Ekonomia — Wroclaw Economic Review 27/3 (2021)
Acta Universitatis Wratislaviensis
No 4081

https://doi.org/10.19195/2658-1310.27.3.5

Adrianna Szalonka
ORCID: 0000-0002-0329-0926
Uniwersytet Wrocławski
Uniwersytet Medyczny we Wrocławiu
ada.szalonka@interia.pl

Funkcjonowanie aplikacji mobilnych pomocnych w walce z pandemią COVID-19 w świetle wybranych norm prawnych

Artykuł nadesłany: 10.10.2021; **artykuł zaakceptowany:** 24.10.2021

Kody klasyfikacji JEL: I10, I18

Keywords: mobile applications, personal data protection

Abstract

Functioning of mobile applications helping in the fight against the COVID-19 pandemic in the light of selected legal standards

The purpose of this article is to review the legal sources that underpin the implementation of mobile health applications in an ongoing global pandemic. The study formulates a research hypothesis — legal sources guarantee the security of personal data protection in the functioning and use of the application. On the basis of the conducted review, it can be concluded that the sources of EU and Polish law guarantee the security and protection of data for obligatory and non-obligatory users. The collected data may not be processed for commercial purposes and should not be processed for the surveillance of citizens.

Abstrakt

Celem niniejszego artykułu jest dokonanie przeglądu źródeł prawnych, które stanowią podstawę do wdrożenia zdrowotnych aplikacji mobilnych podczas trwającej na świecie pandemii. W pracy sformułowano hipotezę badawczą — normy prawne gwarantują bezpieczeństwo ochrony danych osobowych w funkcjonowaniu i korzystaniu z aplikacji. Na podstawie dokonanego przeglądu można stwierdzić, że normy prawa unijnego oraz polskiego gwarantują bezpieczeństwo i ochronę danych

korzystających obligatoryjnie i nieobligatoryjnie. Gromadzone dane nie mogą być przetwarzane w celach komercyjnych i nie powinny być przetwarzane do nadzoru obywateli.

Słowa kluczowe: aplikacje mobilne, ochrona danych osobowych

Wstęp

Wraz z rosnącą liczbą zakażeń, aby usprawnić walkę z pandemią wywołaną wirusem SARS-Cov-2, Komisja Europejska podjęła intensywne działania i wydała wiele zaleceń dotyczących wykorzystywania nowoczesnych technologii, celem zapobiegania rozprzestrzeniania się wirusa.

Dynamicznie rozwijający się rynek nowych technologii pozwala na wdrażanie nowoczesnych rozwiązań. Wykorzystanie internetu ułatwia komunikację oraz umożliwia wdrożenie aplikacji. Proces powszechnego wykorzystania technologii informacyjnych doprowadził do powstania społeczeństwa informacyjnego, które jest przygotowane do wytwarzania i odbioru informacji, potrafi je przechowywać i selekcjonować, a także wykorzystuje informacje z różnych źródeł we wszystkich aspektach życia indywidualnego i zbiorowego (Goban-Klas, Sienkiewicz, 1999; Goban-Klas, 2014). Celem niniejszego artykułu jest dokonanie przeglądu źródeł prawnych, które tworzą podstawę wdrożenia aplikacji mobilnych w trakcie trwającej na świecie pandemii. W pracy sformułowano hipotezę badawczą — normy prawne gwarantują bezpieczeństwo ochrony danych osobowych w funkcjonowaniu i korzystaniu z aplikacji.

Aplikacja mobilna a pandemia COVID-19

Niespodziewane odkrycie pod koniec 2019 roku wirusa SARS-Cov-2 oraz uznanie 11 marca 2020 roku choroby COVID-19 za pandemię zapoczątkowało wiele działań ze strony władz państwa, mających ograniczyć rozprzestrzenianie się choroby w wyniku izolowania chorych i tym samym zapobiegać emisji wirusa. Do takiego działania zastosowano internet i komunikację sieciową. Proces wprowadzania nowoczesnych metod przetwarzania danych za pomocą komputerów oraz ich stosowanie w większości obszarów ludzkiego działania nazwany jest procesem komputeryzacji (Kotecka-Kral, 2021). Następstwem komputeryzacji były różnego rodzaju aplikacje mobilne możliwe do uruchomienia w urządzeniach mobilnych — komórkach, tabletach i komputerach z dostępem do sieci internetowej.

Definicja aplikacji mobilnej

Zgodnie z ustawą z dnia 4 kwietnia 2019 roku o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (art. 4) aplikacja mobilna

to publicznie dostępne oprogramowanie z interfejsem dotykowym zaprojektowane do wykorzystania na przenośnych urządzeniach elektronicznych, z wyłączeniem aplikacji przeznaczonych do użytku na przenośnych komputerach osobistych, potocznie zwanych laptopami. Aplikacje mobilne są dobrem komplementarnym w zakresie usług komunikacyjnych. Oznacza to, że mogą działać, tylko gdy jest przenośne urządzenie elektroniczne wyposażone w łącze z internetem. Pierwszy smartfon zaprezentowany został przez firmę Apple w 2008 roku (Olesch, 2019). Umożliwiał korzystanie z około 500 aplikacji w różnych obszarach życia gospodarczego i społecznego. Podaje się, że w 2019 roku było już ponad 2 mln aplikacji zarówno w systemie Ios, jak i w systemie Android. Smartfon wraz aplikacjami stał się narzędziem codziennego użytku. Jedną z branż wykorzystujących to narzędzie jest ochrona zdrowia. W raporcie OSOZ *Aplikacje mobilne* znajduje się informacja, że w 2019 roku było już 318 tys. aplikacji zdrowotnych (Olesch, 2019).

