dostawców usług telekomunikacyjnych jest prokurator w postępowaniu przygotowawczym – co do zasady – oraz sąd w postępowaniu jurysdykcyjnym. Od strony technicznej, dostęp prokuratora lub sądu do danych nie dotyczących treści jest regulowany w rozporządzeniu wydanym na podstawie art. 218b k.p.k.. Nie wdając się szczegółowo w tę problematykę, podkreślenia wymaga fakt, że ani sąd, ani prokurator nie mogą uzyskać dostęp do danych nie dotyczących treści bez zaangażowania operatora/dostawcy usług łączności lub usług telekomunikacyjnych. Każdorazowo, muszą się zwrócić do odpowiedniego dostawcy – wydając postanowienie w trybie art. 218 k.p.k., a niekiedy – uzyskując uprzednie zwolnienie z tajemnicy, zwłaszcza w odniesieniu np. do tajemnicy dziennikarskiej z art. 180 § 2 k.p.k. – o przekazanie danych o abonencie, danych o lokalizacji lub danych transmisyjnych/danych o ruchu. Należy także podkreślić, że z możliwości pozyskania danych z art. 218 k.p.k. organy procesowe mogą skorzystać **tylko w toku prowadzonego postępowania karnego**.

Jakie są postulaty RPO związane z zarysowanym problemem?

- Próbuąc uporządkować wnioski de lege ferenda, jakie wynikają z analizy standardu konstytucyjnego, konwencyjnego i unijnego, z uwagi na liczbę zidentyfikowanych wadliwości krajowego systemu, podzielone one zostały na trzy grupy:
 - zmiany w przepisach o retencji danych;
 - zmiany w przepisach o dostępie do danych retencyjnych;
 - zewnętrzna kontrola - kontrola społeczna dostępu do danych retencyjnych oraz notyfikacja, jeśli organy ścigania lub organy procesowe uzyskały dostęp do danych retencyjnych.

Zmiany w przepisach o retencji danych niedotyczących treści (1)

- należy „rozbić” dane niedotyczące treści na odrębne kategorie, tj. dane o abonencie, dane o IP, dane o ruchu (dane transmisyjne) i dane o lokalizacji. Prawo unijne i orzecznictwo ETPC różnicuje te kategorie danych biorąc pod uwagę ich „potencjał” ingerencyjny w prawo do prywatności i możliwość odtworzenia/stworzenia „intymnego portretu” danej osoby. Najmniejszy potencjał ingerencyjny mają dane o abonencie, największy – dane o ruchu i dane o lokalizacji;
- w związku z powyższym, konieczna jest zmiana systemowa i odejście od uogólnionej i nieodróżnicowanej retencji danych o lokalizacji, danych o ruchu, danych o IP i danych o abonencie na takich samych zasadach. Takie ukształtowanie systemu krajowego – nawet jeśli służy zwalczaniu i zapobieganiu przestępczości – wiąże się z nieproporcjonalną ingerencją w prawo do prywatności. TSUE różnicuje zasady retencji danych, co powinno znaleźć odzwierciedlenie w prawie krajowym;

Zmiany w przepisach o retencji danych niedotyczących treści (2)

- niedopuszczalna jest uogólniona i niezróżnicowana retencja danych o ruchu i danych o lokalizacji. TSUE dopuszcza taką możliwość wyłącznie w przypadku realnego zagrożenia dla bezpieczeństwa narodowego. Rozwiązanie to ze swojej istoty musi być jednak rozwiązaniem czasowym – przejściowym – i obowiązującym jedynie do ustania realnego i rzeczywistego dla bezpieczeństwa narodowego, i nie może obowiązywać jako „domyślny” czy podstawowy system zatrzymywania danych. Zgodna z prawem unijnym jest natomiast ukierunkowana retencja danych o ruchu i o lokalizacji pod warunkiem, że kryteria ukierunkowanej retencji są obiektywne, niedyskryminacyjne, ograniczone czasowo i obszarowo (np. wprowadzono retencję danych każdej osoby znajdującej się na dworcach kolejowych, lotniskach itp.);
- dopuszczalna jest uogólniona i niezróżnicowana retencja danych o abonencie i danych o IP pod warunkiem, że przepisy wprost wskazują cele zatrzymywania danych, okres ich przechowywania;

