Security, Economy & Law
Nr 2/2020 (XXVII), (50–60)
DOI: 10.24356/SEL/27/4

INWIGILACJA JAKO ŹRÓDŁO ZAGROŻEŃ CHRONIONYCH OSÓB

INVIGILATION AS A SOURCE OF THREATS TO PROTECTED PERSONS

Krystian Krupa

ABSTRACT
The purpose of the paper is to characterize surveillance activities and threats that may result from them, and to discuss concisely anti-surveillance devices and behaviours. First, the historical outline of the phenomenon of surveillance is presented, as well as its past and present causes. Three types of detective inquiry are also discussed: white, grey and black. Then, technical and physical threats concerning surveillance, from the protected persons' perspective, are indicated. Finally, the author presents major anti-surveillance activities related to technical and physical protection. This results in a conclusion that a good protection plan for persons should primarily include all preparatory and preventive activities as well as the usage of anti-surveillance devices so as to prevent the leakage of sensitive information and the emergence of threat to life or property. In order to effectively counteract threats resulting from surveillance, it is necessary to use both appropriate technical equipment, knowledge, and often also physical abilities.

* Lic. Krystian Krupa, Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie; correspondence address: Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, Krupnicza 3, 31-123 Kraków, Poland

KEYWORDS
surveillance, protection of persons, detective inquiry, anti-surveillance activities

ABSTRAKT
Celem artykułu jest scharakteryzowanie działań inwigilacyjnych i zagrożeń, które mogą być ich następstwem, a także zwięzłe omówienie urządzeń i zachowań antyinwigilacyjnych. Na początku przedstawiono rys historyczny zjawiska inwigilacji i jego dawne i obecne przyczyny. Omówione zostają również trzy rodzaje wywiadu detektywistycznego: biały, szary i czarny. Następnie wskazano zagrożenia techniczne i fizyczne związane z inwigilacją z punktu widzenia chronionych osób. Wreszcie autor przedstawia najważniejsze działania antyinwigilacyjne związane z ochroną zarówno techniczną, jak i fizyczną. Pozwala to dojść do wniosku, że dobry plan ochrony osób powinien uwzględniać przede wszystkim działania przygotowawcze i prewencyjne oraz użycie urządzeń antyinwigilacyjnych w celu zapobiegnięcia przeciekowi informacji wrażliwych i powstania zagrożenia dla życia lub mienia. By skutecznie przeciwdziałać zagrożeniom płynącym z inwigilacji, konieczne jest wykorzystanie zarówno odpowiedniego sprzętu technicznego, jak i wiedzy, a nierzadko również umiejętności fizycznych.

SŁOWA KLUCZOWE
inwigilacja, ochrona osób, wywiad detektywistyczny, działania antyinwigilacyjne

WSTĘP

Ochrona osób, czyli działania mające na celu zapewnienie bezpieczeństwa życia, zdrowia i nietykalności osobistej[1], wraz z rozwojem technologii staje się coraz trudniejsza z uwagi na różnorodne i ogólnodostępne narzędzia inwigilacji, którą można definiować jako tajną obserwację kogoś lub tajny nadzór nad kimś[2]. Działania inwigilacyjne mogą wpływać na niską odporność na niepożądane przecieki danych, co z kolei ma bezpośredni wpływ na poziom bezpieczeństwa osoby lub też grupy osób inwigilowanych. Celem

[1] Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. 1997 nr 114 poz. 740 z późn. zm.).

[2] *Inwigilacja*, [w:] *Słownik języka polskiego PWN*, https://sjp.pwn.pl/sjp/inwigilacja;2561945.html (dostęp: 5.12.2019).

artykułu[3] jest scharakteryzowanie działań inwigilacyjnych oraz zagrożeń, które mogą być ich następstwem, a także zwięzłe omówienie urządzeń i zachowań antyinwigilacyjnych. Metoda badawcza zastosowana w pracy to krytyczna analiza literatury.

