Sylwia Kotecka-Kral[1]
Uniwersytet Wrocławski
Wydział Prawa, Administracji i Ekonomii
ORCID: 0000-0002-4425-805X

DOI: 10.34616/144505

Interoperacyjność aplikacji mobilnych śledzących kontakty zakaźne

Interoperability of mobile applications tracking infectious contacts

Streszczenie: W niniejszym opracowaniu poruszono zagadnienia aplikacji mobilnych śledzących kontakty zakaźne, danych przez nie gromadzonych oraz podmiotów, które mogą mieć do nich dostęp. Niektóre z danych zebranych przy pomocy aplikacji mobilnych zakwalifikowano jako informacje sektora publicznego, które mogą być ponownie wykorzystywane. Na przykładzie polskiej aplikacji STOP COVID – ProteGO Safe omówiono przydatność aplikacji mobilnych do innych celów niż ostrzeganie o kontakcie z osobą zakażoną wirusem SARS-CoV-2. Uwzględniono kontekst interoperacyjności aplikacji mobilnych śledzących kontakty zakaźne, w tym interoperacyjności transgranicznej na obszarze Unii Europejskiej.

Słowa kluczowe: aplikacja mobilna, COVID-19, dane osobowe

Abstract: The study discusses issues of mobile applications tracking infectious contacts, data collected by them and entities that may have access to them. Some of the data collected with the use of mobile applications has been classified as public sector information that can be reused. Using the example of the Polish STOP COVID – ProteGO Safe application, the usefulness of mobile applications for purposes other than warning about contact with a person infected with the SARS-CoV-2 virus was discussed. The context of interoperability of mobile applications tracking infectious contacts, including cross-border interoperability within the European Union, has been taken into account.

Keywords: mobile application, COVID-19, personal data

[1] Adres poczty elektronicznej: sylwia.kotecka-kral@uwr.edu.pl.

1. Dane publiczne

W wyniku wykonywania zadań publicznych gromadzi się, produkuje, reprodukuje i rozpowszechnia szeroki zakres informacji w wielu obszarach działalności, takich jak społeczeństwo, polityka, ekonomia, prawo, geografia, środowisko, pogoda, sejsmiczność (w znaczeniu skłonności danego terenu do występowania naturalnych trzęsień ziemi na danym obszarze)[2], turystyka, przedsiębiorczość, patenty czy edukacja[3]. Dane te zwykło się określać mianem publicznych, w odróżnieniu od danych prywatnych[4], które definiuje nowa polska ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego[5], uchwalona w wyniku implementacji dyrektywy Parlamentu Europejskiego i Rady (UE) z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego

[2] Zob. np. https://www.usgs.gov/ [dostęp: 19.09.2021].

[3] Zob. np. Portal Otwartych Danych Unii Europejskiej, https://data.europa.eu/euodp/pl/data/ [dostęp: 19.09.2021], repozytorium najczęściej używanych dokumentów w krajach członkowskich Unii Europejskiej – *Repository of most commonly used public documents*, https://ec.europa.eu/internal_market/imi-net/repositories/commonly-used-public-documents/index_en.htm [dostęp: 19.09.2021], repozytorium publicznych danych o działalności naftowej na norweskim szelfie kontynentalnym, prowadzone przez Norwegian Petroleum Directorate, https://www.npd.no/en/about-us/information-services/open-data/ [dostęp: 19.09.2021)], estoński portal otwartych danych, https://opendata.riik.ee/en/andmehulgad/ [dostęp: 19.09.2021], fiński portal otwartych danych, https://www.avoindata.fi/en [dostęp: 19.09.2021], repozytorium Statistics Finland, http://www.stat.fi/org/avoindata/index_en.html [dostęp: 19.09.2021], repozytorium danych publicznych Stanów Zjednoczonych Ameryki Północnej, https://www.data.gov/ [dostęp: 19.09.2021] czy informacji związanych z wirusem SARS-CoV-2 – *Coronavirus (COVID-19)* w USA, https://www.coronavirus.gov/ [dostęp: 19.09.2021], repozytorium danych National Institut of Standards and Technology (NIST), https://data.nist.gov/sdp/#/ [dostęp: 19.09.2021].

[4] Danymi prywatnymi jest każda treść lub jej część, niezależnie od sposobu utrwalenia, w szczególności w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej, będąca w posiadaniu podmiotu innego niż podmiot zobowiązany i przez niego wytworzona, z wyjątkiem danych osobowych (art. 2 pkt 5). Za dane prywatne w rozumieniu ustawowym uznaje się wszelkie treści będące w posiadaniu (i przez nie wytworzone) podmiotów innych niż te, które wymienione zostały w art. 3 ustawy. W szczególności będą to zasoby danych znajdujące się w posiadaniu przedsiębiorców czy też organizacji pozarządowych (i przez nich wytworzone); zob. *Uzasadnienie rządowego projektu ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego*, druk sejmowy nr IX.1338, s. 13.

[5] Dz. U. z 2021 r. poz. 1641, dalej jako u.o.d.p.w.i.

wykorzystywania informacji sektora publicznego[6]. Przykładem polskiej bazy danych publicznych jest Centralne Repozytorium Informacji Publicznej[7], które zawiera dane mające potencjał dla rozwoju społeczeństwa informacyjnego i dalszego wykorzystywania w produktach, usługach czy aplikacjach. Powstało ono na podstawie art. 9a ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej[8]; mowa o nim także w art. 5 ustawy z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego[9]. Ostatnia z wymienionych ustaw została uchylona z dniem 8.12.2021 r. przez wspomnianą już ustawę z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, która posługuje się pojęciem „portal danych" w miejsce „Centralnego Repozytorium Informacji Publicznej". Portal danych został zdefiniowany w jej art. 2 pkt 13 jako prowadzony przez ministra właściwego do spraw informatyzacji, powszechnie dostępny system teleinformatyczny, służący do udostępniania informacji sektora publicznego w celu ponownego wykorzystywania oraz danych prywatnych w celu wykorzystywania. Zmiana nazewnictwa nastąpiła także w ustawie o dostępie do informacji publicznej[10].

W polskim systemie prawnym zamiast pojęcia „dane publiczne" funkcjonuje pojęcie „informacji sektora publicznego". Informacja sektora publicznego to każda treść lub jej część, niezależnie od sposobu utrwalenia, w szczególności w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej, będąca w posiadaniu podmiotu zobowiązanego (art. 2 pkt 8 u.o.d.p.w.i.); podmioty zobowiązane zostały wskazane w art. 3 tej ustawy. Pojęcie to należy odnieść do definicji „dokumentu" w rozumieniu art. 2 pkt 6 dyrektywy 2019/1024, zgodnie z którym „dokument" oznacza dowolną treść lub dowolną część tej treści niezależnie

[6] Dz. Urz. UE L 172 z 26.06.2019 r., s. 56. Termin na jej implementację minął 17.07.2021 r.

[7] https://dane.gov.pl/pl/ [dostęp: 31.10.2020]; przepisy art. 9a ustawy o dostępie do informacji publicznej weszły w życie z dniem 8.09.2012 r.

[8] T.j. Dz. U. z 2020 r. poz. 2176.

[9] T.j. Dz. U. z 2019 r. poz. 1446.

[10] Zob. art. 50 pkt 2-5 u.o.d.p.w.i.

od jej nośnika (papier lub forma elektroniczna lub zapis dźwiękowy, wizualny bądź audiowizualny). Dla jasności wywodów zawartych w niniejszym opracowaniu należy jedynie wskazać, że pojęcie informacji sektora publicznego wyznacza zakres przedmiotowy ponownego wykorzystywania, a dla zakwalifikowania określonej informacji jako informacji sektora publicznego nie ma znaczenia jej treść. Istotne jest natomiast jej utrwalenie oraz fakt posiadania przez podmioty udostępniające lub przekazujące ją w celu ponownego wykorzystywania. Definicja informacji sektora publicznego jest szersza niż pojęcie informacji publicznej i zawiera w sobie informację publiczną oraz inne treści (wykraczające poza zakres pojęcia informacji publicznej), tj. np. zasoby bibliotek, archiwów i muzeów niebędących informacjami publicznymi oraz inne informacje niebędące ani informacją publiczną, ani zasobem bibliotek, archiwów i muzeów[11].

W czasach pandemii wywołanej przez wirus SARS-CoV-2[12] do zakresu danych publicznych włączyć należy także dane obrazujące rozprzestrzenianie się choroby COVID-19[13], a więc dane dotyczące zdrowia publicznego[14]. Rozwój społeczeństwa informacyjnego objawiającego się

[11] Zob. *Uzasadnienie rządowego projektu ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego*, druk sejmowy nr IX.1338, s. 14-15.

[12] Od ang. *Severe Acute Respiratory Syndrome* – zespół ciężkiej ostrej niewydolności oddechowej.

[13] Od ang. *Coronavirus Disease 2019*.

[14] „Zdrowie publiczne to nauka i sztuka zapobiegania chorobom, przedłużania życia i promowania zdrowia poprzez zorganizowane wysiłki społeczeństwa"; zob. *WHO European Action Plan for Strengthening Public Health Capacities and Services*, https://www.euro.who.int/__data/assets/pdf_file/0005/171770/RC62wd12rev1-Eng.pdf, s. 5 [dostęp: 18.09.2021], które odwołuje się do dokumentu: *Public health in England. The report of the Committee of Inquiry into the Future Development of the Public Health Function*, London, HMSO, 1988. Zgodnie z polską ustawą z dnia 11 września 2015 r. o zdrowiu publicznym (t.j. Dz. U. z 2021 r. poz. 183) zadania z zakresu zdrowia publicznego obejmują m.in.: monitorowanie i ocenę stanu zdrowia społeczeństwa, zagrożeń zdrowia oraz jakości życia związanej ze zdrowiem społeczeństwa; edukację zdrowotną dostosowaną do potrzeb różnych grup społeczeństwa, w szczególności dzieci, młodzieży i osób starszych; profilaktykę chorób; działania w celu rozpoznawania, eliminowania lub ograniczania zagrożeń i szkód dla zdrowia fizycznego i psychicznego w środowisku zamieszkania, nauki, pracy i rekreacji; analizę adekwatności i efektywności udzielanych świadczeń opieki zdrowotnej w odniesieniu

wszechobecnym wykorzystaniem technologii, także tej, która działa w tle[15] i zbiera dane na temat swoich użytkowników, czy mobilność osób fizycznych spowodowały poważne potrzeby transgranicznego[16] wykorzystywania informacji, również w zakresie zapobiegania rozprzestrzenianiu się chorób zakaźnych. Informacje te są w przeważającym stopniu gromadzone i przechowywane w postaci elektronicznej, w sposób zdecentralizowany (a więc na urządzeniach końcowych użytkownika, takich jak np. smartfony) lub scentralizowany, na serwerach zarządzanych np. przez organy administracji publicznej. Za pomocą aplikacji mobilnych służących do śledzenia kontaktów zakaźnych zbierane są bowiem dane, na podstawie których, pod pewnymi warunkami, chociażby związanymi z liczbą aktywnych użytkowników takich aplikacji, można tworzyć modele rozprzestrzeniania się

do rozpoznanych potrzeb zdrowotnych społeczeństwa; inicjowanie i prowadzenie: działalności naukowej w zakresie zdrowia publicznego, a także współpracy międzynarodowej dotyczącej działalności naukowej w zakresie zdrowia publicznego.

[15] Warto w tym momencie nawiązać do koncepcji *ubiquitous computing*, czyli przetwarzania bez granic lub systemów wszechobecnych, oraz *ambient intelligent*. Pierwsze z pojęć oznacza użycie urządzeń komputerowych, w szczególności mobilnych oraz sieci bezprzewodowych we wszystkich możliwych dziedzinach życia. Jest także rozszerzane na zastosowanie urządzeń, o których obecności lub przynajmniej zasadach działania zwykły użytkownik nie wie, jak procesory wbudowane w wiele urządzeń codziennego użytku (tzw. Internet rzeczy). M. Weiser po raz pierwszy zaproponował swoją koncepcję *ubiquitous computing* w 1988 r., a następnie w latach 1991-1993 opublikował jej założenia; zob. M. Weiser, *The Computer for the 21st Century*, https://web.archive.org/web/20141022035044/http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html [dostęp: 17.09.2021]. Z kolei *ambient intelligence* przedstawia się jako wizję komputeryzacji otoczenia człowieka, zgodnie z którą „człowiek otoczony będzie przez obliczeniowo i sieciowo zaawansowaną technologię, która jest świadoma jego obecności, jego osobowości, jego potrzeb i jest zdolna do inteligentnego odpowiadania na indykacje dotyczące pragnień, wyrażone w postaci gestu lub mowy, a nawet do angażowania się w inteligentny dialog; zob. C. Weyrich, *Orientations for WP2000 and beyond*, "ISTAG" 1999, za: J. Banasikowska, A. Sołtysik-Piorunkiewicz, *Zasady interoperacyjności i standaryzacji w systemach wszechobecnych e-Government krajów Unii Europejskiej*, „Roczniki Kolegium Analiz Ekonomicznych" 2013, nr 29, s. 13-14.

[16] Przekraczającego granice państw, istniejącego ponad granicami państw; zob. *Słownik języka polskiego PWN*, https://sjp.pwn.pl/sjp/transgraniczny;2578512.html [dostęp 19.09.2021], ale także: dotyczącego obszarów po obu stronach granicy, odbywającego się między dwoma graniczącymi ze sobą państwami; zob. B. Dunaj (red.), *Słownik współczesnego języka polskiego*, Warszawa 1996.

wirusa SARS-CoV-2. Służyć one mogą ocenie ogólnej skuteczności środków ograniczających rozprzestrzenianie się COVID-19, ale także być pomocne prywatnym przedsiębiorcom, jak np. apteki czy hurtownie medyczne, do przewidywania zapotrzebowania na środki ochrony indywidualnej przed wirusem SARS-CoV-2, ale i na specjalistyczny sprzęt medyczny, jak respiratory czy ECMO. W dalszej części niniejszego opracowania zostaną poruszone kwestie dostępu podmiotu zarządzającego polską aplikacją śledzącą kontakty zakaźne do zarówno jednostkowych danych zgromadzonych na urządzeniach końcowych użytkowników tejże aplikacji, jak i możliwości dalszego wykorzystania danych przechowywanych na centralnym serwerze do celów związanych z ochroną zdrowia publicznego.

Dnia 11.03.2020 r. Światowa Organizacja Zdrowia ogłosiła, że epidemia wirusa SARS-CoV-2 jest już pandemią[17], co oznacza, że ten rodzaj koronawirusa jest epidemiologicznym zagrożeniem dla całego świata. Wobec ciągle wzrastającej mobilności ludzkiej transgraniczna wymiana danych dotyczących rozprzestrzeniania się wirusa SARS-CoV-2 jest niezwykle istotna dla organów ds. zdrowia publicznego[18] i instytucji badawczych[19] różnych państw.

[17] Zob. *WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020*, https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020 [dostęp: 19.09.2021].

[18] Zgodnie z ustawą z dnia 11 września 2015 r. o zdrowiu publicznym do organów ds. zdrowia publicznego (którym to pojęciem posługują się przedstawiane w niniejszym opracowaniu dokumenty wydane przez organy UE) zalicza się: organy administracji rządowej, zgodnie z kompetencjami określonymi w ustawie z dnia 4 września 1997 r. o działach administracji rządowej (t.j. Dz. U. z 2020 r. poz. 1220), państwowe jednostki organizacyjne, w tym agencje wykonawcze, a także jednostki samorządu terytorialnego, realizujące zadania własne polegające na promocji lub ochronie zdrowia (art. 3 ust. 1). Z analizy dalszych przepisów cytowanej ustawy wynika, że organami ds. zdrowia publicznego są: minister właściwy ds. zdrowia, Narodowy Fundusz Zdrowia, Narodowy Instytut Zdrowia Publicznego – Państwowy Zakład Higieny, jednostki właściwe w sprawach przeciwdziałania uzależnieniom, Instytut Medycyny Wsi, Główny Inspektor Sanitarny, Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, Główny Inspektor Sanitarny Wojska Polskiego (zob. art. 5 ust. 1 cyt. ustawy).

