WIEDZA OBRONNA
2020, Vol. 272 No. 3
ISSN: 2658-0829 (Online) 0209-0031 (Print)
Journal homepage: http://wiedzaobronna.edu.pl
DOI: https://doi.org/10.34752/vs7h-g942

JUSTYNA KUREK*
Towarzystwo Wiedzy Obronnej, Warszawa, Polska

OCHRONA DANYCH OSOBOWYCH W DZIAŁANIACH SŁUŻB I PODMIOTÓW BEZPIECZEŃSTWA W DOBIE COVID-19

PERSONAL DATA PROTECTION IN THE ACTIVITIES OF SECURITY SERVICES AND SECURITY ENTITIES DURING THE COVID-19

ABSTRAKT: Światowa pandemia wywołana Covid-19 wymusiła na państwach narodowych reorganizację sposobu funkcjonowania i odwrót od procesów globalizacji. Doświadczenia te wykazały jak kluczowe dla bezpieczeństwa państwa są informacje o charakterze osobowym dotyczące stanu zdrowia osób zamieszkujących na danym terytorium. Nie dziwią więc coraz częstsze tendencje do zarządzania zdrowiem publicznym poprzez aplikacje takie jak domowa kwarantanna lub brytyjska aplikacja modelująca ryzyko zakażeń. W każdym jednakże przypadku utrata kontroli lub zakłóceń w funkcjonowania systemu będzie miała katastrofalne skutki dla bezpieczeństwa państwa i jego funkcjonowania. Sabotaż i zakłócenie funkcjonowania systemów mogą doprowadzić do zamknięcia w kwarantannie całych społeczności bez uzasadnienia lub wręcz przeciwnie multiplikować rozszerzanie się zarazy. Także wrogie przejęcie informacji lub wroga manipulacja danymi przetwarzanymi w systemie może osłabić zdolności ochronne i obronne państwa. W przypadku więc podmiotów wykorzystujących dane osobowe w celach związanych z realizacją zadań z obszaru bezpieczeństwa, wyzwania mają charakter podwójny. Zadaniem, przed którym stają jest z jednej strony ochrona kluczowych wartości o charakterze narodowym, przy zachowaniu jednocześnie ochrony prywatności i godności obywateli. Szczególnym wyzwaniem jest więc w praktyce zapewnienie równowagi pomiędzy efektywnym przeciwdziałaniem zagrożeniom dla bezpieczeństwa państwa a ochroną prywatności obywateli.

SŁOWA KLUCZOWE: Dane sensytywne, dane osobowe, pandemia covid-19

* dr Justyna Kurek, Society of Defence Knowledge, Warsaw, Poland
https://orcid.org/0000-0002-8754-5243 j.kurek@akademia.mil.pl

ABSTRACT: The global Covid-19 pandemic forced states to change and reorganize their way of functioning, it has also slowed down the processes of globalization. These experiences have shown the importance of the health information of people for the purpose of state security. Considering the above, it's no surprise we can observe a growing trend to manage public health through applications such as home quarantine or the UK infection risk modeling application. In any case, however, the loss of control or disturbance in the functioning of the system, will have catastrophic consequences for the security of the state and its functioning. Sabotage and system disruption can lead to unjustified quarantine of entire communities or, on the contrary, multiply the spread of the pandemic. Also, hostile interception of information or hostile manipulation of data processed in the system may disturb the state's protective and defense capabilities. Therefore, in the case of entities using personal data for purposes related to the implementation of tasks in the area of security, the challenges are twofold. The task facing security entities is protection of key national values - on one hand - while at the same time preserving the privacy and dignity of citizens. A particular challenge in practice is therefore to ensure a balance between effective counteracting threats to state security and the protection of citizens' privacy.

KEYWORDS: Sensitiv data, personal data, Covid-19 pandemic

UWAGI WSTĘPNE

Doświadczenia funkcjonowania państw narodowych w warunkach lockdownu wywołanego pandemią covid 19 utwierdzają w słuszności postulowanej w doktrynie nauk o bezpieczeństwie redefinicji zadań państwa i nowego postrzegania bezpieczeństwa narodowego oraz jego wagi dla zapewnienia bytu państwa i jego obywateli. Zmiana sposobu funkcjonowania wymusza szersze wykorzystanie narzędzi i potencjału informacyjnego celem skutecznego zarządzania w nowych warunkach społeczno-gospodarczych. W tych warunkach strategiczne znaczenie odgrywają informacje o charakterze osobowym – zarówno już posiadane przez państwo narodowe, jak i pozyskiwane w związku z wykonywaniem nowych zadań lub tradycyjnych zadań w sposób wymuszony warunkami lockdownu. Warto również podkreślić, że dane osobowe w kontekście bezpieczeństwa państwa muszą być postrzegane w dwóch odsłonach – stanowią one z jednej strony kluczowe narzędzie służące realizacji zadań z zakresu bezpieczeństwa. Z drugiej jednak strony jest to zasób, który musi być chroniony z uwagi na ryzyko naruszenia jego integralności i prawidłowości. Prawidłowe zabezpieczenie zasobów powinno jednocześnie umożliwić ich animizację a być może nawet ich unicestwienie, jeżeli dojdzie do ryzyka utraty pod nimi kontroli. Należy także postawić pytania w kierunku dopuszczalności wykorzystania danych w innym celu niż pierwotny cel ich pozyskania jeżeli działania te będą służyły bezpieczeństwu państwa.

