Piotr Chlebowicz

Metody sztucznej inteligencji

E. Nawarecki, G. Dobrowolski, M. Kisiel – Dorohnicki (red.) *Metody sztucznej inteligencji w działaniach na rzecz bezpieczeństwa publicznego****, Kraków 2009, Wydawnictwa AGH, s. 291.***

Recenzowana monografia prezentuje wyniki projektów badawczo-rozwojowych realizowanych w Katedrze Informatyki AGH w Krakowie w związku z udziałem Katedry w pracach Polskiej Platformy Bezpieczeństwa Wewnętrznego. Zasługuje ona na uwagę gdyż w interesujący sposób przedstawia potencjały nowych narzędzi informatycznych w zakresie zwalczania zaawansowanych form zjawiskowych przestępczości, w tym przestępczości zorganizowanej i ekonomiczno - finansowej, jak również terroryzmu i aktywności obcych wywiadów. Warto zwłaszcza zwrócić uwagę, iż omawiana publikacja AGH łączy w sobie zarówno wymiar „technologiczny", jak i prawny. W związku z powyższym, adresowana jest nie tylko do przedstawicieli nauk technicznych, ale także do prawników karnistów, kryminologów i kryminalistyków. Ze względu na obszerność i złożoność materii zawartej w 13 rozdziałach, należy skoncentrować się na wybranych kwestiach, najbardziej istotnych z punktu widzenia bezpieczeństwa wewnętrznego.

Znaczna część rozważań dotyczy propozycji usprawnień narzędzi informatycznych wykorzystywanych w ramach wywiadu kryminalnego. Zagadnienie analizy kryminalnej będącej centralnym elementem wywiadu jest oczywiście znane zarówno praktyce policyjnej, jak i środowiskom akademickim, lecz Autorzy proponują oryginalne rozwiązanie polegające na uzupełnieniu katalogu technik analitycznych o metody badań sieci społecznych (*Social Network Analysis*). Otwiera to nowe możliwości w zakresie analizy kryminalnej w szczególności przy ustalaniu powiązań osobowych. Na marginesie trzeba zauważyć, iż znaczenie SNA wzrasta, gdyż opiera się na trafnych socjologicznych koncepcjach sieci społecznych, które wiernie odzwierciedlają stosunki społeczne ery informacyjnej. Pierwotnie wymieniona metoda była wykorzystywana w obrocie cywilnym. Wymienia się tutaj na przykład badania struktur organizacji, analizę relacji pomiędzy firmami i instytucjami, a nawet przy badaniach współautorstwa i cytowań w literaturze naukowej. Obecnie jednak SNA jest również wykorzystywana, zwłaszcza w USA, przez instytucje odpowiedzialne za bezpieczeństwo (systemy *CrimeNet Explorer*, COPLINK, NETEST). Polska koncepcja metody identyfikacji struktury związków i grup przestępczych zawarta jest w narzędziu informatycznym KASS (Kryminalna Analiza Sieci Społecznych).

KASS wykorzystuje w swym działaniu możliwość odtworzenia sieci społecznej na podstawie bilingów telefonicznych. Szczegółowe omawianie parametrów tej aplikacji nie mieści się w ramach recenzji. Warto jednak w tym miejscu wskazać, iż jeden z elementów KASS odnosi się do typologii ról, które mogą pełnić przestępcy (terroryści) w sieci społecznej opracowanym przez J. Arquillę i D. Ronfeldt'a analityków znanego *think tanku* RAND. W związku z powyższym wydaje się, iż powstaje dylemat posłużenia się metodami sieci badań społecznych w aspekcie kryminalistycznym i dowodowym. Chodzi o to, czy terminologia zaproponowana przez Autorów KASS,

