Alexander Dix

# Przestępczość w środkach informacji i komunikacji.
## Dwanaście tez, wyrażających punkt widzenia Krajowego Pełnomocnika ds. Ochrony Danych

„Kriminalistik" 2004, nr 2, s. 81–85

W społeczeństwie informacyjnym podstawowym prawem człowieka jest tajemnica komunikacyjna. Chroni ona nie tylko interes jednostki, ale w równym stopniu także całej społeczności. Wszelkie jej ograniczenia muszą być zgodne z konstytucją. Rutynowe przechowywanie na zapas wszystkich danych o połączeniach w celu ułatwienia przyszłego postępowania karnego byłoby – zdaniem autora – niezgodne z konstytucją. Nowe wynalazki techniczne, jak np. identyfikacja częstotliwości radiowych (RFID), wymagają ponownego określenia stanu równowagi między wolnością (czyli ochroną sfery prywatności) i bezpieczeństwem, z zachowaniem zasady proporcjonalności. W związku z przewidywaną rewizją przepisów dotyczących nadzoru telekomunikacyjnego przedstawiono poniżej w dwunastu punktach poglądy Pełnomocnika do spraw Ochrony Danych.

Dyskusja nad kwestią równowagi między wolnością i bezpieczeństwem nasiliła się szczególnie po zamachu z 11 września. W związku z tym często cytuje się – na ogół niedokładnie – wypowiedź jednego z ojców założycieli Stanów Zjednoczonych Benjamina Franklina, która brzmi: „Ten, kto jest gotów zrezygnować w znaczącym stopniu z wolności, aby uzyskać chwilowe bezpieczeństwo, nie zasługuje ani na wolność, ani na bezpieczeństwo".

Nawet jeżeli moralizujący podtekst tego zdania może być irytujący, wydaje się ono warte zastanowienia w kontekście współczesnej techniki informacji i komunikacji.

**1.** Tajemnica telekomunikacji jest podstawowym prawem człowieka w społeczeństwie informacyjnym. Federalny Trybunał Konstytucyjny w swoich orzeczeniach podkreśla stale, że korzystanie z mediów komunikacyjnych w sensie ogólnym (a więc zarówno w odniesieniu do treści, jak i okoliczności) musi mieć w miarę możliwości zapewniony charakter poufny. W związku z tym warunki swobody telekomunikacji powinny podlegać ochronie. Ochrona ta musi obejmować także korzystanie z usług telefonicznych i medialnych (szczególnie internetowych), które uważa się za podstawę telekomunikacji.

**2.** Podobnie jak prawo do ochrony danych, także tajemnica telekomunikacyjna leży nie tylko w interesie jednostek, ale całego społeczeństwa. Każdy tajny nadzór nad środkami łączności zakłóca normalną komunikację wewnątrzspołeczną i obniża jej jakość, a także narusza obiektywizm telekomunikacji i jakość przekazu oraz wywołuje u obywateli niemiłe uczucie, że są podsłuchiwani. Mówi się o tym w orzeczeniu Trybunału Konstytucyjnego z marca 2003 r. Stwierdzenia te – mimo zagrożeń spowodowanych przez międzynarodowy terroryzm i nowych form przestępczości komputerowej, w obliczu coraz większego rozpowszechnienia pornografii dziecięcej i treści rasistowskich w Internecie – nic nie tracą ze swojej słuszności. Jeżeli posługujemy się kategorią „subiektywnego poczucia bezpieczeństwa" (a wydaje się to całkiem uprawnione), powinniśmy do tego dodać wymienione w orzeczeniu Trybunału Konstytucyjnego „uczucie, że jest się podsłuchiwanym".

Trzeba się zastanowić, czy szeroko stosowane przez państwo środki nadzoru podwyższają subiektywne poczucie bezpieczeństwa – czy też przeciwnie.

**3.** Poufność telekomunikacji wcale nie jest nienaruszalna. Ograniczenia jej są dopuszczalne, jeżeli w sposób uprawniony służą wyjaśnianiu i ści-

ganiu ciężkich przestępstw, przy czym lista tych przestępstw stale się wydłuża. Jak dotąd, nie było jeszcze wypadku, żeby w krytycznej sytuacji odmówiono założenia podsłuchu. Trudno się jednak oprzeć wrażeniu, że prawie w każdym przypadku nowej formy przestępczości, którą uznaje się za szczególnie szkodliwą społecznie, bardzo szybko pojawia się wniosek o ograniczenie tajemnicy telekomunikacyjnej. Najnowszymi tego przykładami są korupcja i „praca na czarno". Ograniczenie tajemnicy telekomunikacyjnej – jeżeli ma służyć niesprecyzowanym celom przyszłego dochodzenia – jest sprzeczne z konstytucją. Trybunał Konstytucyjny uznał, że musi zaistnieć konkretne podejrzenie o dokonanie poważnego przestępstwa i stwierdzone zostaną niewątpliwe fakty, pozwalające uznać, że nadzorowana osoba – o ile nie jest identyczna ze sprawcą – pełni wobec niego funkcję pośrednika dostarczającego informacji.