POJĘCIE DANYCH OSOBOWYCH I DANYCH WRAŻLIWYCH W KONTEKŚCIE REALIZACJI ZADAŃ Z OBSZARU BEZPIECZEŃSTWA

Informacje o charakterze osobowym stanowią szczególną kategorię danych wykorzystywanych przez Państwo i jego organy w ramach realizacji zadań z obszaru bezpieczeństwa. Współcześnie, w procesach zarządzania bezpieczeństwem szczególne znaczenie odgrywają informacje o stanie zdrowia. W warunkach zamkniętego w ramy lockdownu społeczeństwa informacyjnego, coraz częściej zarządzanie stanem zdrowia poszczególnych obywateli oraz zdrowiem publicznym odbywa się poprzez systemy informatyczne. Te procesy przy zaletach i niewątpliwym skutku optymalizacyjnym niosą za sobą ogromne ryzyko. Jako więc wyzwanie, szczególnie w obliczu takich zjawisk jak światowa pandemia, należy postrzegać tendencję do informatyzacji informacji wrażliwych.

Niebezpieczeństwo dla państwa i jego niezakłóconego funkcjonowania implikuje dodatkowo fakt, iż pojęcie danych osobowych jest niezwykle pojemne i cechuje je zmienność w czasie. Informacje, których obecnie nie jesteśmy w stanie połączyć z konkretną osobą, w perspektywie postępującego rozwoju cywilizacyjnego i technologicznego potencjalnie mogą być zakwalifikowane w ten właśnie sposób w przyszłości[1]. W zależności więc od technicznych i technologicznych możliwości identyfikacyjnych, danymi osobowymi mogą być między innymi zdjęcia, filmy, dane biometryczne, cechy twarzy czy linie papilarne. Nie można więc z góry wykluczyć osobowego charakteru w zasadzie prawie żadnych informacji. Zadaniem, przed którym stają więc podmioty wykonujące zadania z obszaru bezpieczeństwa jest ochrona kluczowych wartości o charakterze narodowym, przy zachowaniu jednocześnie ochrony prywatności i godności obywateli. Zachowanie właściwej równowagi między prywatnością a bezpieczeństwem narodowym jest często postrzegane jako „gra zerojedynkowa”[2]. Szczególnym wyzwaniem jest więc w praktyce zapewnienie równowagi pomiędzy efektywnym przeciwdziałaniem zagrożeniom dla bezpieczeństwa państwa i a ochroną prywatności obywateli. W niemieckiej doktrynie wskazuje się, że działanie organów ścigania oraz organów bezpieczeństwa musi cechować minimalizm celem zagwarantowania ochrony istoty życia prywatnego[3].

[1] B. Fisher, M. Górski, A. Nerka, M. Sakowska-Baryła, K. Wygoda w Komentarz do Ogólne Rozporządzenie o ochronie danych osobowych M. Sakowska-Baryła red., Warszawa 2018 s. 71/72.
[2] B. Adams striking a balance: privacy and national security in section 702 u.s. person queries WASHINGTON LAW REVIEW 2019 Vol. 94:401 s. 450.
[3] M. Rössel, Teilweise Verfassungswidrigkeit des BKAG, ITRB 2016, s. 149.

Pojęcie danych osobowych

Zgodnie z art. 4 ust. 1 RODO dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Przyjęta w RODO[4] definicja danych osobowych ma charakter horyzontalny i odnosi się całościowo do ochrony danych osobowych w ramach prawa Unii Europejskiej. W odróżnieniu od poprzedniego stanu prawnego, pojęcie danych osobowych ma szerszy zakres przedmiotowy, niż w przypadku ustawy o ochronie danych osobowych z 1997 r.[5] Wynika z niego, że dane osobowe to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej jednak bez kryterium limitacyjnego, które wynikało z art. 6 ust. 3 ustawy. Zgodnie bowiem z tym przepisem informacji nie uważało się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań[6].

Na gruncie RODO nie ma wątpliwości, iż pod pojęciem danych osobowych należy rozumieć poszczególne informacje o osobistych i rzeczowych stosunkach określonej lub możliwej do określenia osoby fizyczne. Z zakresu pojęcia danych osobowych wyłączone są informacje o charakterze anonimowym, uniemożliwiające ponad wszelką wątpliwość identyfikację osób fizycznych. Także z zakresu pojęcia danych osobowych wyłączone są informacje umożliwiające identyfikację innych podmiotów niż osoby fizyczne. Przypisanie danej informacji przymiotu danych osobowych będzie więc uzależnione od czynników zewnętrznych i technologicznych możliwości identyfikacji tej osoby. Nie jest istotne, aby osoba, której dane dotyczą była znana podmiotowi przetwarzającemu dane. Przepisy wymagają jedynie, aby była ona określona[7]. Identyfikacja oznacza natomiast możliwość odróżnienia w grupie danej osoby od pozostałych członków grupy. Przy czym identyfikacja nie musi oznaczać wskazania tej osoby z imienia i z nazwiska. Wystarczające jest wskazanie okoliczności

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

[5] Ustawa o ochronie danych osobowych z 1997 r.

[6] B. Fisher, M. Górski, A. Nerka, M. Sakowska-Baryła, K. Wygoda w Komentarz do Ogólne Rozporządzenie o ochronie danych osobowych M. Sakowska-Baryła red., Warszawa 2018, s. 71.

[7] W. Däubler, J.P. Hjort, M. Schubert M. Wolmerath, Arbeitsrecht, Komentarz. wydanie 2, C.H. Beck 2010, Komentarz do § 3 BDSG. Mimo iż komentarz wydany na gruncie niemieckiej ustawy BDSG, pozostaje on aktualny także na gruncie definicji danych osobowych w RODO.

pozwalających na określenie tej osoby w sposób niepowtarzalny[8]. Przyjmuje się ponadto, iż dana osoba jest możliwa do zidentyfikowania, jeżeli, mimo że nie została jeszcze zidentyfikowana, taka identyfikacja jest możliwa[9].