Zmiany w przepisach o retencji danych niedotyczących treści (4)

- konieczne jest wskazanie celów retencji danych niedotyczących treści. W zależności od kategorii danych, dostęp do nich może być uzasadniony zwalczaniem poważnej przestępczości (np. jak w przypadku danych o ruchu i danych o lokalizacji), jeśli zostały zatrzymane w wyniku ukierunkowanej retencji danych albo ochroną bezpieczeństwa narodowego. Określenie celu retencji danej kategorii danych zapobiegałoby sytuacji, kiedy dane zatrzymane w celu bezpieczeństwa narodowego byłyby wykorzystywane np. dla realizacji celu w postaci zwalczania przestępczości. Wprowadzając przepisy konkretyzujące cele retencji danych należy uwzględnić „hierarchię celów”, na którą zwraca uwagę przede wszystkim TSUE (celem o najwyższej randze jest ochrona bezpieczeństwa narodowego, bezpieczeństwo powszechne i zwalczanie poważnej przestępczości są celami istotnymi, ale znajdującymi się niżej w hierarchii celów; dostęp do danych o lokalizacji i ruchu/transmisyjnych nie powinien być możliwy w sprawach, które należą do kategorii „drobnej” przestępczości z uwagi na brak proporcjonalności ingerencji w prawo do prywatności).

Zmiany w przepisach o retencji danych niedotyczących treści (5)

- Obecnie, mimo tego, że ustawa - Prawo komunikacji elektronicznej weszła w życie 10 listopada 2024 r., nie zostały wydane rozporządzenia wykonawcze, o których mowa w art. 49 ust. 2 i 3 p.k.e. Rozporządzenie z art. 49 ust. 2 p.k.e. dotyczy określenia konkretnych kategorii danych, jakie podlegają obowiązkowi retencji. Z uwagi na niewydanie nowego rozporządzenia, w mocy pozostaje poprzednio obowiązujące – wydane na podstawie uchylonej ustawy - Prawo telekomunikacyjne – ale nie jest ono w pełni spójne (zwłaszcza jeśli chodzi o terminologię) z nowymi przepisami. Warto także zwrócić uwagę, że Komisja Wenecka krytycznie odniosła się do modelu, w którym zakres danych retencyjnych jest precyzowany w akcie prawnym wykonawczym (rozporządzeniu), a nie w ustawie. Uregulowanie tego rodzaju kwestii w rozporządzeniu stwarza ryzyko nadużyć i rozszerzania kategorii danych retencyjnych.

Zmiany w przepisach o dostępie do danych retencyjnych (1)

- dostęp do danych o ruchu i danych o lokalizacji powinien być możliwy wyłącznie po uzyskaniu uprzedniej zgody niezależnego organu. Kontrola uprzednia powinna mieć merytoryczny charakter (nie sprowadzać się do analizy spełnienia przesłanek formalnych, np. prawidłowości sformułowania żądania), a organ, który podejmuje decyzję powinien mieć możliwość odmówić dostępu albo ograniczyć zakres żądania (np. skrócić okres/liczbę miesięcy, za które służby/prokurator żądają dostępu do danych). W wypadkach niecierpiących zwłoki, służby specjalne i policyjne powinny móc niezwłocznie zabezpieczyć dane lokalizacyjne i dane transmisyjne/dane o ruchu, ale konieczna jest następcza zgoda niezależnego organu udzielana *post factum*;

Zmiany w przepisach o dostępie do danych retencyjnych (2)

