

## Wstęp

Obecnie mamy do czynienia z nieznaną wcześniej w historii intensywnością zdarzeń zachodzących w otaczającej nas rzeczywistości<sup>1</sup>. Poszczególne jednostki i ich organizacje codziennie podejmują wiele decyzji, uczestniczą w wydarzeniach w sposób aktywny lub bierny. Co więcej, wszystko to jest nam relacjonowane przez tradycyjne i nowoczesne środki masowego przekazu 24 godziny na dobę, 7 dni w tygodniu. Jesteśmy zalewani przez morze danych i informacji dochodzących do nas różnymi kanałami, niezależnie czy tego chcemy, czy też nie. Stajemy się społeczeństwem informacyjnym ze wszystkim dobrymi i złymi tego stronami<sup>2</sup>.

Ponadto rozwój techniki, zwłaszcza teleinformatycznej, nie jest tutaj bez winy<sup>3</sup>. Umożliwia ona nam dostęp do danych o wydarzeniach, które działy się lub dzieją się nawet w najdalszych zakątkach świata. Mamy dostęp do przekazów wideo, nagrań dźwiękowych, tekstowych, innymi słowy multimedialnych. Nie potrzebujemy już żadnych skomplikowanych lub ciężkich urządzeń, które pozwalałyby na odbiór danych i informacji. Ponieważ jest takie zapotrzebowanie, to znajdują się podmioty, które oferują nam odpowiednie usługi i urządzenia. Słowem-kluczem staje się mobilność nie tylko osób, lecz także oferowanych nam usług.

Nie musimy być tylko biernymi odbiorcami przekazywanych nam treści. Technika pozwala nam stać się także kreatorem rzeczywistości, komentatorem wydarzeń. Możemy wchodzić w interakcje z rzeczywistością na wielu poziomach, za pomocą wielu kanałów dystrybucji informacji. Niektórzy idą krok dalej i manipulują nią. Pozwalają odbiorcom informacji na dostęp tylko do wybranej części rzeczywistości,

---

<sup>1</sup> K. Dobrzeński, *Lex Informatica*, Toruń 2008, s. 41.

<sup>2</sup> R. Tadeusiewicz, *Nowe technologie dowodowe dla przestępstw popełnionych w obszarze Społeczeństwa Informacyjnego*, [w:] L. Gardocki, J. Godyń, M. Hudzik, L.K. Paprzycki (red.), *Nowe technologie dowodowe a proces karny*, Warszawa 2007, s. 19 i n.

<sup>3</sup> A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. XV i n.

narzucają nam swój pogląd na wydarzenie, mieszają dane o zdarzeniu i osobach w nim uczestniczących z własną narracją, komentarzem.

Współcześnie podstawowym problemem jest możliwość (lub w zasadzie jej brak) oddzielenia samych danych o zdarzeniu od komentarzy dodanych przez podmioty przedstawiające nam te dane, a które mogą w sposób mniej lub bardziej świadomy przekłamywać opis zdarzenia.

Oczywiście organy państwowe zawsze poszukiwały źródeł informacji, które byłyby pomocne w podejmowaniu decyzji lokalnie, jak i ważnych dla całego państwa. Decyzji, od których zależało często bezpieczeństwo państwa: wewnętrzne i zewnętrzne. Od wieków wykorzystywano informatorów, agentów, inne osobowe źródła informacji, przechwytywano i czytano dokumenty zanim stały się one publicznymi. Wszystko to, aby wiedzieć więcej, poznać zamiary wroga, wyprzedzić go, mieć czas na przygotowanie strategii obronnej lub właśnie wykonać wyprzedzający atak.

Jedną z takich technik był i jest tzw. biały wywiad<sup>4</sup>. W odróżnieniu od innych metod pozyskiwania i analizowania informacji przez agendy państwowe, nie miał on charakteru skrytego, tajnego, nielegalnego. Wręcz przeciwnie, korzystał on z powszechnie dostępnych, jawnych źródeł informacji, nie stosowano przy tym żadnych działań operacyjnych. Przymiotnik „biały” miał wprost sugerować jego swoistą niewinność w odróżnieniu od innych metod. Dawniej polegał on na czytaniu książek, ulotek, napisów na murach czy wycinaniu z gazet informacji, które mogły się przydać, a które to dotyczyły zdarzeń, osób lub miejsc będących w zainteresowaniu odpowiednich służb specjalnych<sup>5</sup>, w tym wywiadowczych, kontrwywiadowczych albo dyplomatycznych.

Wraz z intensywnym rozwojem społeczeństwa informacyjnego ilość i kategorie źródeł danych i informacji uległy multiplikacji. Wynika to z oddania w ręce każdego obywatela możliwości komunikowania się za pomocą światowej sieci informatycznej – Internetu. Coś, co w założeniu miało pomóc w koncentracji i wymianie wiedzy naukowej lub wojskowej, uległo całkowitemu upowszechnieniu. Jednocześnie ze wzrostem ilości i kategorii źródeł spadła jakość przekazywanych danych i informacji, w kontekście jej wiarygodności i przydatności dla innych użytkowników sieci, w tym organów państwowych.

