KOMENDANT GŁÓWNY POLICJI

KR-NNZC-980|826|2016

Warszawa, dn. 05 lipca 2016 r.

Pan
Adam Bodnar
Rzecznik Praw Obywatelskich

Szanowny Panie Ministrze

W odpowiedzi na pismo II.519.1253.2015.NBe z dnia 2 czerwca 2016 roku, poruszające kwestie związane z zabezpieczaniem przez Policję urządzeń zawierających dane informatyczne na potrzeby postępowania karnego i wynikające z tego niedogodności dla osób będących właścicielami zatrzymywanych rzeczy, należy w pierwszej kolejności zaznaczyć, że jednym z podstawowych zadań Policji jest wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców. Policja realizując ustawowe zadania, wykonuje czynności wskazane w kodeksie postępowania karnego oraz innych odrębnych ustawach i przepisach wykonawczych.

Zgodnie z art. 297 § 1 k.p.k. - celem postępowania przygotowawczego jest m.in. zebranie, zabezpieczenie i w niezbędnym zakresie utrwalenie dowodów dla sądu, może się to wiązać z koniecznością zatrzymania sprzętu komputerowego. Ustawodawca nie przewiduje odrębnych procedur wobec zabezpieczenia urządzeń zawierających dane informatyczne.

Odnosząc się do podniesionej w Pańskim piśmie kwestii uciążliwości z tym związanej, chciałbym zauważyć, że Policja stara się korzystać z możliwości wykonywania kopii danych zawartych na informatycznych nośnikach danych. Jednakże każdy przypadek należy rozpatrywać indywidualnie. Decyzje o sposobie zabezpieczania dowodów są konsultowane z nadzorującymi czynności prokuratorami.

Prowadzący czynności procesowe policjanci stosują się do wymogu określonego w art. 227 k.p.k, z którego wynika, iż czynność przeszukania i zatrzymania powinny być dokonywane w możliwie jak najmniej szkodliwy i dolegliwy sposób, a także

z poszanowaniem godności osób, których te czynności będą dotyczyć. Przepis art. 227 k.p.k nakreśla pewne ramy prowadzenia czynności procesowych, które sprowadzają zbieranie materiału procesowego do działań podporządkowanych toczącemu się postępowaniu i nie wykraczających poza podstawowe cele, jakie zamierza się w nim osiągnąć.

Kodeks postępowania karnego rozróżnia czynności, z których musi być sporządzony protokół. Dokument taki sporządza się zarówno po przeprowadzeniu zatrzymania rzeczy lub też przeszukaniu i zawierać on powinien podstawowe dane związane z prowadzoną czynnością, osobom, których prawa zostały naruszone – przysługuje zażalenie na podstawie art. 236 k.p.k.

Ocena sposobu w jaki dane informatyczne zostaną zabezpieczone zależy zwykle od kilku czynników. Pierwszym są możliwości techniczne osób realizujących zabezpieczenie. Policja konsekwentnie buduje struktury skupiające w sobie zarówno funkcjonariuszy o odpowiednich kompetencjach zawodowych jak i właściwe narzędzia informatyczne. Obok istniejących już wcześniej policyjnych laboratoriów kryminalistycznych, od 2014 roku funkcjonują także komórki organizacyjne do walki z cyberprzestępczością, których zadaniem jest m.in. pomoc w realizacji spraw wymagających odpowiedniej wiedzy informatycznej oraz narzędzi sprzętowo-programowych.

Drugim czynnikiem mającym wpływ na sposób zabezpieczania danych informatycznych są parametry techniczne nośników danych, zastanych na miejscu prowadzenia czynności procesowych. Wzrost pojemności nośników postępuje zdecydowanie szybciej niż możliwych do osiągnięcia prędkości ich kopiowania za pomocą odpowiednich narzędzi. W konsekwencji może to powodować sytuacje, w których wykonanie procesowych kopii kilku nośników o dużej pojemności może trwać nawet dziesiątki godzin, a w przypadku ich uszkodzeń, nawet kilka dni, z czego zapewne nie zdają sobie sprawy osoby wnoszące skargi na Pana ręce. Zasadnym w tej sytuacji jest postawienie pytania, co byłoby bardziej uciążliwe dla osób, u których przeprowadzane są czynności procesowe – zatrzymanie sprzętu i zbadanie go przez specjalistę w terminie późniejszym czy wykonywanie kopii danych przez tak długi okres na miejscu prowadzonych czynności.

Kolejnym czynnikiem, właściwie wykluczającym możliwość wykonania kopii danych i pozostawienia sprzętu w dyspozycji osób zainteresowanych, jest sposób zabezpieczenia dostępu do danych zawartych na nośnikach. Niektóre rozwiązania wykorzystują do szyfrowania zawartości dysków moduł sprzętowy, umiejscowiony na płycie głównej komputera (a więc poza nośnikiem danych). Odszyfrowanie danych zawartych na dysku jest możliwe tylko za pomocą modułu, który je zaszyfrował, stąd konieczność zabezpieczenia całego komputera.

Kwestia możliwości dokonania wstępnego przeszukania urządzenia zawierającego dane informatyczne lub systemu informatycznego - przy użyciu odpowiedniego oprogramowania - w celu znalezienia danych mogących stanowić dowód w sprawie, generuje podobne problemy do tych wynikających z rosnącej pojemności nośników. Także i tu występuje uciążliwość wynikająca z długotrwałości weryfikacji cyfrowego materiału dowodowego. Poza tym czynność taka odbiega od przyjętych tzw. dobrych praktyk informatyki śledczej, mówiących m.in. o tym, że jeśli to tylko możliwe wszelkie czynności powinny być przeprowadzane na odpowiednio wykonanych kopiach nośników i w zasadzie powinna dotyczyć tylko najprostszych przypadków.

Podsumowując pragnę jeszcze raz zaznaczyć, że Policja – poza sytuacjami opisanymi powyżej, stanowiącymi przeszkodę w realizacji postulatów zawartych w Pana piśmie – z pewnością będzie nadal zmierzać w kierunku stosowania rozwiązań zmniejszających uciążliwości związane z przeprowadzaniem czynności zabezpieczania cyfrowego materiału dowodowego.

z poważaniem

Komendant Główny Policji

nadinsp. dr Jarosław Szymczyk