INWIGILACJA – RYS HISTORYCZNY, PRZYCZYNY, RODZAJE WYWIADU

Wydawać by się mogło, że nadzór, kontrola przepływu informacji czy monitorowanie zachowań ludzkich są efektem rozwoju współczesnej cywilizacji bądź technologii XXI wieku, jednak istnieją liczne dokumenty czy przekazy, które dowodzą, że zjawisko inwigilacji towarzyszy naszej cywilizacji w całej jej historii.

Terry Crowdy podaje, że do pierwszego udokumentowanego działania inwigilacyjnego doszło około 1274 roku p.n.e. w starożytnym Egipcie, kiedy dwóch szpiegów hetyckich, udając dezerterów, pojawiło się w obozie faraona Ramzesa przed bitwą pod Kadesz[4]. Inny przykład działań inwigilacyjnych opisany jest w Drugiej Księdze Samuela – Dawid, chodząc po dachu swojego pałacu, obserwował kąpiel Batszeby, żony Uriasza. Keith Laidler pisze z kolei: „szpiegostwo i inwigilacja są co najmniej tak stare jak sama cywilizacja. Powstanie miast i imperiów (…) oznaczało, że każde z nich musiało znać nie tylko usposobienie i morale wroga, ale także lojalność i ogólne nastroje własnej ludności"[5].

W przeszłości źródłem działań inwigilacyjnych była głównie potrzeba uzyskania informacji militarnych, ekonomicznych bądź politycznych. Obecnie potrzeb jest zdecydowanie więcej, co jest związane ze zmieniającym się światem i rozwojem technologii. Przykładów dzisiejszego zastosowania inwigilacji można doszukiwać się między innymi w korporacjach, zakładach pracy, podczas dokonywania transakcji czy używania (lub samego faktu posiadania) telefonu komórkowego. Pracodawcy używają zebranych w ten sposób informacji głównie po to, by przedstawić pracownikom ocenę ich pracy bądź udzielić rad, dzięki którym będą wykonywać swoje zadania jeszcze efektywniej, zaś informacje związane z dokonywanymi przez konsu-

[3] Artykuł jest skróconą i opracowaną wersją pracy licencjackiej autora pt. *Inwigilacja jako źródło zagrożeń chronionych osób*, napisanej pod kierunkiem dra hab. Juliusza Piwowarskiego, prof. WSBPI na Wydziale Bezpieczeństwa i Nauk Społeczno-Prawnych Wyższej Szkoły Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, Kraków 2020.

[4] T. Crowdy, *Historia szpiegostwa i agentury*, J. Mikołajczyk (tłum.), Warszawa 2010, s. 15.

[5] K. Laidler, *Surveillance Unlimited. How We've Become the Most Watched People on Earth*, Cambridge 2008, s. 17.

mentów transakcjami wykorzystywane są przez różne instytucje do wykrycia oszustw, jak i w celach optymalizacji kampanii reklamowych i zwiększenia dochodów. Posiadacze telefonów komórkowych są z kolei śledzeni właściwie na każdym kroku, co przy ogromie wad i wzbudzanych kontrowersji ma również zalety, a jedną z nich jest możliwość namierzenia danej osoby w przypadku zagrożenia jej życia lub zdrowia przez odpowiednie służby.

W tym miejscu pojawia się jednak pytanie: czy inwigilacja stwarza zagrożenie dla obywateli? „Władza tłumaczy ingerencję w prywatność obywateli koniecznością walki z przestępczością i zapobiegania terroryzmowi. Organizacje broniące praw obywatelskich ostrzegają przed nadmierną inwigilacją pod pozorem dbania o bezpieczeństwo”[6].

W skład działań inwigilacyjnych wchodzą różnego rodzaju działania operacyjne. Ze względu na sposób, w jaki prowadzona jest obserwacja, można je podzielić na trzy rodzaje:

- obserwację fizyczną;
- zdobywanie informacji w sposób elektroniczny;
- połączenie fizycznej inwigilacji z wykorzystaniem sprzętu elektronicznego i nowych technologii.

Jedną z metod inwigilacji, kojarzoną zwłaszcza ze środowiskiem detektywistycznym, jest wywiad. Można wyróżnić wywiad biały, czarny i szary.