- przepisy o dostępie do danych retencyjnych, tj. art. 20c ustawy o Policji i analogiczne przepisy w pozostałych ustawach o służbach specjalnych i służbach policyjnych oraz art. 218 k.p.k. powinny zawierać przesłanki ograniczające możliwość „łatwego” sięgania po dane retencyjne. Konieczne jest dodanie przesłanki subsydiarności (dostęp do danych o ruchu/transmisyjnych i danych o lokalizacji jest możliwy wtedy, gdy inne środki, mniej inwazyjne, są bezskuteczne albo okazałyby się bezskuteczne), proporcjonalności i konieczności oraz wprowadzenie wymogu, by osoba, o dane której służby się zwracają, miała związek z popełnieniem/popełnianiem przestępstwa;

Zmiany w przepisach o dostępie do danych retencyjnych (3)

- w odniesieniu do spraw, kiedy służby mogą uzyskać dostęp do danych retencyjnych, konieczne jest wprowadzenie ograniczeń przedmiotowych – zwłaszcza w ustawie o CBA. Służby nie mogą sięgać po dane nie dotyczące treści – zwłaszcza dane o lokalizacji i dane o ruchu – w związku z oceną partnerstwa publiczno-prywatnego czy kontrolą oświadczeń majątkowych. W przypadku przestępstw i przestępstw skarbowych należy również ograniczyć zakres dopuszczalnego dostępu do danych o lokalizacji i danych o ruchu. Co do zasady służby mogłyby pozyskać ww. dane wyłącznie w sprawach zagrożonych karą co najmniej 3 lat pozbawienia wolności oraz w tych sprawach, zagrożonych karą łagodniejszą, w których przestępstwo popełniono przy wykorzystaniu środków komunikowania się na odległość/przy wykorzystaniu Internetu. Nowe regulacje powinny zatem obejmować także m.in. art. 200a § 2 k.k., art. 257 k.k., art. 212 k.k., art. 216 k.k., art. 226 k.k. Alternatywnie można rozważyć wprowadzenie rozwiązań w k.p.k., które pozwalają na dostęp do danych retencyjnych w sprawach zagrożonych karą łagodniejszą niż 3 lata pozbawienia wolności wyłącznie w trybie procesowym. W sprawach o średniej społecznej szkodliwości, np. zagrożonych karą do 5 lat pozbawienia wolności można rozważyć wprowadzenie ograniczenia w zakresie temporalnym żądania dostępu do danych o lokalizacji i danych o ruchu. Pozyskanie danych za 12 miesięcy wstecz, w sprawach o średniej społecznej szkodliwości, może być środkiem nadmiernie nieproporcjonalnym;

Zmiany w przepisach o dostępie do danych retencyjnych (4)

- należy wzmocnić kontrolę sądową/organu sądowego. Konieczne jest zatem usunięcie – ze wszystkich ustaw – trybu dostępu do danych poza kontrolą sądową, o którym mowa w art. 20cb ustawy o Policji i analogicznych przepisach pozostałych ustaw policyjnych i o służbach specjalnych. Pojawia się jednak pytanie o kształt kontroli sądowej następcej. Z rozwiązań prawnomiędzynarodowych wynika, że konieczna byłaby uprzednia kontrola dostępu do danych lokalizacyjnych i danych transmisyjnych/danych o ruchu. Następca kontrola sądowa mogłaby znaleźć zastosowanie wyłącznie w odniesieniu do danych o abonencie i danych o IP;

Zmiany w przepisach o dostępie do danych retencyjnych (5)

- konieczne jest wprowadzenie pełnej rozliczalności dostępu do danych retencyjnych, w szczególności w sytuacji korzystania ze „stałego łącza”, tj. dostępu bez zaangażowania dostawców usług łączności. Rozliczalność dostępu do danych, zwłaszcza danych o ruchu i danych o lokalizacji nie może ograniczać się do ewidencji liczby zapytań lub logowań, ale powinna obejmować rejestry operacji pozwalające ustalić: kto, kiedy, w jakim trybie, w jakiej sprawie, w jakim celu i w jakim zakresie pozyskał dane. Rejestry powinny uniemożliwiać modyfikowanie ich treści po fakcie, a jeśli taka modyfikacja nastąpiła – powinna być odnotowana w systemie, żeby możliwe było prześledzenie i przeanalizowanie wersji aktualnej i wersji historycznej;

Zmiany w przepisach o dostępie do danych retencyjnych (6)

