Ochrona danych osobowych w Internecie rzeczy w prawie UE

Wstęp

Wstęp

As this election demonstrated,
technology now plays a ubiquitous role in our daily lives.
But people will not use technology they do not trust.

– Brad Smith (President and Chief Legal Officer,
Microsoft Corporation)

Przyjmuje się, że pojęcia „Internet rzeczy" (*Internet of things*, *IoT*[1]) po raz pierwszy użył *K. Ashton* podczas prezentacji wygłoszonej w 1999 r.[2], choć pierwsze udokumentowane posłużenie się przez niego tym pojęciem to dopiero wywiad w magazynie „Forbes" trzy lata później[3]. Internet rzeczy najczęściej definiowany jest jako architektura[4], infrastruktura[5] lub świat[6], w którym dochodzi do łączenia urządzeń codziennego użytku z Internetem, a także pomiędzy sobą. Wizja Internetu rzeczy zakłada połączenie niemal nieograniczonej liczby obiektów, które zbierają dane o swojej pracy oraz o otoczeniu, prze-

[1] W niniejszej pracy jednolicie używane jest pojęcie „Internetu rzeczy", mimo że termin *Internet of things* czasami tłumaczony jest na język polski również jako „Internet przedmiotów" (zob. m.in. *P. Grabiec*, Internet of Things, https://www.spidersweb.pl/2015/04/internet-of-things-internet-rzeczy.html (dostęp: 17.11.2021 r.); *P. Grabiec*, Internet przedmiotów, https://www.computerworld.pl/news/Internet-przedmiotow-i-technologie-ubieralne-to-przyszlosc-pelna-watpliwosci,396614.html (dostęp: 17.11.2021 r.).

[2] *T. Kramp*, *R. van Kranenburg*, *S. Lange*, Introduction to the Internet, s. 1.

[3] *C.R. Schoenberger*, The Internet of Things, https://www.forbes.com/forbes/2002/0318/155.html (dostęp: 17.11.2021 r.).

[4] *R.H. Weber*, Internet of things – Need for, s. 522.

[5] Grupa Robocza Art. 29, Opinion 8/2014 on the on Recent Developments on the Internet of Things (WP 223), 14/EN, 2014 (zachowano oryginalną pisownię tytułu – przyp. aut.); o ile w pracy wyraźnie nie zaznaczono odmiennie, odniesienia do dokumentów Grupy Roboczej Art. 29 dotyczą ich anglojęzycznych wersji, ponieważ przez cały okres funkcjonowania grupy wersje pierwotne dokumentów sporządzane były w tym języku (dopiero w dalszej kolejności tłumaczone na pozostałe języki urzędowe UE).

[6] *S. Haller*, *S. Karnouskos*, *C. Schroth*, The Internet of Things, s. 15.

chowują te dane i wymieniają je między sobą[7]. Przewiduje się, że w 2022 r. liczba urządzeń, które będą połączone z Internetem, wyniesie nawet 50 mld[8].

W niniejszej pracy Internet rzeczy będzie rozumiany jako sieć łącząca ze sobą urządzenia, w ramach której dochodzi do zbierania, wymiany i analizy informacji przez te urządzenia oraz której funkcjonowanie jest zautomatyzowane w taki sposób, że do dokonywania wymiany danych nie jest wymagany udział człowieka. Należy jednak pamiętać, że Internet rzeczy w zasadzie nie jest odrębnym bytem[9], nie stanowi bowiem oddzielnej sieci informatycznej ani nawet wyodrębnionego fragmentu Internetu. Internet rzeczy funkcjonuje jako część globalnej sieci Internet, a kluczowe dla jego wyróżnienia jest korzystanie z technologii, które umożliwiają samodzielne komunikowanie się urządzeń bez konieczności manualnego nawiązania połączenia przez człowieka (np. użytkownika danego urządzenia).