**4.** Z orzeczenia Trybunału Konstytucyjnego można wyciągnąć tylko taki wniosek, że przy braku konkretnego podejrzenia nadzór telekomunikacyjny i w Internecie na zapas jest niezgodny z ustawą zasadniczą. W odniesieniu do nadzoru i rejestracji treści rozmów nikt tego dotychczas nie kwestionował. Jednak najnowsze propozycje senackiej Komisji Prawa w ramach projektu zmian ustawy telekomunikacyjnej przewidują, że providerzy sieci mają być zobowiązani do przechowywania wszelkich danych o połączeniach przez pół roku. Już samo przechowywanie, a co dopiero wykorzystanie danych dotyczących bliższych okoliczności wszystkich połączeń komunikacyjnych (kto, kiedy, jak długo i skąd z kim się komunikował), pomijając trudności techniczne, stanowi wyjątkowo duże naruszenie tajemnicy komunikacji. Konstytucja przewiduje rozróżnienie między nadzorowaniem treści rozmów i nadzorowaniem okoliczności komunikowania się i to ostatnie uważane jest za ciężkie naruszenie podstawowych swobód obywatelskich. Użytkownik nowoczesnych sieci komunikacyjnych nie może być traktowany jedynie jako obiekt przetwarzania danych, służący bliżej nieokreślonym celom instytucji państwa.

**5.** Rutynowe, nie oparte na podejrzeniu o przestępstwo przechowywanie wszystkich danych o połączeniach, które miałoby na celu ułatwienie ewentualnego postępowania karnego w przyszłości byłoby nie tylko sprzeczne z konstytucją, ale także niezgodne z Europejską Konwencją Praw Człowieka (art. 8). Odpowiednio do tego zakłada się, że ograniczanie prawa do prywatności i tajemnicy komunikacji byłoby uwarunkowane „pilną potrzebą społeczną". Abstrakcyjna możliwość, że dostęp do przechowywanych na skalę masową danych o połączeniach może w przyszłości ułatwić postępowanie karne – to jednak za mało. Nie wszystko, co jest potrzebne do zwalczania przestępczości i ścigania sprawców, jest równie niezbędne do funkcjonowania demokratycznego społeczeństwa i przez to uzasadnione. Wymagany przez Europejski Trybunał Praw Człowieka warunek przewidywalności ingerencji państwa nie będzie spełniony, jeżeli bezwarunkowo każde skorzystanie z sieci informacyjnych i komunikacyjnych będzie rejestrowane przez organy państwa lub na ich zlecenie. Użytkownicy sieci nie mogliby wówczas przewidzieć, w jakich sytuacjach muszą się liczyć z możliwością podsłuchu. Pewność, że dla celów bezpieczeństwa państwa każda forma komunikacji będzie rejestrowana, nie jest tym samym, co przewidywalność zgodna z konwencją. Korzystanie ze wszystkich danych niezależnie od tego, w jakim celu zostały one zgromadzone (np. w celach obrachunkowych), jest sprzeczne nie tylko z konstytucją, ale także z Konwencją Praw Człowieka.

**6.** W sieciach telekomunikacyjnych obserwuje się coraz większą personalizację użytkowników. Zjawisko to jest następstwem rozwoju techniki komputerowej i wprowadzania „inteligentnych" urządzeń do życia codziennego, zintegrowanych np. z częściami odzieży („wearable computing", „wearware"). Mikrochipy i sensory wyposażone w pasywną lub aktywną funkcję pojemnościową (RFID – Radio-Frequency Identification – identyfikacja częstotliwości radiowych) mogą rejestrować każdy ruch człowieka. Aktualnie obsługa stanowisk wyposażona jest w mobilną sieć łączności radiowej. Wkrótce będą do dyspozycji ulepszone możliwości identyfikacji, które technicznie będą wspomagać samookreślenie informacyjne. Nie tylko reakcja pracodawcy na atak terrorystyczny 11 września, ale także ten kierunek rozwoju techniki wiążą się z potrzebą określenia na nowo równowagi między wolnością (ochroną sfery prywatności) i bezpieczeństwem. Przy tym widać coraz wyraźniej, że ochrona prywatności i prawo do poufności komunikacji zyskują na znaczeniu.

