Wstęp

Granice między światem wirtualnym a realnym rozmywają się coraz bardziej a Internet przestaje być już tylko medium łączącym ludzi. Zdalne rozpoznawanie, lokalizowanie, analizowanie i kontrolowanie milionów obiektów możliwe jest także bez każdorazowego udziału człowieka. Z projektowaniem i wykorzystywaniem takich rozwiązań wiążą się nowe korzyści, ale i zagrożenia. Współautorzy tej książki, którzy uczestniczą w pracach nad modelem regulacji jawności i jej ograniczeń, analizują techniczne, ekonomiczne i prawne aspekty rozwoju Internetu rzeczy i Inteligentnego miasta.

Internet of Things (IoT) to określenie, które pojawiło się u schyłku XX wieku, ale tłumaczone jest – także w systemie informacji prawnej eur-lex – niejednolicie: jako Internet rzeczy albo Internet przedmiotów. Również znaczenie tego terminu, od dekady występującego w wielu dokumentach urzędowych, w tym dokumentach programowych Unii Europejskiej[1], objaśnia się różnie. Jego geneza i istota charakteryzowane są przez informatyków, ekonomistów i prawników w pierwszej części tego tomu. Deklarowana przez władze publiczne potrzeba regulacji prawnej w tym zakresie, czyni uzgodnienia terminologiczne pilnym zadaniem. Optując za wprowadzeniem do polskiego języka prawnego raczej określenia Internet rzeczy, należy uwzględnić zawartą w ostatnim rozdziale tego tomu kontekstową definicję projektującą obejmującą obiekty realne i wirtualne.

Smart city to określenie, które w dokumentach unijnych agreguje innowacje w zarządzaniu przestrzenią publiczną. Tłumaczy się je zwykle jako Inteligentne miasto, ale też – rozszerzając zakres – jako inteligentną miejscowość. Stopniowe rozbu-

[1] Szerzej por. Komunikat Komisji Europejskiej – Internet przedmiotów: plan działań dla Europy COM (2009) 278; Rezolucja Parlamentu Europejskiego z 15.6.2010 r. w sprawie Internetu przedmiotów (2009/2224(INI). Decyzja Rady z 3.12.2013 r. ustanawiająca program szczegółowy wdrażający program „Horyzont 2020" – program ramowy w zakresie badań naukowych i innowacji (2014–2020) i uchylająca decyzje 2006/971/WE, 2006/972/WE, 2006/973/WE, 2006/974/WE i 2006/975/WE (2013/743/UE); Komunikat Komisji Europejskiej – Europejska agenda bezpieczeństwa COM(2015) 185 oraz Komunikat Komisji Europejskiej – Strategia jednolitego rynku cyfrowego dla Europy COM(2015) 192.

dowywanie katalogu cech, kwalifikujących miejscowość jako inteligentną, ma istotne znaczenie dla finansowania innowacyjnych rozwiązań, których główne obszary, związane m.in. z usługami internetowymi, transportem, energią i zdrowiem prezentowane są w drugiej części książki. Należy je także uwzględniać w planowanym konstruowaniu nowych prawnych instrumentów wspierania innowacyjności.

Rozwój Internetu rzeczy (IoT) i wdrażanie idei inteligentnego miasta (*smart city*), otwiera nowe możliwości redukcji ryzyka: ekologicznego, energetycznego, zdrowotnego, komunikacyjnego i socjalnego. Szansom redukcji różnych rodzajów ryzyka towarzyszą jednak nowe zagrożenia społeczne, ekonomiczne i polityczne, związane ze stałym zwiększaniem dostępu krajowych i zagranicznych producentów i usługodawców, do informacji o użytkownikach rzeczy podłączonych do Internetu. Trudności w ochronie prywatności i interesu publicznego wiążą się także z rozrostem niepublicznych zasobów pochodzących z monitoringu i geolokalizacji, które pozostają w dużej części w gestii grup kapitałowych o płynnej proweniencji. Pojawiają się również wątpliwości, jak funkcjonowałoby państwo i jego „infrastruktura krytyczna" przy aktualnym poziomie podłączenia milionów różnych rzeczy do Internetu w warunkach ekstremalnego zagrożenia. Autorzy rozdziałów trzeciej części tej książki koncentrują się właśnie na problemach zapewniania bezpieczeństwa w korzystaniu z Internetu rzeczy w inteligentnym mieście.