- przepisy powinny wprowadzać obowiązek dokumentowania „ścieżki decyzyjnej” po stronie służb, tj. nie tylko samego żądania dostępu do danych, ale również decyzji wewnętrznej o wyborze kategorii danych, zakresu czasowego (tj. czy 6 czy 12 miesięcy wstecz); celem jest zapewnienie, by organ kontrolujący miał do dyspozycji materiał pozwalający na rekonstrukcję procesu decyzyjnego, a nie wyłącznie końcowy „efekt” w postaci pozyskanych danych;
- konieczne jest wprowadzenie w ustawach policyjnych i o służbach specjalnych oraz wprost w przepisach k.p.k. (np. w art. 218 k.p.k.) odrębnych gwarancji chroniących tajemnice prawnie chronione, zwłaszcza tajemnicę dziennikarską i tajemnicę obrończą, w obszarze metadanych, tj. rozwiązań, które zapobiegają obejściu ochrony tajemnic przez sięganie po dane o ruchu i dane o lokalizacji (np. w celu identyfikacji źródeł dziennikarskich albo ustalenia kontaktów obrońcy z klientem).

Zmiany w przepisach o dostępie do danych retencyjnych (7)

- konieczne jest wprowadzenie do k.p.k. regulacji, które uniemożliwią „obchodzenie” przepisów o postępowaniu dowodowym przez „wyprowadzanie” czynności dowodowych do czynności operacyjnych. Jeżeli dane retencyjne są pozyskiwane w związku z toczącym się postępowaniem karnym, tj. na potrzeby prowadzonego postępowania przygotowawczego lub sądowego, ich pozyskanie powinno następować co do zasady w trybie procesowym przewidzianym w k.p.k., a nie w trybach właściwych dla czynności operacyjno-rozpoznawczych. Cel ten może zostać osiągnięty tylko w sytuacji, kiedy uprawnienia prokuratora w postępowaniu karnym będą „lustrzanym” odbiciem uprawnień, jakie ma Policja, czy inne służby. Sytuacja, w której prokurator ma mniejsze możliwości działania niż funkcjonariusze służb, a dodatkowo nadzór zewnętrzny nad działalnością służb jest mocno ograniczony, skłania do „wyprowadzania” czynności dowodowych do czynności operacyjnych;

Zmiany w przepisach o dostępie do danych retencyjnych (8)

- doręczenie postanowienia z art. 218 k.p.k. może zostać odroczone, ale obecny termin z art. 218 § 2 k.p.k. pozwalający na odroczenie doręczenia postanowienia aż do prawomocnego zakończenia postępowania jest nieproporcjonalnie długi (zwłaszcza jak uwzględni się okoliczność, że odroczenie postanowienia o procesowej kontroli i utrwalaniu rozmów może nastąpić najpóźniej do czasu zakończenia postępowania przygotowawczego – art. 239 § 2 k.p.k.). Odroczenie doręczenia postanowienia z art. 218 § 1 k.p.k. w postępowaniu przygotowawczym powinno być możliwe do czasu zakończenia postępowania przygotowawczego. W postępowaniu sądowym – taka decyzja powinna być ogłaszana niezwłocznie stronom postępowania. Na tym etapie procesu, z uwagi na pełną jawność akt postępowania – art. 156 § 1 k.p.k. – niecelowe jest odroczenie doręczenia decyzji procesowej, z której treścią strona będzie mogła się zapoznać uzyskując dostęp do akt sprawy karnej, a jednocześnie nie będzie mogła jej zaskarżyć.