Wdrażanie technologii Internetu rzeczy w praktyce opiera się na istniejącej infrastrukturze internetowej, a polega w szczególności na rozwijaniu komunikacji pomiędzy poszczególnymi obiektami (tzw. zjawisko połączonych urządzeń, *connected devices*). Może ona wykorzystywać standardowe sieci telekomunikacyjne, ale również np. interfejsy typu M2M (*machine-to-machine*)[10], czyli rozwiązania technologiczne pozwalające na bezpośrednią – tj. odbywającą się bez pośrednictwa sieci telekomunikacyjnej – wymianę danych pomiędzy urządzeniami, w szczególności z użyciem technologii NFC (*near-field communication*), RFID (*radio-frequency identification*) lub *Bluetooth*. Dzięki stosowaniu tego rodzaju technologii Internet rzeczy pozwala na komunikację z urządzeniami, które nie posiadają samodzielnego połączenia z Internetem (np. możliwość identyfikacji przesyłek kurierskich zawierających chip komunikujący się z czytnikami przy użyciu technologii RFID).

Technologie Internetu rzeczy mogą znaleźć zastosowanie w każdej sferze życia społecznego, gospodarczego itd. Rozwój Internetu rzeczy ma m.in. ułatwić wymianę towarów i usług[11], wpłynąć na poprawę procesów decyzyjnych opartych na danych gromadzonych w czasie rzeczywistym czy zapewnić lep-

[7] *J.H. Ziegeldorf*, *O.G. Morchon*, *K. Wehrle*, Privacy in the Internet, s. 2728.

[8] Zob. IoT Connections to Grow, https://www.juniperresearch.com/press/iot-connections-to-grow-140pc-to-50-billion-2022 (dostęp: 17.11.2021 r.).

[9] *T. Kramp*, *R. van Kranenburg*, *S. Lange*, Introduction to the Internet, s. 2.

[10] „Interfejsy M2M" (*machine-to-machine interface*) to ogólne pojęcie obejmujące wszystkie interfejsy służące komunikacji pomiędzy dwoma urządzeniami bez udziału czynnika ludzkiego.

[11] *R.H. Weber*, Internet of things: Privacy issues, s. 618.

szą kontrolę procesów związanych ze zdrowiem człowieka[12]. Do praktycznych przykładów wdrożenia technologii Internetu rzeczy zaliczyć można w szczególności:

1) inteligentne sieci energetyczne (tzw. *smart grid*) i systemy zdalnego opomiarowania zużycia energii (tzw. *smart metering*);
2) urządzenia „ubieralne" (*wearable*) – takie jak opaski, soczewki kontaktowe, okulary lub elementy garderoby – służące m.in. do dokonywania płatności lub monitorowania aktywności fizycznej;
3) technologie śledzenia pojazdów i maszyn oraz zbierania parametrów i innych informacji o ich pracy (w tym system szybkiego powiadamiania o wypadkach drogowych eCall, który stanowi obligatoryjny element wyposażenia wszystkich samochodów homologowanych po 31.3.2018 r.);
4) systemy monitoringu wizyjnego (np. CCTV, kamery instalowane w pojazdach), w tym rozwiązania umożliwiające automatyczną analizę obrazu, np. w celu rozpoznawania twarzy;
5) inteligentne sprzęty domowe (np. lodówki umożliwiające zdalne tworzenie i aktualizowanie listy zakupów)[13].

Do najbardziej zaawansowanych wdrożeń Internetu rzeczy można zaliczyć w szczególności ich kompleksowe zastosowanie na dużą skalę w wielu powiązanych ze sobą obszarach funkcjonowania przestrzeni miejskiej (np. sterowanie ruchem drogowym, łączność, bezpieczeństwo, dostarczanie mediów i usług komunalnych). Zjawisko to określane jest jako tworzenie tzw. inteligentnych miast (*smart cities*)[14].

Jako ciekawostki warto wskazać jedne z pierwszych zastosowań technologii Internetu rzeczy w historii. Można zaliczyć do nich przede wszystkim czujniki w automacie z napojami na wydziale informatyki Carnegie Mellon, które (już w połowie lat siedemdziesiątych!) umożliwiały sprawdzenie z użyciem komputera, czy w automacie są dostępne zimne butelki coli[15]. Innym przykładem jest pierwsza kamera internetowa zastosowana w latach 90. XX w. na Cambridge University. Transmitowała ona obraz dzbanka, żeby umożliwić badaczom z innych pięter sprawdzenie, czy znajduje się w nim kawa (co

[12] *T. Kramp*, *R. van Kranenburg*, *S. Lange*, Introduction to the Internet, s. 7.