[19] W polskim systemie prawnym funkcjonuje pojęcie „instytutu badawczego". Ustawa o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi w zakresie definicji

2. Aplikacje mobilne śledzące kontakty zakaźne

Interoperacyjność aplikacji mobilnych śledzących kontakty zakaźne stanowi część szerszego zagadnienia, dotyczącego balansu pomiędzy koniecznością przekazywania danych o rozprzestrzenianiu się wirusa SARS-CoV-2 do innych systemów informacyjnych, w tym przekazywania transgranicznego, a ochroną danych osobowych i ochroną prywatności użytkowników tych aplikacji – a więc poszanowaniem cyfrowych praw jednostki – i zarządzaniem ryzykiem przy wdrażaniu polityk i inicjatyw dotyczących danych publicznych. Korzystanie z aplikacji mobilnych śledzących kontakty zakaźne może rodzić obawy związane z przetwarzaniem danych osobowych, w tym danych dotyczących zdrowia użytkowników tych aplikacji. Z uwagi na priorytet redakcyjny publikacji, jakim jest osadzenie zasadniczych wątków w obszarze otwartości

tego pojęcia odsyła do art. 1 ust. 1 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (t.j. Dz. U. z 2020 r. poz. 1383). Instytutem badawczym jest państwowa jednostka organizacyjna, wyodrębniona pod względem prawnym, organizacyjnym i ekonomiczno-finansowym, która prowadzi badania naukowe i prace rozwojowe ukierunkowane na ich wdrożenie i zastosowanie w praktyce. Do podstawowej działalności instytutu badawczego należy: prowadzenie badań naukowych i prac rozwojowych, przystosowywanie wyników badań naukowych i prac rozwojowych do potrzeb praktyki, wdrażanie wyników badań naukowych i prac rozwojowych. W związku z prowadzoną działalnością podstawową instytut może (m. in.): upowszechniać wyniki badań naukowych i prac rozwojowych, wykonywać badania i analizy oraz opracowywać opinie i ekspertyzy w zakresie prowadzonych badań naukowych i prac rozwojowych, opracowywać oceny dotyczące stanu i rozwoju poszczególnych dziedzin nauki i techniki oraz sektorów gospodarki, które wykorzystują wyniki badań naukowych i prac rozwojowych oraz w zakresie wykorzystywania w kraju osiągnięć światowej nauki i techniki, prowadzić działalność normalizacyjną, certyfikacyjną i aprobacyjną, prowadzić i rozwijać bazy danych związane z przedmiotem działania instytutu, prowadzić działalność w zakresie informacji naukowej, technicznej i ekonomicznej, wynalazczości oraz ochrony własności przemysłowej i intelektualnej, a także wspierającej innowacyjność przedsiębiorstw, wytwarzać w związku z prowadzonymi badaniami naukowymi i pracami rozwojowymi aparaturę, urządzenia, materiały i inne wyroby oraz prowadzić walidację metod badawczych, pomiarowych oraz kalibrację aparatury, prowadzić działalność wydawniczą związaną z prowadzonymi badaniami naukowymi i pracami rozwojowymi; zob. szer. art. 2 cyt. ustawy). Instytut prowadzący badania naukowe i prace rozwojowe w zakresie nauk medycznych uczestniczy w systemie ochrony zdrowia (art. 3 cyt. ustawy).

danych publicznych, nie zostaną omówione szczegółowe kwestie związane z regulacjami prawnymi i rozwiązaniami technicznymi zapewniającymi ochronę prywatności użytkowników aplikacji mobilnych śledzących kontakty zakaźne. W zakresie przetwarzania danych osobowych odesłać należy także do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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)[20].

Na obszarze samej tylko UE obowiązują akty prawne dotyczące zdrowia publicznego w kontekście chorób zakaźnych, jak np. decyzja Parlamentu Europejskiego i Rady nr 1082/2013/UE z dnia 22 października 2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylająca decyzję nr 2119/98/WE[21]. Ustanowiono w niej szczegółowe przepisy dotyczące nadzoru epidemiologicznego, monitorowania, wczesnego ostrzegania i zwalczania poważnych transgranicznych zagrożeń zdrowia.

Wielu Europejczyków łączy się z Internetem przez urządzenia mobilne, a zatem technologie i dane cyfrowe mają do odegrania ważną rolę w walce z kryzysem wywołanym przez COVID-19. Takie technologie i dane mogą stać się ważnym narzędziem służącym informowaniu społeczeństwa, oferującym organom publicznym, wykonującym zadania z zakresu zdrowia publicznego[22], pomoc w ich wysiłkach na rzecz

[20] Dz. Urz. UE L 119 z 4.05.2016 r., s. 1; dalej jako: RODO.

[21] Dz. Urz. UE L 293 z 5.11.2013 r., s. 1.

[22] Odnosząc to stwierdzenie do polskich warunków, należy wskazać, że zgodnie z ustawą z dnia 11 września 2015 r. o zdrowiu publicznym, która określa m.in. zadania z zakresu zdrowia publicznego oraz podmioty uczestniczące w realizacji tych zadań, do organów ds. zdrowia publicznego zalicza się: organy administracji rządowej, zgodnie z kompetencjami określonymi w ustawie z dnia 4 września 1997 r. o działach administracji rządowej, państwowe jednostki organizacyjne, w tym agencje wykonawcze, a także jednostki samorządu terytorialnego, realizujące zadania własne polegające na promocji lub ochronie zdrowia (art. 3 ust. 1). Z analizy dalszych przepisów cytowanej ustawy wynika, że organami ds. zdrowia publicznego są: minister właściwy ds. zdrowia, Narodowy Fundusz Zdrowia, Narodowy Instytut Zdrowia Publicznego – Państwowy Zakład Higieny, jednostki właściwe

powstrzymania rozprzestrzeniania się wirusa czy też umożliwiającym organizacjom opieki zdrowotnej wymianę danych dotyczących zdrowia. Fragmentaryczne i nieskoordynowane podejście może jednak ograniczyć skuteczność środków mających na celu walkę z kryzysem wywołanym przez COVID-19, stanowiąc jednocześnie poważne zagrożenie dla jednolitego rynku i podstawowych praw i wolności[23]. Aplikacje mobilne mogą pomagać organom ds. zdrowia w monitorowaniu i ograniczaniu pandemii COVID-19 na szczeblu krajowym i unijnym. Mogą udzielać wskazówek obywatelom i ułatwiać organizację opieki medycznej nad pacjentami. Aplikacje umożliwiające śledzenie mogą odgrywać ważną rolę w ustalaniu kontaktów zakaźnych, ograniczaniu rozprzestrzeniania się choroby i przerywaniu łańcuchów zakażeń. W połączeniu z odpowiednimi strategiami wykonywania testów i ustalaniem kontaktów zakaźnych aplikacje te mogą być szczególnie przydatne, jeśli chodzi o dostarczanie informacji na temat poziomu występowania wirusa, ocenę skuteczności środków służących ograniczeniu kontaktów i środków izolacji, oraz mogą wnieść istotny wkład w strategie deeskalacji[24].

Wobec powyższego organy UE wydały szereg niewiążących wytycznych i zaleceń, dotyczących gromadzenia danych związanych z rozprzestrzenianiem się COVID-19 poprzez aplikacje mobilne. Są nimi m.in.:

1) European Data Protection Board Letter concerning the European Commission's Draft Guidance on apps supporting the fight against the COVID-19 pandemic z 14.04.2020 r.,

w sprawach przeciwdziałania uzależnieniom, Instytut Medycyny Wsi, Główny Inspektor Sanitarny, Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, Główny Inspektor Sanitarny Wojska Polskiego (zob. art. 5 ust. 1 ustawy o zdrowiu publicznym).

[23] Zalecenie Komisji (UE) 2020/518…, pkt 2 preambuły.

[24] Pkt 4 preambuły Zalecenia Komisji (UE) 2020/518.

2) European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak z 21.04.2020 r.[25],
3) European Data Protection Board Mandate on geolocation and other contact tracing tolls in the context of the COVID-19 outbreak z 7.04.2020 r.[26],
4) European Data Protection Board Statement in the data protection impact of the interoperability of contact tracing apps z 16.06.2020 r.[27],
5) Zalecenie Komisji (UE) 2020/518 z dnia 8.04.2020 r. w sprawie wspólnego unijnego zestawu instrumentów ułatwiającego wykorzystanie technologii i danych w celu zwalczania kryzysu wywołanego przez COVID-19 i wyjścia z niego, w szczególności w odniesieniu do aplikacji mobilnych i wykorzystywania zanonimizowanych danych dotyczących mobilności[28],
6) Komunikat Komisji „Wytyczne dotyczące aplikacji pomocnych w walce z pandemią COVID-19 w odniesieniu do ochrony danych" (2020/C 124 I/01) z 17.04.2020 r.[29],
7) eHealth Network: Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States z 15.04.2020 r.[30]

[25] https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en [dostęp: 19.09.2021].

[26] https://edpb.europa.eu/our-work-tools/our-documents/other/mandate-geolocation-and-other-tracing-tools-context-covid-19_en [dostęp: 19.09.2021].

[27] https://edpb.europa.eu/our-work-tools/our-documents/sonstiges/statement-data-protection-impact-interoperability-contact_en [dostęp: 19.09.2021].

[28] Zalecenie Komisji (UE) 2020/518 z dnia 8 kwietnia 2020 r. w sprawie wspólnego unijnego zestawu instrumentów ułatwiającego wykorzystanie technologii i danych w celu zwalczania kryzysu wywołanego przez COVID-19 i wyjścia z niego, w szczególności w odniesieniu do aplikacji mobilnych i wykorzystywania zanonimizowanych danych dotyczących mobilności, Dz. Urz. UE L 114 z 14.04.2020 r., s. 7.

[29] Dz. Urz. UE C 124 I z 17.04.2020 r., s. 1.

[30] https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf [dostęp: 19.09.2021].

2.1. Funkcjonalności aplikacji mobilnych śledzących kontakty zakaźne

Od początku kryzysu wywołanego przez COVID-19 opracowane zostały różne aplikacje mobilne, w tym przez organy publiczne[31]. Decyzja Wykonawcza Komisji (UE) 2020/1023 z dnia 15 lipca 2020 r. zmieniająca decyzję wykonawczą (UE) 2019/1765 w zakresie transgranicznej wymiany danych między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania w związku ze zwalczaniem pandemii COVID-19[32] zawiera definicję pojęcia „krajowa aplikacja mobilna służąca do ustalania kontaktów zakaźnych i ostrzegania". Oznacza ona zatwierdzone na szczeblu krajowym oprogramowanie działające na urządzeniach inteligentnych, w szczególności smartfonach, zaprojektowane zazwyczaj do szeroko zakrojonej i ukierunkowanej interakcji z zasobami internetowymi, które przetwarza dane dotyczące bliskości fizycznej i inne informacje kontekstowe gromadzone za pomocą wielu czujników, w które wyposażone są urządzenia inteligentne (jak np. smartfony), w celu wykrywania kontaktów z osobami zakażonymi SARS-CoV-2 i ostrzegania osób, które mogły mieć styczność z wirusem SARS-CoV-2. Wspomniane aplikacje mobilne mają możliwość wykrywania obecności innych urządzeń korzystających z technologii Bluetooth i wymiany

[31] Publiczne aplikacje mobilne, skierowane do ogółu użytkowników (nie tylko do profesjonalistów, jakimi są np. lekarze), śledzące kontakty zakaźne: Coronalert (Belgia), Koronavilkku (Finlandia), Coronamelder (Holandia), Stayaway Covid (Portugalia), Protego Safe (Polska), Ostanizdrav (Stay Healthy) – Słowenia, Hoia (Estonia), Virusafe (Bułgaria), Apturi Covid Latvia – SPKC (Łotwa), Immuni (Włochy), Radar Covid (Hiszpania), Covid Tracker Ireland (Irlandia), Corona-Warn-App (Niemcy), Stopcovid (Francja), Virusradar (Węgry), Stop Covid-19 (Chorwacja), Smitte | Stop (Dania), Covidtracker (Szwajcaria), Smittestopp (Digital Contact Tracing) – Norwegia, Sicilia Si Cura (Włochy), Covidmeter (Dania), Rakning C-19 (Islandia), Covtracer (Cypr), Erouška (Czechy), Stopp Corona (Austria), Allertalom – Cercacovid (Włochy); zob. więcej https://mhealth-hub.org/mhealth-solutions-against-covid-19 [dostęp: 19.09.2021].

[32] Dz. Urz. UE L 227 I z 16.07.2020 r., s. 1.

informacji z serwerami wewnętrznymi (ang. *backend servers*) przy użyciu Internetu. Podobną definicję zawiera Zalecenie KE nr 2020/518[33].

Aplikacje śledzące kontakty zakaźne pełnią zazwyczaj trzy funkcje ogólne; pierwszą z nich jest informowanie obywateli i doradzanie im oraz ułatwianie organizacji opieki medycznej nad osobami z objawami, często w połączeniu z kwestionariuszem pozwalającym na postawienie samodzielnej diagnozy; po drugie, ostrzeganie osób znajdujących się w pobliżu osoby zakażonej w celu przerwania łańcuchów zakażeń i zapobiegania ponownemu wystąpieniu zakażeń w fazie „ponownego otwarcia"; oraz po trzecie, monitorowanie i egzekwowanie kwarantanny osób zakażonych, ewentualnie w połączeniu z funkcjami pozwalającymi na ocenę ich stanu zdrowia w okresie kwarantanny. Niektóre aplikacje są dostępne dla ogółu społeczeństwa, zaś inne są przeznaczone wyłącznie dla zamkniętych grup użytkowników i służą śledzeniu kontaktów w miejscu pracy. Organy ds. zdrowia publicznego powinny być zaangażowane na wszystkich etapach selekcji, opracowywania, pilotowania, wdrażania i oceny aplikacji, aby zapewnić najlepszą ochronę zdrowia publicznego z należytym uwzględnieniem prywatności i ochrony danych. Aplikacje mobilne mają wyraźne mocne strony, które mogą pomóc w uzupełnieniu niedociągnięć nieodłącznie związanych z konwencjonalnym śledzeniem kontaktów zakaźnych, nie polegają bowiem na zdolności osoby do przypomnienia sobie, z kim się kontaktowała, jak blisko i jak długo; rozwiązują też kwestie, jak skontaktować się z nieznajomymi osobami, w których obecności przebywała osoba zakażona, np. w kinie czy sklepie. Aplikacje mogą ułatwić śledzenie kontaktów transgranicznych, pod warunkiem że ich interoperacyjność zostanie zapewniona, najlepiej już na etapie projektowania.

W zaleceniu nr 2020/518 Komisja Europejska stwierdza, że niektóre z omawianych aplikacji mobilnych można uznać za wyroby medyczne, w przypadku gdy producent przewiduje ich zastosowanie między innymi

[33] Pkt 3 lit. a Zalecenia Komisji (UE) 2020/518.

do celów diagnozy, zapobiegania, monitorowania, przewidywania, prognozowania, leczenia lub łagodzenia przebiegu choroby, a zatem byłyby one objęte zakresem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG[34] lub dyrektywy Rady 93/42/EWG dotyczącej wyrobów medycznych[35]. W odniesieniu do aplikacji służących do samodzielnej diagnozy i weryfikacji objawów, jeżeli dostarczają one informacji dotyczących diagnozy, zapobiegania, monitorowania, przewidywania lub prognozowania, należy ocenić ich potencjalną kwalifikację jako wyroby medyczne zgodnie z ramami regulacyjnymi dotyczącymi wyrobów medycznych (dyrektywa 93/42/EWG lub rozporządzenie (UE) 2017/745)[36]. Aplikacje mobilne, o których mowa, gromadzą więc dane dotyczące zdrowia ich użytkowników[37].

Aplikacje mobilne są zaprojektowane tak, aby uzupełniać tradycyjne działania w zakresie śledzenia kontaktów. Podczas oceny skuteczności i bezpieczeństwa aplikacji mobilnych w centrum uwagi powinna znajdować się perspektywa zdrowia publicznego. Aplikacje nie są platformami społecznościowymi do rozpowszechniania społecznych ostrzeżeń lub wzbudzania jakiegokolwiek rodzaju stygmatyzacji osób zakażonych. Wyłącznym celem aplikacji jest, aby organy publicznej opieki zdrowotnej zidentyfikowały osoby, które miały kontakt z osobą zakażoną COVID-19, wezwały je do samokwarantanny, szybko poddały je testom, a także udzieliły im, w odpowiednich przypadkach, informacji o kolejnych etapach, m.in. o tym, co należy robić w przypadku wystąpienia objawów.

[34] Dz. Urz. UE L 117 z 5.05.2017 r., s. 1.

[35] Dz. Urz. UE L 169 z 12.07.1993 r., s. 1.

[36] Zalecenie Komisji (UE) 2020/518…, pkt 13 preambuły.

[37] Zgodnie z art. 4 pkt 15 RODO dane dotyczące zdrowia oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

W działaniach tych nadrzędne znaczenie ma jakość i prawdziwość przetwarzanych danych.