Biały wywiad jest metodą pozyskiwania i analizy informacji pochodzących z otwartych, ogólnodostępnych źródeł[7], np. zdjęć satelitarnych i lotniczych, rejestrów pojazdów, ksiąg wieczystych, publikacji internetowych czy archiwów. Taki sposób zdobywania danych jest zgodny z przepisami prawa, a informacje, które udało się zdobyć tą drogą, mogą zostać wykorzystane w sądzie i są wiarygodnym materiałem dowodowym.

Szary wywiad stanowi połączenie białego wywiadu ze źródłami i metodami, które nie są do końca legalne. Można tu wskazać m.in. analizę kryminalną, pomoc osób trzecich, obserwację miejsc oraz osób, wnikanie w określone środowisko.

Jeśli chodzi o analizę kryminalną, to są to wszystkie metody zarezerwowane dla profesjonalnych i państwowych służb śledczych. Detektyw może więc zlecić na przykład zbadanie odcisków palców czy analizę śladów DNA,

---

[6] *Inwigilacja obywateli* [temat], „Sonar.wyborcza.pl”, https://sonar.wyborcza.pl/sonar/0,158721,Inwigilacja-obywateli.html (dostęp: 7.12.2019).

[7] K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej*, Warszawa 2011, s. 57–74.

lecz są to usługi kosztowne i w związku z tym agencje prywatne sięgają po nie rzadko. Pomoc osób trzecich to z kolei nic innego jak wywiad środowiskowy – detektyw rozpytuje o daną osobę czy sytuację na przykład sąsiadów lub współpracowników. Wniknięcie w określone środowisko może natomiast wiązać się z przyjęciem fałszywej tożsamości oraz zdobyciem zaufania grupy lub osoby. To trudna, a zarazem ryzykowna metoda.

O ile szary wywiad jest balansowaniem na granicy prawa, o tyle czarny wywiad jest już jego ewidentnym łamaniem. Wiąże się z zakładaniem podsłuchów, łamaniem haseł dostępu, kradzieżą tożsamości, prowokacją, wywieraniem nacisku. Detektyw, który decyduje się na stosowanie czarnego wywiadu, musi zdawać sobie sprawę, że zdobyte w ten sposób informacje nie będą mogły być wykorzystane w sądzie. Więcej – wymienione metody mogą być stosowane jedynie przez Policję, i to dopiero po pozytywnej opinii sądu, zaś wykorzystującym je detektywom grozi poważna odpowiedzialność karna oraz utrata prawa do wykonywania zawodu.

ZAGROŻENIA ZWIĄZANE Z INWIGILACJĄ Z PUNKTU WIDZENIA CHRONIONYCH OSÓB

Zagrożenia związane z inwigilacją można podzielić na techniczne i fizyczne. Technologia może wspierać bezpieczeństwo informacji lub je naruszać. Dane dotyczące danej osoby mogą być obecnie wyszukiwane na wiele sposobów, m.in. w mediach społecznościowych. Każdy użytkownik internetu powinien zdawać sobie sprawę, że nawet z pozoru błaha informacja może stanowić kluczowy element w budowaniu wysokiego poziomu bezpieczeństwa, zarówno własnego, jak i naszych bliskich. W mediach społecznościowych można znaleźć wiele informacji dotyczących życia osobistego i upodobań użytkowników, np. ulubionych potraw, poglądów politycznych, gustu muzycznego, aktualnego miejsca pobytu, zdjęć mieszkania itp. Agresorzy obserwują często nie tylko daną jednostkę, ale również jej otoczenie. Starają się zdobyć informacje na temat partnera, rodziny, znajomych z pracy, sąsiadów, np. poprzez wyszukiwanie i analizowanie nieoficjalnych baz danych, takich jak prywatne serwery. Taka wiedza może być bardzo przydatna dla inwigilującego, np. w razie chęci przyjęcia fałszywej tożsamości.

Bardziej zaawansowanymi informatycznie formami inwigilacji zajmują się hakerzy. Cyberprzestępcy są w stanie w krótkim czasie wykraść znaczące ilości cennych danych, złamać system zabezpieczeń w firmach czy wykraść dane do logowania na konta bankowe. Świadomość tych zagrożeń pozwala

organizacjom wdrożyć odpowiednie rozwiązania ochronne, jednak należy je regularnie aktualizować.

