RZECZPOSPOLITA POLSKA
PROKURATOR GENERALNY

Warszawa, dnia 29.10. 2014 r.

PG I A 021/1/14

Państwo
Prokuratorzy Apelacyjni
WSZYSCY

Na podstawie art. 10 ust. 1 ustawy o prokuraturze (Dz.U. t.j. z 2011r. Nr 270 poz. 1599 ze zm.) w sprawach związanych z przestępstwami z nienawiści dokonywanymi z wykorzystaniem Internetu polecam stosowanie się do następujących zasad:

I. Zagadnienia ogólne

1. W toku dokonywanych czynności należy uwzględnić wytyczne w sprawie udziału prokuratora w sprawach o przestępstwa prywatnoskargowe z dnia 29 października 2012r., PG VII 021/24/12 oraz w zakresie prowadzenia postępowań o przestępstwa z nienawiści z dnia 26 lutego 2014r., PG VII G 021/54/13.

2. Wykorzystanie Internetu do popełniania przestępstw z nienawiści jest szczególnie niebezpieczne z uwagi na trudności w identyfikacji sprawców oraz zasięg przekazywanej informacji, zarówno w odniesieniu do liczby osób pokrzywdzonych, jak ewentualnego inspirowania dalszych działań w stosunku do pokrzywdzonych przez inne osoby, dlatego też w szerszym zakresie należy podejmować czynności z urzędu.

3. Argumentacja prokuratora w uzasadnieniach powinna odwoływać się również do orzeczeń Europejskiego Trybunału Praw Człowieka i ich uzasadnień, tak w odniesieniu do nowych technologii, jak i mowy nienawiści. Orzeczenia te są dostępne także za pośrednictwem stron internetowych Ministerstwa Sprawiedliwości w zestawieniach tematycznych.
(http://bip.ms.gov.pl/pl/prawa-czlowieka/europejski-trybunal-praw-czlowieka/opracowania-i-analizy-standardy-w-zakresie-ochrony-praw-czlowieka/wybrane-zestawienia-tematyczne-orzecznictwa-etpcz/)

4. W toku podejmowanych czynności należy rozważać odpowiedzialność usługodawców w rozumieniu ustawy z dnia 18 lipca 2002r. o świadczeniu usług drogą elektroniczną (Dz. U. t.j. z 2013r. poz. 1422), przy uwzględnieniu okoliczności wyłączających odpowiedzialność karną, cywilną i administracyjną, które zostały wskazane w art. 12-14 tej ustawy.

5. Stwierdzając, iż zostały naruszone przepisy Działu VIII ustawy z dnia16 lipca 2004r. Prawo telekomunikacyjne (Dz. U. t.j. z 2014r. poz. 243), zwłaszcza w zakresie przechowywania i udostępniania uprawnionym organom danych i informacji właściwy prokurator apelacyjny lub okręgowy niezwłocznie zawiadamia o tym Prezesa UKE (art. 209 ust 1 pkt 10 i art. 210 ust. 1 cyt. ustawy Prawo telekomunikacyjne).

II. Zabezpieczenie i utrwalenie dowodów

1. W toku przesłuchania pokrzywdzonego należy uwzględnić, czy treści i obrazy stanowiące przedmiot postępowania wpłynęły na zachowanie innych osób, nie tylko w aspekcie realizacji znamion czynów zabronionych (podżeganie do znieważenia, naruszenia nietykalności cielesnej itp.), ale także szerzenia mowy nienawiści tworząc poczucie zagrożenia, co może przyczynić się do zapewnienia skuteczności wniosków o pomoc prawną kierowanych do USA (szersze ujęcie groźby, niż normatywne na gruncie polskiego prawa karnego), a nadto powinno znaleźć odzwierciedlane w uzasadnieniu stopnia szkodliwości społecznej czynu.

2. Utrwalenie treści i obrazów powinno nastąpić poprzez skopiowanie plików źródłowych oraz ekranów na nośnik jednokrotnego zapisu z ich ewentualnym wydrukiem, a w przypadku gdy czynności takie wcześniej dokonywał pokrzywdzony - także poprzez skopiowanie dokonanych przez niego czynności.