W literaturze przedmiotu zwraca się również uwagę na fakt, iż za dane osobowe może zostać uznana każda informacja, niezależnie od sposobu i formy jej wyrażenia, bez względu na to czy jest ona powszechnie zrozumiała. Charakter prawny każdej takiej informacji powinien być oceniany dla każdego jej dysponenta w sposób indywidulany[10]. Przykładowo, numer telefonu może być uznany za dane osobowe w związku z tym, iż umożliwia operatorowi identyfikację abonenta, podobnie numer IP komputera a nawet jego MAC adres, będzie dla dostawcy usług pocztowych wystarczający dla zidentyfikowania użytkownika. O tym, na ile poszczególne czynniki identyfikujące pozwalają na ostateczne ustalenie tożsamości, decydują szczególne okoliczności. W przypadku, gdy dostępne czynniki identyfikacyjne nie pozwalają *prima facie* na wyodrębnienie konkretnej osoby, osoba ta może pomimo to być możliwa do zidentyfikowania, ponieważ informacje te w połączeniu z innymi danymi, (którymi dysponuje administrator danych), pozwalają na odróżnienie tej osoby od innych.

W związku z tym należy przyjąć, iż pojęcie danych osobowych i zakres informacji, które mogą być traktowane jako dane umożliwiające identyfikację odbiorcy, są zmienne w zależności od okoliczności i posiadanych przez administratora technicznych i organizacyjnych możliwości identyfikacji. Nie możliwe jest z góry wyłączenie jakiejkolwiek kategorii informacji z zakresu danych osobowych. Dlatego z punktu widzenia realizacji zadań publicznych w obszarze bezpieczeństwa wszelkie informacje, które mogą mieć potencjał identyfikowalny muszą być poddane szczególnej ochronie.

Dane wrażliwe

Z punktu widzenia bezpieczeństwa państwa szczególne zagrożenia wiążą się z całą pewnością z danymi sensytywnymi. Stanowią one szczególną kategorią danych osobowych. Obowiązujące przepisy nie zawierają pozytywnej definicji danych sensytywnych. Art. 9 RODO wskazuje natomiast na pewne kategorie danych osobowych, których przetwarzanie jest uzależnione od spełnienia dodatkowych wymogów. Zgodnie z art. 9 ust. 1 RODO, zabrania się, o ile nie zostanie spełniony jeden

[8] A. Drozd, Pojęcie danych osobowych [w:] Ochrona danych osobowych z perspektywy dziesięciolecia, P. Fajgielski red. Lublin 2008, str. 24.
[9] Opinia 4/2007 w sprawie pojęcia danych osobowych przyjęta w dniu 20 czerwca 2007 r. Grupy Roboczej ds. Danych Osobowych powołanej na mocy art. 29, str. 12.
[10] G. Sibiga, Postępowanie w sprawie ochrony danych osobowych, Warszawa 2003, str. 33.

z warunków uregulowanych w art. 9 ust. 2 RODO[11] przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych[12], danych biometrycznych[13] w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących

[11] Dopuszczalność przetwarzania uzależniona jest od spełnienia przynajmniej jednego z warunków (1) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania (2) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą. (3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody (4) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą (5) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą, (6) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy; (7) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą; (8) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3; (9) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową; (10) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

[12] Zgodnie z art. 4 pkt. 13 RODO dane genetyczne oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej. Są to więc dane osobowe, które dotyczą cech genetycznych osoby fizycznej odziedziczonych przez tę osobę lub nabytych[12]. W Preambule w motywie 34 do RODO wskazuje się, iż dane genetyczne należy zdefiniować jako dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, uzyskane z analizy próbki biologicznej danej osoby fizycznej, w szczególności z analizy chromosomów, kwasu dezoksyrybonukleinowego (DNA) lub kwasu rybonukleinowego (RNA) lub z analizy innych elementów umożliwiających pozyskanie równoważnych informacji.

[13] Zgodnie z art. 4 pkt. 14 RODO, dane biometryczne oznaczają one dane osobowe, które wynikają ze specjalnego przetwarzania technicznego i dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne

zdrowia[14], seksualności lub orientacji seksualnej tej osoby. Wszystkie te kategorie danych mogą stanowić istotny przedmiot analiz podmiotów z sektora bezpieczeństwa państwa[15].

W kontekście sytuacji wymuszonych pandemią covid-19 kluczowe znaczenie wśród informacji osobowych odgrywają informacje o stanie zdrowia. Są to dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie zdrowia. Jak wskazuje się w motywie 35 Preambuły RODO, do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej.

PRZETWARZANIE DANYCH WRAŻLIWYCH

W stosunku do danych wrażliwych, inaczej niż w przypadku zwykłych danych osobowych wprowadzony został ogólny zakaz przetwarzania. Jedynie na zasadzie wyjątku, w przypadku, gdy spełniona będzie jedna z dziesięciu przesłanek legalizujących wskazanych w art. 9 ust. 2 dopuszczalne jest przetwarzanie. W przypadku RODO, następujące przesłanki mogłyby legalizować działanie służb wykonujących zadania z obszaru bezpieczeństwa (1) art. 9 ust. 2 pkt. e - przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą, (2.) art. 9 ust. 2 pkt. g przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Pierwszą ze wskazanych przesłanek jest upublicznię danych przez podmiot danych. Może ono nastąpić zarówno poprzez podanie danych np. w formularzu, rejestrze jak również poprzez udostępnienie informacji których skutkiem jest udostępnienie informacji sensytywnych, przykładowo: zamieszczenie zdjęcia z papierosem lub widoczną niepełnosprawnością. W doktrynie wskazuje się także dopuszczalność podania danych przez inną osobę, ale za wyraźną zgodą osoby,

[14] Trzecią szczególną kategorią danych są dane dotyczące zdrowia. Są to dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie zdrowia.
[15] M.A.Kamiński, *Uprawnienia służb specjalnych w zakresie dostępu do danych osobowych* [w:] *Reforma ochrony danych osobowych – cele, narzędzia, skutki*, J. Taczkowska-Olszewska, M. Nowikowska, A. Brzostek (red), Poznań 2018, s. 138-139.

której dane dotyczą[16] o tyle w żadnym wypadku nie można przyjąć, że podstawa z art. 9 ust. 2 lit. e RODO znajdzie zastosowanie w przypadku upublicznienia danych bez wyraźnej zgody osoby, której one dotyczą (nawet gdy została ona o upublicznieniu należycie poinformowana).

