Wstęp

Niezbędnym elementem sprawnego i rzetelnego wykonywania zadań publicznych jest posiadanie odpowiednich pod względem zakresu i treści informacji. Tylko działanie w warunkach pełnej wiedzy o okolicznościach istotnych dla realizacji konkretnego zadania pozwala na eliminację lub zminimalizowanie możliwości powstania nieprawidłowości. Nie bez znaczenia są także wyraźnie artykułowane oczekiwania społeczeństwa dotyczące poziomu i sposobu realizacji usług publicznych. Standardy ich świadczenia mają być takie same jak w sferze komercyjnej. Poza tym nie ma przyzwolenia na podejmowanie błędnych decyzji lub działanie w warunkach niewiedzy lub braku pełnego rozeznania w realizowanej sprawie. Nie oznacza to jednak akceptacji dowolności, szerokiego i nieograniczonego pod względem zakresu zbierania informacji. Trzeba przyjąć bowiem założenie, że dobrem, które ponad wszelką wątpliwość wymaga szczególnej ochrony, jest godność i prywatność osoby. W ten sposób dochodzi do powstania swoistego konfliktu pomiędzy limitowaniem ingerencji w prywatność osoby poprzez ograniczanie przetwarzania informacji o charakterze osobowym a koniecznością szybkiego i skutecznego reagowania na zagrożenia, szczególnie te w sferze bezpieczeństwa zarówno wewnętrznego, jak i zewnętrznego.

Przetwarzanie informacji w administracji publicznej wymaga podjęcia przez nią także skutecznych działań w zakresie stworzenia organizacyjnych i technicznych warunków jej przetwarzania. Problematyka bezpieczeństwa informacji kojarzona jest przede wszystkim z ochroną danych osobowych i ochroną prywatności, ponieważ nieuprawnione ujawnienie informacji o charakterze osobowym godzi bezpośrednio w prawa i wolności człowieka, zwłaszcza zaś w jego godność. A przecież nie mniej istotna jest kwestia ochrony informacji z uwagi na ich szczególną rolę w funkcjonowaniu państwa. Mowa tu oczywiście o ochronie informacji niejawnych. W dyskursie na temat bezpieczeństwa informacji niezmiernie rzadko porusza się kwestie ich autorsko prawnej ochrony, zwłaszcza w działaniach o charakterze promocyjnym, wizerunkowym czy też tajemnicy przedsiębiorstwa. Warto w tym miejscu podkreślić, że problematyka zabezpieczenia przetwarzanych informacji nie jest przez ustawodawcę w sposób precyzyjny określana. Przepisy o ochronie danych osobowych a także regulacje o charakterze wykonawczym w sprawie dokumentacji i warunków technicznych przetwarzania danych osobowych nie zawierają wyraźnie określonych rozwiązań organizacyjnych w zakresie ochrony fizycznej i informatycznej, do stosowania których zobowiązany byłby administrator danych. Raczej wskazywane są metody, sfery wymagające zainteresowania organu administracji publicznej pod kątem ich właściwego zorganizowania, tak aby uzyskać właściwy poziom zabezpieczeń. Brak dokładnej specyfikacji technicznej należy ocenić pozy-

tywnie, ponieważ jej przydatność byłaby niewielka. Każdy bowiem administrator danych ma wypracować własny system zabezpieczeń, dostosowany do jego potrzeb i warunków przetwarzania danych osobowych.

Nie mniej istotnym elementem przetwarzania informacji, który ma też bezpośredni wpływ na przyjęty sposób i poziom stosowanych zabezpieczeń, jest metoda, sposób wykonywania operacji na informacji. Rozwój technik informatycznych i możliwości, jakie daje informatyka, czynią niezbędnym nie tylko zainteresowanie się nowymi formami przetwarzania i zabezpieczania informacji, ale też ich stosowanie. Przykładem jest choćby korzystanie z chmury obliczeniowej, czyli z modelu organizacji pracy polegającego na korzystaniu z usług dostarczonych przez wybranego, zewnętrznego dostawcę w ramach opłaty licencyjnej. Daje ona możliwość zwiększenia efektywności całej gospodarki i poszczególnych organizacji dzięki osiągnięciu większej optymizacji funkcjonowania infrastruktury informatycznej. To właśnie konieczność zapewnienia odpowiedniego poziomu zabezpieczeń czyni niezwykle aktualną dyskusję nad możliwością korzystania także przez administrację z nowych technologii i wykorzystywania nowych proponowanych rozwiązań w zakresie informatyki.

Prezentowana monografia zbiorowa wiąże się z realizowanym w latach 2016-2017 r. w Instytucie Administracji i Prawa Wyższej Szkoły Humanitas projektem badawczym pt. „Bezpieczeństwo informacji w administracji publicznej", finansowanego z dotacji Ministerstwa Nauki i Szkolnictwa Wyższego na podtrzymanie i rozwój potencjału badawczego. Zaproszenie do współpracy przy jej tworzeniu przyjęli naukowcy specjalizujący się nie tylko w zakresie prawa administracyjnego, ale także niezwiązani bezpośrednio z tym obszarem badań naukowych. Z pewnością tak złożone zagadnienie, jakim jest bezpieczeństwo informacji przetwarzanych w administracji publicznej, nie zostało wyczerpane, tym niemniej Autorzy wywodzący się z różnych ośrodków akademickich podjęli się przedstawienia istotnych pod względem prawnym zagadnień dotyczących sfery informacyjnej funkcjonowania administracji publicznej. Wyniki przeprowadzonych badań złożyły się na niniejszą monografię. Podejmowane w niej zagadnienia zostały podzielone na trzy tematyczne rozdziały.