[13] Szerzej w piśmiennictwie m.in. *Z. Bareisis*, The Internet of Things, s. 236–246; *T. Kramp*, *R. van Kranenburg*, *S. Lange*, Introduction to the Internet, s. 3–10; *W. Iszkowski*, Internet of Things, s. 4–5; Grupa Robocza Art. 29, Opinion WP 223, s. 5–6.

[14] *J. Olbrycht*, Idea smart city, s. 85–86.

[15] Zob. CMU SCS Coke Machine, https://www.cs.cmu.edu/~coke (dostęp: 17.11.2021 r.).

ograniczało ryzyko bezowocnej przerwy kawowej)[16]. W tych przykładach, choć z perspektywy czasu nieco humorystycznych, można już dostrzec jeden z głównych celów wdrożenia Internetu rzeczy – możliwość podejmowania decyzji (np. o przerwie na kawę) na podstawie aktualnych, dostarczonych w czasie rzeczywistym danych o obiekcie.

Pomimo zróżnicowanej natury samych technologii i ich zastosowań w piśmiennictwie podkreśla się, że istnieją dwie dominujące cechy Internetu rzeczy: „po pierwsze, poczucie że łączność internetowa staje się coraz bardziej wszechobecna i powszechna; po drugie, idea że ostatecznie wszystko, w tym zwykłe obiekty fizyczne – zostaną połączone"[17]. Bezpośrednią konsekwencją rozwoju Internetu rzeczy jest zjawisko „wszechobecnej komputeryzacji" czy też „powszechnego przetwarzania" (*ubiquitous computing*), które dostrzegła zresztą w 2014 r. również Grupa Robocza Art. 29 w swojej opinii dotyczącej najnowszych osiągnięć Internetu rzeczy[18]. Wszechobecna komputeryzacja oznacza powszechność technologii informatycznych w otaczającym świecie i możliwość wykorzystania ich w zasadzie w każdym przedmiocie codziennego użytku[19]. Dla przykładu, wg badań GfK udział telewizorów z funkcją *smart TV* w okresie od stycznia do czerwca 2018 wynosił już 85% rynku sprzedaży telewizorów na świecie, a regionalnie w państwach Ameryki Łacińskiej nawet 93%[20]. W piśmiennictwie podkreśla się wręcz, że niezbędne jest ukształtowanie nowego podejścia do produktów, ponieważ coraz częściej nabywane produkty składają się jednocześnie z osprzętu (*hardware*), oprogramowania (*software*) i usługi (*service*), co znacznie komplikuje obrót prawny, w szczególności procesy kontraktowania[21].

---

[16] *R. Kesby*, How the world's first webcam made a coffee pot famous, https://www.bbc.co.uk/news/technology-20439301 (dostęp: 17.11.2021 r.).

[17] *T. Kramp*, *R. van Kranenburg*, *S. Lange*, Introduction to the Internet, s. 2, tł. własne.

[18] Pojęcie to jest niejednorodnie tłumaczone na język polski, w środowisku akademickim można spotkać się m.in. z pojęciami „przetwarzania bez granic" [*A. Romanowski*, Przetwarzanie bez granic, UbiComp, https://www.kis.p.lodz.pl/research,ubiquitous,computing.html (dostęp: 17.11.2021 r.)] i „powszechnej komputeryzacji" [*P. Chrobak*, The Internet of Things – wprowadzenie, http://rfid-lab.pl/the-internet-of-things-wprowadzenie (dostęp: 17.11.2021 r.)], zaś Grupa Robocza Art. 29 używa określenia „wszechobecnej informatyzacji"; zob. Grupa Robocza Art. 29, Opinion WP 223 oraz polska wersja opinii: Grupa Robocza Art. 29, Opinia 8/2014 w sprawie najnowszych osiągnięć w zakresie internetu przedmiotów (WP 223), 1471/14/PL, 2014, s. 4.

