CZYNNOŚCI OPERACYJNE W XXI WIEKU. GRANICE WYKŁADNI PRAWA W INTERESIE PUBLICZNYM

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.

mł. insp. dr Maria Hapunik, Uniwersytet w Białymstoku

Czy możemy mówić o „szarej strefie" czynności operacyjnych? Jakie czynności – patrząc z perspektywy zewnętrznego obserwatora - są „niedoregulowane” w krajowych przepisach?

- Tylko kilka metod czynności operacyjno – rozpoznawczych jest uregulowana ustawowo (ustawy kompetencyjne służb);
- Formy i metody pracy operacyjnej regulują niejawne instrukcje poszczególnych służb policyjnych oraz służb specjalnych;
- Brak informacji o charakterze stosowanych niejawnych środków może budzić pytania oraz sprzeciw;
- Odpowiedzią jest regulacja w postaci ustawy o czynnościach operacyjno – rozpoznawczych, która wskaże, nazwie i zdefiniuje możliwości służb w obszarze czynności operacyjno – rozpoznawczych;
- Klauzulami niejawności należałoby objąć szczegółowe algorytmy postępowania podczas prowadzenia pracy operacyjnej oraz indywidualne sprawy operacyjne.

Czy art. 19 ust. 6 ustawy o Policji wymaga nowelizacji, a jeśli tak, to w jakim kierunku?

Kontrola operacyjna prowadzona jest niejawnie i polega na:

1. uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych;
2. uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne;
3. uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej;
4. **uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;**
5. uzyskiwaniu dostępu i kontroli zawartości przesyłek.

art. 19 ust. 6 pkt 4 ustawy o Policji

Problematyczne brzmienie przepisu w punkcie 4.

Czy sformułowanie pozwalające na uzyskiwanie i utrwalanie danych zawartych w systemach informatycznych jest wystarczająco precyzyjne, aby stanowić podstawę dla tak zaawansowanych narzędzi jak spyware przejmujące pełną kontrolę nad urządzeniem?

art. 19 ust. 6 ustawy o Policji

- Pkt 4 przepisu został sformułowany technologicznie neutralnie, aby obejmował nowe formy komunikacji i przechowywania danych;
- Nie rozróżnia zwykłego dostępu do konkretnych danych od pełnego przejęcia urządzenia;
- Nie określa wyraźnie, czy dopuszczalne jest pozyskiwanie danych zgromadzonych w chmurze, które nie znajdują się fizycznie na telefonie;
- Zasadnym jest wprowadzenie precyzyjnego przepisu ustawy dotyczącego rodzaju pozyskiwanych informacji, jak również charakteru stosowanych środków operacyjnych.

Jakimi gwarancjami procesowymi należałoby objąć pozyskiwanie/uzyskiwanie dostępu do danych zapisanych w chmurze (na dysku iCloud, GoogleDysku, dropboxie itp.?) Dostosowanymi do przeszukania urządzenia, czy kontroli operacyjnej?

Przeciętny użytkownik np. iphona nie wie, czy wybierając zdjęcie to tylko miniatura w pamięci telefonu czy łączy się z chmurą w iCloud.

Pamięć telefonu podczas wykonywania czynności procesowych (oględzin zawartości telefonu) powinna być traktowana jako całość.

Przepisy należy skonstruować w sposób umożliwiający dostanie się biegłego do pamięci (nie tylko za zgodą użytkownika) podczas badania urządzenia, po procesowym zatrzymaniu rzeczy.

Kontrola operacyjna dotycząca usług chmurowych – regulacja dostępu

Chmura jako odpowiednik dysku twardego

W tym podejściu konto w usługach takich jak:

- Google Drive,
- Microsoft OneDrive,
- Apple iCloud
- itp.

jest traktowane podobnie jak komputer lub telefon użytkownika.

Model wskazany do badania podczas czynności procesowych.

Chmura jako odrębna przestrzeń ,wymagająca zgody sądu na jej kontrolę

- telefon zawiera tylko część danych;
- konto chmurowe może obejmować wiele lat aktywności (przeszłość), zdjęcia rodzinne, dokumenty zawodowe, kopie zapasowe i dane osób trzecich;
- dostęp do całego konta jest znacznie bardziej ingerujący niż podsłuch rozmów.