3. W przypadku osoby wysyłającej wiadomości elektroniczne do zindywidualizowanych użytkowników niezbędne jest nie tylko ustalenie użytkownika skrzynki pocztowej lub/i numeru urządzenia mobilnego, ale także IP i ewentualnie - odwzorowania binarnego logów u ISP (Internet Service Provider).

4. Nie można poprzestać na samym uzyskaniu IP, bez zabezpieczenia kopii źródłowych logów dotyczących jego nadania i wykorzystywania, zwłaszcza w przypadku, gdy dostęp do Internetu z danego urządzenia nie ma stale przypisanego IP, albowiem może to uniemożliwić późniejszą weryfikację dokonanych ustaleń (wydruk nie zastąpi binarnego odwzorowania zapisów logów, albowiem jest tylko dowodem, tego co wydrukowano). Szczególnie istotne jest skopiowanie logów z serwerów proxy, w zakresie umożliwiającym identyfikację konkretnego urządzenia, który za jego pośrednictwem uzyskuje adres IP i na tej podstawie wyselekcjonowanie jednostek, które muszą być poddane dalszym czynnościom.

5. Dokonywanie czynności powinno zapobiegać naniesieniu zmian w systemach, z których pobierane są dane, a tym samym wymaga stosowania tzw. blokerów oraz innych urządzeń i programów, które powinny być wskazane w protokole z dokonania czynności.

6. Realizacja czynności związanych z koniecznością kontaktu ze sprzętem (hardware) powinna uwzględniać podstawowe zasady dotyczące

zabezpieczania dowodów rzeczowych (czynności powinny być realizowane w rękawiczkach, opisywane i w miarę możliwości rejestrowane za pomocą urządzeń utrwalających obraz i dźwięk) z ewentualnym następczym zleceniem badania zabezpieczonych śladów kryminalistycznych, celem ustalenia użytkowników urządzenia.

7. W przypadku wątpliwości związanych z identyfikacją sprzętu i jego użytkownika niezbędne jest podjęcie czynności zmierzających do ustalenia, czy z tego samego IP, w zbliżonym czasie były dokonywane inne czynności – przykładowo: logowanie do portali społecznościach, banków itp. stron, z których korzystanie umożliwia indywidualna nazwa użytkownika (login) i hasło, a także czy na innych stronach, w zbliżonym czasie występowała osoba posługująca się tym samym pseudonimem (nick'iem).

8. Przeszukanie zawartości urządzeń pracujących w sieci i wykorzystywanych do przekazywania treści i obrazów stanowiących przedmiot postępowania, a w tym skrzynek pocztowych powinno następować stosownie do art. 236a kpk (w zw. z art. 219 kpk), a w przypadku braku możliwości ustalenia osoby lub podmiotu dysponującego zasobami lub urządzeniem, zarządzenie o doręczeniu odpisu postanowienia powinno być wydane niezwłocznie po ich ustaleniu. Przeszukanie to może się odbywać także w drodze udostępnienia przez operatora określonych zasobów (zdalny pulpit, itp.).

9. Aktualnie obowiązujące przepisy uniemożliwiają - bez skierowania wniosku o pomoc prawną - dokonanie przeszukania na odległość w przypadku ustalenia, iż urządzenie lub zasoby znajdują się poza granicami kraju.

10. Bieżąca kontrola i utrwalanie informacji przekazywanych drogą elektroniczną może być realizowane stosownie do przepisów rozdziału 26 kpk.

11. W toku czynności zmierzających do dokonania ustaleń w Internecie należy uwzględnić uwarunkowania związane z funkcjonowaniem tzw. głębokiej (Deep Web) i ciemnej części sieci (Dark Web), które czasami traktowane są zamiennie lub różnie rozumiane, niemniej wydaje się, iż najwłaściwsze jest rozróżnienie ze względu na zawartość sieci, której sposób indeksacji nie pozwala na standardowe wyszukanie poszczególnych plików (Deep Web/Deepnet) oraz sieć zapewniającą w sposób zaawansowany animizację, chociażby w postaci sieci TOR (Dark Web/Darknet). W pierwszym przypadku wystarczające jest zastosowanie zaawansowanych metod wyszukiwania, z ewentualnym udziałem specjalistów. W drugim ustalenie IP, czy to samodzielnie, czy poprzez współpracę z ISP zazwyczaj nie jest możliwe. W takich przypadkach należy dokonywać czynności niestandardowych, licząc na błąd sprawcy, jak to miało miejsce w USA w sprawie zakończonej oskarżeniem R. Williama Ulbrichta, która dotyczy sklepu Jedwabny Szlak (Silk Road) zajmującego się transakcjami przestępczymi, w tym handlem narkotykami.
(http://www.fbi.gov/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-charges-against-three-individuals-in-virginia-ireland-and-australia-for-their-roles-in-running-silk-road-website).