[19] *M. Friedewald*, *O. Raabe*, Ubiquitous computing, s. 55.

[20] Zob. Sprzedaż najwyższych modeli telewizorów zapewnia wzrost rynku, https://www.gfk.com/pl/prasa/sprzedaz-najwyzszych-modeli-telewizorow-zapewnia-wzrost-rynku/ (dostęp: 17.11.2021 r.).

[21] *J. Lindqvist*, New challenges, s. 18.

Skokowy wzrost liczby urządzeń oraz możliwość automatycznego łączenia się urządzeń między sobą stanowi rewolucyjną zmianę w obszarze technologii informatycznych[22]. Korzystanie z Internetu coraz rzadziej wymaga aktywnego udziału użytkownika – całe środowisko otaczające człowieka jest bowiem nasycone obiektami, które samodzielnie zbierają dane, wymieniają je między sobą, a także dokonują ich analizy i udostępniają innym osobom (np. usługodawcom lub innym użytkownikom). Dla zobrazowania tego, jak duży jest przyrost wolumenu informacji przetwarzanych w Internecie (zwłaszcza w ciągu ostatniej dekady), warto wskazać, że zgodnie z danymi opublikowanymi przez ITU całkowita światowa przepustowość łączy internetowych w początkach 2016 r. wynosiła 185 000 Gbit/s, podczas gdy jeszcze w 2008 r. – „tylko" 30 000 Gbit/s[23]. Oczywiste jest więc spostrzeżenie, że rozwój Internetu rzeczy musi mieć inherentny, fundamentalny wpływ na ochronę danych osobowych.

Z rozwojem Internetu rzeczy związane są duże nadzieje, m.in. w zakresie poprawy komfortu życia, efektywności procesów decyzyjnych czy rozwoju gospodarczego. Osiągnięcie tych celów nie powinno jednak odbywać się kosztem podstawowych praw i wolności, w tym ochrony danych osobowych użytkowników. W świetle szybkiego rozwoju technologii informatycznych zapewnienie gwarancji tych praw i wolności jest jednym z głównych wyzwań dla prawa UE. Poszanowanie praw człowieka stanowi fundament UE, którego znaczenie podkreślają w szczególności traktaty unijne (m.in. w art. 2 TUE), Karta Praw Podstawowych i orzecznictwo TSUE.

Celem niniejszej pracy jest próba odpowiedzi na pytanie, w jaki sposób przepisy o ochronie danych osobowych odpowiadają na wyzwania związane z rozwojem Internetu rzeczy i czy ta odpowiedź jest adekwatna do charakteru i skali zagrożenia. W szczególności uwaga zostanie poświęcona możliwości sprawowania przez osobę fizyczną kontroli nad przetwarzaniem jej danych osobowych w warunkach wszechobecnej komputeryzacji (tj. gdy otoczenie pozostaje nasycone znaczną liczbą czujników, które zbierają informacje dotyczące tej osoby).

Wydaje się zasadne postawienie hipotezy, że klasyczne instrumenty ochrony danych osobowych, zmierzające do zapewnienia osobie fizycznej kontroli nad swoimi danymi, nie stanowią wystarczającej odpowiedzi na zagrożenia związane z rozwojem Internetu rzeczy. Jednocześnie, biorąc pod uwagę, że

[22] *Ü. Mehmet Bilal*, Turning the crossroad, s. 93–94.

[23] Zob. ICT Facts and Figures 2016, https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf (dostęp: 17.11.2021 r.).

źródłem analizowanych w niniejszej pracy zagrożeń dla ochrony danych osobowych jest rozwój nowych technologii, celowe jest poszukiwanie przez prawodawcę rozwiązań wzorowanych na podejściu stosowanym przy rozwijaniu technologii informatycznych.