Wytyczne KE dotyczące aplikacji pomocnych w walce z pandemią COVID-19 w odniesieniu do ochrony danych dotyczą wyłącznie dobrowolnie stosowanych aplikacji, które oferują co najmniej jedną z następujących funkcji: przekazywanie osobom fizycznym rzetelnych informacji o pandemii COVID-19; udostępnianie kwestionariuszy do samodzielnej diagnozy i wytycznych dla obywateli (funkcja weryfikacji objawów); ostrzeżenia dla osób, które znajdowały się przez pewien czas w pobliżu osoby zakażonej, w celu przekazania informacji np. o konieczności samoizolacji i o miejscach, gdzie można poddać się badaniu (funkcja ustalania kontaktów zakaźnych i ostrzegania); zapewnienie forum komunikacji między pacjentami i lekarzami w przypadku samoizolacji lub zapewnienie dalszej diagnostyki i doradztwa w zakresie leczenia (wykorzystywanie telemedycyny na szerszą skalę)[38]. W niniejszym opracowaniu omawiane będą zagadnienia dotyczące dobrowolnie instalowanych aplikacji mobilnych o takich właśnie funkcjonalnościach.

Funkcja weryfikacji objawów to narzędzie przeznaczone dla organów zdrowia publicznego, aby mogły udzielać obywatelom wskazówek dotyczących badań na obecność COVID-19, jak również przekazywać informacje o samoizolacji, sposobach unikania zakażenia innych osób oraz potrzebie zgłoszenia się po pomoc medyczną. Może być ona również uzupełnieniem podstawowej opieki zdrowotnej i zapewniać lepsze informacje na temat wskaźników zakażeń COVID-19 w danej populacji.

Funkcja ustalania kontaktów zakaźnych i ostrzegania to narzędzie pozwalające identyfikować osoby, które znalazły się w pobliżu osoby zakażonej COVID-19, także jeśli chodzi o kontakty transgraniczne, oraz poinformować je o właściwych sposobach działania w takiej sytuacji, np. o potrzebie poddania się kwarantannie w domu czy testom na obecność wirusa.

[38] Wytyczne nie obejmują aplikacji mających na celu egzekwowanie obowiązku kwarantanny (w tym aplikacji, których stosowanie jest obowiązkowe).

Śledzenie kontaktów ma szczególne znaczenie. Nie można powiedzieć, że aplikacje mobilne wykonują „śledzenie kontaktów", ale raczej „śledzenie bliskości" i „powiadamianie o narażeniu", tj. śledzenie i ostrzeganie użytkowników, którzy byli blisko siebie, co może wspierać śledzenie kontaktów. Większość z nich jest oparta na technologii Bluetooth, która umożliwia wykrywanie bliskości, ale nie pozwala na śledzenie lokalizacji. Istnieją także aplikacje oparte na technologii GPS. Z punktu widzenia ochrony danych osobowych i prywatności, ale także samych funkcji aplikacji, dane dotyczące lokalizacji nie są konieczne ani zalecane, np. przez Europejską Radę Ochrony Danych, do celów aplikacji służących do śledzenia kontaktów. Gromadzenie danych o przemieszczaniu się osób fizycznych w ramach aplikacji służących do ustalania kontaktów zakaźnych naruszałoby zasadę minimalizacji danych ustanowioną w RODO. Dodatkowo stwarzałoby poważne zagrożenia dla bezpieczeństwa i prywatności ich użytkowników. Informacja o bliskości pomiędzy użytkownikami aplikacji może przecież zostać pozyskana bez ustalania ich lokalizacji. Ten rodzaj aplikacji nie wymaga – i stąd też nie powinien obejmować – wykorzystywania danych o lokalizacji. Europejska Rada Ochrony Danych podkreśla, że jeśli chodzi o wykorzystanie danych o lokalizacji, zawsze rekomendowane jest przetwarzanie danych zanonimizowanych, zamiast danych osobowych[39]. Dane o lokalizacji uważane za

[39] Anonimizacja oznacza wykorzystanie zestawu technik w celu usunięcia możliwości powiązania danych ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną pomimo wszelkich „rozsądnych" starań. Ten „test racjonalności" musi uwzględniać zarówno obiektywne aspekty (czas, środki techniczne), jak i elementy kontekstowe, które mogą się różnić w zależności od przypadku (rzadkość zjawiska, biorąc pod uwagę m.in. gęstość zaludnienia, charakter i ilość danych). Jeśli dane nie przejdą tego testu, nie zostały zanonimizowane, a zatem pozostają w zakresie RODO. Ocena odporności anonimizacji zależy od trzech następujących kryteriów: wyodrębnienia (wyizolowanie konkretnej osoby z większej grupy na podstawie danych); możliwości powiązania (powiązanie dwóch wpisów dotyczących tej samej osoby); oraz wnioskowania (wydedukowanie, z istotnym prawdopodobieństwem, nieznanych informacji na temat konkretnej osoby). Zgodnie z definicją zawartą w art. 2 pkt 1 u.o.d.p.w.i. anonimizacja to proces zmiany informacji sektora publicznego w informacje anonimowe, które nie odnoszą się do zidentyfikowanej lub możliwej do zidentyfikowania

zanonimizowane mogą w rzeczywistości nie być anonimowe. Ślady mobilności osób fizycznych są ze swej natury wysoce skorelowane i niepowtarzalne. W związku z tym mogą one być podatne na próby deanonimizacji w określonych okolicznościach[40]. Pojęcie anonimizacji jest często źle rozumiane i mylone z pojęciem pseudonimizacji. Według art. 4 pkt 5 RODO „pseudonimizacja" oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej[41]. Podczas gdy anonimizacja umożliwia wykorzystanie danych bez żadnych ograniczeń, dane pseudonimiczne wciąż są objęte zakresem RODO. Dane nie mogą zostać zanonimizowane same w sobie, tj. anonimizować można jedynie całe zbiory danych. W tym sensie każdy zabieg na pojedynczym schemacie danych (z wykorzystaniem szyfrowania lub jakichkolwiek innych matematycznych przekształceń) można uznać za pseudonimizację[42].

Technologia mobilna do obsługi śledzenia kontaktów została po raz pierwszy zastosowana w Singapurze. Używana tam aplikacja *Trace Together*

osoby fizycznej, lub proces zmiany danych osobowych w dane anonimowe w taki sposób, że identyfikacja osoby, której dane dotyczą, nie jest lub już nie jest możliwa.

[40] Zob. Y.-A. de Montjoye, C.A. Hidalgo, M. Verleysen, V.D. Blonde, *Unique in the Crowd: The privacy bounds of human mobility*, DOI: 10.1038/srep01376, https://web.media.mit.edu/~yva/papers/deMontjoye2013unique.pdf [dostęp: 19.09.2021]; A. Pyrgelis, C. Troncoso, E. De Cristofaro, *Knock Knock, Who's There? Membership Inference on Aggregate Location Data*, https://arxiv.org/pdf/1708.06145.pdf [dostęp: 19.09.2021].

[41] Zob. szerzej P. Litwiński, P. Barta, M. Kawecki, komentarz do art. 4, [w:] P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018, s. 207-208; K. Witkowska-Nowakowska, komentarz do art. 4 pkt 5, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 203-208.

[42] Zob. *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, s. 5-7.

jest pobierana dobrowolnie i gromadzi przez Bluetooth dane o innych urządzeniach, które znajdowały się w pobliżu urządzenia użytkownika[43].

Komisja zaleca dobrowolne korzystanie z aplikacji. Zgodnie z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[44] narzucenie obowiązku stosowania aplikacji wiążącego się z prawami do poufności komunikacji, o których mowa w jej art. 5, jest możliwe jedynie w drodze przepisów prawa, które są konieczne, właściwe i proporcjonalne w celu ochrony pewnych celów szczegółowych.

Skuteczność aplikacji mobilnych zależy od wielu czynników, m.in. stopnia ich wykorzystania przez użytkowników, czyli odsetka ludności korzystającej z urządzenia mobilnego, a wśród nich odsetka osób, które pobrały aplikację i wyraziły zgodę na przetwarzanie dotyczących ich danych osobowych i nie wycofały jej. Szczególnie narażone na infekcję wirusem SARS-CoV-2 są osoby starsze, które nie zawsze korzystają z urządzeń mobilnych, podobnie jak osoby z dysfunkcjami fizycznymi czy psychicznymi. Inne ważne czynniki skuteczności aplikacji mobilnych śledzących kontakty zakaźne to zaufanie obywateli, że dane będą chronione z wykorzystaniem odpowiednich zabezpieczeń i stosowane wyłącznie w celu ostrzegania osób, które mogły być narażone na kontakt z wirusem. W tym zakresie konieczna jest odpowiednia polityka komunikacji, a zwłaszcza szeroko zakrojona kampania informacyjna. Duże znaczenie dla skuteczności aplikacji śledzących kontakty zakaźne mają: zatwierdzenie tych aplikacji przez organ ds. zdrowia, zdolność organów ds. zdrowia do podejmowania działań na podstawie danych generowanych przez aplikacje, integracja i wymiana danych z innymi systemami i aplikacjami oraz transgraniczna i międzyregionalna interoperacyjność

[43] Zob. szerzej: https://www.tracetogether.gov.sg/ [dostęp: 17.09.2021].
[44] Dz. Urz. UE L 201 z 31.07.2002 r., s. 37.

z innymi systemami. Aplikacje muszą być częścią kompleksowej strategii zdrowia publicznego w celu zwalczania pandemii, obejmującej m.in. testowanie, a następnie ręczne śledzenie kontaktów w celu usunięcia wątpliwości. Stosowaniu aplikacji powinny towarzyszyć środki wspierające, aby zapewnić, że informacje dostarczane użytkownikom są dostosowane do ogólnego kontekstu działań skierowanych przeciwko pandemii, a wysyłane alerty mogą być przydatne dla publicznego systemu opieki zdrowotnej. W przeciwnym razie aplikacje te mogą nie przynieść w pełni oczekiwanego rezultatu.

2.2. Polska aplikacja mobilna STOP COVID – ProteGO Safe

Większość państw członkowskich UE posiada publiczne aplikacje do śledzenia kontaktów zakaźnych; niektóre z nich oparte są na wykorzystaniu technologii udostępnionej przez prywatne spółki technologiczne[45]. W kwietniu 2020 r. Apple i Google ogłosiły zamiar udostępnienia interfejsów programowania aplikacji śledzących kontakty zakaźne, czyli „systemu powiadomień o narażeniu" (*Exposure Notification System*), w celu obsługi aplikacji, które przyjmują zdecentralizowaną architekturę, będącą jednym z podejść przewidzianych w tzw. wspólnym zestawie narzędzi[46]. Interfejsy API zostały wydane 22 maja 2020 r. Aby zapewnić zgodność rozwiązania interoperacyjnego opracowanego przez Sieć

[45] Zob. Repozytorium aplikacji mobilnych śledzących kontakty zakaźne dostępnych w państwach europejskich, https://mhealth-hub.org/mhealth-solutions-against-covid-19 [dostęp: 19.09.2021]. Lista aktualnych inicjatyw w tym zakresie, obrazująca m.in. dane takie jak data uruchomienia aplikacji, sposób przechowywania danych (scentralizowany, zdecentralizowany), dobrowolność instalacji znajduje się w dokumencie *Mobile applications to support contact tracing in the EU's fight against COVID-19, Progress reporting June 2020*, https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progressreport_en.pdf, s. 5 [dostęp: 17.09.2021].

[46] Zob. *eHealth Network Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States*, https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf [dostęp: 19.09.2021].

e-Zdrowie z interfejsami API, odbyły się oddzielne dyskusje na poziomie technicznym między poszczególnymi państwami członkowskimi i Komisją a Google i Apple.

Polską aplikacją śledzącą kontakty zakaźne jest STOP COVID – ProteGO Safe[47]. Regulamin ProteGO Safe stanowi, iż korzystanie z aplikacji możliwe jest bez ograniczeń terytorialnych[48]. Aplikacja została udostępniona 17.04.2020 r.[49] przez Ministerstwo Cyfryzacji[50]. Dostępna jest poprzez Sklep Play (dla urządzeń z systemem operacyjnym Android, stworzonym przez Google) lub AppStore (dla urządzeń z systemem operacyjnym iOS, wytworzonym przez Apple). Celem aplikacji nie jest powiadamianie organów ds. ochrony zdrowia, a użytkowników aplikacji o ryzyku epidemiologicznym wynikającym z kontaktu z osobą zakażoną.

Administratorem danych osobowych zbieranych przez aplikację jest Główny Inspektor Sanitarny[51], natomiast aplikację wytworzono na zlecenie Ministra Cyfryzacji. Do przetwarzania danych osobowych w STOP COVID – ProteGO Safe zastosowanie znajduje art. 11 RODO, gdyż cel przetwarzania nie wymaga identyfikacji, zatem użytkownicy STOP COVID

[47] Zob. https://www.gov.pl/web/koronawirus/protegosafe [dostęp: 19.09.2021]; dalej jako: ProteGO Safe.

[48] Zob. § 4 ust. 2 Regulaminu STOP COVID – ProteGO Safe v. 4.8, https://www.gov.pl/web/protegosafe/dokumenty [dostęp: 19.09.2021].

[49] Informacja zawarta w opisie aplikacji w sklepie Google Play; w repozytorium aplikacji mobilnych śledzących kontakty zakaźne dostępnych w państwach europejskich widnieje data 20.04.2020 r., z kolei na stronie https://dane.gov.pl/pl/application/1244,protego-safe [dostęp: 19.09.2021]: 23.04.2020.

[50] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2021 r. poz. 670) w art. 19e-19j reguluje publiczną aplikację mobilną – jednakże jedynie taką, której celem jest pobranie, przechowywanie i prezentacja dokumentów elektronicznych przechowywanych na urządzeniach mobilnych, co ma pozwolić na zastąpienie użycia odpowiednich dla tych czynności dokumentów nieelektronicznych. Aplikacja ProteGO Safe nie mieści się zatem w ramach tej regulacji i nie może być nazywana publiczną aplikacją mobilną w rozumieniu ustawy o informatyzacji. Zob. także G. Kubalski, M. Małowiecka, *Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz*, Warszawa 2019, Legalis, komentarz do art. 19e-19j.

[51] Zob. § 2 pkt 5 Regulaminu STOP COVID – ProteGO Safe.

– ProteGO Safe nie są identyfikowani[52]. Dane osobowe przetwarzane są na podstawie art. 6 ust. 1 lit. e RODO w związku z zadaniem realizowanym w interesie publicznym polegającym na zapobieganiu, przeciwdziałaniu i zwalczaniu COVID-19 wynikającym z art. 1, 2, 3, 6 oraz 8a ust. 1, 4 i 5 ustawy z dnia 14 marca 1985 r o Państwowej Inspekcji Sanitarnej[53]. Dane osobowe dotyczące zdrowia użytkownika są przetwarzane także na podstawie art. 9 ust. 2 lit. i RODO w zw. z zadaniem publicznym polegającym na zapobieganiu, przeciwdziałaniu i zwalczaniu COVID-19 wynikającym z art. 1, 2, 3, 6 oraz 8a ust. 1, 4 i 5 ustawy o PIS, gdyż przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi na podstawie prawa państwa członkowskiego[54]. Już w tym miejscu należy zasygnalizować, że dane dotyczące zdrowia są przetwarzane wyłącznie na urządzeniu końcowym użytkownika i żaden z podmiotów zaangażowanych w wytwarzanie czy zarządzanie aplikacją ProteGO Safe nie ma do nich dostępu[55].

Korzystanie z aplikacji ProteGO Safe jest bezpłatne i obejmuje swym zakresem moduł triażu, moduł analityczny, moduł dziennik zdrowia, wsparcie w profilaktyce i zapobieganiu zarażeniu, informowanie o istotnych informacjach związanych z pandemią COVID-19, „przypominacz" bezpiecznych zachowań i nawyków codziennej higieny oraz informowanie o bieżącym statusie powiatu (status żółty lub czerwony). W ramach ProteGO Safe możliwe jest ustalenie czynników ryzyka infekcji, tworzenie i prowadzenie historii medycznej, istniejących schorzeń, aktualnej farmakoterapii oraz prowadzenie dziennika profilaktyki. ProteGO Safe przekazuje użytkownikom informacje i wytyczne WHO oraz GIS, ale przekazywane

[52] Zob. § 2 pkt 4 Regulaminu STOP COVID – ProteGO Safe.

[53] Dz. U. z 2019 r. poz. 59; dalej jako: ustawa o PIS. Zob. także § 3 ust. 3 Polityki prywatności STOP COVID – ProteGO Safe v. 4.8.

[54] Zob. § 3 ust. 4 Polityki prywatności STOP COVID – ProteGO Safe.

[55] Kwestia ta zostanie poruszona także w dalszej części niniejszego opracowania.

informacje nie mają charakteru konsultacji medycznej lub świadczenia zdrowotnego (w tym w szczególności medycznego lub farmaceutycznego)[56].