Drugim przypadkiem jest dopuszczalność z uwagi na realizację zadań wynikających bądź z prawa krajowego bądź prawa Unii Europejskiej. Co również istotne, przepisy RODO nie nakazują aby przesłanki przetwarzania były uregulowane w konkretnym rodzaju aktu. Jednocześnie jednak w polskim systemie prawnym jako tego rodzaju ograniczenie należy traktować art. 31 ust. 3 Konstytucji, zgodnie z którym, ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.

Przepisy RODO nakazują jednakże, aby w takim przypadku spełnione były dodatkowe warunki (1) konieczne jest zagwarantowanie że przetwarzanie jest proporcjonalne do wyznaczonego celu (2) nie narusza istoty prawa do ochrony danych (3) przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą (art. 9 ust. 2 lit. g RODO).

PROFILOWANIE W SŁUŻBIE BEZPIECZEŃSTWA PAŃSTWA

Szczególnie istotną formą przetwarzania danych osobowych z punktu widzenia podmiotów bezpieczeństwa i procesów analizy danych jest profilowanie. Oznacza ono dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Wzrost znaczenia profilowania w działaniach operacyjnych wiąże się z ogólną redefinicją modelu działania służb oraz obserwowanym przejściem od procesów ukierunkowanego nadzoru na działania o charakterze prewencyjnym, prowadzone na masową skalę i opartym na hurtowej analizie informacji i masowej inwigilacji, także z wykorzystaniem różnych form agregacji danych oraz ich analizy[17].

[16] J. Barta, P. Fajgielski, R. Markiewicz, Ochrona Danych Osobowych, Kraków 2004, s. 586

[17] J. Kurek, Bezpieczeństwo Państwa w warunkach hybrydowej regulacji danych osobowych w dobie analizy *Big data*. Aspekty prawne, organizacyjne i systemowe, Wydawnictwo ASzWOj. W druku

Wykorzystanie takich narzędzi musi opierać się na założeniu, że zapewnienie odpowiedniego poziomu ochrony nie jest możliwe bez ingerencji w prawa człowieka i polega na inwigilacji nie tylko aktualnych lub potencjalnych przestępców, lecz także niewinnych osób[18]. Jak wskazuje W. Wiewiórowski, profilowaniem nazywamy dwie grupy czynności podejmowanych przez przetwarzającego dane. W pierwszej zbierane są dane z różnych źródeł, o których wiadomo, że dotyczą tej samej zidentyfikowanej osoby. Jest to więc operacja obejmująca zespół technik data miningu dokonywana na zbiorach, w których przetwarzamy dane, co do których mamy silne podstawy, by sądzić, że dotyczą tej samej osoby i są one wystarczająco dobrej jakości, by wspólnie tworzyć wartość dodaną. Metoda oddziałuje przede wszystkim w autonomię informacyjną osoby, powodując, że dane na jej temat zestawiane są ponad standard, jaki wynika z prawa i ponad zakres, na jaki osoba się zgodziła[19]. W drugim rozumieniu profilowanie odnoszone do pojedynczej osoby polega na wnioskowaniu o cechach nieznanych dla data minera z cech przypisanych już wcześniej danej osobie. Ta metoda obejmuje zazwyczaj tworzenie profili grupowych, w których gromadzone są cechy wielu osób, umożliwiając statystyczne wnioskowanie o występowaniu cechy, której u danej osoby nie znamy, na podstawie przynależności tej osoby do populacji wykazującej te same cechy, które u danej osoby już rozpoznaliśmy[20].

WYKORZYSTANIE DANYCH SENSYTYWNYCH W SŁUŻBIE BEZPIECZEŃSTWA PAŃSTWA

Intensyfikację zagrożeń dla wrażliwych danych implikują procesy informatyzacji. Aplikacje mobilne z całą pewnością niosą ogromny potencjał wsparcia usług zdrowia publicznego oraz służb odpowiedzialnych za zapewnienie porządku i bezpieczeństwa. Warto w tym kontekście przyjrzeć się zakresom danych przetwarzanych w rejestrze e-recepta lub danych, które są zbierane przez aplikacje służące zarządzaniu zdrowiem publicznym w czasie kwarantanny. W przypadku lockdownu wywołanego covid-19, kluczową rolę odgrywają dwie kategorie rozwiązań technologicznych. Po pierwsze są to aplikacje służące kontroli przepływów międzyludzkich i dokonujące na tej podstawie modelowania prawdopodobieństwa zachorowań konkretnych członków populacji. Programy takie

[18] Podobnie A. Adamski Dane telekomunikacyjne jako środek inwigilacji masowej w demokratycznym państwie prawa [w:] J. Majewski (red.) Przeciwdziałanie przestępczości. Jawność i jej ograniczenia Tom X s. 2

[19] W. Wiewiórowski, Założenia wstępne dla zrównoważonego przetwarzania informacji ze źródeł publicznych w czasach Big data, [w:] Jawność i jej ograniczenia. Tom XII. Model regulacji. T. Bąkowski (red.) Warszawa 2016, SIP Legalis

[20] W. Wiewiórowski, Założenia wstępne dla zrównoważonego przetwarzania informacji ze źródeł publicznych w czasach Big data , [w:] Jawność i jej ograniczenia. Tom XII. Model regulacji. T.Bąkowski (red.) Warszawa 2016 SIP Legalis za M. Hildebrandt, Who is Profiling Who?, s. 241 oraz A. Canhoto, J. Blackmore, General Description of the Process of Behavioural Profiling, s. 47–48.

dokonują analizy przeszłych kontaktów z osobami zdefiniowanymi jako zagrożone i wskazują, które osoby z uwagi na historię kontaktów powinny być skierowane na kwarantannę. Druga kategoria to aplikacje których celem jest odciążenie służb w kontroli osób przebywających na kwarantannie.