Biorąc pod uwagę zróżnicowanie technologii Internetu rzeczy i ich zastosowań, w niniejszej pracy proponuje się przyjęcie przez prawodawcę podejścia, które dążyłoby do kreowania przez niego „skalowalnych"[24] instrumentów prawnych, tj. instrumentów dostosowanych do skali rozwiązań i związanego z nimi ryzyka naruszenia praw i wolności osoby fizycznej. Takie instrumenty wymagają w szczególności przyjęcia przez prawodawcę podejścia opartego na ryzyku (*risk-based approach*) oraz tworzenia regulacji sektorowych, które ze swojej istoty łatwiej nadążają za rozwojem technologicznym. W pracy zostanie dokonana ocena, czy i w jakim stopniu podejście oparte na ryzyku zostało zastosowane w przepisach RODO, a także przedstawione zostaną postulaty *de lege ferenda*.

W tym miejscu należy dodać, że problematyka stosowania regulacji prawnych z zakresu ochrony danych osobowych w związku z rozwojem Internetu rzeczy była już przedmiotem wcześniejszego zainteresowania w piśmiennictwie, choć temat wciąż stanowi pewną nowość w literaturze prawniczej. Jednak chociaż od pewnego czasu można zaobserwować stopniowy wzrost zainteresowania tą tematyką, a do pojęcia Internetu rzeczy odwołuje się już nawet rozporządzenie 2018/1807[25], dorobek nauki nadal jest w tym zakresie niewielki. Nieco większą uwagę tematyce tej poświęca piśmiennictwo zagraniczne, zwłaszcza anglojęzyczne (dla przykładu przywołać można m.in. prace *L. Moerel* i *C. Prins*[26], *R.H. Webera*[27], *M.-H. Maras*[28] czy *J. Lindqvist*[29]). W li-

[24] „Skalowalność" jest pojęciem stosowanym m.in. w naukach informatycznych i jest definiowana jako funkcja opisująca relację pomiędzy obciążeniem a przepustowością (*a function that represents the relationship between workload and throughputy*); zob. *C. Shallahamer*, Forecasting, s. 229.

[25] Dokładnie – motyw 1 oraz motyw 9; Rozp. Parlamentu Europejskiego i Rady (UE) 2018/1807 z 14.11.2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Dz.Urz.UE L Nr 303, s. 59).

[26] *L. Moerel*, *C. Prins*, Privacy for the Homo Digitalis, *passim*.

[27] *R.H. Weber*, Internet of things – Need for; *R.H. Weber*, Internet of things: Privacy; *R.H. Weber*, Internet of Things – New security, *passim*; we współautorstwie z *R. Weber* także: *R.H. Weber*, *R. Weber*, Internet of Things. Legal perspectives, *passim*.

[28] *M.-H. Maras*, Internet of Things, *passim*.

[29] *J. Lindqvist*, New challenges, *passim*; pozycja ta weszła w skład cyklu artykułów stanowiących pracę doktorską autorki nt. ochrony danych osobowych w Internecie rzeczy na Uniwersytecie w Helsinkach (częściowo w oparciu o stan prawny przed RODO). Chociaż autorka w swoim

teraturze polskiej tematyka ta cieszyła się mniejszym zainteresowaniem, ale także wśród krajowych autorów zajmujących się ochroną danych osobowych w kontekście rozwoju Internetu rzeczy można wymienić m.in. *W. Wiewiórowskiego*[30], *M. Czerniawskiego*[31] czy *M. Sakowską-Baryłę*[32]. Biorąc pod uwagę znaczenie problemu, z którym przychodzi się mierzyć regulacjom prawnym, oraz szybkość, z jaką dokonuje się postęp techniczny, niezbędne wydaje się kontynuowanie badań w tym obszarze i dążenie do pogłębienia dotychczasowego stanu wiedzy.

Punktem wyjścia dla analizy prawnej przeprowadzonej w niniejszej pracy jest rozdział pierwszy, koncentrujący się na wynikających z rozwoju technologii Internetu rzeczy zagrożeniach dla ochrony danych osobowych. Obok analizy piśmiennictwa z obszaru ochrony danych osobowych kluczową częścią rozdziału jest przegląd badań empirycznych, które jednoznacznie wskazują, że w obliczu zjawiska powszechnego przetwarzania (*ubiquitous computing*) coraz trudniejsze jest świadome i aktywne sprawowanie kontroli nad swoimi danymi przez osobę, której dane dotyczą.