12. Zabezpieczenie dowodów powinno nastąpić przy udziale specjalisty i w miarę możliwości z udziałem pokrzywdzonego, a dokumentem sporządzanym z tej czynności musi być protokół (art. 143§1 pkt 3 oraz 6-7), w którym niezbędne jest odnotowanie parametrów sprzętu, oprogramowania, sposobu dokonywania utrwalenia oraz indywidualne oznaczenia nośnika, na którym dane i informacje zostały utrwalone.

III. Czynności pozakarne

1. W przypadku postępowania przygotowawczego wszczętego o przestępstwo ścigane z oskarżenia publicznego prokurator z urzędu powinien na podstawie art. 14 ustawy z dnia 18 lipca 2014r. o świadczeniu usług drogą elektroniczną (Dz. U. t.j. z 2013r. poz. 1422) skierować do osoby świadczącej usługi elektroniczne urzędowe zawiadomienie, wskazujące na bezprawny charakter

danych zamieszczonych w Internecie przez tegoż usługodawcę, o ile wcześniej dane te nie zostały usunięte.

2. Zgodnie z § 366 ust. 2 Regulaminu urzędowania powszechnych jednostek organizacyjnych prokuratury, prokurator samodzielnie ocenia przesłanki określone w art. 7 kpc uzasadniające żądanie wszczęcia postępowania cywilnego lub zgłoszenia w nim udziału.

3. W sprawach o przestępstwa ściągane z oskarżenia prywatnego, w których prokurator odmówił wszczęcia postępowania z urzędu oraz w przypadku stwierdzenia braku podstaw do podjęcia przez prokuratora działań pozakarnych, uzasadniając na piśmie swoje stanowisko prokurator powinien poinformować pokrzywdzonego o środkach prawnych o charakterze cywilnym lub administracyjnym, które może podjąć samodzielnie. W szczególności należy wskazać pokrzywdzonemu na przysługujące mu uprawnienia:
   - zawiadomienia usługodawcy o bezprawnym charakterze danych przez niego publikowanych i żądanie ich usunięcia (art. 14 ust. 1 o świadczeniu usług drogą elektroniczną oraz art. 24 kc),
   - uzyskania danych osoby lub podmiotu, któremu przydzielono dany adres IP (wyroki Naczelnego Sądu Administracyjnego z dnia 21 lutego 2014r., sygn. akt I OSK 2324/10 oraz dnia 27 czerwca 2014r., sygn. akt II SA/Wa 643/14),
   - dochodzenia roszczeń na podstawie art. 23 i 448 kc.

4. Na podstawie art. 8§1 ustawy z dnia 30 sierpnia 2002r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. t.j. z 2012 r. poz. 279 ze zm.) zasadne jest na wniosek pokrzywdzonych - zgłoszenie przez prokuratora udziału w postępowaniach przed sądami administracyjnymi, toczącymi się w związku ze skargami osób pokrzywdzonych przestępstwami internetowymi, którym decyzją ostateczną odmówiono ujawnienia danych sprawców tych przestępstw.