w szczególności zaś rozbudowana typologia ról w organizacji przestępczej (11 ról) będzie „kompatybilna" ze schematami pojęciowymi i nomenklaturą używaną przez prawników i funkcjonariuszy organów ścigania. Kwestia ta będzie istotna choćby z tego względu, iż argumentowanie w sporach prawnych (w tym konkretnym przypadku udowodnienie udziału określonej osoby - podejrzanego lub oskarżonego w zorganizowanej grupie) opiera się na prawniczej interpretacji rzeczywistości. Wydaje się zatem, iż typologia ról funkcjonująca w ramach KASS nie będzie mogła mieć bezpośredniego zastosowania w postępowaniu przygotowawczym i sądowym. Użytkownicy KASS będą zatem mogli w swych analizach opierać się na dotychczasowych typologiach (ale tylko wyłącznie w ramach czynności operacyjno-rozpoznawczych, lub analityczno-informacyjnych), lecz w przypadku gdyby analiza miała stanowić fragment materiału dowodowego, używanie sformułowań „izolator", „komunikator", „strażnik" nie byłoby z punktu widzenia taktyki śledztwa i ewentualnego procesu karnego właściwym zabiegiem. Jest tak również dlatego – pomijając podane wyżej argumenty – iż prawniczy sposób myślenia nie obejmuje sformułowań, które nie mają żadnego związku z obowiązujacym stanem prawnym i tradycyjną kryminalistyką. Z drugiej jednak strony, rewolucja informatyczna i realia stechnicyzowanego świata muszą wpływać na taktykę i technikę kryminalistyczną XXI wieku. Można natomiast zaproponować, aby typologia ta mogła być przekształcona w argumentację o charakterze prawniczym. Przykładowo można wskazać, iż rola X jest kierownicza, istotna, drugorzędna, peryferyjna i poprzez opis zachowań X uzasadnić wymienione stwierdzenia.

Powyższe rozważania na kanwie fragmentu opracowania AGH stanowią jedynie przyczynek do szerszego zagadnienia wskazania miejsca analizy kryminalnej w praktyce śledczej. Obecnie, bowiem, analiza kryminalna i rozwijane instrumentarium informatyczne znajduje swe zastosowanie przede wszystkim w płaszczyźnie wykrywczej a nie dowodowej. Z tym faktem należy się liczyć, gdyż pomimo zwiększających się możliwości technologicznych i technicznych narzędzi informatycznych (w tym również narzędzi wspierających analizę kryminalną) w zakresie uzyskiwania i łączenia danych w logiczną całość, wyniki procesów przetwarzania informacji nie zawsze będą możliwe do wykorzystania procesowego.

Trzeba również dodać, iż KASS stanowi zaledwie jeden z komponentów narzędzi informatycznych określanych mianem Zintegrowanego Środowiska Analizy Kryminalnej. Narzędzia tworzące Zintegrowane Środowisko umożliwiają analizę danych pochodzących z różnych źródeł (bazy danych, bilingi) i wizualizację uzyskanych wyników. Istota tego instrumentu sprowadza się do ekstrakcji informacji ze źródeł elektronicznych, w szczególności Internetu. Tym samym, wymieniony produkt informatyczny w połączeniu z systemem IBIS stanowi idealne narzędzie do prowadzenia białego wywiadu. Dużym atutem omawianych aplikacji jest wysoki stopień automatyzacji wyszukiwania i selekcji danych, co korzystnie wpływa na ekonomikę prac analitycznych. Wydajność tego systemu jest duża, gdyż podstawowe moduły IBIS zapewniają możliwość przeanalizowania zbioru obiektów liczącego kilkadziesiąt milionów stron.

Niewątpliwie interesującym aspektem monografii jest rozdział dotyczący analizy przepływów finansowych, w którym przedstawiony został *modus operandi* prania brudnych pieniędzy. Techniki stosowane przez „praczy" stanowią punkt odniesienia dla konstrukcji prototypu systemu wspomagającego analityka w zakresie spraw z art. 299 kk. Jako ostatni, ale nie najmniej ważny można wskazać opis funkcjonowania systemu „Wizjer", który monitoruje aktywność użytkowników komputerów oraz techniki zarządzania dokumentami tekstowymi w postaci elektronicznej.

Reasumując należy stwierdzić, iż recenzowana publikacja prezentuje oryginalny dorobek zespołu badawczego Katedry Informatyki AGH. *Novum* tego opracowania polega na tym, iż technologie informatyczne i oparte na tych technologiach narzędzia zostały zaprojektowane w celu podniesienia efektywności działań organów i instytucji odpowiedzialnych za bezpieczeństwo narodowe kraju. Ważnym zagadnieniem jest także wykorzystanie najnowszych osiągnięć techniki kryminalistycznej nie tylko w celach wykrywczych lub analityczno – informacyjnych, lecz również procesowych. W literaturze przedmiotu dostrzega się bowiem, iż rozwój nauki powoduje konieczność uwzględniania w procesach tzw. dowodów naukowych. Wydaje się, iż niniejsza publikacja może stanowić punkt wyjścia do dalszych poszukiwań nowych możliwości zarówno w sferze wykrywczej, jak i dowodowej.