W rozdziale drugim zawarto syntetyczne omówienie podstaw konstrukcyjnych oraz normatywnych systemu ochrony danych osobowych w prawie UE. Szczególna uwaga została zwrócona na relację pomiędzy dynamicznym rozwojem technologii informatycznych w drugiej połowie XX wieku a wykształceniem się koncepcji autonomii informacyjnej i jej implementacji w systemie prawa UE. Dodatkowo w rozdziale zostały podsumowane najważniejsze zasady ochrony danych osobowych oraz wyjaśniono samo pojęcie danych osobowych i jego szeroką wykładnię w piśmiennictwie i judykaturze.

Rozdziały trzeci i czwarty zostały poświęcone analizie stosowania klasycznych instrumentów ochrony danych osobowych (tj. instrumentów opartych na koncepcji autonomii informacyjnej) w odniesieniu do technologii Internetu rzeczy. W rozdziale trzecim poddano analizie ogólne przepisy inkorporujące zasadę autonomii informacyjnej do prawa ochrony danych osobowych (podstawy prawne przetwarzania danych, obowiązki informacyjne administratora danych oraz uprawnienia osoby, której dane dotyczą). W rozdziale czwartym omówiono natomiast wybrane ograniczenia przetwarzania danych osobowych

doktoracie poruszyła podobny problem badawczy, przyjęła odmienne podejście do tematu (koncentracja na punktowych, wąsko określonych zagadnieniach), a udzielona odpowiedź wydaje się niewystarczająca z perspektywy złożoności tematyki.

[30] *W. Wiewiórowski*, Ochrona danych osobowych, *passim*.

[31] *M. Czerniawski*, Prawne aspekty, *passim*.

[32] *M. Sakowska-Baryła*, Prywatność w inteligentnym mieście, *passim*.

w warunkach Internetu rzeczy. Obydwie części podkreślają znaczenie autonomii informacyjnej dla kształtowania unijnego systemu ochrony danych osobowych (mimo że istnieją silne argumenty przemawiające przeciwko skuteczności tego podejścia, co zostało opisane w rozdziale pierwszym).

Przedmiotem ostatniego rozdziału jest identyfikacja oraz wyjaśnienie alternatywnego podejścia do problematyki ochrony danych osobowych, tj. podejścia opartego na ryzyku. Idea ta została przyjęta przez prawodawcę unijnego w toku prac legislacyjnych nad RODO. Punktem wyjścia dla analizy jest przedstawienie pojęcia ryzyka w znaczeniu, w jakim jest ono stosowane w przepisach RODO. Podkreślono również centralną rolę, jaką dla podejścia opartego na ryzyku odgrywają instrumenty analizy i zarządzania tym ryzykiem (w tym ocena skutków dla ochrony danych). Szczegółowa analiza prawna prowadzi do identyfikacji luk w zakresie stosowania przez prawodawcę unijnego podejścia opartego na ryzyku. Przedstawione zostają również postulaty *de lege ferenda*, mające na celu zamknięcie zidentyfikowanych luk oraz zapewnienie spójności w zakresie stosowania przepisów o ochronie danych osobowych.

Z uwagi na obszerność przedmiotu analizy, a także zarysowaną powyżej dużą elastyczność technologii Internetu rzeczy i możliwość wdrożenia ich w niemal każdej sferze życia, celowe wydaje się zarysowanie wyraźnych granic i założeń definicyjnych analizy prawnej prowadzonej w niniejszej pracy.

Sformułowanie „w warunkach Internetu rzeczy" (wymiennie z bliskoznacznymi określeniami „w Internecie rzeczy" oraz „z wykorzystaniem technologii Internetu rzeczy") jest używane w odniesieniu do przetwarzania danych i innych zjawisk, które charakteryzują obszar rozwoju technologicznego związany z rozwojem Internetu rzeczy.