Najbardziej interesujący z punktu widzenia tematyki niniejszego opracowania jest moduł analityczny aplikacji, zdefiniowany jako funkcjonalność ProteGO Safe umożliwiająca zapisywanie, tworzenie historii oraz analizowanie spotkania urządzenia[57] użytkownika[58] z innymi urządzeniami użytkowników aplikacji.

Moduł analityczny ma charakter dobrowolny, a zatem to od działania użytkownika zależy, czy zostanie uruchomiony; możliwe jest korzystanie z aplikacji ProteGO Safe bez aktywowania modułu analitycznego. Usługi przewidziane w tym module świadczone są przy użyciu technologii Bluetooth i wymagają włączenia modułu Bluetooth w urządzeniu, a także odpowiednio dla urządzeń z systemem operacyjnym Android: włączenia systemowej opcji rejestrowania narażenia na COVID-19 oraz udzielenia zgody na lokalizację (w zakresie modułu Bluetooth, ProteGO Safe nie wykorzystuje danych GPS), a dla urządzeń z systemem operacyjnym iOS: zaznaczenia opcji „rejestrowanie narażenia na COVID-19". W celu skutecznego korzystania z pełnej funkcjonalności modułu analitycznego należy pozostawić uruchomioną aplikację w tle. Aplikacja uruchomiona w tle będzie skanować otoczenie w poszukiwaniu urządzeń innych użytkowników aplikacji, jak również sama będzie podlegać skanowaniu przez inne urządzenia. Urządzenie użytkownika aplikacji

[56] Zob. § 3 ust. 1 Regulaminu STOP COVID – ProteGO Safe v. 4.8. Każdy z modułów zdefiniowany jest w § 2 Regulaminu.

[57] Elektroniczne urządzenie, za pośrednictwem którego użytkownik uzyskuje dostęp do STOP COVID – ProteGO Safe (tablet, smartfon itp.) z aktywnym modułem Bluetooth, systemem Android 5.0 lub wyższym z dostępem do sklepu Google Play albo z systemem iOS w wersji nie niższej niż 13.5 z dostępem do sklepu AppStore. Moduł analityczny będzie działał jedynie w urządzeniach z systemem Android 6.0 wspierających technologię BLE lub wyższym albo z systemem iOS w wersji nie niższej niż 13.5; zob. § 2 pkt 21 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

[58] Osoba posiadająca pełną zdolność do czynności prawnych, która po zaakceptowaniu Regulaminu i Polityki prywatności korzysta z STOP COVID – ProteGO Safe; zob. § 2 pkt 22 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

zapisuje historię spotykanych urządzeń, na których jest zainstalowana aplikacja. Dane osobowe w postaci historii spotykanych urządzeń pozostają na urządzeniach użytkowników przez 14 dni.

Konsultant Centrum Kontaktu[59], przekazując telefonicznie informację o zarażeniu COVID-19 osobie chorej[60], zapyta, czy jest ona użytkownikiem ProteGO Safe. Jeżeli osoba chora jest użytkownikiem ProteGO Safe, konsultant Centrum Kontaktu zaproponuje wprowadzenie do ProteGO Safe kodu PIN w celu anonimowego potwierdzenia, że urządzenie należy do osoby chorej i zainicjowania procesu przekazania komunikatu o narażeniu na zakażenie innym użytkownikom aplikacji (poprzez przesłanie klucza diagnostycznego). Wprowadzenie kodu PIN inicjuje proces wysłania klucza diagnostycznego na serwer ProteGO Safe, który następnie przekazuje klucz diagnostyczny do urządzeń użytkowników aplikacji[61]; na serwer ładowane są wyłącznie dane dotyczące bliskich kontaktów osoby, u której badanie potwierdziło zakażenie COVID-19[62]. Serwer ProteGO Safe to infrastruktura chmurowa utrzymywana przez Operatora Chmury Krajowej służąca do przekazania klucza diagnostycznego do urządzeń użytkowników. Klucze diagnostyczne są przechowywane na serwerze STOP COVID – ProteGO Safe w postaci zaszyfrowanej przez 14 dni[63]. Kod PIN to generowane losowo i aktywne przez pół godziny alfanumeryczne hasło przekazywane użytkownikowi, który jest osobą chorą, przez konsultanta Centrum Kontaktu. Kod PIN może być

[59] Jednostka powiadamiająca telefonicznie o wyniku testu na COVID-19 oraz przekazująca kod PIN użytkownikom aplikacji i udzielająca informacji związanych z COVID-19; zob. § 2 pkt 3 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

[60] Osoba fizyczna, posiadająca pełną zdolność do czynności prawnych, która uzyskała pozytywny wynik testu na COVID-19. Osoba chora nie musi być użytkownikiem; zob. § 2 pkt 14 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

[61] Zob. § 3 ust. 3 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

[62] Zob. P. Litwiński, A. Leńczuk, A. Krzyżak, A. Siwek, *Raport z audytu prywatności aplikacji ProteGO Safe przeprowadzonego na zlecenie Ministerstwa Cyfryzacji*, Barta, Litwiński. Kancelaria Radców Prawnych i Adwokatów Spółka Partnerska, 5.08.2020 r., https://www.gov.pl/web/protegosafe/dokumenty [dostęp: 19.09.2021], s. 46.

[63] Zob. § 2 pkt 19 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

wprowadzony do ProteGO Safe w celu anonimowego potwierdzenia, że urządzenie należy do osoby chorej i zainicjowania procesu przekazania klucza diagnostycznego do serwera ProteGO Safe[64]. Po otrzymaniu przez urządzenie użytkownika aplikacji klucza diagnostycznego moduł analityczny dokonuje analizy, porównując klucz diagnostyczny z danymi historycznymi dotyczącymi spotkań innych urządzeń z zainstalowaną aplikacją zapisanymi lokalnie na urządzeniu użytkownika w celu oceny ryzyka narażenia na zarażenie COVID-19. Jeśli analiza prawdopodobieństwa zarażenia COVID-19 wykaże wysokie lub średnie ryzyko narażenia na zakażenie COVID-19, status użytkownika w aplikacji zmieni się odpowiednio[65]. Wprowadzenie przez użytkownika kodu PIN do ProteGO Safe jest dobrowolne[66].

Z analizy wyżej powołanych fragmentów regulaminu ProteGO Safe wynika, że tylko osoby zweryfikowane przez służby medyczne jako chore na COVID-19 mogą zainicjować proces wysyłania swoich kluczy diagnostycznych na serwer ProteGO Safe, aby możliwe było wysłanie ostrzeżenia innym użytkownikom. Konieczne jest bowiem wpisanie do aplikacji ProteGO Safe, zainstalowanej na urządzeniu, kodu PIN, otrzymanego od pracownika Centrum Kontaktu. Takie rozwiązanie gwarantuje poprawność danych. Przetwarzanie niepotwierdzonych danych potęgowałoby chaos, gdyż użytkownicy otrzymywaliby fałszywe powiadomienia o możliwym zarażeniu[67].

Moduł analityczny jest oparty na *Privacy-Preserving Contact Tracing API* wytworzonym oraz udostępnionym przez gigantów technologicznych Google oraz Apple. Informacje generowane przez moduł analityczny wraz z wynikami jego pracy są przechowywane lokalnie na

[64] Zob. § 2 pkt 8 Regulaminu STOP COVID – ProteGO Safe v. 4.8.
[65] Zob. § 3 ust. 4 Regulaminu STOP COVID – ProteGO Safe v. 4.8.
[66] Zob. § 3 ust. 5 Regulaminu STOP COVID – ProteGO Safe v. 4.8.
[67] Zob. *Technologia w walce z koronawirusem – 7 filarów zaufania*, https://panoptykon.org/7-filarow-zaufania [dostęp: 19.09.2021].

urządzeniu przez 14 dni. Google oraz Apple w swojej dokumentacji[68] zapewniają, że stosują najwyższe standardy bezpieczeństwa, aby chronić anonimowość użytkowników[69].

Polityka prywatności STOP COVID – ProteGO Safe[70] w zakresie funkcjonalności i opisu działania modułu analitycznego dodaje, że klucz diagnostyczny wysłany z urządzenia na serwer STOP COVID – ProteGO Safe nie będzie zawierać danych umożliwiających identyfikację ani informacji o urządzeniach, z którymi użytkownik miał styczność. To użytkownik będzie decydować o tym, czy chce oznaczyć swoje urządzenie jako urządzenie osoby chorej, co zainicjuje wysłanie anonimowego klucza diagnostycznego na serwer STOP COVID – ProteGO Safe, a następnie do innych użytkowników aplikacji. Każda z aplikacji po otrzymaniu klucza diagnostycznego dokonuje automatycznej analizy spotkań poprzez odpowiednie porównanie otrzymanego klucza diagnostycznego z historią spotkań urządzeń z zainstalowaną aplikacją z ostatnich 14 dni. Analiza wykonywana jest niezależnie na urządzeniu każdego użytkownika, brana jest w niej pod uwagę w szczególności odległość użytkowników (siła sygnału) oraz czas przebywania w pobliżu osoby zakażonej i w jej wyniku może zostać zmieniony status aktualnej grupy ryzyka.

Z dokumentacji udostępnionej przez Ministerstwo Cyfryzacji na stronie internetowej https://www.gov.pl/web/protegosafe/dokumenty wynika, że Minister Cyfryzacji dysponuje informacjami o liczbie przesłanych na serwer ProteGO Safe kluczy diagnostycznych oraz dacie ich wysłania. Znane Ministrowi Cyfryzacji i Głównemu Inspektorowi Sanitarnemu, który jest administratorem danych osobowych w ramach aplikacji ProteGO Safe, „są dane przetwarzane w aplikacji i związane z wykorzystywaniem serwera zapewniającego przekazywanie Użytkownikom komunikatów,

[68] https://www.google.com/covid19/exposurenotifications/ oraz https://developer.apple.com/documentation/exposurenotification [dostęp: 17.09.2021].

[69] Zob. § 2 pkt 11 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

[70] Polityka prywatności STOP COVID – ProteGO Safe v. 4.8., https://www.gov.pl/web/protegosafe/dokumenty [dostęp: 17.09.2021].

jak UID – losowy identyfikator Urządzenia Użytkownika oraz średni czas korzystania z Aplikacji przez Użytkowników (dane statystyczne, których nie można powiązać z poszczególnymi użytkownikami)"[71]. Aplikacja ProteGO Safe uzyskuje dostęp do informacji przechowywanych na urządzeniu użytkownika jedynie wtedy, gdy w wyniku odebrania informacji z serwera ProteGO Safe o kluczu diagnostycznym osoby chorej, bazując na wbudowanych skryptach analitycznych, porównuje otrzymany klucz z identyfikatorami kontaktów, które zostały przez nią odnotowane, w celu ustalenia ryzyka[72]. Dane otrzymane od użytkowników z pozytywnym wynikiem testu na obecność COVID-19 są przetwarzane centralnie, a klucz diagnostyczny osoby chorej przechowywany jest na serwerze ProteGO Safe przez okres 14 dni. Dane osobowe użytkownika oraz inne informacje wprowadzone do aplikacji ProteGO Safe przez użytkownika, jak np. dane dotyczące zdrowia, są przechowywane lokalnie, czyli na urządzeniu końcowym użytkownika, i nie są wymieniane z serwerami centralnymi czy urządzeniami końcowymi innych użytkowników. Przyjęto zatem hybrydowy model przechowywania danych, posiadający zarówno element modelu scentralizowanego, jak i zdecentralizowanego. Serwery są odseparowane od siebie – serwer nadający anonimowe identyfikatory urządzenia użytkownika oraz serwer przesyłający klucze diagnostyczne nie są ze sobą połączone. Identyfikacja osób chorych na COVID-19 jest więc niemożliwa z perspektywy aplikacji ProteGO Safe i serwerów ProteGO Safe[73]. Serwer ProteGO Safe nie umożliwia przechowywania lub połączenia (porównania) identyfikatorów urządzenia użytkownika z kluczami diagnostycznymi.

W zakresie audytowania realizacji zasad *privacy by design* i *privacy by default* w aplikacji ProteGO Safe stwierdzono, że dane nie podlegają

[71] Zob. § 3 ust. 6 pkt 1 Polityki prywatności ProteGO Safe.
[72] Zob. P. Litwiński, A. Leńczuk, A. Krzyżak, A. Siwek, *Raport…*, s. 19.
[73] *Ibidem*, s. 16.

autouzupełnianiu z innych źródeł. Aplikacja nie jest powiązana i nie może zostać sparowana np. z kontami w mediach społecznościowych[74].

W komunikacji pomiędzy urządzeniami użytkowników przekazywane są dane zakodowane w kluczu diagnostycznym, umożliwiające wskazanie ryzyka transmisji wirusa SARS-CoV-2 od użytkownika, u którego wykryto obecność wirusa lub chorobę COVID-19. Udostępnianiu może podlegać klucz diagnostyczny, zawierający informację o chorym użytkowniku oraz o tymczasowych identyfikatorach jego urządzenia, przy czym sygnał odbierany przez aplikację jest przez nią interpretowany automatycznie, bez wskazywania użytkownikom, które z zarejestrowanych spotkań stanowiło podstawę zagrożenia zakażeniem, zatem nie dochodzi do udostępnienia danych osoby chorej lub innego użytkownika. Dla innych podmiotów, w tym Głównego Inspektora Sanitarnego czy Ministra Cyfryzacji, który zarządza serwerem ProteGO Safe, dane te są anonimowe w rozumieniu art. 11 RODO[75]. Aplikacja ProteGO Safe przechowuje na urządzeniu użytkownika informacje, które można podzielić na dwie grupy: po pierwsze, informacje niezbędne dla zapewnienia funkcjonalności modułu Triażu, dziennika zdrowia i modułu analitycznego; po drugie, informacje niezbędne dla zapewnienia bezpieczeństwa aplikacji i danych w niej zapisanych, w szczególności w zakresie plików *cookies* dostarczonych przez Cloudflare w celu ochrony przed atakami DDOS[76].

ProteGO Safe gromadzi informacje niezbędne dla zapewnienia możliwości przeprowadzania analiz dotyczących aplikacji, w celu umożliwienia dalszego rozwoju aplikacji i doskonalenia jej, przy zastosowaniu technologii Google Analytics. Wykorzystywana technologia Google Analytics w projekcie ProteGO Safe nie umożliwia analizowania sposobu korzystania z aplikacji, a jedynie daje informacje statystyczne dotyczące liczby pobrań, modelów telefonów (aby efektywniej dobierać

[74] *Ibidem*, s. 17.
[75] *Ibidem*, s. 14.
[76] *Ibidem*, s. 18.

zasoby usług utrzymania w zakresie obsługi błędów) i przybliżonej lokalizacji pobrania (chodzi głównie o kraj pobrania aplikacji)[77].

Zastanowienia wymagają kwestie, czy dane, którymi dysponuje GIS, można, po pierwsze, zaliczyć do kategorii danych otwartych, czyli informacji sektora publicznego udostępnianych lub przekazywanych w postaci elektronicznej, bezwarunkowo lub z uwzględnieniem warunków, o których mowa w rozdziale 3 u.o.d.p.w.i., kompletnych, aktualnych, w wersji źródłowej, w otwartym i niezastrzeżonym formacie przeznaczonym do odczytu maszynowego, które są przeznaczone do bezpłatnego ponownego wykorzystywania na tych samych zasadach dla każdego użytkownika, bez konieczności potwierdzania tożsamości przez użytkownika, a po drugie – czy GIS ma podstawy prawne do przekazywania tych danych innym podmiotom publicznym w celu realizacji zadań związanych ze zdrowiem publicznym w okresie pandemii COVID-19.

3. Używanie danych z aplikacji śledzących kontakty zakaźne do innych celów niż ostrzeganie osób, które mogły mieć styczność z SARS-CoV-2

Powoływane we wcześniejszej części niniejszego opracowania akty prawne, wytyczne i zalecenia organów UE, jak również Regulamin i Polityka prywatności polskiej aplikacji ProteGO Safe wskazują, że podstawą prawną przetwarzania danych osobowych przez aplikacje mobile śledzące kontakty zakaźne jest niezbędność przetwarzania danych do wykonania zadania realizowanego w interesie publicznym, polegającego na ochronie przed poważnymi, wewnątrzkrajowymi, jak i transgranicznymi zagrożeniami zdrowotnymi. Konkretyzując, zadanie to ma na celu zapobieganie, przeciwdziałanie i zwalczanie COVID-19 poprzez umożliwienie poszczególnym osobom fizycznym śledzenia kontaktów

[77] *Ibidem*.

zakaźnych, powiadamianiu ich o tym, że znalazły się one w bliskiej odległości od osoby, która ostatecznie została uznana za nosiciela wirusa, w celu jak najszybszego przerwania łańcucha zakażenia.