Zagrożenia techniczne nie wiążą się wyłącznie z internetem. Na rynku dostępny jest sprzęt, które ułatwia gromadzenie danych: rejestratory audio (podsłuchy, dyktafony), rejestratory wideo (kamery ukryte, fotopułapki) i lokalizatory[8]. Można go wykorzystać do każdego z trzech rodzajów wywiadu.

Zagrożenia fizyczne są z reguły następstwem inwigilacji, czy to fizycznej, czy elektronicznej. Do zagrożeń fizycznych z punktu widzenia chronionych osób zaliczyć można: atak z niedużej lub dużej odległości, atak z użyciem materiałów wybuchowych, uprowadzenia[9].

DZIAŁANIA ANTYINWIGILACYJNE

Ochrona techniczna

Rynek oferuje liczne urządzenia służące ograniczaniu ryzyka wystąpienia powyższych zjawisk. Wśród nich można wskazać wykrywacze metali, podsłuchów, kamer, generatory szumu, urządzenia szyfrujące.

Wykrywacze metali dzielą się na ręczne i stacjonarne. Są to urządzenia wykorzystujące zjawisko indukcji elektromagnetycznej do wykrywania elementów metalowych.

Wykrywacze podsłuchów najczęściej opierają swoje działanie na transmitowaniu danych za pośrednictwem fal radiowych. Weryfikacja przestrzeni może odbywać się w zakresie 10 metrów. Mankamentem jest jednak brak możliwości wykrycia urządzeń podsłuchowych, które zapisują dane w pamięci wewnętrznej, takich jak dyktafony. Tej wady pozbawione są profesjonalne (aczkolwiek droższe) wykrywacze, które zasięgiem działania obejmują zarówno sygnały analogowe, jak i cyfrowe. Mogą być również wykorzystane do wykrywania lokalizatorów i telefonów komórkowych.

Wykrywacze kamer dzielimy na dwa rodzaje: optyczne i skanujące. Pierwsze z nich działanie opierają na świetle, które odbija się od powierzchni i wraca do urządzenia. Dzięki takiemu rozwiązaniu da się namierzyć nawet dobrze zakamuflowane obiektywy kamer, które mogą być wyłączone. Wykry-

[8] D. Mrowiec, *Sprzęt do inwigilacji*, „B-secure", 1.04.2019, https://bezpieczenstwobiznesu.com.pl/index.php/2019/04/01/sprzet-do-inwigilacji/ (dostęp: 7.06.2020).

[9] M. Pyclik, *Ochrona osobista (cz. 2). Zjawiska wymuszające potrzebę stosowania ochrony osobistej*, „Zabezpieczenia.com.pl", 29.05.2007, https://www.zabezpieczenia.com.pl/ochrona-osobista/ochrona-osobista-cz-2-zjawiska-wymuszaj%C4%85ce-potrzeb%C4%99-stosowania-ochrony-osobistej (dostęp: 6.06.2020).

wacze skanujące wykorzystuje się do odnajdywania kamer bezprzewodowych oraz działających z wykorzystaniem sieci wi-fi. Skanują one częstotliwości, na których przesyłany jest obraz, i rozkodowują go. Dodatkowym atutem jest w tym przypadku możliwość wyświetlenia przechwyconego obrazu na ekranie, co umożliwia identyfikację położenia kamery[10].

Generatory szumu również można podzielić na kilka kategorii: ręczne, stacjonarne, samochodowe, akustyczne. Pierwsze trzy rodzaje są dostępne przede wszystkim dla uprawnionych do ich stosowania instytucji, dlatego nie można uzyskać o nich zbyt wielu informacji. Mówiąc ogólnie, są to urządzenia, które emitują sygnał na określonych częstotliwościach, uniemożliwiając w ten sposób łączność bezprzewodową w promieniu nawet kilkudziesięciu metrów[11]. Zagłuszacze akustyczne (mikrofonu) są natomiast urządzeniami dostępnymi dla każdego. Uniemożliwiają one pracę wszystkim mikrofonom znajdującym się w określonej odległości od nich. Generują losowy sygnał dźwiękowy, który sprawia, że słyszany lub nagrywany dźwięk jest bezwartościowy, a co więcej – odporny na próby wyczyszczenia w specjalistycznych programach do edycji dźwięku.