5. W przypadku ustalenia w toku postępowania przygotowawczego, że treść lub obraz stanowiące przedmiot postępowania zostały umieszczone na stronie partii politycznej lub stowarzyszenia, bądź na tej stronie znajduje się link (w tym tzw. głęboki – wyrok Sądu Apelacyjnego w Krakowie z dnia 20 lipca 2004r., sygn. akt I ACa 564/04, LEX 142138) umożliwiający otwarcie strony z tym obrazem lub treścią, a także w sytuacji, gdy w obrazie lub treści umieszczono odwołanie do symboli lub programu partii, bądź stowarzyszenia prokurator powinien dokonać oceny, czy nie zachodzą okoliczności uzasadniające uruchomienie procedur prowadzących do delegalizacji partii lub stowarzyszeń określonych w ustawie z dnia 27 czerwca 1997r. o partiach politycznych (Dz. U. t.j. z 2011r., Nr 155 poz. 924) i ustawie z dnia 7 kwietnia 1989r. Prawo o stowarzyszeniach (Dz. U. t.j. z 2001r. Nr 79 poz. 855 ze zm.). Należy ustalić, czy działania osób, którym zarzucono popełnienie przestępstw z nienawiści miały charakter incydentalny, czy też stanowiły swoistą manifestację celów i założeń przyjętych w działalności konkretnych organizacji. Podjęcie czynności delegalizacyjnych będzie bowiem uzasadnione i skuteczne jedynie wówczas, gdy zostanie udowodnione, że wymienione partie lub stowarzyszenia w swoich programach odwołują się do totalitarnych metod i praktyk działania, nazizmu, faszyzmu i komunizmu albo, że ich program zakłada lub dopuszcza nienawiść rasową lub narodowościową. W przypadku:

   - zebrania materiału dowodowego uzasadniającego w ocenie prokuratora wystąpienie o delegalizację partii politycznej z powodu naruszenia art. 13 Konstytucji RP, materiały te wraz ze stosowym pismem należy skierować do Prokuratora Generalnego, który zgodnie z wymienioną ustawą jest uprawniony do wystąpienia do Trybunału Konstytucyjnego o zbadanie zgodności działalności partii politycznej z Konstytucją;

   - stwierdzenia rażącego lub uporczywego naruszenia prawa przez stowarzyszenie, zarówno organ nadzoru (starosta właściwy ze względu na miejsce rejestracji stowarzyszenia), jak i prokurator rejonowy, są uprawnieni do wystąpienia do sądu rejonowego z wnioskiem o rozwiązanie stowarzyszenia. Prokurator rejonowy powinien powiadomić o swoich ustaleniach

uzasadniających delegalizację stowarzyszenia organ nadzoru, a jeśli organ ten nie podejmie działań skorzystać z posiadanych uprawnień i wystąpić do sądu rejonowego ze stosownym wnioskiem.

IV. Współpraca

1. W planowaniu i realizacji czynności należy uwzględniać współpracę także z innymi instytucjami i organami państwowymi oraz pozarządowymi, a także korzystać ze zbiorów dobrych praktyk, nie tylko publikowanych w kraju. Przykładowo można wskazać opublikowane m.in. przez Home Office opracowanie zatytułowane „Hate Crime. Delivering a quality services. Good practice and tactical guidance" (marzec 2005).
(http://www.bedfordshire.police.uk/pdf/tacticalguidance.pdf)

2. W przypadku trudności w identyfikowaniu sprawców oraz konieczności zebrania dowodów poza granicami kraju należy rozważyć zlecenie Policji dokonanie stosownych ustaleń we współdziałaniu z Europolem, bądź też zwrócić się o pomoc do Europolu za pośrednictwem Eurojust'u m.in. w aspekcie Komunikatu Wspólnego 7 lutego 2013r. „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń". Wskazać bowiem należy, iż dnia 11 stycznia 2013r. zostało utworzone Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3),. Centrum to jest odpowiednikiem Narodowego Centrum do Walki z Przestępczością Białych Kołnierzyków w USA (NW3C). Co prawda zajmuje się ono przede wszystkim cyberprzestępczością ekonomiczną, niemniej również przypadkami rasizmu i ksenofobii.
(http://www.europarl.europa.eu/meetdocs/2009_2014/documents/join/com_join(2013)0001_/com_join(2013)0001_pl.pdf)
(https://www.europol.europa.eu/content/megamenu/european-cybercrime-centre-ec3-1837)

3. Kierowanie wniosków o udzielenie pomocy prawnej do USA powinno być poprzedzone analizą możliwości ich realizacji, w której pomocne będzie dostępne w Internecie opracowanie „Investigating hate crimes on the Internet. Technical Assistance Brief", którego współwydawcą jest m.in. Departament Sprawiedliwości USA. Nadto szereg informacji dotyczących przestępstw z nienawiści umieszczonych jest na stronach Federalnego Biura Śledczego i Departamentu Sprawiedliwości USA.

(http://www.partnersagainsthate.org/publications/investigating_hc.pdf)

A. Seremet

Andrzej Seremet