**7.** Sieci telekomunikacyjne nie są obszarem bezprawia. To, co jest zabronione lub karalne offline, również nie jest legalne online. Dlatego zwalczanie przestępczości musi być możliwe także ponad granicami państw w światowych sieciach. Trzeba jednak ściśle przestrzegać

zasady proporcjonalności. Federalny minister spraw wewnętrznych porównał wynalazek Internetu z narodzinami sztuki drukarskiej. Porównanie to jest trafne także z innego względu. Czy istnieją powody, aby wymianę informacji online kontrolować bardziej dokładnie niż offline, czyli w świecie realnym? Zdaniem autora – nie. Przedstawiciele władz bezpieczeństwa żądają zrównania ich uprawnień w cyberprzestrzeni z tymi, które mają w świecie offline. Żądanie takie wydaje się w zasadzie uprawnione, jednak nieuzasadnione jest domaganie się uprawnień, dla których nie ma odpowiedników w świecie analogowym. Zrównanie musi tu działać w obie strony. To, co jest dozwolone offline, a mianowicie zasadnicza swoboda ruchów bez obowiązku każdorazowego legitymowania się, musi być możliwa także online. Jeżeli ktoś kupuje książkę lub gazetę i płaci gotówką, nie musi w świecie realnym tego udowadniać. Pełny nadzór wszystkich ruchów i aktywności życiowej byłby sprzeczny z konstytucją nawet wtedy, gdyby był technicznie możliwy. Kompletna i nie wymagająca zezwoleń rejestracja połączeń w sieci WWW byłaby nieuzasadnionym naruszeniem swobody poglądów i wolności informacji.

Nieco inaczej można traktować spotkania na czacie, w których śledczy może uczestniczyć na tych samych warunkach (czyli pod pseudonimem), co inni użytkownicy Internetu. Tak, jak w realnym świecie, można tu mówić o działaniu agenta – prowokatora, ale nie jest to istotny problem dla ochrony danych. Także zapobiegawczemu przeglądaniu oferty informacyjnej na stronach WWW, które od pewnego czasu praktykowane jest w BKA, nie można w zasadzie nic zarzucić. Natomiast rutynowe i niewymagające zezwoleń rejestrowanie na zapas danych o połączeniach w celu ewentualnego wykorzystania ich w przyszłych dochodzeniach oznaczałoby niepożądaną zmianę charakteru sieci. Żaden pełnomocnik ochrony danych, który spotkałby się z takim żądaniem, nie zgodziłby się na to, co w istocie jest budowaniem państwa policyjnego. Prawodawca nie powinien nadawać uprawnień, które przekraczałyby dopuszczalną miarę.

**8.** Wyniki badań porównawczych nad międzynarodowym prawem karnym zmuszają do wprowadzania zmian w systemie nadzoru komunikacji. Wzrost liczby dochodzeń, w których zarządzono nadzór telekomunikacyjny od 1990 do 2000 r. był sześciokrotny i nie można tego wyjaśnić jedynie rozpowszechnieniem telefonii komórkowej. Nadzór telekomunikacyjny staje się coraz częściej standardowym środkiem dochodzenia. Przewidziana w kodeksie postępowania karnego proporcja wyjątków od reguły w praktyce została postawiona na głowie i to na dwa sposoby: nadzór telekomunikacyjny zbyt często zarządza się przed dokładniejszym sprawdzeniem, czy nie wystarczyłyby tu mniej drastyczne środki, a z drugiej strony, przewidziany prawem jako wyjątkowy środek pilny nakaz prokuratury (akceptacja sądu tylko w określonych sytuacjach) coraz częściej staje się regułą. Tylko w 17% przypadków założenie podsłuchu pomogło w śledztwie; 70% posiadaczy telefonów, którym założono podsłuch, nie zostało o tym poinformowanych.

**9.** Zapowiedziana przez ministra spraw wewnętrznych RFN rewizja nadzoru telekomunikacyjnego zdaniem Pełnomocnika Ochrony Danych powinna uwzględniać następujące zagadnienia:

- Statystyka nadzoru musi być bardziej transparentna, a naukowa ocena jego skuteczności musi zostać poszerzona i rozwinięta: prawodawca powinien dopasować regulacje prawne do wyników tej oceny.
- Nadzór sędziowski nie powinien zostać osłabiony, a przeciwnie – musi być wzmocniony.
- Szczególnie w przypadkach pilnych zgłoszeń potrzeby założenia nadzoru, które nie tylko są coraz częstsze, ale stają się wręcz regułą, prawodawca powinien zastrzec, aby wyniki tych czynności podlegały ocenie dopiero po kontroli sędziowskiej.
- Należy zwrócić uwagę na poprawę jakości sędziowskich decyzji, ponieważ braki w uzasadnieniu często prowadzą do zakazu wykorzystania dowodu.
- Zadania sędziego śledczego powinny się koncentrować na niewielkiej liczbie osób.
- Trzeba krytycznie przejrzeć katalog przestępstw i prawnie unormować próg interwencji.
- Należy sprecyzować i zapewnić realizację obowiązku poinformowania we właściwym czasie wszystkich znanych uczestników podsłuchanej rozmowy o fakcie jej zarejestrowania.
- Podsłuchane rozmowy między podejrzanym i świadkiem uprawnionym do odmowy zeznań w zasadzie nie powinny być wykorzystywane.
- Dane z podsłuchu telefonicznego muszą być oznakowane; należy zapewnić niezbędne ku temu warunki techniczne.
- Najdłuższy czas nadzoru telekomunikacyjnego nie powinien przekraczać dwóch miesięcy.
- Kody PIN i PUK objęte są tajemnicą telekomunikacyjną, ich naruszenie może nastąpić tylko pod tym sa-