Aplikacje modelujące prawdopodobieństwo zachorowalności na covid-19 na przykładzie rozwiązań brytyjskich

Przykładem pierwszego programu jest aplikacja NHS Covid-19 udostępniona mieszkańcom Anglii oraz Walii. Aplikacja alarmuje użytkownika i wskazuje mu na konieczność udania się do samoizolacji w przypadku, gdy zarejestrowane fizyczne kontakty użytkownika i ich analiza wskazują na wysokie prawdopodobieństwo zakażenia koronawirusem. Algorytm działa w jaki sposób, iż zdarzeniom w postaci kontaktu z osobą zidentyfikowaną w systemie jako nosiciel przypisuje się punkty. Użytkownikowi przypisuje się punkty, jeżeli miał styczność z osobą zakażoną dłużej niż 5 minut. Jeżeli użytkownik znajdował się w odległości większej niż cztery metry punkty nie są dopisywane. Jeżeli odległość fizyczna od zakażonej osoby wynosiła 2-4 metrów przypisywane jest 150 punktów, kontakt poniżej dwóch metrów – 300 punktów. Aplikacja „nakazuje" udanie się na kwarantannę, jeżeli użytkownik uzyskał łącznie 900 punktów. Program nie informuje użytkownika, które z jego kontaktów zostały zakwalifikowane jako groźne i spowodowały dopisanie punktów w systemie. Dane użytkowników są zgodnie z informacjami przekazanymi przez NHS anonimowe. Zgodnie z przepisami prawa komunikat nie jest równoznaczny z bezwarunkowym nakazem udania się na kwarantannę[21]. Nakaz udania się może być jedynie wydany po przeprowadzeniu diagnostyki przez brytyjską służbę zdrowia NHS[22]. Przy czym aplikacja posiada wbudowany moduł zwrócenia się do NHS o przeprowadzenie testów.

Aplikacja wykorzystuje technologię opracowaną przez Apple i Google o nazwie „powiadomienie o narażeniu" i „rejestrowanie narażenia". Ta technologia umożliwia aplikacji wysyłanie alertów przy użyciu losowych identyfikatorów, w przypadku gdy użytkownik znajdował się w pobliżu innego użytkownika aplikacji, u którego wykryto koronawirusa (COVID-19). Zgodnie z oficjalnymi informacjami podanymi na stronie NHS, aplikacja wykorzystuje jedynie siłę sygnału bluetooth dla określenia odległości między obiektami a dane nie są przekazywane poza urządzenie użytkownika,

[21] Statutory Instrument 2020 No. 1045 Public Health, England, The Health Protection (Coronavirus, Restrictions) (Self-Isolation) (England) Regulations 2020, https://www.legislation.gov.uk/uksi/2020/1045/made

[22] https://www.nhs.uk/conditions/coronavirus-covid-19/testing-and-tracing/nhs-test-and-trace-if-youve-been-in-contact-with-a-person-who-has-coronavirus/

jeżeli nie wyrazi on na to zgody[23]. Także identyfikacja w systemie użytkownika jako zakażonego jest zależna od jego woli i musi on wyrazić zgodę na przekazanie takich informacji po uzyskaniu pozytywnego testu covid-19[24]. Aplikacja zgodnie z oficjalnymi informacjami wykorzystuje jedynie nieliczne informacje o charakterze osobowym są to bowiem: numer okręgu pocztowego (kod pocztowy) podawany przez użytkownika podczas instalacji, informacje o objawach wprowadzone dobrowolnie przez użytkownika, kody QR miejsc, które zostaną przez użytkownika zeskanowane do aplikacji, oraz kody generowane codziennie co piętnaście minut celem śledzenia kontaktów. Co istotne, dane składowane są na urządzeniu użytkownika. Jeżeli użytkownik wyrazi dobrowolną zgodę na przekazanie informacji, dane przekazywane poza system są anonimizowane. Analizując sposób działania tego mechanizmu można jednak podejrzewać, że nie mówimy tutaj faktycznie o anonimizacji tylko pseudonimizacji która pozwala na przywrócenie osobowego charakteru informacji.

Prawidłowe funkcjonowanie aplikacji zależy od retencji danych i analizy przeszłych informacji. Zgodnie z założeniami aplikacja ma przechowywać informacje przez minimalny okres konieczny do sprawnego działania. Dane diagnostyczne przechowywane są przez okres 14 dni jako przyjęty termin inkubacji wirusa, klucze zabezpieczające dane przechowywane są w bezpiecznej infrastrukturze DHSC przez kolejne 14 dni. Kody QR przechowuje się przez 21 dni co odpowiada 14 dniowemu okresowi inkubacji wirusa i 7 – dniowemu okresowi zakaźności wirusa. Wszelkie dane analityczne są anonimizowane[25]. Jak wskazują dalej informacje odnoszące się do retencji informacji o charakterze osobowym lub mogących spełniać taki warunek, dane przekazywane poza urządzenie użytkownika nie zawierają żadnych informacji umożliwiających bezpośrednią i pośrednią identyfikację w związku z tym nie są kwalifikowane jako dane osobowe i nie podlegają regulacjom RODO i innym przepisom dotyczącym danych osobowych. Informacje przechowywane są w postaci danych analitycznych. Przechowywanie rekordów powiązanych z aplikacją można podzielić na 2 kategorie według czasu przechowywania. Dane służące rozliczeniom – 8 lat. Informacje służące monitorowaniu chorób zakaźnych w postaci zanonimozowanej przechowywane są przez 20 lat celem ochrony zdrowa publicznego[26].

