MARTA FILIPIAK ▶▶

Uniwersytet Warszawski

ORCID ID: <https://orcid.org/0000-0003-4539-0658>**Bezpieczeństwo – cel realny czy mrzonka?**[recenzja książki *Koordinacja informacji w systemie bezpieczeństwa państwa*]**Security – a Real Goal or Mere Fantasy?**[book review *Koordinacja informacji w systemie bezpieczeństwa państwa*]**Безопасность – реальная цель или фантастика?**[рецензия книги *Koordinacja informacji w systemie bezpieczeństwa państwa*]

Bezpieczeństwo jest największym dobrem człowieka, jest fundamentem „funkcjonowania świata i każdego państwa z osobna, jest wartością najwyższą, bez której całe otoczenie nie ma znaczenia. (...) jest podmiotem biorącym udział w walce w ringu, gdzie jego przeciwnikiem jest zagrożenie” – tymi słowami Paweł Chodak, doktor nauk społecznych w zakresie nauk o bezpieczeństwie, adiunkt w Wyższej Szkole Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie, badacz zagadnień z zakresu cyberbezpieczeństwa i analizy kryminalnej, rozpoczyna swoje rozważania.

W swojej najnowszej publikacji, wydanej w 2019 roku, Paweł Chodak dotyka problematyki bardzo współczesnej – podkreśla znaczenie społeczeństwa informatycznego – „ekshibicjonizmu” udostępniania danych i wzrastającej statystycznie cyberprzestępczości; omawia ponadto rolę służb, zwłaszcza

policyjnych i specjalnych wobec wyzwania ochrony państwa (por. Marszałek-Kawa et al., 2018).

Rozważania zawarte w książce zatytułowanej *Koordinacja informacji w systemie bezpieczeństwa państwa* są impulsem do spojrzenia na problematykę informacji z innej perspektywy – Chodak inspiruje czytelnika do postawienia tezy, iż wszystko wokół jest informacją i wszystko można na tę informację przetworzyć. Problematyka informacji pozwala na postawienie wielu pytań i problemów badawczych, jednak samo zdefiniowanie tezy może okazać się kluczowe dla dalszych rozważań. Czym jest informacja? Paweł Chodak wskazuje, iż jest to pytanie prozaiczne, a zarazem zawile i złożone w uzyskaniu jednoznacznej odpowiedzi. Można wyjść od przyjęcia, iż informacja jest opisem istniejącego obiektywnego stanu rzeczy, a jej geneza sięga końca XIX wieku, kiedy to termin ten został wprowadzony do działu fizyki, jakim jest termodynamika, a następnie ewoluował od języka potocznego i zawodowego, aż do informatyczno-technicznych nauk szczególnych.

Informacja jest jednym z najtrudniejszych do zdefiniowania pojęć i wymaga dalszych analiz, w tym w ujęciu prawnym. Zdaniem autora nawet regulacje funkcjonujące na gruncie polskiego systemu prawnego, których celem jest ochrona informacji, nie są ze sobą skorelowane, co jest efektem wpływu wielu czynników. Począwszy od wieloznaczności terminu (zdaniem W. Góralczyka), przez brak możliwości powiązania informacji z konkretnym działem prawa, aż po określenie informacji jako terminu niedefiniowalnego i stanowiącego pojęcie pierwotne (Petzel).

Metamorfoza związana z rozwojem technik informacyjnych miała nieodzowny wpływ na rozwój społeczeństwa informacyjnego, którego początków szukać można w badaniach i działalności japońskiego socjologa Tadao Umesamo oraz futurologa Kenichi Koyame. Praktyka społeczeństwa informacyjnego oznacza podporządkowanie innych aspektów życia oraz gospodarki „nowym mediom”, komunikacji masowej czy też nowoczesnym technologiom, co przejawia się m.in. w znacznym ograniczeniu kontaktów międzyludzkich. Informacja staje się fundamentalnym składnikiem życia społecznego i towarem o wymiernej wartości, jest kluczowym składnikiem zarówno pracy, jak i całego życia. Cyberprzestrzeń, powołana do życia w świecie powieści science-fiction przez Williama Gibsona, na przełomie XX i XXI wieku przestaje być fikcją.