Przypomnieć jednak należy, że w wyniku szukania balansu pomiędzy koniecznością zyskania akceptacji społecznej do używania aplikacji mobilnych śledzących kontakty zakaźne i związanych z tym ochroną danych osobowych oraz prywatności użytkowników a koniecznością opanowywania pandemii COVID-19 organy UE wybrały rozwiązania chroniące dane i prywatność użytkowników, co zdaje się, ograniczyło jednocześnie możliwości wykorzystania tych danych przez organy ds. zdrowia publicznego. Dane, którymi dysponuje polski GIS jako administrator danych osobowych w ramach ProteGO Safe, można określić jako szczątkowe – w porównaniu z tymi, które są (lub mogą być) gromadzone za pomocą tej aplikacji (w zależności od stopnia wykorzystania jej różnych funkcjonalności przez poszczególnych użytkowników). Tymi danymi są: informacje o liczbie przesłanych na serwer ProteGO Safe kluczy diagnostycznych oraz daty ich wysłania, a także dane przetwarzane w aplikacji i związane z wykorzystywaniem serwera zapewniającego przekazywanie użytkownikom komunikatów, jak UID – losowy identyfikator urządzenia użytkownika oraz średni czas korzystania z aplikacji przez użytkowników (dane statystyczne, których nie można powiązać z poszczególnymi użytkownikami)[78]. Bez wątpienia dane te spełniają kryteria definicji pojęcia „informacja sektora publicznego", zawartej w u.o.d.p.w.i. GIS powinien udostępniać te dane do ponownego wykorzystywania. Obecnie dane dotyczące zarówno liczby wysłanych kluczy z ostatnich 7 dni, jak i od początku funkcjonowania aplikacji są dostępne w trybie bezwnioskowym jedynie w aplikacji ProteGO Safe w zakładce *Home*[79].

[78] Zob. § 3 ust. 6 pkt 1 Polityki prywatności ProteGO Safe.

[79] Nie można ich znaleźć np. na stronie internetowej https://www.gov.pl/web/protego safe czy https://dane.gov.pl/. Na stronie https://dane.gov.pl/pl/application/1244,protego -safe [dostęp: 19.09.2021] znajduje się tylko opis aplikacji wraz z linkiem do jej pobrania.

Otwarte dane to dane o szczególnym znaczeniu dla rozwoju innowacji w państwie i rozwoju społeczeństwa informacyjnego, wytworzone przez sektor publiczny lub prywatny, działający w celu realizacji zadań publicznych. Jak już wspomniano, pojęcie to zostało zdefiniowane w art. 2 pkt 11 u.o.d.p.w.i. Dane, nawet zanonimizowane, służące ochronie zdrowia publicznego w czasie pandemii wywołanej przez wirus SARS-CoV-2, są danymi o szczególnym znaczeniu i mogą prowadzić do wytworzenia nowych usług[80]. Nieco na marginesie rozważań odnotować należy, że pojęcie „otwartych danych publicznych" zostało po raz pierwszy zdefiniowane przez grupę zwolenników otwartego rządu na spotkaniu w Sewastopolu w Kalifornii w 2007 r. Otwarte dane rządowe (*Open Government Data*) to filozofia, a coraz częściej zbiór polityk, która promuje przejrzystość, odpowiedzialność i tworzenie wartości poprzez udostępnianie wszystkim danych sektora publicznego. W 2007 r. zespół trzydziestu specjalistów z różnych dziedzin zdefiniował także kryteria (warunki) otwartości danych[81]. W 2012 r. sformułowana została prosta,

[80] Byłyby to dane dynamiczne w rozumieniu art. 2 pkt 8 dyrektywy 2019/1024, a więc „dokumenty w formie cyfrowej podlegające częstym aktualizacjom lub aktualizacjom w czasie rzeczywistym, w szczególności ze względu na ich zmienność lub szybką dezaktualizację; dane wygenerowane przez czujniki zasadniczo uznaje się za dane dynamiczne".

[81] Są nimi: 1) kompletność; 2) źródłowość; 3) aktualność; 4) dostępność niezależna od platformy informatycznej wykorzystywanej przez użytkownika (neutralność technologiczna); 5) przetwarzalność maszynowa (publikowanie w ustrukturyzowany sposób wraz z opisem struktury pliku, np. w formie metadanych); 6) udostępnienie w sposób niedyskryminujący (dostępność dla każdego, bez konieczności rejestracji czy podpisywania umów); 7) otwarty format plików (pełna specyfikacja formatu ma być dostępna za darmo w sieci); 8) dostępność bez ograniczeń licencyjnych (np. prawa autorskiego, patentowego, tajemnicy handlowej); zob. T. Kulisiewicz, *Redukcja pozaprawnych barier ponownego wykorzystywania informacji sektora publicznego*, [w:] A. Piskorz-Ryń (red.), *Jawność i jej ograniczenia*, t. V. *Dostęp i wykorzystywanie*, Warszawa 2015, s. 202. Kryteria podstawowe uzupełnione zostały później przez kilka warunków dodatkowych. Są nimi: wymagania bezpłatnej dostępności *on-line* danych w stałej lokalizacji sieciowej i w stabilnym formacie, opatrzenia danych potwierdzeniami autentyczności i integralności, otwartości z definicji, odpowiedniego udokumentowania, bezpieczeństwa dla użytkowników oraz wykorzystania inicjatyw obywatelskich przy zbieraniu danych i projektowaniu mechanizmów ich udostępniania.

pięciostopniowa skala poziomu otwartości danych, nazwana *5-Star Open Data*[82]. W 2015 r. wydano Międzynarodową kartę otwartych danych[83].

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024, dotycząca ponownego wykorzystywania informacji sektora publicznego, reguluje także „otwarte dane", co podkreślono już w jej tytule. Ma to przede wszystkim wymiar aksjologiczny; ponowne wykorzystywanie służy polityce publicznej otwierania danych. Prawodawca UE położył nacisk również na konieczność udostępniania danych w czasie rzeczywistym, w formatach nadających się do maszynowego przetwarzania, co ma służyć rozwijaniu innowacyjnych produktów, usług i aplikacji z wykorzystaniem nowoczesnych technologii, takich jak sztuczna inteligencja czy Internet rzeczy[84].

Jak już kilkukrotnie wspominano, GIS nie posiada danych identyfikujących zakażonych użytkowników aplikacji ProteGO Safe, ich wieku, aktualnego samopoczucia zdrowotnego, stanu zdrowia, w tym chorób współistniejących, na które zapadli i które mogą przyczynić się do cięższego przebiegu COVID-19 lub większego ryzyka zgonu na tę chorobę zakaźną, danych adresowych czy lokalizacji użytkowników. Z pomocą danych pozyskanych z polskiej aplikacji nie jest więc możliwe określenie, czy wirus SARS-CoV-2 przenosi się, a jeśli tak, to w jakim stopniu intensywności (jak szybko), na inne grupy wiekowe niż osoby starsze. Dane te albo nie są w ogóle gromadzone (jak np. dane o lokalizacji), albo są przetwarzane na urządzeniu końcowym użytkownika (np. smartfonie), do których GIS ani MC nie mają dostępu. W odniesieniu do danych gromadzonych bezpośrednio z urządzenia końcowego zastosowanie znajduje art. 5 ust. 3 dyrektywy 2002/58. W związku z tym dostęp dostawcy usługi łączności elektronicznej, którym jest Minister Cyfryzacji, do informacji przechowywanej na

[82] Skala zaproponowana przez Tima Bernersa-Lee dostępna jest na stronie internetowej http://5stardata.info/en/ [dostęp: 17.09.2021].

[83] *International Open Data Charter*, zob. https://opendatacharter.net/wp-content/uploads/2015/10/opendatacharter-charter_F.pdf [dostęp: 19.09.2021].

[84] Zob. D. Sybilski, *Dane o wysokiej wartości – nowy rodzaj informacji sektora publicznego*, „Informacja w Administracji Publicznej" 2019, Nr 4, s. 11.

urządzeniu końcowym (np. do ankiety samooceny stanu zdrowia w aplikacji ProteGO Safe) jest dozwolony tylko wtedy, gdy użytkownik wyraził na to zgodę lub dostęp jest niezbędny dla usługi społeczeństwa informacyjnego, o którą wyraźnie poprosił. Ograniczenia praw i obowiązków przewidzianych w dyrektywie 2002/58 są co prawda możliwe na mocy jej art. 15, ale może stać się tak jedynie wtedy, jeżeli stanowią one niezbędny, odpowiedni i proporcjonalny środek w ramach społeczeństwa demokratycznego dla osiągnięcia wyraźnie określonych celów[85]. Nie ma zatem podstaw prawnych do dostępu Ministra Cyfryzacji (dostawcą publicznie dostępnej usługi łączności elektronicznej w publicznych sieciach łączności w UE) czy Głównego Inspektora Sanitarnego (administratora danych gromadzonych przez aplikację) do danych przechowywanych na smartfonach użytkowników aplikacji ProteGO Safe. Nie są uprawnione sugestie, jakoby MC czy GIS mogli tymi danymi dysponować bez zgody użytkowników i przekazywać je np. inspekcjom sanitarnym w celu ułatwienia prowadzenia tzw. dochodzeń epidemiologicznych.

Na zagadnienie związane z aplikacjami mobilnymi służącymi do śledzenia kontaktów zakaźnych można bowiem spojrzeć nieco szerzej niż przez pryzmat ostrzegania osób fizycznych (użytkowników aplikacji) o kontakcie z osobą chorą na COVID-19, co jest podstawowym celem aplikacji śledzących kontakty zakaźne. Aplikacje posiadające funkcjonalność samodzielnej diagnozy oraz weryfikacji objawów chorobowych mogłyby dostarczać istotnych informacji na temat liczby osób wykazujących objawy choroby COVID-19, w podziale na wiek i tydzień roku, pochodzących ze ściśle określonych obszarów, na których dana aplikacja jest w powszechnym użyciu (oczywiście gdyby gromadzono dane o lokalizacji użytkowników).

Mimo ograniczonego zakresu gromadzonych danych, zanonimizowane i zagregowane dane pochodzące z aplikacji śledzących kontakty

[85] Zob. szerzej: W.R. Wiewiórowski, *Rola Unii Europejskiej w koordynacji zastosowania narzędzi informatycznych do walki z pandemią*, „Europejski Przegląd Sądowy" 2020, nr 6, LEX.

zakaźne, w połączeniu np. z informacjami na temat częstości występowania choroby COVID-19, zbieranymi przez organy ds. ochrony zdrowia, chociażby bez użycia narzędzi elektronicznych, hipotetycznie można byłoby wykorzystać, przykładowo, do oceny skuteczności środków społecznych i środków w zakresie ograniczania kontaktów społecznych, wprowadzania ograniczeń związanych z pandemią wirusa SARS-CoV-2 na danym obszarze kraju, a także ustalania zapotrzebowania na środki ochrony indywidualnej czy specjalistyczny sprzęt medyczny i liczby placówek służby zdrowia, które powinny specjalizować się w leczeniu COVID-19 w danym regionie kraju, ale pod warunkami określonymi w art. 6 i art. 9 dyrektywy 2002/58[86]. Dane te hipotetycznie mogłyby być użyte przez inne niż GIS organy sektora publicznego. W takiej sytuacji nie można mówić o „ponownym wykorzystywaniu" (ang. *re-use*) informacji. Zgodnie z definicją zawartą w art. 2 pkt 11 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1024 w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego ponowne wykorzystywanie oznacza wykorzystywanie przez osoby fizyczne lub podmioty prawne dokumentów będących w posiadaniu (m.in.) organów sektora publicznego do celów komercyjnych lub niekomercyjnych innych niż ich pierwotne przeznaczenie w ramach zadań publicznych, dla którego to celu dokumenty te zostały wyprodukowane, z wyjątkiem wymiany dokumentów między organami sektora publicznego służącej wyłącznie wykonywaniu ich zadań publicznych. Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego zawiera, co oczywiste, podobną w treści definicję[87]. W zakresie definicji ponownego wykorzystywania nie mieści się zatem wykorzystywanie danych zebranych przez aplikację ProteGO Safe i znajdujących się na centralnym serwerze (a nie na urządzeniach końcowych

[86] Zob. szerzej: W.R. Wiewiórowski, *Rola Unii Europejskiej…*

[87] Ponowne wykorzystywanie oznacza wykorzystywanie przez użytkowników informacji sektora publicznego w jakimkolwiek celu, z wyjątkiem wymiany informacji sektora publicznego między podmiotami zobowiązanymi wyłącznie w celu realizacji zadań publicznych (art. 2 pkt 12).

użytkowników aplikacji mobilnych) przez organy publiczne zajmujące się np. ochroną zdrowia publicznego. Ponownym wykorzystywaniem byłoby użycie tych danych np. przez podmioty z sektora prywatnego.

Ustalanie kontaktów zakaźnych oznacza, że organy ds. zdrowia publicznego szybko identyfikują wszystkie osoby, z którymi kontaktował się pacjent z pozytywnym wynikiem badania na obecność wirusa SARS-CoV-2, proszą je o pozostanie w domu i szybko badają i izolują te osoby, jeżeli wystąpią u nich objawy. Funkcja śledzenia kontaktów zakaźnych jest więc przydatna zarówno dla jednostek, jak i organów zdrowia publicznego. Może ona również odgrywać ważną rolę w zarządzaniu środkami ograniczającymi rozprzestrzenianie się wirusa w fazie deeskalacji. Jej wpływ można zwiększyć za pomocą strategii wspierającej szerzej zakrojone testowanie osób z łagodnymi objawami COVID-19. Obie te funkcje mogą również stanowić istotne źródło danych dla organów zdrowia publicznego i ułatwić przekazywanie takich danych krajowym organom epidemiologicznym oraz ECDC[88]. Ułatwiłoby to zrozumienie sposobów rozprzestrzeniania się choroby oraz, w połączeniu z wynikami badań, oszacowanie wartości predykcyjnej wyniku dodatniego dla objawów z układu oddechowego w danej społeczności i zapewnienie informacji na temat poziomu występowania wirusa.

Tymczasem ogromna większość dochodzeń epidemiologicznych w Polsce wykonywana jest przez organy do spraw ochrony zdrowia środkami konwencjonalnymi, bez użycia aplikacji mobilnych czy innego rodzaju technologii wspierającej. Opierają się one głównie na relacjach osób zakażonych, które nie zawsze mogą być prawdziwe z powodu ulotności pamięci ludzkiej, jak i intencji zachowania ich w tajemnicy, np. z powodu złamania zakazów przemieszczania się czy udziału w określonych zgromadzeniach. Jak już wielokrotnie wskazywano w niniejszym opracowaniu, aplikacje śledzące kontakty zakaźne nie umożliwiają identyfikacji użytkowników

[88] Zob. https://www.ecdc.europa.eu/en [dostęp: 19.09.2021].

między sobą ani identyfikacji użytkowników, którzy mieli kontakt z osobą zakażoną, przez organy do spraw ochrony zdrowia czy pozostałych użytkowników aplikacji. Rozwiązanie to podyktowane zostało chęcią wzmocnienia zaufania do tego rodzaju aplikacji poprzez zapewnienie wysokiego stopnia ochrony prywatności ich użytkowników. Przypomnieć należy, że w Polsce administratorem danych osobowych, który samodzielnie ustala cele i sposoby przetwarzania danych osobowych w ramach ProteGO Safe, jest Główny Inspektor Sanitarny. Gdyby osoby mające kontakt z osobami zakażonymi, znanymi przecież organom ds. ochrony zdrowia z imienia i nazwiska, również były identyfikowane, przeprowadzanie dochodzeń epidemiologicznych, a w konsekwencji nakładanie obowiązku kwarantanny czy wykonywanie testów na obecność wirusa SARS-CoV-2, byłoby o wiele szybsze i łatwiejsze, a przez to walka z rozpowszechnianiem się COVID-19 stałaby się bardziej skuteczna. Warunkiem takiego założenia jest jednak aktywne korzystanie z aplikacji, aktywowanie modułu analitycznego oraz wpisanie kodu PIN do aplikacji przez znaczną część społeczeństwa, a nie jedynie jego niewielki odsetek[89], a przede wszystkim – podstawa prawna do korzystania przez dostawcę aplikacji (Ministra Cyfryzacji) – i podmioty, którym przekazywałby dane – z danych zgromadzonych na urządzeniu końcowym użytkownika, czyli zgoda użytkownika. Obecnie użytkownik nawet nie ma możliwości wyrażenia takiej zgody, nie istnieje system przekazywania danych zgromadzonych przy pomocy aplikacji na urządzeniu końcowym do jakiegoś systemu informacyjnego organów ds. ochrony zdrowia.