[23] https://www.nhs.uk/conditions/coronavirus-covid-19/testing-and-tracing/
[24] https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-test-and-trace-app-early-adopter-trial-august-2020-privacy-notice
[25] https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/the-nhs-test-and-trace-app-early-adopter-trial-august-2020-data-protection-impact-assessment
[26] https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/the-nhs-test-and-trace-app-early-adopter-trial-august-2020-data-protection-impact-assessment#retention

Dostępne informacje w żaden sposób nie odnoszą się do kwestii dostępu do danych przez podmioty trzecie nienależące do służb odpowiedzialnych za zdrowie publiczne. Zgodnie z informacjami pochodzącymi od twórców aplikacji informacje są przechowywane na urządzeniach końcowych użytkowników i nie są przekazywane do centralnej bazy. Pytaniem jednak bez odpowiedzi jest czy dane podlegają przykładowo automatycznemu back-upowi danych w chmurach obliczeniowych np. w usłudze icloud, jeżeli użytkownik korzysta z takiego urządzenia. Zgodnie z informacją producenta, aplikacja nie wykorzystuje dostępu do pamięci urządzenia mobilnego czy repozytorium zdjęć. Nie jest jednakże jednoznaczne czy ma taką potencjalną funkcjonalność. Także zgodnie z przekazanym oficjalnie informacjami po odinstalowaniu wszelkie informacje są usuwane, zasadniczym jednak pytaniem jest czy po odinstalowaniu aplikacja może generować tylne wejście do systemu operacyjnego dla służb bezpieczeństwa państwa. Należy także zwrócić uwagę, że zakres informacji które nawet przy założeniu ich anonimizacji są przetwarzane jest bardzo szeroki w szczególności na urządzeniach końcowych. Powstaje też pytanie, czy dane które w taki sposób zostały zebrane i poddane na poziomie urządzenia końcowego pseudonimizacji mogą być przez administratora systemu poddane procesom odwróconym. Czy administrator posiada informacje, które pozwalają przekazanym danym o charakterze anonimowym przypisać charakter osobowy. A także czy może po stronie administratora dojść do zmiany celu przetwarzania.

Również wyobrażalne ryzyko utraty przez administratora i podmioty zarządzające zdrowiem publicznym kontroli nad danymi może mieć katastrofalne skutki dla bezpieczeństwa państwa. Rozproszona koncepcja przetwarzania danych wydaje się być rozwiązaniem wspierającym ochronę zarówno prywatności użytkowników jak i bezpieczeństwo państwa. Nie jest ona jednak wolna od ryzyka. Powszechność użycia może generować atrakcyjność tworzenia wirusów, które pod pretekstem aktualizacji aplikacji doprowadzą do zainfekowania i przejęcia kontroli nad danymi.

Aplikacje w służbie kontroli przebywania na kwarantannie

Przykładem aplikacji o bardzo dużym potencjale użytkowym dla służb bezpieczeństwa są rozwiązania technologiczne które mają wspierać kontrolę przebywania osób na kwarantannie. Rozwiązaniem takim jest polska aplikacja e-kwarantanna. Celem wsparcia służb policyjnych w kontroli osób przebywających na kwarantannie udostępniona została aplikacja kwarantanna domowa. Pierwotnie program ten był dobrowolny, jednak od 1 kwietnia, zgodnie z art. 7e ust. 1 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem

i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych[27] instalacja aplikacji stała się obowiązkowa. Głównym celem aplikacji jest kontrola czy osoby poddane kwarantannie przebywają w miejscu wskazanym do jej odbycia. Użytkownicy aplikacji mają wysyłane polecenia wykonania zdjęć selfie i przesłania ich poprzez aplikację do podmiotu nadzoru. Niewykonanie zadania w terminie dwudziestu minut powoduje uruchomienie kontroli fizycznej i powiadomienie stosownych służb.

Aby aplikacja kwarantanna domowa mogła służyć celom bezpieczeństwa i zdrowia publicznego zbiera ona informacje o użytkownikach w tym dane osobowe. Zgodnie z regulaminem[28] pozyskuje ona ID obywatela – techniczny identyfikator, imię, nazwisko, numer telefonu, deklarowany adres pobytu, zdjęcie, lokalizację obywatela oraz datę końca kwarantanny. Aplikacja ma jednak szerszy zakres uprawnień, zgodnie z informacją przekazaną przez Fundację Panoptykon ma ona także dostęp do informacji o: sieci Wi-Fi z która łączy się użytkownik, zawartości pamięci urządzenia wraz z możliwością modyfikowania lub kasowania jego zawartości. Jak wskazuję się, jest to funkcjonalność potrzebna w sytuacji gdy użytkownik posiada aplikacje oszukujące lub zakłócające funkcjonowanie aplikacji. Ponadto odczytuje ona identyfikator urządzenia i informacje o połączeniu, ma dostęp do aparatu i mikrofonu mogąc nagrywać dźwięk i wideo. Aplikacja odczytuje ponadto lokalizację na bazie danych z sieci komórkowej i GPS. Ma również kontrolę nad latarką. Po zainstalowaniu aplikacji okazuje się, że sprawdza też, jakie inne aplikacje są zainstalowane na telefonie i czy nie ma wśród nich takiej, która oszukuje lokalizację[29]. Aplikacja nie kontroluje w sposób stały lokalizacji użytkownika, a jedynie w czasie wykonywania zadania. Dane w sposób centralny przechowywane są przez okres sześciu lat. Szeroki jest również zakres podmiotów mających dostęp do danych. Są to: Komenda Główna Policji, Wojewódzkie Komendy Policji, wojewodowie, Centralny Ośrodek Informatyki, Centrum Systemów Informacyjnych Ochrony Zdrowia oraz prywatna firma będąca twórcą aplikacji Take Task SA.

