

Biznes nadzoru

10 stycznia 2013

Przez ostatnie dekady techniki kontroli nad ludźmi dynamicznie się rozwinęły. Globalny przemysł nadzoru przynosi rocznie 5 miliardów dolarów przychodu. Jego klienci mogą wybierać z szerokiej palety technik: od złośliwego oprogramowania, które infekuje komputer, pozwalając na śledzenie każdego ruchu wykonywanego na klawiaturze, po systemy do monitorowania ruchu w kablach światłowodowych, dzięki czemu kontroli podlega komunikacja wszystkich odbiorców usług przez nie dostarczanych (np. Internetu).

Międzynarodowy handel technologią służącą do inwigilacji stwarza poważne wątpliwości natury etycznej. Kiedy tego typu trafiają w ręce represyjnych reżimów, otwierają pole do naruszeń wolności słowa, tłumienia protestów czy represjonowania opozycjonistów. Różne techniki nadzoru stają się wówczas dokładnie tym samym, czym były dotychczas karabiny i bomby. Niestety przepisy umożliwiające eksport oprogramowania (zwykle rozumianego jako kompleksowa usługa obejmująca instalację, dostosowanie do potrzeb klienta i serwis) nie nadążają za rozwojem technologicznym, a producenci, mając na uwadze przede wszystkim własny zysk, nie weryfikują celów, jakim będą służyć ich produkty.

Państwa europejskie i USA eksportują produkowane przez siebie systemy między innymi do Turkmenistanu, Syrii, Maroka czy Egiptu – krajów, w których prawa człowieka są nagminnie łamane. Niektóre rządy wręcz zachęcają swoje firmy do takiego handlu poprzez stosowanie różnych gwarancji kredytowych dla eksporterów.

Już w 1995 roku brytyjska organizacja Privacy International (PI) opublikowała pierwszy raport, który przedstawiał ówczesną sytuację międzynarodowego obrotu technikami nadzorczymi. Jednak od tego czasu sytuacja diametralnie się zmieniła, a

przypadki nieetycznych praktyk tylko przybrały na sile. PI rozpoczęła badania branży technologii nadzoru, które pozwolą ocenić, jak wygląda ona dziś. Przyczynkiem do badań była m.in. nagłośniona niedawno przez PI sprawa firmy Gamma International, produkującej oprogramowanie do podsłuchiwania rozmów telefonicznych, przechwytywania SMS-ów i maili. Brytyjscy aktywiści oskarżają ją o eksportowanie, z naruszeniem prawa, swoich produktów do krajów łamiących prawa człowieka (Egipt, Turkmenistan czy Bahrajn). Brytyjskie władze potwierdziły, że prowadzą już kontrolę działalności tej spółki.

Również politycy europejscy zaczynają zauważać skalę problemu. Pod koniec grudnia Parlament Europejski przyjął rezolucję wzywającą do wprowadzenia zakazu eksportu technologii i usług informatycznych do państw rażąco naruszających prawa człowieka. Pomimo że regulacja ma niewiążący charakter, stanowi ważny polityczny sygnał dla rządów wszystkich krajów Unii Europejskiej. Z kolei europejska komisarz ds. agendy cyfrowej – Neelie Kroes zapowiedziała, że firmy powinny ponosić odpowiedzialność prawną i etyczną za sprzedaż narzędzi nadzorczych do krajów niedemokratycznych.

Niedawno francuska sekretarz stanu ds. gospodarki cyfrowej Fleur Pellerin, potwierdziła, że również Paryż przyjmie odpowiednie przepisy w tym zakresie. W podobnym duchu wypowiedział się niemiecki szef dyplomacji Guido Westerwelle. Polskie władze, jak dotąd, nie przedstawiły żadnego stanowiska w tej sprawie. Tymczasem sytuacja polskiego biznesu nadzoru nie jest jeszcze nawet dobrze rozpoznana. Według informacji opublikowanych dotychczas przez PI, w naszym kraju działa przynajmniej jedna firma oferująca oprogramowanie służące inwigilacji.

Z perspektywy globalnej kontrowersje wokół eksportu technologii nadzoru zmierzają już do punktu krytycznego. Nie ulega wątpliwości, że państwa demokratyczne, w tym również Polska, powinny przyjąć zasady ścisłej kontroli dotyczące

rozwoju tej gałęzi gospodarki. W krajach, gdzie możliwe są tortury i uwięzienie bez wyroku sądu, a polityczne zabójstwa należą do codzienności, technologie przeznaczone do inwigilacji zagrażają życiu aktywistów i dysydentów. Szpiegowskie oprogramowanie czy systemy podsłuchowe mogą stać się takim samym zagrożeniem dla praw człowieka i życia ludzkiego jak tradycyjna broń. Z drugiej strony otwarte pozostaje niełatwe pytanie, jak ukształtować przepisy ograniczające rozprzestrzenianie i eksport tego typu technologii tak, aby nie ograniczały wolności słowa, która w dobie Internetu wyraża się także poprzez wolność programowania.

Opracowanie: Jędrzej Niklas, Katarzyna Szymielewicz

Źródło: [Fundacja Panoptikon](#)