[89] Tylko niecałe 2% Polaków zainstalowało do tej pory rządową aplikację do śledzenia kontaktów z osobami zakażonymi koronawirusem; zob. D. Maciejasz, *Polacy nie zaufali rządowej aplikacji do walki z pandemią. A ci, którzy ją mają, nie raportują zakażeń*, „Gazeta Wyborcza" 2.09.2020, https://wyborcza.pl/7,156282,26260940,aplikacja-tropiaca-wirusa-w-wirtualnym-schowku-polacy-nie-chca.html [dostęp: 20.09.2021]. Dnia 26.10.2020 r. do Prezesa rady Ministrów wpłynęła interpelacja nr 13367 w sprawie aplikacji ProteGO Safe; do czasu zakończenia prac nad niniejszym opracowaniem nie udzielono odpowiedzi na interpelację; https://www.sejm.gov.pl/sejm9.nsf/InterpelacjaTresc.xsp?key=BUUE8Y [dostęp: 20.09.2021].

W przypadku dużej popularności tych aplikacji krajowe organy ds. zdrowia publicznego mogłyby zdecydować się na wykorzystanie zanonimizowanych danych pochodzących z aplikacji do celów nadzoru syndromicznego nad COVID-19 w ramach podstawowej opieki zdrowotnej. Nadzorem syndromicznym (ang. *syndromic surveillance*) jest monitorowanie częstości występowania pojedynczych objawów lub ich zespołów bez odnoszenia ich do specyficznych chorób. Taki system służy do wczesnego wykrywania epidemii (ognisk epidemicznych), szczególnie z wielu źródeł. Jest wprowadzany w przypadkach masowych zgromadzeń lub w stanach zagrożenia bioterrorystycznego[90].

W przepisach ustawy o PIS nie wskazano, że Główny Inspektor Sanitarny jest zobowiązany do zarządzania aplikacją śledzącą kontakty zakaźne. Spoczywa na nim obowiązek zarządzania systemem wymiany informacji w ramach systemów wymiany informacji, o których mowa w przepisach wykonawczych wydanych na podstawie art. 2 ust. 2 ustawy o PIS, w zakresie dotyczącym zadań PIS. Rozporządzenie Ministra Zdrowia z dnia 17 października 2014 r. w sprawie systemów wymiany informacji w zakresie dotyczącym zadań Państwowej Inspekcji Sanitarnej[91] określa: wykaz systemów wymiany informacji w zakresie dotyczącym zadań PIS (wśród których znajduje się System Nadzoru Epidemiologicznego nad Chorobami Zakaźnymi) oraz zasady zarządzania przez Głównego Inspektora Sanitarnego wymianą informacji.

Główny Inspektor Sanitarny zarządza wymianą informacji w zakresie systemów, którymi zarządza, przez: zbieranie danych, zapewnianie ciągłej, wielostronnej i szybkiej wymiany danych w sposób, który zapewni kompletność i niezbędną jakość informacji, określanie jednolitych zasad oceny ryzyka sanitarnego i epidemiologicznego, organizowanie specjalistycznych

[90] Zob. A. Zieliński (red.), *Słowniczek terminów epidemiologicznych*, „Przegląd Epidemiologiczny" http://www.przeglepidemiol.pzh.gov.pl/slowniczek-terminow-epidemiologicznych [dostęp: 20.09.2021].

[91] Dz. U. z 2014 r. poz. 1474 ze zm.

szkoleń w zakresie gromadzenia i przetwarzania danych w tych systemach oraz ich obsługi, administrowanie i utrzymywanie centralnych baz danych tych systemów, z wyłączeniem Systemu Wczesnego Ostrzegania o Niebezpiecznej Żywności i Paszach (RASFF) w Polsce. Natomiast w § 2 pkt 10 zd. 2 Regulaminu ProteGO Safe znajduje się następujące postanowienie: „Minister Cyfryzacji w oparciu o porozumienie wspiera GIS w rozwoju i utrzymaniu STOP COVID – ProteGO Safe". Wydaje się, że biorąc pod uwagę wskazane akty prawne, a więc ustawę o PIS i rozporządzenie Ministra Zdrowia z dnia 17 października 2014 r. w sprawie systemów wymiany informacji w zakresie dotyczącym zadań PIS, obecnie GIS nie ma prawnej podstawy do takiej formy zarządzania aplikacją śledzącą kontakty zakaźne, która obejmuje pobieranie z danych z serwera ProteGO Safe, następnie przekazywanych do innych systemów informacyjnych w celu realizacji zadań PIS, ani do systemów informacyjnych innych organów ds. ochrony zdrowia.

Tymczasem podejście polegające na maksymalnym wykorzystaniu, oczywiście w granicach zakreślonych przez prawo, danych posiadanych przez organy publiczne, jest zgodne z ideą tzw. otwartego rządu. Rząd jest otwarty (*Open Government*), gdy uwalnia technologię i napędza innowacje w granicach dostępnego prawodawstwa i w równowadze z interesem krajowym i publicznym. Podejście otwarte domyślnie (*open by default*) opisuje zakres, w jakim sprawny i proaktywny rząd (czy szerzej – organy administracji publicznej) wykorzystuje i współużytkuje cyfrowe technologie i narzędzia do komunikowania się, angażowania, współpracy i budowania mostów między wszystkimi podmiotami w celu gromadzenia spostrzeżeń w kierunku bardziej opartego na wiedzy sektora publicznego. Obejmuje to nie tylko dostarczanie bodźców do promowania współpracy i innowacji (np. otwarte dane rządowe, *open source*), poszanowanie cyfrowych praw obywateli (np. przepisów dotyczących ochrony danych osobowych, prywatności, bezpieczeństwa, poufności), ale także otwieranie i współtworzenie procesów rządowych (np. cykl życia polityki,

świadczenie usług publicznych i uruchamianie ICT)[92]. Pojęcie „rząd oparty na danych" (*data driven government*) oznacza rząd (czy szerzej – organy administracji publicznej), który zapewnia, że dane sektora publicznego są udostępniane wewnątrz i na zewnątrz sektora publicznego w sposób godny zaufania, z zachowaniem jasnych zasad ochrony, prywatności, bezpieczeństwa i zasad etycznych dla interesu narodowego i publicznego. Aby ułatwić dzielenie się nimi, rządy budują właściwe podstawy, ustanawiając jasne polityki, które mogą pomóc w przystąpieniu do rządu, promując tym samym integrację sektora publicznego. Rządy oparte na danych przełamują silosy polityczne, promując spójność polityk związanych z danymi, w tym w zakresie ochrony danych, otwartych danych i sztucznej inteligencji, zapewniają wiodącą rolę w rozwoju polityk dotyczących danych i budują zarządzanie potrzebne do promowania koordynacji i odpowiedzialności. Obejmują one międzysektorowe standardy danych oraz replikowalne i skalowalne infrastruktury danych, które ułatwiają szybki i bezpieczny dostęp do danych oraz ich wymianę[93].

Dyrektywa 2019/1024, zgodnie z brzmieniem jej art. 1 ust. 4, pozostaje bez uszczerbku dla krajowych i unijnych przepisów dotyczących ochrony danych osobowych, w szczególności RODO i dyrektywy 2002/58/WE, a także odpowiadających im przepisów prawa krajowego. Przy podejmowaniu decyzji w sprawie zakresu i warunków ponownego wykorzystywania dokumentów sektora publicznego zawierających dane osobowe, np. w sektorze zdrowia, wymagane może być przeprowadzenie oceny skutków dla ochrony danych zgodnie z art. 35 RODO[94]. Proces otwierania danych publicznych powinien podlegać odpowiednim zasadom także w zakresie ochrony prywatności, przejrzystości, etyki i praw cyfrowych, w tym w przypadkach, gdy informacje zawarte w indywidualnym

[92] Zob. *OECD Open, Useful and Re-usable data (OURdata) Index: 2019*, http://www.oecd.org/governance/digital-government/ourdata-index-policy-paper-2020.pdf, s. 14 [dostęp: 20.09.2021].

[93] Zob. *ibidem*, s. 13-14.

[94] Pkt 53 preambuły dyrektywy 2019/1024.

zbiorze danych samodzielnie nie stwarzają ryzyka identyfikacji lub wskazania osoby fizycznej, natomiast mogą stwarzać takie ryzyko, gdy informacje te są połączone z innymi dostępnymi informacjami.

4. Zdolność aplikacji mobilnych śledzących kontakty zakaźne do transgranicznej wymiany danych

Jednym z czynników warunkujących otwartość danych publicznych jest ich interoperacyjność. Ma ona także zasadnicze znaczenie z punktu widzenia rozprzestrzeniania się wirusa SARS-CoV-2, który nie respektuje granic państwowych. W celu umożliwienia wykrywania bliskich kontaktów między użytkownikami różnych aplikacji służących do ustalania kontaktów zakaźnych (scenariusz, który jest najbardziej prawdopodobny wśród osób przemieszczających się między krajami/regionami) należy zadbać o interoperacyjność między aplikacjami w poszczególnych państwach. Współpraca między nimi, opracowanie, testowanie, wdrażanie i stosowanie interoperacyjnych interfejsów elektronicznych zwiększy wydajność i bezpieczeństwo usług skierowanych na ochronę zdrowia publicznego. Jeżeli osoba zakażona pozostaje w kontakcie z użytkownikiem aplikacji śledzącej kontakty zakaźne z innego państwa, np. członkowskiego UE, powinno być możliwe transgraniczne przekazywanie danych osobowych takiego użytkownika organom ds. zdrowia w jego państwie członkowskim, w zakresie, w jakim jest to absolutnie niezbędne. Krajowe organy ds. zdrowia nadzorujące łańcuchy zakażeń powinny mieć możliwość wymiany z innymi państwami lub regionami interoperacyjnych informacji na temat użytkowników, u których wykryto obecność wirusa, aby móc zaradzić transgranicznym łańcuchom zakażeń.

Pojęcie „interoperacyjność" to w najogólniejszym znaczeniu „zdolność do współdziałania". Interoperacyjność jest rozumiana na trzech wzajemnie na siebie oddziałujących płaszczyznach: interoperacyjności

organizacyjnej, interoperacyjności informacyjnej oraz interoperacyjności technicznej.

Interoperacyjność organizacyjna oznacza uzyskanie możliwości efektywnego współdziałania podmiotów publicznych, jednostek i przedsiębiorców – co dotyczy zwłaszcza zdolności współdziałania podczas czynności administracyjnych realizowanych przy wsparciu systemów teleinformatycznych. Interoperacyjność informacyjna to zdolność do efektywnej wymiany informacji pomiędzy podmiotami publicznymi, jednostkami i przedsiębiorcami, rozumianej zarówno w wymiarze zgodności syntaktycznej danych (sposobu opisu struktury przesyłanych danych), jak i spójności semantycznej informacji. Syntaktyczna zgodność opisu danych stanowi podstawę dla uzyskania zgodności semantycznej informacji. Uzyskanie pełnej spójności informacyjnej systemów teleinformatycznych pozwoli uniknąć niejednoznaczności interpretacji przesyłanych informacji, co powinno zapewnić wyższy poziom bezpieczeństwa informacyjnego, w tym teleinformatycznego dla systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych. Interoperacyjność techniczna rozumiana jest w wymiarze technologii wymiany danych pomiędzy systemami teleinformatycznymi administracji publicznej a jednostkami i biznesem. Poziom interoperacyjności technicznej jest zrozumiały głównie dla programistów[95].

Interoperacyjność zapewnia szereg konkretnych korzyści: zwiększa elastyczność, umożliwiając „mieszanie i dopasowywanie" komponentów poszczególnych usług publicznych, zwiększa opłacalność, umożliwiając ponowne wykorzystanie istniejących komponentów i możliwości, tworzy wirtualnie zintegrowane systemy, które są łatwiejsze w użyciu w różnych organizacjach i regionach lub krajach, a także ułatwia tworzenie nowych możliwości poprzez komponowanie nowych funkcji z już istniejących.

[95] Zob. B. Szafrański, G. Bliźniuk, J. Karnowski, Z. Świerczyński, R. Weydmann, L. Żurek (red.), *Interoperacyjność i bezpieczeństwo systemów informatycznych administracji publicznej*, Katowice 2006, s. 20-21.

Dokumentem o priorytetowym znaczeniu dla interoperacyjności w UE są Europejskie Ramy Interoperacyjności (*European Interoperability Framework – EIF*). W czerwcu 2002 r., podczas szczytu w Sewilli, przedstawiciele rządów krajów członkowskich UE przyjęli dokument *eEurope Action Plan 2005*[96], który zobowiązywał kraje członkowskie do przygotowania ram interoperacyjności, umożliwiających dostarczanie paneuropejskich usług *e-Government* obywatelom i przedsiębiorcom. W lipcu 2003 r. uznano, że założenia Europejskich Ram Interoperacyjności stanowią kluczowy element rozwoju usług e-Administracji w Europie. Pierwsza wersja EIF została wydana w listopadzie 2004 r. w ramach programu *Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens* (*IDABC*)[97]. Zalecano w nich rządom państw członkowskich tworzenie krajowych ram interoperacyjności w spójności z EIF, aby umożliwić interoperacyjność wspólnotową. Od grudnia 2009 r. prace nad EIF były kontynuowane w ramach programu *Interoperability Solutions for European Public Administrations* (*ISA*)[98]. W 2017 r. program ten został zastąpiony, poprzez Komunikat Komisji z dnia 23 marca 2017 r. do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Europejskimi Ramami Interoperacyjności – strategią wdrażania*[99], czyli tzw. Nowymi Europejskimi Ramami Interoperacyjności.

[96] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0263:FIN:EN:PDF [dostęp: 19.09.2021].

[97] Zob. https://wayback.archive-it.org/12090/20200210174143/https://ec.europa.eu/idabc/ [dostęp: 19.09.2021].

[98] Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z 16.12.2010 r. *W kierunku interoperacyjności europejskich usług użyteczności publicznej*, COM/2010/0744 final, https://eur-lex.europa.eu/resource.html?uri=cellar:f132547a-7d66-4626-8eb6-9f7428394de7.0022.03/DOC_1&format=PDF [dostęp: 19.09.2021].

[99] COM(2017) 134 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52017DC0134&from=PL [dostęp: 19.09.2021].

Regulują one przede wszystkim sposób, w jaki zasady i modele interoperacyjności powinny być stosowane w praktyce. Zaktualizowane zalecenia dotyczące interoperacyjności zostały uściślone, położono większy nacisk na otwartość i zarządzanie informacjami, przenoszenie danych, zarządzanie interoperacyjnością i zintegrowane świadczenie usług. Ważniejsze rekomendacje Nowych Europejskich Ram Interoperacyjności dotyczą przede wszystkim: dostępności – oznaczającej wielokanałowe udostępnienie treści w formie zrozumiałej dla użytkowników, wielojęzyczności – udostępniania treści nie tylko w językach narodowych, bezpieczeństwa – dostosowanego do poziomu paneuropejskiego, prywatności, w tym ochrony danych osobowych, subsydiarności – EIF działa pomocniczo i nie wnika w działania wewnątrznarodowe, stosowania otwartych standardów, preferowania oprogramowania o otwartym kodzie źródłowym, tworzenia rozwiązań wielostronnych, pochodzących z różnych źródeł i od różnych dostawców. Szczególnie duży nacisk w Europejskich Ramach Interoperacyjności kładzie się na realizowanie ich założeń przez wybieranie w projektach *e-Government* otwartych standardów oraz wolnego oprogramowania o otwartym kodzie źródłowym[100].

Zgodnie z treścią zaleceń Sieci e-Zdrowie z 15.04.2015 r.[101] funkcjonowanie aplikacji śledzących kontakty zakaźne powinno spełniać wymagania interoperacyjności, sprecyzowane w *eHealth Interoperability Framework* z 23.11.2015 r.[102] Ramy te są zatwierdzone przez Sieć

[100] Według Europejskich Ram Interoperacyjności otwarte standardy powinny charakteryzować się następującymi cechami: zostały przyjęte przez organizację *not-for-profit*, a ich rozwój będzie opierał się na otwartej procedurze decyzyjnej dostępnej dla każdej zainteresowanej strony, zostały opublikowane, a opłaty za korzystanie ze standardu są niskie i nie stanowią bariery w dostępie do standardu, własność intelektualna standardu lub jego części udostępniona jest bez pobierania dodatkowych opłat, a sposób udostępnienia nie może być zmieniony, nie ma żadnych ograniczeń w ponownym wykorzystaniu standardu.

[101] Zob. *Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States* z 15.04.2020 r., https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf [dostęp: 19.09.2021].