W mediach społecznościowych związanych z ochroną prywatności zwraca się uwagę, iż tego rodzaju aplikacje i zbierane przez nie informacje mogą być wykorzystywane do udoskonalania algorytmów rozpoznawania cech biometrycznych przez służby specjalne. Eksperci zwracają także uwagę, iż ogromna liczba zdjęć wraz z tłem, na którym są zrobione trafia na serwery rządowe. Wskazuje się ponadto, iż przyjęte w Polsce rozwiązanie jest mocno ingerujące w prywatność. Jak

[27] Dz. U. poz. 374, z późn. zm.
[28] file:///Users/admin/Downloads/Kwarantannadomowaregulamin_60501397%20(1).pdf
[29] https://panoptykon.org/aplikacja-kwarantanna-domowa

wskazuje dla Panoptykon M. Chrobak, z punku widzenia ochrony prywatności użytkowników, przy jednoczesnym zachowaniu korzyści funkcjonalnej byłoby wykorzystanie analizy zgodności twarzy na urządzeniu. Takie algorytmy mogą tworzyć lokalny model cech biometrycznych. Suma kontrolna takiego wzoru mogłaby być przechowywana na serwerze, by weryfikować, czy wzór się nie zmienił w czasie. W przypadku nadejścia żądania weryfikacji lokacji oraz twarzy sprawdzane byłoby tylko to, czy lokalny wzorzec się nie zmienił, a następnie – również lokalnie – następowałoby porównanie twarzy z wzorcem.[30]

Analizując wykorzystanie aplikacji kwarantanna domowa dla celów związanych z bezpieczeństwem państwa należy zwrócić uwagę, iż przy całej rozpiętości zalet i korzyści związanych z użyciem tej aplikacji istnieją także poważne ryzyka dla bezpieczeństwa zarówno samych obywateli jak i bezpieczeństwa państwa. Sytuacją mocno niepokojącą jest zakres dostępu do informacji przez podmiot prywatny, twórcę aplikacji. Należy w takim przypadku zawsze postulować wzorem rozwiązań przyjętych w innych państwach, aby aplikacje i oprogramowanie strategiczne z punktu widzenia bezpieczeństwa państwa i obywateli były rozwijane w ramach struktur publicznych. Outsourcing takich aplikacji do sektora prywatnego implikuje ryzyko dla bezpieczeństwa państwa i obywateli. Podobnie, jak w przypadku innych aplikacji i oprogramowania strategicznego z punktu widzenia bezpieczeństwa państwa i działania służb porządkowych, konieczne wydaje się ponadto postawienie pytań o dopuszczalny zakres współpracy między organami ściągania a sektorem prywatnym w rozwoju takich narzędzi. Czy państwo może korzystać z gotowych rozwiązań komercyjnych, czy też konieczne jest zamawianie rozwiązań tworzonych wyłączenie na zlecenie podmiotów publicznych? Trzeba podkreślić, że nawet w przypadku rozwiązań dedykowanych organom ścigania, ich stosowanie wiąże się z ryzykiem pozostawienia tzw. tylnych wejść do programu oraz trudnościami z zabezpieczeniem poufności kodów źródłowych. Zapewne bezpieczniejsze, ale i kosztowniejsze, byłoby rozwijanie takich narzędzi w obrębie wyspecjalizowanych jednostek w ramach organów ścigania[31].

[30] https://panoptykon.org/aplikacja-kwarantanna-domowa

[31] J. Kurek, *Wykorzystanie szpiegowskiego oprogramowania w działalności operacyjnej organów ścigania. Gwarancje konstytucyjne i procesowe z perspektywy doświadczeń niemieckich*, „Przegląd Policyjny" 2016, nr 1 s. 159-171

PODSUMOWANIE

Światowa pandemia wywołana Covid-19 wymusiły na państwach narodowych reorganizację sposobu funkcjonowania i odwrót od procesów globalizacji. Społeczeństwo XXI wieku, przyzwyczajone do otwartego funkcjonowania, podróży, alokacji produkcji i zasobów na drugim końcu globu oraz snujące wizje poszerzania przestrzeni życiowej poprzez nieuchronną kolonizację kosmosu – zostało z dnia na dzień zmuszone do funkcjonowania w warunkach izolacji - zamknięcia granic i ograniczenia aktywności społecznej, kulturowej i gospodarczej. Aby przetrwać należało wdrożyć szybkie procesy deglobalizacji i jeszcze bardziej rozwijać usługi on-line. Pogłębiło to tendencje cyfryzacji i informatyzacji. Doświadczenia ostatnich tygodni utwierdzają w słuszności koncepcji wspierania rozwoju informatyzacji i cyfryzacji wielu obszarów życia społecznego i gospodarczego w warunkach gwarantowanego przez państwo cyberbezpieczeństwa.

Doświadczenia funkcjonowania państwa w warunkach deglobalizacji i lockdownu pokazują jak kluczowe dla bezpieczeństwa państwa są informacje o charakterze osobowym dotyczące stanu zdrowia osób zamieszkujących na danym terytorium. Nie powinno więc dziwić, iż coraz częściej podnoszone są postulaty zarządzania zdrowiem publicznym poprzez aplikacje takie jak domowa kwarantanna lub brytyjska aplikacja modelująca ryzyko zakażeń. Trzeba jednak zwrócić uwagę, iż w każdym przypadku utraty kontroli lub zakłóceń w funkcjonowaniu systemu skutki dla bezpieczeństwa państwa i jego funkcjonowania mogą być bardzo poważne. Sabotaż i zakłócenie funkcjonowania systemów mogłoby doprowadzić do zamknięcia w kwarantannie całych społeczności bez uzasadnienia lub wręcz przeciwnie multiplikować rozszerzanie się zarazy. Każdych z wariantów w przypadku sytuacji zagrożeń doprowadzi do paraliżu funkcjonowania państwa i osłabi jego zdolność ochronną. Przeniesienie informacji o stanie zdrowia populacji do systemu informatycznego może ułatwić zarządzenie usługami medycznymi, może jednak zdestabilizować funkcjonowanie państwa i jego zdolność obronną i ochronę obywateli w sytuacji utraty kontroli nad danymi. Także wrogie przejęcie informacji lub wroga manipulacja danymi przetwarzanymi w systemie może osłabić zdolności ochronne i obronne państwa. W przypadku więc podmiotów wykorzystujących dane osobowe w celach związanych z realizacją zadań z obszaru bezpieczeństwa, wyzwania mają charakter podwójny. Zadaniem, przed którym stają jest z jednej strony ochrona kluczowych wartości o charakterze narodowym, przy zachowaniu jednocześnie ochrony prywatności i godności obywateli. Szczególnym wyzwaniem jest więc w praktyce zapewnienie równowagi pomiędzy efektywnym przeciwdziałaniem zagrożeniom dla bezpieczeństwa państwa a ochroną prywatności obywateli. Jak podkreślił bowiem niemiecki Federalny Trybunał Konstytucyjny (BVerfG) „Bezpieczeństwo państwa