Pod pojęciem prawa UE rozumiany jest dorobek prawny UE oraz wspólnot europejskich przed Traktatem z Maastricht. Niniejsza analiza nie obejmuje analizy przepisów o ochronie danych osobowych, które zostały przyjęte w zakresie tzw. dawnego II i III filara (tj. w zakresie wspólnej polityki zagranicznej i bezpieczeństwa oraz przestrzeni wolności, bezpieczeństwa i sprawiedliwości)[33]. W tym obszarze kluczowym aktem prawnym jest tzw. dyrektywa policyjna[34], przyjęta niemal równocześnie z RODO, obok której funkcjonuje jed-

[33] Wiele uwagi tematyce ochrony danych osobowych w kontekście współpracy państw członkowskich w obszarze zwalczania przestępczości poświęciła *A. Grzelak*, zob. m.in. *A. Grzelak*, Ochrona danych osobowych; *A. Grzelak*, Wzajemne zaufanie; *A. Grzelak*, *M. Wróblewski*, Niezależność organu.

[34] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy

nak szereg innych aktów prawnych regulujących m.in. funkcjonowanie systemów VIS[35], SIS II[36] i EURODAC[37] czy wymianę danych między organami ścigania[38].

Poza zakresem analizy pozostaje również analiza ochrony danych osobowych w zakresie wdrażania technologii Internetu rzeczy przez podmioty sektora publicznego dla realizacji ich zadań. Ten obszar regulacji posiada bowiem wysoką specyfikę oraz ścisły związek z krajowymi regulacjami, określającymi ustrojowe aspekty funkcjonowania administracji publicznej (w tym materię prawa konstytucyjnego). Dla zapewnienia spójności i integralności prowadzonej analizy celowe jest zatem wyłączenie tych zagadnień z niniejszej pracy[39].

Niniejsza publikacja została oparta na rozprawie doktorskiej „Ochrona danych osobowych w warunkach Internetu rzeczy w prawie Unii Europejskiej", obronionej przeze mnie na Uniwersytecie Jagiellońskim we wrześniu 2019 r. pod kierunkiem prof. *Sławomira Dudzika*, któremu dziękuję za opiekę naukową przez cały okres studiów doktoranckich. Oryginalna wersja pracy została zaktualizowana oraz znacznie skrócona w celu uwzględnienia uwag recenzentów oraz przygotowania do publikacji. Chciałbym w tym miejscu zło-

do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.Urz.UE L Nr 119, s. 89).

35 Rozp. Parlamentu Europejskiego i Rady (WE) Nr 767/2008 z 9.7.2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozp. w sprawie VIS) (Dz.Urz.UE L Nr 218, s. 60)

36 Rozporządzenie (WE) Nr 1987/2006 Parlamentu Europejskiego i Rady z 20.12.2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.Urz.UE L Nr 381, s. 4) oraz Decyzja Rady 2007/533/WSiSW z 12.6.2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.Urz.UE L Nr 205, s. 63).

37 Rozp. Parlamentu Europejskiego i Rady (UE) Nr 603/2013 z 26.6.2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) Nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) Nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (Dz.Urz.UE L Nr 180, s. 1).

38 Decyzja ramowa Rady 2006/960/WSiSW z 18.12.2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej (Dz.Urz.UE L Nr 386, s. 89).

39 Szerzej zob. m.in. *M. Gumularz*, Ochrona danych, *passim*.

żyć również wyrazy wdzięczności recenzentom pracy – prof. *Agnieszce Grzelak* oraz prof. *Robertowi Grzeszczakowi* – za nieocenione uwagi krytyczne. Dodatkowo serdecznie dziękuję dr. *Krzysztofowi Korusowi* za wsparcie mojej wieloletniej pracy badawczej, której owocem jest niniejsza monografia. Wreszcie dziękuję mojej żonie *Joannie*, która nie ograniczyła się do codziennego wsparcia w trudach pracy naukowej, ale pomogła mi ukierunkować poszukiwania w odniesieniu do empirycznej, psychologiczno-społecznej warstwy pracy (pracując równolegle nad swoją rozprawą doktorską).

Praca uwzględnia stan prawny na dzień 1.1.2022 r.