Zewnętrzna kontrola - kontrola społeczna, dostępu do danych retencyjnych oraz notyfikacja, jeśli organy ścigania lub organy procesowe uzyskały dostęp do danych retencyjnych (1)

- konieczne jest wprowadzenie realnego mechanizmu notyfikacji jednostki o tym, że jej dane zostały pozyskane przez Policję lub inne służby. Możliwe jest przyjęcie rozwiązania analogicznego do mechanizmu funkcjonującego przy pozyskiwaniu danych w trybie procesowym (218 k.p.k.), tj. jednostka zostałaby poinformowana o tym, że jej dane zostały pozyskane od dostawców usług łączności przez organy ścigania po upływie odpowiedniego okresu, np. 1 roku albo 2 lat od pozyskania danych retencyjnych. W wąskiej kategorii spraw – np. tych dotyczących bezpieczeństwa narodowego – możliwe byłoby wyłączenie obowiązku notyfikacji z uwagi na przeważający interes publiczny;

Zewnętrzna kontrola - kontrola społeczna, dostępu do danych retencyjnych oraz notyfikacja, jeśli organy ścigania lub organy procesowe uzyskały dostęp do danych retencyjnych (2)

- równocześnie konieczne jest pełne wdrożenie art. 17 dyrektywy 2016/680, tj. zapewnienie jednostce możliwości wykonywania praw w trybie pośrednim w sytuacjach, gdy – z przyczyn dopuszczalnych w dyrektywie – ogranicza się jej prawo do informacji lub odmawia się udzielenia informacji o przetwarzaniu/pozyskaniu danych osobowych. Tryb pośredni powinien polegać na tym, że niezależny organ (organ nadzorczy) dokonuje weryfikacji legalności i zasadności przetwarzania oraz informuje jednostkę co najmniej o tym, że weryfikacja została przeprowadzona i czy stwierdzono naruszenia, a także zapewnia skuteczny środek zaskarżenia. Brak implementacji art. 17 dyrektywy 2016/680 w praktyce uniemożliwia wykonywanie praw jednostki w sytuacjach, w których notyfikacja jest odraczana albo ograniczana (w tym wyłączona dla ochrony bezpieczeństwa narodowego). Pełna implementacja dyrektywy 2016/680 wzmocniłaby nadzór nad czynnościami operacyjnymi i zwiększyłaby kompetencje Prezesa UODO;

Zewnętrzna kontrola - kontrola społeczna, dostępu do danych retencyjnych oraz notyfikacja, jeśli organy ścigania lub organy procesowe uzyskały dostęp do danych retencyjnych (3)

- konieczne jest wprowadzenie standardów raportowania/sprawozdawczości, które pozwolą ocenić nie tylko „skalę” korzystania z danych retencyjnych. Sprawozdawczość powinna być pełna - obejmować informacje nie tylko o dostępie pozaprocesowym, ale także całościowo dostęp w trybie art. 218 k.p.k. Sprawozdania, oprócz danych obecnie prezentowanych, powinny obejmować:
 - liczbę przypadków, w których uprawnione organy uzyskiwały od przedsiębiorców telekomunikacyjnych wyłącznie dane osobowe użytkownika;
 - liczbę przypadków (rozumianych jako liczbę numerów telefonicznych lub numerów IP), w których uprawnione organy uzyskiwały dane telekomunikacyjne (z wyłączeniem ustaleń danych abonenckich) z podzieleniem na odpowiednie kategorie (np. dane transmisyjne, dane o lokalizacji);
 - łączną liczbę przypadków, w których wnioski uprawnionego podmiotu nie mógł być zrealizowany;
 - liczbę osób, których dane telekomunikacyjne były pozyskiwane i wykorzystywane przez uprawnione organy (z wyłączeniem ustaleń danych abonenckich)”.
- [Raport NIK, KPB-P/12/191](#), Warszawa 2013, s. 71.

Zewnętrzna kontrola - kontrola społeczna, dostępu do danych retencyjnych oraz notyfikacja, jeśli organy ścigania lub organy procesowe uzyskały dostęp do danych retencyjnych (4)

- Warto byłoby wskazać, jaki był cel uzyskania dostępu do danych nie dotyczących treści. Jeśli celem było pozyskanie tych danych w związku z zapobieganiem lub zwalczaniem przestępstw (a nie np. w związku z działaniami ratunkowymi lub poszukiwawczymi), rozważenia wymaga uzupełnienie sprawozdań publicznie dostępnych o rodzaj (kwalifikację prawną) przestępstwa.

DZIĘKUJĘ ZA UWAGĘ