Upowszechnienie dostępu do Internetu sprawiło, że informacja znacznie się wzbogaciła i jednocześnie stała się źródłem nowych zagrożeń. Podstawowym aktem prawnym dotyczącym cyberprzestępczości jest Konwencja Rady Europy o cyberprzestępczości z 2001 roku, która definiuje podstawowe pojęcia związane ze wspomnianym zjawiskiem oraz wprowadza katalog czynów, które powinny być uznawane za niedozwolone. Przywołana wcześniej tzw. konwencja budapesztańska wprowadza katalog podzielony na cztery kategorie, a mianowicie: przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów, przestępstwa komputerowe, przestępstwa kontentowe oraz przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych. Problematyka dotycząca ataków na systemy informatyczne została ponadto ujęta w dyrektywie Parlamentu Europejskiego i Rady 2013/40/UE z 2013 roku. Następnym regulacji międzynarodowych było unormowanie zachowań w cyberprzestrzeni na gruncie rodzimego kodeksu karnego. Chodak w swojej publikacji przywołuje rozważania J. Kosińskiego, który to dokonał analizy zestawu cech wspólnych cyberprzestępczości i wskazał m.in. na kwestie związane z teoretyczną anonimowością sprawcy, niskimi kosztami przy jednoczesnym stosunkowo dużym zasięgu działania (czyny te nie są najczęściej nakierowane na konkretną ofiarę, a na wybraną grupę), czy też na brak społecznej świadomości, przejawiający się niejednokrotnie poprzez traktowanie przestępcy komputerowego jako sprawcy „nieszkodliwego”.

Dostęp do informacji od zawsze był szczególnie cenny i niezbędny dla rozwoju człowieka. Jest tak zwłaszcza obecnie, dlatego też należy bezsprzecznie wskazać, iż informacja jest najważniejszym „składnikiem” pracy służb specjalnych i policyjnych, które są legitymizowane przez państwo do zdobywania wiedzy – wiedzy traktowanej jako wartość, towar, środek do realizacji działań i osiągania celów, informacja o organizacji czy też strategia. Konsekwencją rozwoju, co stanowi wyzwanie dla powołanych do zapewnienia bezpieczeństwa służb i organów, był rozwój cyberterroryzmu. Za prekursora tej formy przestępczości uznaje się Giangiacomo Feltrinelliego, przywódcę Grupy Akcji Partyzanckiej i włoskiego multimilionera, którego działalność polegała na atakach na centrum komputerowe domów towarowych w Mediolanie, biura administracji rządowej w Rzymie czy też bazę danych, która zawierała informacje o skradzionych i zarejestrowanych we

Włoszech samochodach. Jednym z najbardziej znanych aktów tego rodzaju terroryzmu było przeprowadzenie operacji mającej na celu uszkodzenie systemów identyfikacji samolotów porwanych i wykorzystanych przez Al-Kaidę 11 września 2001 roku. Cyberterroryzm ewoluował – nie jest już konieczne niszczenie samego sprzętu, aby utrudnić kontakt ze światem – całkowicie skuteczne jest jego zablokowanie czy też przejęcie nad nim kontroli.

Gromadzenie, opracowywanie i wykorzystywanie informacji jest podstawową rolą służb w systemie bezpieczeństwa państwa. Przyjmuje się, iż czynności operacyjno-rozpoznawcze pełnią przede wszystkim rolę wykrywczą, dowodową i zapobiegawczą. Metody prowadzenia tychże czynności przez służby uprawnione do tego z mocy prawa są rozmaite i należą do nich m.in.: wywiad, penetracja terenu, zasadzka, eksperyment, analiza operacyjna, obserwacja osób miejsc i środków transportu, pułapka, współpraca z osobami fizycznymi, kontrola korespondencji czy też zakup kontrolowany. Istotą działania służb jest zdobywanie informacji – postęp technologiczny nie tylko umożliwia zdobywanie i przekazywanie informacji, ale przede wszystkim daje oręż do ich ukrywania, przez co narzędzia wywiadowcze również muszą być uaktualniane i dopasowywane do zmieniających się warunków. Kluczową rolę w zapewnianiu bezpieczeństwa powinna stanowić analiza kryminalna, której celem jest pozyskiwanie, wstępne przetwarzanie i graficzna prezentacja informacji pochodzących z niezależnych od siebie źródeł.