Techniczne systemy zabezpieczeń służą do zabezpieczania pomieszczeń, zwłaszcza tych wymagających szczególnej ochrony i kontroli. Na nowoczesne elektroniczne systemy zabezpieczeń technicznych składają się systemy ostrzegawcze, sygnalizujące, ale także kontroli dostępu i monitoringu oraz automatyka sterująca.

Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia w ramach działań w zakresie ochrony mienia i zabezpieczenia technicznego wyróżnia[12]:

- montaż elektronicznych urządzeń i systemów alarmowych sygnalizujących zagrożenie chronionych osób i mienia oraz eksploatację, konserwację i naprawę w miejscach ich zainstalowania;
- montaż urządzeń i środków mechanicznego zabezpieczenia oraz ich eksploatację, konserwację, naprawę i awaryjne otwieranie w miejscach zainstalowania.

[10] D. Mrowiec, *Technologia w służbie bezpieczeństwa firmy*, „B-secure", 20.03.2019, https://bezpieczenstwobiznesu.com.pl/index.php/2019/03/20/technologia-w-sluzbie-bezpieczenstwa-firmy/ (dostęp: 6.06.2020).

[11] Ibidem.

[12] Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. 1997 nr 114 poz. 740 z późn. zm.).

Profesjonalne systemy kontroli dostępu umożliwiają wejście na teren wybranych stref tylko uprawnionym osobom, posiadającym określony sposób dostępu. Może to być kod, specjalna karta czy odcisk palca.

W skład systemu dozorowego (monitorowania) wchodzą: telewizja przemysłowa, monitoring wizyjny, wideonadzór, telewizyjne systemy dozorowe (CCTV, ang. *Closed Circuit Television*). Bieżąca obserwacja oraz zapis obrazu z terenu objętego monitoringiem wizyjnym to istotny aspekt bezpieczeństwa wielu miejsc. Coraz częściej tego typu systemy stanowią ważną część polityki bezpieczeństwa wielu obszarów wymagających kontroli oraz są stosowane tam, gdzie liczy się bezpieczeństwo osób oraz ochrona mienia również po zmroku, co umożliwia technologia kamer cyfrowych IP[13].

System alarmowy to zespół urządzeń połączonych ze sobą instalacją kablową albo drogą radiową lub mieszaną (kablowo-radiową). Alarm uruchamia się w momencie wystąpienia zmiany stanu uznanego za pożądany[14]. Wśród systemów alarmowych można wskazać m.in.: systemy wykrywania i sygnalizacji pożaru, systemy oddymiania i przewietrzania, dźwiękowe systemy ostrzegawcze, systemy sygnalizacji włamania i napadu.

Ochrona fizyczna

Wykonywanie zawodu ochroniarza osób (bodyguarda) kojarzy się głównie z tężyzną fizyczną. Fizyczny aspekt tej pracy to jednak tylko jej niewielka część, znacznie więcej stanowi zapobieganie potencjalnym zagrożeniom, prewencja, a w tej kwestii sprawność fizyczna, siła i wygląd nie zawsze są najważniejsze. Liczy się solidna wiedza operacyjna i teoretyczna, a także ciągłe samodoskonalenie. Trenować trzeba właściwie nieustannie, podobnie jak szkolić się z zakresu nowinek technologicznych służących chociażby inwigilacji, by móc jej skutecznie zapobiegać[15].

---

[13] *Systemy zabezpieczeń technicznych – przegląd oferty producentów*, „Instalacje budowlane.pl", 6.03.2020 [aktualizacja], http://www.instalacjebudowlane.pl/10254-27-86-systemy-zabezpieczen-technicznych--przeglad-oferty-producentow.html (dostęp: 6.06.2020).

[14] Ibidem.

[15] M. Pyclik, *Ochrona osobista (cz. 3). Taktyka i technika ochrony osób*, „Zabezpieczenia.com.pl", 14.11.2006, https://www.zabezpieczenia.com.pl/ochrona-osobista/ochrona-osobista-cz-3-taktyka-i-technika-ochrony-os%C3%B3b (dostęp: 6.06.2020).