Pierwszy rozdział zatytułowany „Zakres przetwarzania informacji w administracji publicznej" grupuje teksty związane z procesem przetwarzania informacji w administracji publicznej, ze szczególnym uwzględnieniem ich gromadzenia, przechowywania i udostępniania. Grzegorz Krawiec („Działalność Rzecznika Praw Obywatelskich w zakresie ochrony prywatności") ujmuje problematykę prywatności z perspektywy praw człowieka, co jest przedmiotem zainteresowania Rzecznika Praw Obywatelskich. Kontynuuje ten wątek Wojciech Papis („Autonomia informacyjna jednostki w kontekście gromadzenia danych osobowych w postępowaniu karnym"), poruszając kwestię autonomii informacyjnej jednostki w postępowaniu

karnym, czynnościach operacyjno-rozpoznawczych prowadzonych przez policję oraz w działaniach antyterrorystycznych. Z kolei Tomasz Miłkowski („Uprawnienie do gromadzenia informacji w ramach działań antyterrorystycznych") koncentruje się na problematyce gromadzenia informacji (w szerokim ujęciu, a więc również narzędzi do tego służących) w ramach działań antyterrorystycznych, na przykładzie dwóch ustaw: o zarządzeniu kryzysowym i o działaniach antyterrorystycznych. Natomiast Mariusz Koroblowski („Przepadek pojazdu w świetle art. 130a ust. 10 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym – przyczynek do dyskusji") podejmuje problematykę postępowania przed sądem cywilnym inicjowanym na wniosek starosty w sprawie wydania orzeczenia przepadku pojazdu w trybie art. 130a ust. 10 w związku z art. 130a ust. 1 i 2 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym. W toku postępowania sąd może napotkać na szereg rozmaitych trudności, np. w zakresie ustalenia danych osobowych właściciela pojazdu. Istotne znaczenie ma podanie przez wnioskodawcę prawidłowych oraz aktualnych danych adresowych uczestnika postępowania.

Rozdział drugi, traktujący o organizacji zabezpieczenia informacji w administracji publicznej, otwiera opracowanie Doroty Fleszer (Zabezpieczenie danych osobowych – zakres obowiązku i sankcje za jego naruszenie") dotyczące elementów tworzonego przez administratora danych systemu zabezpieczeń przetwarzanych danych osobowych. Tę problematykę uzupełnia Anna Rogacka-Łukasik („Ochrona informacji w jednostkach samorządu terytorialnego poprzez stosowanie polityki bezpieczeństwa informacji"), analizując jeden z dokumentów, którego opracowanie jest wymagane dla właściwie funkcjonującego systemu zabezpieczeń, a mianowicie politykę bezpieczeństwa informacji. Inny aspekt bezpieczeństwa informacji analizuje Katarzyna Płonka-Bielenin („Programy ochrony infrastruktury krytycznej jako dokumenty podlegające przepisom ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych"). Na płaszczyźnie zarządzania kryzysowego ochrona informacji niejawnych dotyczy infrastruktury krytycznej oraz jej ochrony. Potrzeba objęcia wskazanych powyżej dokumentów i informacji ochroną informacji niejawnych podyktowana jest faktem, że zawierają one szczególnie istotne informacje dotyczące bezpieczeństwa państwa i jego obywateli.

W rozdziale trzecim „Sposób i metody przetwarzania informacji w administracji publicznej" Adrianna Paroń („Chmura obliczeniowa a administracja publiczna") podejmuje zagadnienie wykorzystania w administracji publicznej nowej usługi informatycznej, jaką jest chmura obliczeniowa .

Rozległość zagadnienia bezpieczeństwa w administracji informacji publicznej, znaczna ilość aktów normatywnych ją regulujących powoduje, że swobodne poruszane w tej materii jest trudne. W związku z tym wydaje się uzasadnione szersze i głębsze zainteresowanie tą problematyką. Niewątpliwie wyniki badań służyć będą rozwojowi nauki prawa administracyjnego. Podjęta problematyka ma bowiem

przede wszystkim wymiar praktyczny, stąd też wyniki badań kierowane są przede wszystkim do urzędników przetwarzających w ramach realizacji swoich zadań informacje o różnym charakterze. Niewątpliwie skorzystają z nich również studenci, poszerzając i ugruntowując swoją wiedzę w obszarze funkcjonowania administracji publicznej.

Jako reaktor naukowy pragnę serdecznie podziękować wszystkim Autorom tekstów za wkład naukowy, dzięki któremu niniejsza monografia mogła powstać. Serdeczne podziękowania kieruję również do prof. dr hab. Lidii Zacharko za podjęcie wysiłku sprawnego zrecenzowania tekstów zawartych w monografii. Dziękuję również Uczelni, a przede wszystkim Oficynie Wydawniczej „Humanitas" i Pani Redaktor Danucie Dziewięckiej za pomoc w opracowaniu tej publikacji.

Dorota Fleszer