Przyjmuje się, że to przestępczość zorganizowana w największym zakresie wykorzystuje uzyskane informacje do dokonywania czynów przestępnych i prowadzenia działalności niezgodnej z prawem. Obecnie nawet 90 proc. informacji zdobywanych przez służby pochodzi z tzw. *open source intelligence*. Białe wywiad czy też Darknet są wykorzystywane jako źródła dające możliwość ustalenia powiązań w świecie przestępczym, nie tylko w ramach walki z przestępczością zorganizowaną.

Przechodząc do analizy systemu bezpieczeństwa państwa, kluczową potrzebą wydaje się być zdefiniowanie samego pojęcia bezpieczeństwa, którego – podobnie jak informacji – nie sposób jest umieścić w ściśle określonych ramach. Henry Kissinger podczas przemowy w Międzynarodowym Instytucie Studiów Strategicznych podkreślił, że bezpieczeństwo jest fundamentem wszystkiego, co czynimy. Zwykło się przyjmować, iż bezpieczeństwo nie jest stanem stałym, lecz swoistą pogonią i dążeniem do doskonałości, przy

jednoczesnej ucieczce przed zagrożeniami. Jest to jedna z najważniejszych potrzeb człowieka, grup społecznych i państw. Samo „bezpieczeństwo” można podzielić na międzynarodowe i narodowe, w ramach którego funkcjonuje bezpieczeństwo wewnętrzne i zewnętrzne. W recenzowanej monografii Paweł Chodak omawia prawne aspekty funkcjonowania i rolę wybranych instytucji administracji publicznej i służb odpowiedzialnych za bezpieczeństwo. Analizie poddana została rola Ministerstwa Spraw Wewnętrznych i Administracji, Ministerstwa Obrony Narodowej, Koordynatora Służb Specjalnych, Ministra Finansów, Generalnego Inspektora Informacji Finansowej, Policji, Straży Granicznej, Żandarmerii Wojskowej, Służby Ochrony Państwa, Krajowej Administracji Skarbowej, Biura Nadzoru Wewnętrznego w Ministerstwie Spraw Wewnętrznych i Administracji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Centralnego Biura Antykorupcyjnego, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, a także Straży Marszałkowskiej, Straży Gminnej i Miejskiej oraz Straży Leśnej.

Bezsprzecznie, aby informacja mogła być przydatna dla służb i wykorzystywana w zapewnianiu bezpieczeństwa, musi być aktualna, konkretna i weryfikowalna, bez względu na źródło jej pochodzenia. Aby osiągnąć ten cel, tworzone są krajowe systemy zbierania informacji, a także międzynarodowe zbiory informacji, wykorzystywane w zwalczaniu przestępczości transgranicznej. Rejestry te są wykorzystywane zarówno w charakterze prewencyjnym, jak i wywiadowczym. Paweł Chodak omówił wybrane systemy bazodanowe, w tym Powszechny Elektroniczny System Ewidencji Ludności, Centralną Ewidencję Pojazdów i Kierowców, Krajowy Rejestr Podmiotów Gospodarki Narodowej, Krajowy Rejestr Sądowy, Krajowy Rejestr Karny. Wśród systemów bazodanowych prowadzonych przez służby bezpieczeństwa wewnętrznego analizie poddany został Krajowy System Informacyjny Policji, System Informacji Operacyjnych, Ogólnopolska Baza Osobowych Źródeł Informacji czy też systemy bazodanowe Straży Granicznej, które stanowią niebagatelne wsparcie dla innych służb, ze względu na uniwersalny zakres zadań Straży Granicznej związany z zapewnianiem ochrony granic państwowych, kontrolą ruchu granicznego, przeciwdziałaniem nielegalnym migracjom, które to działania prowadzone są na obszarze całego kraju. Uwagę Autora zwróciły ponadto systemy sprzyjające koordynacji informacji na arenie międzynarodowej, takie jak zbiory informacji EUROPOLU i INTERPOLU,