mym warunkiem, co odsłuchanie treści rozmowy.

● Propozycję przymusowej identyfikacji nabywców telefonów komórkowych na karty prepaid należy odrzucić. Niedawno Federalny Sąd Administracyjny potwierdził, że obowiązujące prawo telekomunikacyjne nie daje podstaw do zobowiązywania administratora sieci do wykonywania usług polegających na rejestracji danych – chyba że nie zostanie ona uprzednio dopuszczona przez Urząd Telekomunikacji. Tego rodzaju obowiązku prawodawca nie może też po prostu narzucić. Zresztą nie jest to sposób na niezawodną identyfikację wszystkich użytkowników telefonów komórkowych. Prowadziłoby to tylko do gromadzenia „na zapas" lub „na wszelki wypadek" olbrzymiej liczby danych – bez sensu ani pożytku. Nabywca telefonu nie zawsze jest identyczny z jego użytkownikiem. Prawdziwi przestępcy często posługują się osobami podstawionymi, a na celowniku służb dochodzeniowych znajdą się ojcowie rodzin, którzy kupują swoim dzieciom telefony na karty.

**10.** Dotychczas nie przedstawiono przekonujących powodów do udzielenia policji uprawnień do prewencyjnego nadzoru telekomunikacyjnego. Jako warunek uprawniający proponuje się powzięcie podejrzenia o przestępstwie, natomiast uprawnienie do tak ciężkiego naruszenia podstawowych praw obywatelskich wyjęto spod kontroli prokuratury i co więcej – w perspektywie próbuje się zlikwidować zasadę sędziowskiego zastrzeżenia, która mogłaby efektywnie skompensować utratę kontroli w przypadkach używania formularzy *in blanco*.

**11.** Wtargnięcia do sieci, infrastruktury i komputera (przestępczość komputerowa) mogą i powinny być dużo efektywniej niż dotychczas uniemożliwione lub utrudnione dzięki podwyższeniu poziomu zabezpieczeń technicznych (produkty, metody). Unia Europejska podejmuje w tym kierunku wzmożone wysiłki (powstanie Europejskiej Agencji Bezpieczeństwa Sieci ENISA). Zagrożenie bezpieczeństwa w Internecie zostało przekonująco opisane przez Helmbrechta i Brunsteina („Kriminalistik" 1/2004). Nie powinno się próbować kompensować zasadniczej niepewności tego medium przez nadmierny nadzór nad użytkownikami. Albo trzeba zdecydowanie podwyższyć bezpieczeństwo infrastruktury, albo nie korzystać z tej niepewnej infrastruktury – w każdym razie do niektórych celów. Jako przykład może tu posłużyć przetwarzanie niezakodowanych danych pacjentów na komputerach podłączonych do Internetu, co prowadzi bezpośrednio do złamania tajemnicy lekarskiej. Na tej samej zasadzie dane osobiste bez uzupełniających przedsięwzięć ochronnych nie powinny być narażone na dostęp osób nieuprawnionych w ogólnoświatowej sieci.

**12.** W państwie demokratycznym musi istnieć ochrona podstawowych praw człowieka, a więc prawo do poufności komunikacji musi być regułą, a jego naruszanie ograniczać się do pojedynczych uzasadnionych przypadków. Wyłącznie na podstawie faktu, że ktoś korzysta z sieci komunikacyjnej, państwo nie może traktować tego jako okazji do wszechstronnego nadzorowania jego wszystkich kroków i zachowań, bo w ten sposób każdy, kto z uprawnionych przyczyn będzie chciał się skomunikować z inną osobą, nie będąc nieustannie obserwowanym – będzie zmuszony do zrezygnowania z tej techniki. Utrata swobód obywatelskich byłaby równoważna z utratą bezpieczeństwa, a konkretnie oznaczałoby to niemożliwość bezpiecznego korzystania z sieci telekomunikacyjnych bez rejestracji i ściągania na siebie podejrzeń. Nie wolno dopuścić do tego, aby sieci informatyczne i komunikacyjne były nadzorowane z zasady, a „bezpieczne" były tylko kontakty osobiste.

**Oprac. Anna Henschke**