Bodyguard w swojej pracy powinien kierować się następującymi zasadami[16]:

- żelazną – nigdy nie powinien robić odstępstw od przyjętych przez siebie metod postępowania;
- kameleona – powinien umieć dostosować się do otoczenia poprzez właściwy ubiór (błędem jest np. ochrona na plaży w garniturze);
- kamiennej twarzy – nie może pokazywać po sobie, że jest zaskoczony;
- małomówności – powinien mówić tylko tyle, ile potrzeba, to VIP ma być bardziej rozmowny niż ochroniarz;
- pozostawania w cieniu – nie może ujawniać o sobie zbyt wielu informacji;
- tłumienia emocji – najważniejsze ma być dla niego wykonanie zadania;
- oceny ryzyka – nie może brać na siebie zadań, których nie wykona;
- kluczenia – dotyczy ochrony podczas przejazdów;
- sługi i pana – VIP decyduje, gdzie pójdzie i co będzie robił, natomiast bodyguard wskazuje, jak się tam dostać i jakie środki bezpieczeństwa przedsięwziąć.

Szczególne zadania w ochronie osobistej mogą wykonywać kobiety[17]. Po pierwsze dlatego, że do niektórych miejsc, np. damskiej toalety czy garderoby, mężczyznom nie wypada wejść bądź jest to krępujące dla chronionej kobiety. Po drugie kobiety mają szereg predyspozycji, które można wykorzystać podczas pracy ochroniarza: zazwyczaj świetnie dostrzegają szczegóły, mają intuicję, a także – przede wszystkim – są zazwyczaj lekceważone przez przeciwników, co daje im ogromną przewagę i może być elementem zaskoczenia.

Zasada, którą kierują się ochroniarze osób mówi, że każda informacja, choćby wydawała się mało znacząca, może okazać się użyteczna przy szacowaniu zagrożenia, dlatego pomocne będzie trzymanie się tzw. szablonu siedmiu „P" (nazwa od określeń w języku angielskim)[18]:

- ludzie (*people*);
- miejsca (*places*);
- osobowość (*personality*);
- uprzedzenia (*prejudices*);
- historia osobista (*personal history*);
- poglądy polityczne i religijne (*political and religious persuasion*);
- życie prywatne (*private life*).

[16] Z. Struk, *Bodyguard czy „goryl"*, „Ochroniarz. Ogólnopolski Magazyn Zawodowców" 1999, nr 23, s. 36.

[17] Idem, *Kobieta bodyguard*, „Ochroniarz. Ogólnopolski Magazyn Zawodowców" 1996, nr 9, s. 21.

[18] M. Pyclik, *Ochrona osobista (cz. 3)…*, op. cit.

Ochroniarz musi mieć drobiazgową wręcz wiedzę na temat osoby, którą chroni. Powinien wiedzieć, gdzie się urodziła, mieszkała, gdzie obecnie pracuje i pracowała, jak spędza wolny czas, jakie ma uprzedzenia, jak wygląda historia jej małżeństwa (lub małżeństw), a ponadto znać historię jej chorób, grupę krwi, ewentualne alergie, przyjmowane regularnie leki itp. Co więcej, ważna jest również wiedza na temat sfery intymnej VIP-a: jego nałogów, rodzinnych sekretów, wstydliwych tajemnic. To wszystko ma znaczenie przy zapewnianiu ochrony. Miejsca i sytuacje dla jednych bezpieczne dla innych mogą takie nie być. Bodyguard zawsze musi pamiętać o związku osoby ochranianej z danym miejscem (osobą) i o wpływie tego powiązania na stopień zagrożenia.