Skuteczna ochrona wolności, własności i bezpieczeństwa nie jest już możliwa bez regulacji zagadnień organizacyjno-technicznych[2]. Zwłaszcza obecny model regulacji jawności i jej ograniczeń[3] wymaga dostosowania do nowych wyzwań związanych z omawianymi w poprzednich tomach tej serii problemami platform internetowych, wielkich zbiorów danych i przetwarzania w chmurze[4], a także Internetu rzeczy i *smart city*. Weryfikacji przez pryzmat interesu publicznego i prywatnego (osób fizycznych i prawnych) wymagają regulacje elektronicznego przetwarzania danych. Dotyczy to m.in. danych o podmiotach publicznych jako użytkownikach Internetu rzeczy. Odnosi się także do roli reglamentacyjnej podmiotów publicznych, m.in. w sferze ochrony i ponownego wykorzystania publicznych baz danych, ułatwiających anonimowym podmiotom identyfikację i nieograniczone niemal profilowanie obywateli.

---

[2] *G. Szpor* (red.), Internet. Ochrona wolności, własności i bezpieczeństwa, Warszawa 2011.

[3] Por. monografie pod red. *G. Szpor*, Jawność i jej ograniczenia: *Z. Cieślak* (red.), t. 2, Podstawy aksjologiczne, Warszawa 2012; *Z. Kmieciak* (red.), t. 3, Skuteczność regulacji, Warszawa 2014; *M. Jaśkowska* (red.), t. 4, Znaczenie orzecznictwa, Warszawa 2014; *A. Piskorz-Ryń* (red.), t. 5, Dostęp i wykorzystywanie; *A. Gryszczyńska* (red.), t. 6, Struktura tajemnic, Warszawa 2014; *Cz. Martysz* (red.), t. 7, Postępowanie administracyjne, Warszawa 2015; *J. Gołaczyński* (red.), t. 8, Postępowania sądowe, Warszawa 2015; *B. Szmulik* (red.), t. 9, Zadania i kompetencje, Warszawa 2015; *J. Majewski* (red.), t. 10, Przeciwdziałanie przestępczości; *C. Mik* (red.), t. 11, Standardy europejskie, Warszawa 2016.

[4] *G. Szpor, W. R. Wiewiórowski* (red.), Internet. Prawno-informatyczne problemy sieci, portali i e-usług, Warszawa 2012; *G. Szpor* (red.), Internet. Cloud computing. Przetwarzanie w chmurach, Warszawa 2013; *G. Szpor* (red.), Internet. Publiczne bazy danych i Big data, Warszawa 2014.

Introduction

Boundaries between virtual and real world are getting blurred and the Internet is starting to be something more than medium merely connecting people. Remote recognition, location, analysis and control of millions of objects is also possible without human intervention. Such solutions bring new possibilities as well as new threats. Co-authors of this book participating in the works concerning the model of regulating of openness and its limitations have been analyzing technical, economic and legal aspects of development of the Internet and smart cities.

The Internet of Things (IoT) is the term which occurred in the late XX century. However its translation into Polish – also in the legal information system EUR-lex – is still not uniform: as the Internet of Things or the Internet of Objects. Also the meaning of mentioned term is appearing in number of official documents including European Union strategy documents in various forms since the las decade. The genesis and essence of this term is characterized by computer scientists, economists and lawyers in the first part of this volume. The necessity of legal regulation in this scope declared by public authorities makes terminological issues urgent. Opting for introduction of the term: Internet of Things to the Polish legal terminology, there is the need of considering context-related definition from the last chapter of this volume which reflects both virtual and real objects.

Smart city is in the European Union documents the term that aggregates innovations concerning public space management. It is commonly translated into Polish as „Inteligentne miasto" but also – broader – as „Inteligentna miejscowość" (smart place). Slow and gradual development of features that qualify the place as smart has significance for the financing of innovative solutions, which main areas concerning e-commerce, transportation and energy are presented in the second part of this book. It should be also considered for designing of new legal instruments of support for innovation.

The development of IoT and implementation of the smart city philosophy opens new possibilities for reduction of ecologic, energetic, health, communication and social

risks. Opportunities of mitigation of various forms of risks are accompanied by new civil, economic and political threats related to the permanent increasing access to the information about end users by domestic and foreign producers and service providers. Difficulties with the protection of privacy and public interest are also connected with the expansion of the non-public information resources obtained from geo-location and monitoring systems which remain in the hands of the corporations with unstable provenance. Concerns occur - how would a country and its critical infrastructure function at actual level of millions of objects connected to the Internet in extreme conditions. The Authors of the third part of this book focus on security issues in usage of the Internet of Things in the smart city.

Effective protection of liberty, property and security will not be possible without the regulation of organizational and technical matters. Above all, current model or regulating of openness and its limitations requires adaptation for new challenges connected with problems elaborated in previous volumes of this series – the Internet platforms, Big Data, cloud computing, Internet of things and smart city. Regulations regarding electronic data processing need verification in the light of public and private (natural and legal person) interest. Among other, it concerns information about public entities as the Internet of Things users. It pertains also to the public entities rationing role, especially in the area of security and re-use of public data bases facilitating anonymous entities identification and almost unlimited profiling of citizens.