[102] https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20151123_co03_en.pdf [dostęp: 19.09.2021].

e-Zdrowie i składają się z następujących warstw: prawnej i regulacyjnej; organizacyjnej (polityka i proces opieki); semantycznej (dane i informacje); technicznej (aplikacje i infrastruktura)[103]. Przykładowo zalecenie IOP-04 stanowi, że organy zdrowia publicznego powinny uzgodnić protokoły wymiany informacji o łańcuchach transgranicznych kontaktów, zwłaszcza o zarażonych mających kontakt z osobami z innych państw. Nie należy oczywiście zapominać o podstawach prawnych przekazywania danych, w tym danych osobowych i danych osobowych dotyczących zdrowia, pomiędzy różnymi systemami informacyjnymi czy podmiotami. Stworzenie możliwości wymiany danych na poszczególnych poziomach interoperacyjności (organizacyjnej, informacyjnej i technicznej) nie warunkuje legalności tego procesu.

Wytyczne dotyczące interoperacyjności dla zatwierdzonych aplikacji mobilnych do śledzenia kontaktów w UE, przyjęte przez Sieć e-Zdrowie w dniu 13 maja 2020 r.[104], opisują interoperacyjność aplikacji mobilnych służących do śledzenia kontaktów i związanych z nimi procedur jako ich zdolności do wymiany między sobą minimum informacji niezbędnych do ostrzeżenia poszczególnych użytkowników aplikacji, bez względu na to, gdzie się znajdują w UE, zgodnie z procedurami określonymi przez organy zdrowia publicznego, jeżeli znajdował się w pobliżu innego użytkownika, który powiadomił aplikację, że przeszedł pozytywnie testy na obecność COVID-19[105]. Wytyczne dotyczące interoperacyjności dla zatwierdzonych aplikacji mobilnych do śledzenia kontaktów w UE określają ponadto, że ostrzeżenie i działania następcze powinny być zgodne z procedurami określonymi przez organy zdrowia publicznego, z oceną potencjalnego wpływu na prywatność i bezpieczeństwo oraz z zastosowaniem odpowiednich zabezpieczeń. Po wdrożeniu odpowiednich

[103] Zalecenie nr IOP-01.

[104] Zob. *eHealth Network Interoperability guidelines for approved contact tracing mobile applications in the EU*, https://ec.europa.eu/health/sites/health/files/ehealth/docs/contact-tracing_mobileapps_guidelines_en.pdf [dostęp: 20.09.2021].

[105] Zob. *eHealth Network Interoperability…*, s. 5.

rozwiązań technicznych aplikacje krajowe będą działać bezproblemowo, gdy użytkownicy będą podróżować do innego uczestniczącego państwa członkowskiego. Osoba podróżująca do innego kraju członkowskiego nie będzie zatem zmuszona do instalacji kolejnej aplikacji śledzącej kontakty zakaźne. Wytyczne dotyczące interoperacyjności aplikacji śledzących kontakty zakaźne mają charakter niewiążący, są one często w doktrynie określane mianem „prawa miękkiego".

Postanowienia dotyczące interoperacyjności znajdują się także w Regulaminie ProteGO Safe. Zgodnie z brzmieniem jego § 2 pkt 6 poprzez „Interoperacyjność lub Ostrzeganie w Europie" rozumie się funkcjonalność ProteGO Safe umożliwiającą wymianę kluczy pomiędzy użytkownikiem a użytkownikami innych aplikacji mobilnych, podobnych do ProteGO Safe, które są wspierane przez inne państwa członkowskie UE i współpracują w ramach bramy federacyjnej (o której za chwilę będzie mowa). Dzięki interoperacyjności użytkownicy mogą otrzymać informację o potencjalnym narażeniu na zakażenie w związku z potencjalnym kontaktem z użytkownikami innych aplikacji mobilnych, podobnych do ProteGO Safe. Z kolei § 3 pkt 7 Regulaminu ProteGO Safe stanowi, że Interoperacyjność (Ostrzeganie w Europie) ma charakter dobrowolny. Interoperacyjność (Ostrzeganie w Europie) jest świadczona za pośrednictwem bramy federacyjnej. W celu skutecznego korzystania z Interoperacyjności należy wyrazić odpowiednią zgodę w aplikacji. Zgoda wyrażona przez użytkownika dotyczy wysyłania i odbierania kluczy w stosunku do wszystkich aplikacji mobilnych, podobnych do ProteGO Safe. Zgodę można w każdej chwili wycofać, bez wpływu na wysłane i odebrane klucze, które zostały wysłane lub odebrane przed cofnięciem zgody. Po wyrażeniu zgody klucze wysyłane są do aplikacji podobnych do ProteGO Safe. Historia spotykanych urządzeń, na których jest zainstalowana aplikacja podobna do ProteGO Safe, będzie przechowywana w bramie federacyjnej przez 14 dni. Nie są oczywiście wymieniane dane identyfikujące użytkowników aplikacji czy dane dotyczące ich stanu zdrowia, nawet jeśli zostały przez użytkowników

wprowadzone do aplikacji. Tego rodzaju dane są przechowywane lokalnie, na urządzeniach końcowych użytkowników.

Komisja wspiera prace państw członkowskich nad rozszerzeniem interoperacyjności również na scentralizowane aplikacje do śledzenia. Aby wesprzeć dalsze usprawnianie systemu, Komisja stworzyła usługę bramy, czyli interfejs umożliwiający wydajne odbieranie i przekazywanie odpowiednich informacji między krajowymi aplikacjami do śledzenia kontaktów i serwerami[106].

W kwietniu 2020 r. KE ogłosiła zamówienie na utworzenie, utrzymanie i funkcjonowanie środowiska współpracy wspierającego ocenę techniczną technologii proponowanych do zwalczania COVID-19 pod względem ich skuteczności, bezpieczeństwa, prywatności, dostępności i interoperacyjności oraz dostosowania do zestawu narzędzi UE. W wyniku tego zamówienia w maju 2020 r. utworzono punkt przeglądu technicznego (reviewfacility.eu)[107].

Decyzja Wykonawcza Komisji (UE) 2020/1023 z dnia 15 lipca 2020 r. zmieniająca decyzję wykonawczą (UE) 2019/1765 w zakresie transgranicznej wymiany danych między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania w związku ze zwalczaniem pandemii COVID-19[108] wprowadziła do regulacji prawnych pojęcie bramy federacyjnej (*Federation Gateway*), czyli bramy sieciowej obsługiwanej przez Komisję za pomocą bezpiecznego narzędzia IT, która służy do odbierania, przechowywania i udostępniania minimalnego zbioru danych osobowych między serwerami wewnętrznymi państw członkowskich w celu zapewnienia interoperacyjności krajowych aplikacji mobilnych służących

[106] Zob. *Mobile applications to support contact tracing in the EU's fight against COVID-19. Progress reporting June 2020*.

[107] Zob. https://reviewfacility.eu/xwiki/bin/view/Utilities/ProjectFeatureMatrix/ [dostęp: 17.09.2021].

[108] Dz. Urz. UE L 227 I z 16.07.2020 r., s. 1.

do ustalania kontaktów zakaźnych i ostrzegania[109]. *European Proximity Tracing – An Interoperability Architecture for contact tracing and warning apps* z 2.09.2020 r.[110] to dokument, w którym zaproponowano gotową do wdrożenia architekturę usługi bramy federacyjnej. Przystąpienie państw członkowskich do usługi Europejskiej Bramy Federacyjnej wymagało odpowiedniego poziomu zaufania i zwrócenia dużej uwagi na bezpieczeństwo, integralność i autentyczność dalszej wymiany danych[111]. Usługa bramy federacyjnej jest najmniej złożonym i najbardziej niezawodnym sposobem połączenia zaplecza wszystkich różnych krajowych aplikacji do śledzenia zbliżeniowego kontaktów zakaźnych. Brama federacyjna akceptuje klucze diagnostyczne ze wszystkich krajów, buforuje je tymczasowo i udostępnia je do pobrania dla wszystkich krajów. Ponadto wszystkie *backendy* mogą być natychmiast informowane, jeśli dostępne są nowe dane, dzięki czemu opóźnienia transmisji są minimalne.

Na mocy powoływanej decyzji wykonawczej nr 2020/1023 Sieć e-Zdrowie zyskała także nowy obowiązek, a mianowicie zapewnienia państwom członkowskim wytycznych dotyczących transgranicznej wymiany danych osobowych za pośrednictwem bramy federacyjnej między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania[112]. Dodano przepisy dotyczące transgranicznej

[109] Zgodnie z § 2 pkt 2 Regulaminu ProteGO Safe v. 4.8. Brama federacyjna to brama sieciowa obsługiwana przez Komisję Europejską za pomocą bezpiecznego narzędzia IT, która służy do odbierania, przechowywania i udostępniania minimalnego zbioru danych osobowych między serwerami wewnętrznymi państw członkowskich UE w celu zapewnienia interoperacyjności krajowych aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania. Brama federacyjna umożliwia Interoperacyjność. Dzięki bramie federacyjnej możliwe jest wysyłanie oraz odbieranie kluczy pomiędzy użytkownikiem a użytkownikami innych aplikacji mobilnych, podobnych do ProteGO Safe. Klucze wysyłane są za pośrednictwem bramy federacyjnej, a okres przechowywania kluczy wynosi 14 dni.

[110] https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interop_architecture_en.pdf [dostęp: 19.09.2021].

[111] Zob. *European Interoperability Certificate Governance - A Security Architecture for contact tracing and warning apps* z 2.09.2020 r., https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interop_certificate_governance_en.pdf [dostęp: 19.09.2021].

[112] Zob. art. 4 ust. 1 lit. h.

wymiany danych między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania za pośrednictwem bramy federacyjnej (art. 7a). Jeżeli dane osobowe są wymieniane za pośrednictwem bramy federacyjnej, przetwarzanie ogranicza się do celów dotyczących ułatwienia interoperacyjności krajowych aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania w ramach bramy federacyjnej oraz zapewnienia ciągłości procesu ustalania kontaktów zakaźnych w kontekście transgranicznym. Dane osobowe, o których mowa, są przekazywane do bramy federacyjnej jako dane spseudonimizowane. Pseudonimiczne dane osobowe wymieniane oraz przetwarzane za pośrednictwem bramy federacyjnej obejmują jedynie następujące informacje: klucze przekazane przez krajowe aplikacje mobilne służące do ustalania kontaktów zakaźnych i ostrzegania w okresie do 14 dni poprzedzających datę przesłania kluczy; dane dziennika dotyczące kluczy zgodnie z protokołem specyfikacji technicznych stosowanym w państwie pochodzenia kluczy; weryfikację zakażenia; państwa będące przedmiotem zainteresowania oraz państwo pochodzenia kluczy[113].

Wyznaczone organy krajowe lub organy urzędowe przetwarzające dane osobowe za pośrednictwem bramy federacyjnej są współadministratorami danych przetwarzanych za pośrednictwem bramy federacyjnej. Podział odpowiednich obowiązków między współadministratorami przebiega zgodnie z załącznikiem II decyzji wykonawczej (UE) 2019/1765 (dodany na mocy decyzji wykonawczej nr 2020/1023). Każde państwo członkowskie, które chce uczestniczyć w transgranicznej wymianie danych między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania, przed przystąpieniem zawiadamia Komisję o swoim zamiarze i wskazuje organ krajowy lub organ urzędowy

[113] Dnia 14.09.2020 r. rozpoczęto testowanie infrastruktury bramy federacyjnej. Komisja rozpoczęła testy między serwerami zaplecza oficjalnych aplikacji z Czech, Danii, Niemiec, Irlandii, Włoch i Łotwy a nowo utworzonym serwerem bramy; zob. *Coronavirus: Commission starts testing interoperability gateway service for national contact tracing and warning apps*, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1606 [dostęp: 19.09.2021].

wyznaczony jako odpowiedzialny administrator. Komisja Europejska jest podmiotem przetwarzającym dane osobowe, które podlegają przetwarzaniu za pośrednictwem bramy federacyjnej. Do kompetencji Komisji jako podmiotu przetwarzającego należy zapewnienie bezpieczeństwa przetwarzania – w tym przesyłu i przechowywania – danych osobowych w ramach bramy federacyjnej oraz wypełnianie obowiązków podmiotu przetwarzającego określonych w załączniku III. Skuteczność środków technicznych i organizacyjnych mających na celu zapewnienie bezpieczeństwa przetwarzania danych osobowych za pośrednictwem bramy federacyjnej jest regularnie sprawdzana i oceniana przez Komisję oraz przez organy krajowe upoważnione do dostępu do bramy federacyjnej. Bez uszczerbku dla decyzji współadministratorów o zakończeniu przetwarzania za pośrednictwem bramy federacyjnej brama federacyjna ulega dezaktywacji najpóźniej 14 dni po zakończeniu przekazywania kluczy za jej pośrednictwem przez wszystkie połączone krajowe aplikacje mobilne służące do ustalania kontaktów zakaźnych i ostrzegania.

Nieco upraszczając, można podsumować, że interoperacyjność jest do pewnego stopnia czynnikiem zagrażającym bezpieczeństwu teleinformatycznemu, ponieważ automatyzuje wymianę informacji przez nowe, wspólne kanały dystrybucji o różnym stopniu ochrony[114]. Uznając jednakże prymat interoperacyjności, trzeba stwierdzić, że warunkiem budowy i wdrożenia systemów interoperacyjnych jest skuteczne zagwarantowanie wymaganych rygorów bezpieczeństwa informacji w nich przetwarzanych. Z tego powodu ramy interoperacyjności muszą uwzględniać względy bezpieczeństwa, a także ochronę danych osobowych i prywatności.

[114] Zob. B. Szafrański [*et al.*] (red.), *Interoperacyjność i bezpieczeństwo...*, s. 56.

5. Interoperacyjność aplikacji mobilnych śledzących kontakty zakaźne a prawo do ochrony danych osobowych i prawo do prywatności

Zdaniem Europejskiej Rady Ochrony Danych (dalej jako: EROD) umożliwienie udostępniania danych o osobach, które zostały zdiagnozowane lub pozytywnie przebadane („dane o infekcji") za pomocą interoperacyjnych aplikacji śledzących kontakty zakaźne, powinno być uruchamiane tylko przez dobrowolne działanie użytkownika i tak się właśnie dzieje. Osoby, których dane dotyczą, muszą mieć kontrolę nad swoimi danymi. Cel, jakim jest interoperacyjność, nie powinien być używany jako argument do rozszerzenia gromadzenia danych osobowych[115].

Zapewnienie interoperacyjności różnych wdrożeń jest technicznie trudne i może wymagać znacznych nakładów finansowych i inżynieryjnych. Aby zapewnić minimalną wymianę i przetwarzanie danych zgodnie z wymogami RODO, twórcy aplikacji do śledzenia kontaktów zakaźnych musieli uzgodnić wspólny protokół i kompatybilne struktury danych. Zatem w przypadku aplikacji, które już mają wspólne ramy lub przynajmniej tę samą podstawę technologiczną, cel interoperacyjności mógł być łatwiejszy do osiągnięcia niż w przypadku tych, które ich nie miały. W rzeczywistości, ze względu na różnice między podejściami, w praktyce może okazać się niemożliwe wdrożenie interoperacyjności bez nieproporcjonalnych kompromisów.

Interoperacyjność doprowadzi do dodatkowego przetwarzania i ujawnienia niektórych danych dodatkowym podmiotom. W tym miejscu opracowania należałoby odwołać się do polskiej aplikacji, a konkretnie do rodzaju danych, jakie ona przetwarza. Jak zawsze osoby, których dane dotyczą, muszą zostać poinformowane o każdym dodatkowym przetwarzaniu ich

[115] Zob. *Statement of EDPB on the data protection impact of the interoperability of contact tracing apps Adopted on 16 June 2020*, https://edpb.europa.eu/sites/default/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_en_0.pdf, s. 2 [dostęp: 10.05.2022].

danych osobowych oraz o stronach zaangażowanych w ich przetwarzanie[116]. Użytkownicy powinni zawsze dobrze rozumieć, na czym polega korzystanie z aplikacji i powinni zachować kontrolę nad swoimi danymi. Najpóźniej w momencie uzyskania danych osobowych przez administratora (administratorów) osoba, której dane dotyczą, musi otrzymać jasne informacje o dodatkowym przetwarzaniu związanym z wykorzystaniem interoperacyjności. W tym miejscu należy poinformować użytkownika o warunkach i zakresie przetwarzania danych. Nadal obowiązują standardowe zasady dotyczące przejrzystości; informacje powinny być podane jasnym i prostym językiem. Obejmuje to informacje o tym, jak udostępnione dane będą przetwarzane przez odbierającą interoperacyjną aplikację do śledzenia kontaktów.

Najważniejsze dla tematyki interoperacyjności w kontekście ochrony danych osobowych i prywatności jest Oświadczenie EROD w sprawie interoperacyjności aplikacji służących do ustalania kontaktów zakaźnych, przyjęte w dniu 16 czerwca 2020 r. Poniżej pokrótce zostaną przedstawione jego postanowienia.