stanowi źródło spokoju i porządku publicznego a wynikające z niego poszanowanie dla godności i własnej wartości jednostki muszą zostać zagwarantowane dla bezpieczeństwa ludności jako wartości konstytucyjne, które stają na równi z innymi konstytucyjnymi dobrami”[32]. Ochrona bezpieczeństwa narodowego i porządku publicznego przyczyniają się bowiem również do ochrony praw i wolności innych osób[33]. Bezpieczeństwo należy więc postrzegać jako pozostające w służbie wolności[34].

BIBLIOGRAFIA
REFERENCES LIST

PIŚMIENNICTWO
LITERATURE

Adams, B. striking a balance: privacy and national security in section 702 u.s. person queries WASHINGTON LAW REVIEW 2019 Vol. 94:401

Adamski, A. Dane telekomunikacyjne jako środek inwigilacji masowej w demokratycznym państwie prawa [w:] J. Majewski (red.) Przeciwdziałanie przestępczości. Jawność i jej ograniczenia Tom X

Barta, J. Fajgielski, P. Markiewicz, R. Ochrona Danych Osobowych, Kraków 2004

Buchholtz, G., Kein Sonderopfer für die Siecherheits BVerfG erklärt BKAG für verfassungswidrig, NVwZ, 2016

Canhoto, A. Blackmore, J. General Description of the Process of Behavioural Profiling.

Däubler, W. Hjort, JP. Schubert M. Wolmerath, M. Arbeitsrecht, Komentarz. wydanie 2, C.H. Beck 2010, Komentarz do § 3 BDSG.

Drozd, A. Pojęcie danych osobowych [w:] Ochrona danych osobowych z perspektywy dziesięciolecia, P. Fajgielski red. Lublin 2008

Fisher, B. Górski, M. Nerka, A. Sakowska-Baryła, M. Wygoda K. w Komentarz do Ogólne Rozporządzenie o ochronie danych osobowych M. Sakowska-Baryła red., Warszawa 2018

Hildebrandt, M. Who is Profiling Who?,

Kamiński M.A., Uprawnienia służb specjalnych w zakresie dostępu do danych osobowych [w:] Reforma ochrony danych osobowych – cele, narzędzia, skutki, J. Taczkowska-Olszewska, M. Nowikowska, A. Brzostek (red.), Poznań 2018.

Kurek, J. Bezpieczeństwo Państwa w warunkach hybrydowej regulacji danych osobowych w dobie analizy *Big data*. Aspekty prawne, organizacyjne i systemowe, Wydawnictwo ASzWOj. W druku

Kurek, J. Wykorzystanie szpiegowskiego oprogramowania w działalności operacyjnej organów ścigania. Gwarancje konstytucyjne i procesowe z perspektywy doświadczeń niemieckich, „Przegląd Policyjny” 2016, nr 1

Rössel, M. Teilweise Verfassungswidrigkeit des BKAG, ITRB 2016

Sibiga, G. Postępowanie w sprawie ochrony danych osobowych, Warszawa 2003

[32] Punkt 100 wyroku BVerfG w spawie: BVR 966/09 i 1 BVR 1140/09
[33] Punkt 53 — wyrok Europejskiego Trybunału Sprawiedliwości z 15 lutego 2016 w sprawie C-601/15,
[34] G. Buchholtz, Kein Sonderopfer für dieSiecherheits BVerfG erklärt BKAG für verfassungswidrig, NVwZ, 2016 s. 909.

Wiewiórowski, W. Założenia wstępne dla zrównoważonego przetwarzania informacji ze źródeł publicznych w czasach Big data, [w:] Jawność i jej ograniczenia. Tom XII. Model regulacji. T. Bąkowski (red.) Warszawa 2016, SIP Legalis

ŹRÓDŁA
SOURCES

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

Ustawa o ochronie danych osobowych z 1997 r.

Statutory Instrument 2020 No. 1045 Public Health, England, The Health Protection (Coronavirus, Restrictions) (Self-Isolation) (England) Regulations 2020, https://www.legislation.gov.uk/uksi/2020/1045/made

Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych Dz. U. poz. 374, z późn. zm.

Opinia 4/2007 w sprawie pojęcia danych osobowych przyjęta w dniu 20 czerwca 2007 r. Grupy Roboczej ds. Danych Osobowych powołanej na mocy art. 29, str. 12.

Wyrok BVerfG z 20.04.2016 w spawie: BVR 966/09 i 1 BvR 1140/09 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs201604201bvr096609.html

Wyrok Europejskiego Trybunału Sprawiedliwości z 15 lutego 2016 w sprawie C-601/15,

https://www.nhs.uk/conditions/coronavirus-covid-19/testing-and-tracing/nhs-test-and-trace-if-youve-been-in-contact-with-a-person-who-has-coronavirus/

https://www.nhs.uk/conditions/coronavirus-covid-19/testing-and-tracing/

https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-test-and-trace-app-early-adopter-trial-august-2020-privacy-notice

https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/the-nhs-test-and-trace-app-early-adopter-trial-august-2020-data-protection-impact-assessment

https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/the-nhs-test-and-trace-app-early-adopter-trial-august-2020-data-protection-impact-assessment#retention

file:///Users/admin/Downloads/Kwarantannadomowaregulamin_60501397%20(1).pdf

https://panoptykon.org/aplikacja-kwarantanna-domowa