Dostęp selektywny

Służby policyjne i specjalne mogłyby uzyskać dostęp w określonym zakresie czasowym, zamiast pełnej kopii całego konta.
konkretne wiadomości
wybrane foldery lub kategorie danych

Konstrukcje (mechanizmy) prawne kształtowane z myślą o realizacji funkcji ochronnej w trakcie prowadzonego postępowania

DOPRECYZOWANIE PRZEPISÓW

Nie oznaczałoby to koniecznie zakazu dostępu do danych w chmurze, lecz bardziej szczegółowe określenie:

- jakie dane można pozyskiwać,
- katalog przestępstw, co do których można stosować oprogramowanie infiltracyjne,
- limity czasowe,
- w jaki sposób chronić dane osób postronnych/tajemnice.
- Takie rozwiązanie wydaje się realne w celu dążenia do równowagi między skutecznością działań służb a ochroną prywatności w erze usług chmurowych i zaawansowanego nadzoru cyfrowego.

Przełamanie zabezpieczeń szyfrowanych komunikatorów. Dostęp do szyfrowanych komunikatorów/powinno być odrębną/wyróżnioną/wyodrębnioną czynnością operacyjną.

- Służby specjalne i policyjne powinny mieć dostęp do szyfrowanych komunikatorów;
- Regulacje ustawowe w obszarze katalogu przestępstw/wskazanie katalogu metod operacyjnych;
- Regulacje dotyczące charakteru środka umożliwiającego przełamanie zabezpieczeń urządzenia;
- Dostęp do komunikatorów byłby formą ukierunkowanego nadzoru, stanowiącego konieczny i proporcjonalny środek zwalczania przestępczości;
- Postęp technologiczny determinuje rozwój metod operacyjnych.

Czy rodzaj, katalog i gwarancje procesowe jednostki w ramach czynności operacyjnych powinny być dostosowane do rodzaju/charakteru przestępstwa i służby, która prowadzi czynności, tj. inne dla przestępczości (w tym poważnej przestępczości) kryminalnej, a inne dla spraw odnoszących się do bezpieczeństwa państwa, integralności terytorialnej i bezpieczeństwa narodowego?

- Tak, praca operacyjna służb specjalnych charakteryzuje się szerszymi uprawnieniami niż odpowiednio praca operacyjna prowadzona przez służby policyjne.
- Służby specjale prowadzą czynności operacyjno – rozpoznawcze w granicach swoich zadań ustawowych.
- Służby policyjne powinny stosować zamknięty katalog, enumeratywnie wskazujący kwalifikacje prawne, które są podstawą do stosowania poszczególnych czynności operacyjno – rozpoznawczych.

Czy brakuje przepisów stanowiących podstawę dla działań (chroniących) funkcjonariuszy podmiotów państwowych wykonujących czynności operacyjno - rozpoznawcze?

Przepisy są różnie interpretowane

- Brak jest kontratypów sankcjonujących trudne do rozwiązania sytuacje operacyjne, które dotyczą działań wypełniających znamiona czynów zabronionych, które nie mają na celu popełnienie przestępstwa, a mogą zapobiec groźnym przestępstwom.
- Brak jest przepisu wskazującego możliwość pokonywania zabezpieczeń w miejscach prywatnych w celu realizacji postanowienia sądu o zarządzeniu kontroli operacyjnej.

Wnioski

- Państwo utraciło monopol na działania wywiadowcze, coraz więcej podmiotów sektora prywatnego prowadzi działalność szpiegowską.
- Obowiązek działań prewencyjnych służb specjalnych, jako zapobiegających przestępstwom i innym negatywnym zdarzeniom, uderzającym w szeroko pojęte dobro człowieka, jako współcześnie najważniejsze.
- Służby policyjne powinny mieć dostęp do narzędzi umożliwiających niejawną ingerencję, w postaci ukierunkowanego nadzoru, na którego zastosowanie zgodę wyraził sąd.

Dziękuję za uwagę

m.hapunik@uwb.edu.pl