Nadal mają zastosowanie te same podstawy prawne, o których mowa w wytycznych EROD nr 04/2020. W przypadku wyrażenia zgody konieczne będzie zebranie dodatkowej zgody na przetwarzanie interoperacyjne spełniające wszystkie jego wymagania. W szczególności cel przetwarzania musi być konkretny, a zatem wystarczająco szczegółowy. Jeżeli różni administratorzy danych w aplikacjach służących do śledzenia kontaktów korzystają z różnych podstaw prawnych, mogą być wymagane dodatkowe środki w celu realizacji praw osoby, której dane dotyczą, związanych z podstawą prawną. W przypadku danych dotyczących

[116] Obowiązek informacyjny wynika z art. 13 RODO, w przypadku gdy administrator pozyskuje dane od osoby, której dane dotyczą, i z art. 14 RODO, jeśli pozyskał dane w sposób inny niż od osoby, której dane dotyczą; zob. szer. np. J. Łuczak, komentarz do art. 13, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie...*, s. 477 i n.; P. Litwiński, P. Barta, M. Kawecki, komentarz do art. 13, [w:] P. Litwiński (red.), *Rozporządzenie UE...*, s. 361 i n.

zdrowia stosuje się art. 9 RODO, więc administratorzy będą musieli polegać na jednym z wymienionych w tym przepisie wyjątków dopuszczających przetwarzanie szczególnych kategorii danych osobowych.

W opinii EROD każda operacja lub zestaw operacji, których celem jest zapewnienie interoperacyjności oprócz przetwarzania pod kątem funkcjonalności aplikacji na poziomie państwa członkowskiego, musi być oceniana oddzielnie od wcześniejszych lub późniejszych operacji przetwarzania ze względu na dodatkowy cel przetwarzania danych. Dlatego dodatkowe przetwarzanie należy postrzegać jako oddzielne przetwarzanie. W przypadku tej oddzielnej operacji przetwarzania stronami mogą być indywidualni administratorzy lub współadministratorzy, którzy mogą korzystać z podmiotów przetwarzających. Jakiekolwiek dalsze przetwarzanie podejmowane po wymianie identyfikatorów (obliczanie ryzyka narażenia na zakażenie, powiadamianie o zidentyfikowanych kontaktach itp.) odbywałoby się w ramach odrębnego administrowania przez otrzymującego dostawcę aplikacji.

Konieczne będzie określenie odpowiednich ról, relacji i obowiązków współadministratorów w odniesieniu do osoby, której dane dotyczą, a następnie informacje te powinny zostać udostępnione osobie, której dane dotyczą. Będzie to miało wpływ na zakres oceny skutków dla ochrony danych, która musi być wykonywana, w tym przetwarzanie do celów interoperacyjności. Przetwarzanie w celu zapewnienia interoperacyjności może zostać powierzone podmiotowi przetwarzającemu, który spełnia warunki art. 28 RODO.

Każde rozwiązanie interoperacyjne musi ułatwiać osobom, których dane dotyczą, wykonywanie ich praw. Tam, gdzie wykonanie praw jest możliwe, nie powinno stać się bardziej uciążliwe dla osób, których dane dotyczą i powinno być jasne, do kogo osoby, których dane dotyczą, powinny się zwrócić, aby skorzystać ze swoich praw. Ograniczenia w wykonywaniu praw osoby, której dane dotyczą, są możliwe na podstawie wyjątków określonych w art. 119 i art. 23 RODO.

Interoperacyjność nie powinna prowadzić do zwiększonego gromadzenia informacji z powodu braku skoordynowanego podejścia. Należy to jasno przekazać użytkownikowi przed udostępnieniem danych. Interoperacyjność nie powinna prowadzić również do obniżenia bezpieczeństwa danych i ochrony danych osobowych.

EROD zaleca, aby dostawcy aplikacji służących do śledzenia kontaktów zakaźnych wzięli pod uwagę każdy wzrost zagrożeń bezpieczeństwa informacji spowodowany dodatkowym przetwarzaniem i zaangażowaniem dodatkowych podmiotów. Dotyczy to w szczególności bezpieczeństwa przesyłanych danych w celu ewentualnego połączenia między serwerami. W szczególności środki dotyczące zagrożeń bezpieczeństwa związanych z interoperacyjnością, które mają wpływ na prawa i wolności osób fizycznych, muszą zostać uwzględnione w ocenie skutków dla ochrony danych.

Kiedy dostawcy rozważają, w jaki sposób zapewnić interoperacyjność swoich aplikacji do śledzenia kontaktów, powinni w miarę możliwości zapewnić, że nie prowadzi to do obniżenia poziomu jakości lub dokładności danych. Interoperacyjność w przypadku dużych rozbieżności może prowadzić do utraty jakości danych (np. błędne wnioski z oceny ryzyka narażenia na zakażenie wirusem SARS-CoV-2 powodujące nieproporcjonalnie niskie przypisanie oceny ryzyka), co może prowadzić do wzrostu fałszywie pozytywnych wyników. Te dodatkowe zagrożenia dla dokładności danych będą musiały zostać jasno przekazane osobom, których dane dotyczą. Środki wprowadzone w celu zapewnienia dokładności danych muszą zostać utrzymane w systemie interoperacyjnym.

Stworzenie interoperacyjnej sieci aplikacji nie jest trywialne. Chociaż może to zwiększyć ich skuteczność, może również wymagać poważnych zmian w aplikacjach już istniejących lub opracowywanych. Z punktu widzenia ochrony danych interoperacyjność jest możliwa, jeśli przestrzegane są zalecenia zawarte w Wytycznych EROD nr 04/2020. Przekazywanie informacji i kontroli osobom, których dane dotyczą, zwiększy ich zaufanie do rozwiązań i ich potencjalnego wykorzystania.

6. Wnioski

Przetwarzanie danych dotyczących zdrowia jest co do zasady zabronione, z wyjątkami wynikającymi z art. 9 RODO. Jednym z nich jest niezbędność przetwarzania takich danych ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, 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, przewidujących odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową[117]. Aplikacje śledzące kontakty zakaźne, spełniające warunki określone w licznych unijnych aktach prawnych, wytycznych i zaleceniach im poświęconych, nie zostały przewidziane jako instrumenty obowiązkowe dla społeczeństwa; ich używanie opiera się na zasadzie dobrowolności. Ponadto nie wymieniają one z serwerami centralnymi, w tym obsługującymi wymianę danych ponad granicami państw, danych osobowych umożliwiających identyfikację użytkowników i w ogóle nie gromadzą danych o ich lokalizacji – co zapewnia wysoki stopień ochrony danych osobowych i prywatności, a w konsekwencji zmierzać ma do wysokiego zaufania społecznego do tego narzędzia. Wiele danych osobowych, w tym danych dotyczących zdrowia użytkowników aplikacji mobilnych śledzących kontakty zakaźne, przechowywanych jest lokalnie, na urządzeniach końcowych tychże użytkowników, do których dostawca aplikacji mógłby mieć dostęp jedynie pod warunkami określonymi w dyrektywie 2002/58, do czego obecnie nie ma podstaw prawnych w prawie krajowym.

Wobec faktu, że wirus SARS-CoV-2 nadal się rozprzestrzenia, być może należy rozważyć dwie podstawowe kwestie dotyczące tzw. krajowych

[117] Zob. art. 9 ust. 2 lit. i RODO.

aplikacji mobilnych śledzących kontakty zakaźne. Po pierwsze – czy celowe byłoby identyfikowanie przez organy ds. ochrony zdrowia osób, które poprzez taką aplikację zostały powiadomione o tym, że miały styczność z osobą zakażoną wirusem SARS-CoV-2 w celu skierowania ich na kwarantannę? Przy pozytywnej ocenie takiego rozwiązania należałoby liczyć się z jeszcze bardziej poważnym spadkiem akceptacji społecznej dla używania aplikacji śledzącej kontakty zakaźne (przy założeniu, że nadal jej używanie będzie dobrowolne). Po drugie, czy administrator danych osobowych przetwarzanych przez aplikację mobilną nie powinien móc w sposób zgodny z prawem (a więc wymagana byłaby zmiana prawa w tym zakresie) wykorzystać tych danych do celów nadzoru epidemiologicznego, łącznie z ich ujawnieniem w odpowiednich systemach informatycznych, którymi zarządza? Obecnie dane takie jak wiek użytkownika aplikacji (określony w przedziałach) czy choroby współistniejące, na które cierpi użytkownik, są przechowywane wyłącznie na urządzeniu użytkownika i organy ds. ochrony zdrowia nie mają do nich dostępu. Działanie związane z użyciem danych zebranych przez aplikację mobilną w innych systemach (tele)informatycznych także jest interoperacyjnością i należy je wiązać z koncepcją tzw. otwartego rządu. Otwarty rząd to nie tylko struktury zbudowane i działające w sposób transparentny, lecz dzielące się danymi z obywatelami i innymi strukturami państwa i samorządu. O interoperacyjności czy organach administracji publicznej opartych na danych należy bowiem mówić nie tylko w kontekście wymiany danych poza granicami kraju, ale także w sytuacjach wewnątrzkrajowych. Podjęcie decyzji w przedmiocie dysponowania danymi użytkowników aplikacji śledzących kontakty zakaźne wymagałoby przeprowadzenia oceny skutków dla ochrony danych i oceny skutków dla ochrony prywatności.

Podsumowując, należy stwierdzić, że dane użytkowników urządzeń wygenerowane przez aplikacje śledzące kontakty zakaźne, takie jak ilość kluczy diagnostycznych przesłanych na serwer centralny i daty ich wysłania, stanowią informacje sektora publicznego, ponieważ zostały zebrane

podczas wykonywania zadania publicznego związanego z ochroną zdrowia publicznego i znajdują się w dyspozycji podmiotu zobowiązanego do udostępniania lub przekazywania informacji sektora publicznego w celu ponownego wykorzystywania, zgodnie z art. 3 u.o.d.p.w.i. Powinny one podlegać ponownemu użyciu, zwłaszcza w celu koordynacji systemu ochrony zdrowia, łącznie z ich ujawnieniem w odpowiednich systemach informatycznych, którymi zarządza GIS. Warto także rozważyć identyfikację osób, które miały kontakt z osobą zakażoną wirusem SARS-CoV-2 i korzystają z aplikacji mobilnych śledzących kontakty zakaźne. Dane pozwalające ustalić tożsamość osób „z kontaktu" powinny być znane jedynie upoważnionym pracownikom organów ds. ochrony zdrowia, w celu podjęcia wobec tychże osób określonych czynności związanych z przerwaniem transmisji wirusa SARS-CoV-2. Działający przy ministrze ds. zdrowia krajowy punkt kontaktowy wspólnotowego systemu wczesnego ostrzegania i reagowania dla zapobiegania i kontroli zakażeń oraz chorób zakaźnych, do którego zadań należy wymiana informacji oraz koordynacja działań w zakresie zapobiegania oraz zwalczania zakażeń i chorób zakaźnych z państwami członkowskimi Unii Europejskiej, Komisją Europejską oraz Europejskim Centrum do Spraw Zapobiegania i Kontroli Chorób, także powinien mieć, w sytuacjach przewidzianych ustawą z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi[118], dostęp do danych zgromadzonych przez aplikację śledzącą kontakty zakaźne (lub też wymieniać te dane). W przypadku wystąpienia choroby zakaźnej, której zwalczanie wymaga podjęcia skoordynowanego działania wspólnotowego, krajowy punkt kontaktowy wspólnotowego systemu wczesnego ostrzegania i reagowania przekazuje Europejskiemu Centrum do Spraw Zapobiegania i Kontroli Chorób lub punktom kontaktowym państw członkowskich Unii Europejskiej dane osoby podejrzanej o zakażenie lub zachorowanie, zakażonej lub chorej na chorobę zakaźną, tylko w przypadku gdy jest to

[118] T.j. Dz. U. z 2021 r. poz. 2069.

niezbędne do podjęcia przez te podmioty działań służących zapobieganiu i kontroli chorób zakaźnych i wyłącznie w zakresie niezbędnym do zapewnienia skuteczności tych działań.

Zgłosić należy także postulat szerszej dostępności, zwłaszcza w trybie bezwnioskowym, informacji sektora publicznego związanych z używaniem aplikacji mobilnych śledzących kontakty zakaźne, jak np. liczba jej pobrań ze sklepów internetowych, liczba użytkowników, którzy wyrazili zgodę na śledzenie kontaktów zakaźnych, liczba osób, które odwołały zgodę na śledzenie kontaktów zakaźnych, liczba kluczy diagnostycznych przesłanych na serwer centralny i daty ich wysłania. Kod źródłowy polskiej aplikacji, oparty na oprogramowaniu *open source*, został upubliczniony i może być poddany jak najszerszym badaniom przez osoby, które posiadają odpowiednią wiedzę. Natomiast każdy jest w stanie dokonać samodzielnej analizy danych ilościowych, o których mowa.

Biorąc pod uwagę interes publiczny, może zaistnieć potrzeba dostosowania prawa krajowego, aby przewidywać udostępnianie danych stanowiących informację sektora publicznego innym usługom. Nie należy jednak zapominać, że w przypadku każdego wprowadzanego środka zwiększającego bezpieczeństwo w zakresie zdrowia publicznego należy ocenić, czy mniej inwazyjna alternatywa może osiągnąć ten sam cel oraz zapewnić, że każdy zastosowany środek jest zgodny z prawem, skuteczny i proporcjonalny. Zasada ograniczenia celu wymaga, aby cele przetwarzania danych zostały wystarczająco uszczegółowione, aby wykluczyć dalsze przetwarzanie do celów niezwiązanych z zarządzaniem kryzysem zdrowotnym COVID-19.

Bibliografia

Banasikowska J., Sołtysik-Piorunkiewicz A., *Zasady interoperacyjności i standaryzacji w systemach wszechobecnych e-Government krajów Unii Europejskiej*, „Roczniki Kolegium Analiz Ekonomicznych" 2013, nr 29.

Bielak-Jomaa E., Lubasz D. (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.

Dunaj B. (red.), *Słownik współczesnego języka polskiego*, Warszawa 1996.

Kubalski G., Małowiecka M., *Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz*, Warszawa 2019.

Kulisiewicz T., *Redukcja pozaprawnych barier ponownego wykorzystywania informacji sektora publicznego*, [w:] A. Piskorz-Ryń, *Jawność i jej ograniczenia*, t. V. *Dostęp i wykorzystywanie*, Warszawa 2015.

Litwiński P. (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018.

Litwiński P., Leńczuk A., Krzyżak A., Siwek A., *Raport z audytu prywatności aplikacji ProteGO Safe przeprowadzonego na zlecenie Ministerstwa Cyfryzacji przez Barta, Litwiński Kancelaria Radców Prawnych i Adwokatów Spółka Partnerska w dniu 5.08.2020 r.*, https://www.gov.pl/web/protegosafe/dokumenty.

Maciejasz D., *Polacy nie zaufali rządowej aplikacji do walki z pandemią. A ci, którzy ją mają, nie raportują zakażeń*, „Gazeta Wyborcza" 2.09.2020.

de Montjoye Y.-A., Hidalgo C.A., Verleysen M., Blonde V.D., *Unique in the Crowd: The privacy bounds of human mobility*, DOI: 10.1038/srep01376, https://web.media.mit.edu/~yva/papers/deMontjoye2013unique.pdf.

Pyrgelis A., Troncoso C., De Cristofaro E., *Knock Knock, Who's There? Membership Inference on Aggregate Location Data*, https://arxiv.org/pdf/1708.06145.pdf.

Słownik języka *polskiego PWN*, https://sjp.pwn.pl/sjp.

Sybilski D., *Dane o wysokiej wartości – nowy rodzaj informacji sektora publicznego*, „Informacja w Administracji Publicznej" 2019, Nr 4.

Szafrański B., Bliźniuk G., Karnowski J., Świerczyński Z., Weydmann R., Żurek L. (red.), *Interoperacyjność i bezpieczeństwo systemów informatycznych administracji publicznej*, Katowice 2006.

Weiser M., *The Computer for the 21st Century*, https://web.archive.org/web/20141022035044/http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html.

Weyrich, C., *Orientations for WP2000 and beyond*, "ISTAG" 1999.

Wiewiórowski W.R., *Rola Unii Europejskiej w koordynacji zastosowania narzędzi informatycznych do walki z pandemią*, „Europejski Przegląd Sądowy" 2020, nr 6.

Zieliński A. (red.), *Słowniczek terminów epidemiologicznych*, „Przegląd Epidemiologiczny", http://www.przeglepidemiol.pzh.gov.pl/slowniczek-terminow-epidemiologicznych.