ZAKOŃCZENIE

W czasach, w których przepływ informacji jest nieustanny, istnieje możliwość utraty kontroli nad dostępem do informacji, które mogą stanowić kluczowy element w budowaniu wysokiego poziomu bezpieczeństwa osobistego. Nawet najmniej istotna informacja ma znaczenie, a inwigilacja może stanowić źródło poważnych zagrożeń ochranianych osób. Aby unikanie tych zagrożeń było możliwe, niezbędna jest znajomość działań inwigilacyjnych oraz niebezpiecznych sytuacji, które mogą powodować. Dobry plan ochrony osób powinien zatem uwzględniać działania przygotowawcze i prewencyjne oraz użycie urządzeń antyinwigilacyjnych w celu zapobiegnięcia przeciekowi informacji wrażliwych i powstania zagrożenia dla życia lub mienia. By te działania były skuteczne, konieczne jest wykorzystanie zarówno odpowiedniego sprzętu technicznego, jak i wiedzy, a nierzadko również umiejętności fizycznych.

BIBLIOGRAFIA

Crowdy T., *Historia szpiegostwa i agentury*, J. Mikołajczyk (tłum.), Warszawa 2010.

Inwigilacja, [w:] *Słownik języka polskiego PWN*, https://sjp.pwn.pl/sjp/inwigilacja;2561945.html (dostęp: 5.12.2019).

Inwigilacja obywateli [temat], „Sonar.wyborcza.pl", https://sonar.wyborcza.pl/sonar/0,158721,Inwigilacja-obywateli.html (dostęp: 7.12.2019).

Krupa K., *Inwigilacja jako źródło zagrożeń chronionych osób*, praca licencjacka napisana pod kierunkiem dra hab. Juliusza Piwowarskiego, prof. WSBPI na Wydziale Bezpieczeństwa i Nauk Społeczno-Prawnych Wyższej Szkoły Bezpieczeństwa Publicznego i Indywidualnego „Apeiron" w Krakowie, Kraków 2020.

Laidler K., *Surveillance Unlimited. How We've Become the Most Watched People on Earth*, Cambridge 2008.

Liedel K., Serafin T., *Otwarte źródła informacji w działalności wywiadowczej*, Warszawa 2011.

Mrowiec D., *Sprzęt do inwigilacji*, „B-secure", 1.04.2019, https://bezpieczenstwobiznesu.com.pl/index.php/2019/04/01/sprzet-do-inwigilacji/ (dostęp: 7.06.2020).

Mrowiec D., *Technologia w służbie bezpieczeństwa firmy*, „B-secure", 20.03.2019, https://bezpieczenstwobiznesu.com.pl/index.php/2019/03/20/technologia-w-sluzbie-bezpieczenstwa-firmy/ (dostęp: 6.06.2020).

Pyclik M., *Ochrona osobista (cz. 2). Zjawiska wymuszające potrzebę stosowania ochrony osobistej*, „Zabezpieczenia.com.pl", 29.05.2007, https://www.zabezpieczenia.com.pl/ochrona-osobista/ochrona-osobista-cz-2-zjawiska-wymu szaj%C4%85ce-potrzeb%C4%99-stosowania-ochrony-osobistej (dostęp: 6.06.2020).

Pyclik M., *Ochrona osobista (cz. 3). Taktyka i technika ochrony osób*, „Zabezpieczenia.com.pl", 14.11.2006, https://www.zabezpieczenia.com.pl/ochrona-osobista/ochrona-osobista-cz-3-taktyka-i-technika-ochrony-os%C3%B3b (dostęp: 6.06.2020).

Struk Z., *Bodyguard czy „goryl"*, „Ochroniarz. Ogólnopolski Magazyn Zawodowców" 1999, nr 23.

Struk Z., *Kobieta bodyguard*, „Ochroniarz. Ogólnopolski Magazyn Zawodowców" 1996, nr 9.

Systemy zabezpieczeń technicznych – przegląd oferty producentów, „Instalacje budowlane.pl", 6.03.2020 [aktualizacja], http://www.instalacjebudowlane.pl/10254-27-86-systemy-zabezpieczen-technicznych--przeglad-oferty-producentow.html (dostęp: 6.06.2020).

Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. 1997 nr 114 poz. 740 z późn. zm.).

CITE THIS ARTICLE AS:

K. Krupa, *Inwigilacja jako źródło zagrożeń chronionych osób*, „Security, Economy & Law" 2/2020 (XXVII), s. 50–60, DOI: 10.24356/SEL/27/4.