System Informacyjny Schengen, Wizowy System Informacyjny, system PNR, gromadzący dane dotyczące przelotu pasażera czy też POBYT – system ewidencyjny w sprawach cudzoziemców.

W ramach badań krajowego systemu koordynacji Chodak skupił się na Krajowym Centrum Informacji Kryminalnych, Centralnej Ewidencji Zainteresowań Operacyjnych oraz na koordynacji informacji korupcyjnych na mocy ustawy o Centralnym Biurze Antykorupcyjnym. Autor podkreślił błędy oraz nieścisłości w funkcjonującym systemie, objawiające się brakiem organu, który zapewniałby kompleksową koordynację informacji czy też brakiem instytucji nadzorującej kompleksowo działanie wszystkich powołanych organów.

Konkludując, pomysłodawca publikacji podzielił ją na sześć rozdziałów, z których każdy może być traktowany jako odrębna i wyczerpująca całość. Autor przeprowadza czytelnika przez trzy główne obszary – informację, bezpieczeństwo wewnętrzne i koordynację, ukazane z różnych perspektyw i poddane możliwie kompleksowym rozważaniom w aspektach teoretycznych, prawnych (w tym postulatach *de lege ferenda*) i filozoficznych. Szczegółowej analizie poddana została sama istota informacji, od prób jej zdefiniowania przez omówienie sposobów gromadzenia, opracowywania i wykorzystywania tychże. Paweł Chodak omówił również organy państwa w systemie bezpieczeństwa, a także krajowe i międzynarodowe instytucje oraz mechanizmy wykorzystywane w zwalczaniu przestępczości zarówno zorganizowanej jak transgranicznej oraz zaproponował autorski, teoretyczny model koordynacji informacji w Polsce.

Istotnym walorem publikacji jest podrozdział badawczy, gdzie zamieszczone zostało zbiorcze opracowanie wywiadów z ekspertami, którzy wyrażali swoje poglądy między innymi w zakresie zapewnienia koordynacji informacji przez systemy bazodanowe wykorzystywane do ich uzyskiwania czy też w zakresie kategorii informacji, które powinny być koordynowane. Wspomniani respondenci odnieśli się również do nieprecyzyjnych regulacji prawnych w zakresie dostępu do danych, wyrazili także opinię o potrzebie powołania nowego organu mającego uprawnienia nadzorcze, kontrole i koordynacyjne.

Dodatkowo zasługujące na docenienie są liczne odesłania do literatury przedmiotu, w tym anglojęzycznej, co sprawia, że omawiana pozycja może być polecona zarówno praktykom, związanym zawodowo z obszarem

bezpieczeństwa, jak i laikom, poszerzającym wiedzę oraz poszukującym informacji o otaczającym i zmieniającym się w szybkim tempie świecie.

Czy system koordynacji pomiędzy służbami jest wystarczający a filar egzystencji świata w postaci bezpieczeństwa zapewniony? Na te i inne pytania odpowiada autor, skłaniając jednocześnie do dalszych i pogłębionych refleksji.

MGR MARTA FILIPIAK

Uniwersytet Warszawski
marta.filipiak@student.uw.edu.pl

Bibliografia

- Chodak, P. (2019). *Koordinacja informacji w systemie bezpieczeństwa państwa*. Toruń: Wydawnictwo Adam Marszałek.
- Marszałek-Kawa, J., Plecka, D., Hołub, A. (red.). (2018). *Social Security. Selected Aspects*. Toruń: Wydawnictwo Adam Marszałek.