Ponadto, we współczesnym społeczeństwie informacja staje się jednym z najważniejszych katalizatorów, czynników leżących u podstaw decyzji podejmowanych nie tylko przez pojedyncze osoby czy korporacje, lecz także całe państwa lub ich organizacje. Pozyskiwanie i analiza informacji przestały być domeną tajnych agend państwowych. Stały się normalną praktyką w każdym gospodarstwie domo-

---

<sup>4</sup> Zob. J.W. Wójcik, Kryminologiczne i kryminalistyczne problemy funkcjonowania wywiadu gospodarczego, [w:] R. Borowiecki, M. Romanowska (red.), System informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa, Warszawa 2001, s. 334 i n.

<sup>5</sup> Z tego zakresu są prowadzone szkolenia m.in. przez Agencję Bezpieczeństwa Wewnętrznego pt. „Biały wywiad – zbieranie informacji z otwartych baz danych”, zob. P. Potejko, 10 lat Centralnego Ośrodka Szkoleniowego ABW w Emowie, Przegląd Bezpieczeństwa Wewnętrznego 2011, Nr 3, s. 198.

## Introduction

The intensity of currently occurring events in our environment is unprecedented<sup>1</sup>. Both individuals and organizations make numerous decisions on a daily basis and participate, either passively or actively, in the ensuing events. Moreover, events are reported by both traditional and modern mass media 24 hours a day, 7 days a week. We are flooded with information from different sources, whether we want it or not. We are becoming an information-based society, with all the good and bad consequences of the fact<sup>2</sup>.

One of the reasons for this is the development of technologies, in particular telecommunication and information technologies<sup>3</sup>. Such technologies facilitate access to information on events occurring even in the most distant parts of the world. We have access to various multi-media material: video, audio, and text. We no longer need any complicated or heavy equipment to receive data and information. Our demand for information is met by entities that offer appropriate services and devices. Thus, the key factor is mobility of both persons and the services offered to them.

Individuals are no longer just passive recipients of content. Technology allows them to create the reality and to comment the events. They can interact with the reality on many levels and use many information distribution channels. Some of them take one more step and manipulate the reality. They give information recipients access only to a selected part of the reality, impose their views, and mix their own comments with data on events and the people involved.

---

<sup>1</sup> K. Dobrzeniecki, *Lex Informatica*, Toruń 2008, p. 41.

<sup>2</sup> R. Tadeusiewicz, *Nowe technologie dowodowe dla przestępstw popełnionych w obszarze Społeczeństwa Informacyjnego* [New evidence technologies for offenses committed within the information-based society], [in:] L. Gardocki, J. Godyń, M. Hudzik, L.K. Paprzycki (eds.), *Nowe technologie dowodowe a proces karny* [New evidence technologies and the penal process], Warsaw 2007, p. 19 ff.

<sup>3</sup> A. Adamski, *Prawo karne komputerowe* [Criminal computer law], Warsaw 2000, p. XV ff.

Nowadays, the basic problem is the possibility (or rather impossibility) to separate data concerning events from the comments added by those presenting the data, who may more or less deliberately distort the description of events.

Of course state authorities have always searched for sources of information that could be used in making decisions that are important both locally and to the whole state, decisions on which the internal and external security of the state would depend. For centuries, states used agents, spies, and other informants, have intercepted and read documents before they became known to the public. All this was done to know more, to learn the intentions of the enemy, be quicker than him, have time to prepare a defense strategy or make a preemptive strike.

One of such techniques was the so-called “white intelligence”<sup>4</sup>. Unlike other methods of obtaining and analyzing information used by state agencies, its nature was not covert, secret, or illegal. On the contrary, it used generally available, open sources of information, without the need for any special operations. The adjective “open” suggests its innocence in comparison with other methods. In the past, it consisted of reading books, brochures, and writings on walls or in cutting out information from newspapers which could be useful and which concerned events, persons, or places that special agencies<sup>5</sup>, to including intelligence, counterintelligence, and diplomatic agencies, were interested in.

With the rapid development of information-based society, the number of data, information sources and their categories has skyrocketed. This is due to the fact that every individual is now able to communicate with the whole world using the World Wide Web. The Internet, which was originally intended to help concentrate scientific or military knowledge and exchange it, became popularized world-wide. At the same time, with the increase of the quantity of information data sources and their categories, the credibility and utility of such data and information to other Internet users, to including state authorities, has significantly decreased.

Moreover, in the contemporary society information has become one of the most important catalysts of decisions made by individuals and corporations, as well as states and international organizations. Acquisition and analysis of information is no longer performed only by secret state agencies. They have become a regular practice in every household or business. Also, new services related to what was once called “white espionage” emerged.

---

<sup>4</sup> See: *J.W. Wójcik*, *Kryminologiczne i kryminalistyczne problemy funkcjonowania wywiadu gospodarczego* [Criminological and criminalistic problems of functioning of economic espionage], [in:] *R. Borowiecki, M. Romanowska* (eds.), *System informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa* [A system of strategic information. Economic espionage and enterprises' competitiveness], Warsaw 2001, p. 334 ff.

<sup>5</sup> Training in this area is conducted, among others, by the ABW („White espionage” – gathering information from open data bases”); see: *P. Potejko*, *10 lat Centralnego Ośrodka Szkoleniowego ABW w Emowie* [10 years of the ABW Training Center in Emów], *Przegląd Bezpieczeństwa Wewnętrznego* 2011, No. 3, p. 198.