Funkcjonalność aplikacji mobilnych

Aplikacje zdrowotne można sklasyfikować z zastosowaniem kryterium podmiotowego: dla personelu medycznego, pacjentów i jednostek systemu ochrony zdrowia. Aplikacje opracowane dla personelu medycznego między innymi:

— umożliwiają wypełnianie dokumentów medycznych,
— ułatwiają prowadzenie dokumentacji medycznej,
— koordynują i organizują stanowisko pracy.
— udostępniają informacje medyczne (Olesch, 2019).

Wszystkie aplikacje związane z prowadzeniem dokumentów pacjentów łączą się z koniecznością ochrony wrażliwych danych osobowych. Aplikacje przeznaczone dla pacjentów mają funkcje związane z ochroną zdrowia, na przykład:

— motywujące do aktywności fizycznej,
— ułatwiające kontrolę struktury produktów w procesie zakupu,
— wspomagające proces komunikacji z lekarzem prowadzącym (konsultacje na odległość),
— monitorujące parametry zdrowotne u pacjentów z chorobami przewlekłymi,
— przypominające o zażywaniu leków,
— ułatwiające zakup leków,
— ułatwiające zrozumienie sytuacji zdrowotnej społeczności.

Wśród aplikacji skierowanych do podmiotów medycznych należy wyróżnić te, które:

— wspierają organizację usług medycznych (rejestracja pacjentów, przypomnienie o wizytach, konsultacje online itp.),
— zapewniają dostęp do historii leczenia pacjentów,
— zapewniają migrację wyników badań pacjentów z wielu podmiotów medycznych do karty pacjenta (Olesch, 2019).

Ponadto można wyróżnić aplikacje zdrowotne wprowadzone przez administrację publiczną do monitorowania stanu zdrowia społeczeństwa w trakcie pandemii. Taką aplikacją jest Kwarantanna domowa. W czasie pandemii służyła do monitorowania i usprawniania kontroli obowiązkowej kwarantanny ludności zamieszkałej na terenie Polski. Program umożliwiał identyfikację miejsca pobytu podczas kwarantanny, a także podstawową ocenę stanu zdrowia. Ułatwiał modyfikację podstawowych danych osoby przebywającej na kwarantannie. Izolowanemu i monitorowanemu pacjentowi aplikacja umożliwiała kontakt z pracownikiem inspektoratu sanitarnego i psychologiem. Dla przykładu można wymienić zakres danych osobowych przetwarzanych w ramach realizacji usług dostępnych w aplikacji dotyczących osób objętych kwarantanną (https://www.gov.pl/web/koronawirus/kwarantanna-domowa-regulamin):

— ID obywatela, imię,
— nazwisko,
— numer telefonu,
— deklarowany adres pobytu,
— zdjęcie,
— lokalizacja obywatela (w tym deklarowana lokalizacja odbywania kwarantanny oraz lokalizacja wyznaczona przez system w czasie wykonywania zadania weryfikacji),
— data ukończenia odbywania kwarantanny (Dz.U. z 2000 r. poz. 1842, z późn. zm.).

Uwarunkowania prawne stosowania aplikacji mobilnych

Wszystkie aplikacje generują dane w cyberprzestrzeni, które są niezwykle cennym towarem w XXI wieku. Cyberprzestrzeń można zdefiniować jako przestrzeń, w której połączone urządzenia są w stanie przesyłać dane, informacje. Przesyłanie, przetwarzanie i gromadzenie informacji powinno gwarantować bezpieczeństwo i ochronę każdego użytkownika wirtualnej sieci.

Ochrona danych osobowych

Zgodnie z art. 288 Traktatu o funkcjonowaniu Unii Europejskiej rozporządzenie o ochronie danych osobowych jest aktem prawnym o najszerszym zasięgu, wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich UE. Zawiera przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych. Celem wprowadzenia wskazanego aktu prawnego było ujednolicenie prawa materialnego

w ramach UE i swobodnego przepływu tych danych (GIODO, Generalny Inspektor Ochrony Danych Osobowych). Rozporządzenie zostało przyjęte 27 kwietnia 2016 roku i weszło w życie po dwuletnim okresie przejściowym, bez potrzeby wydawania aktów prawnych wdrażających je do porządku krajowego (rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku). Urząd Generalnego Inspektora Ochrony Danych Osobowych zastąpiono Prezesem Urzędu Ochrony Danych Osobowych (Projekt ustawy o ochronie danych osobowych; ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych). Zgodnie z art. 99 ust. 2 RODO rozporządzenie to obowiązuje od dnia 25 maja 2018 roku.

Wprowadzenie nowych regulacji prawnych umożliwiło:

— dostęp do informacji: łatwiejszy dostęp do danych, w taki sposób, aby informacje były przejrzyste,

— usprawnienie przesyłania danych między dostawcami usług,

— usunięcie danych, czyli tak zwane prawo do bycia zapomnianym,

— informację bez zbędnej zwłoki w razie ataku hakerskiego na dane,

— proces pseudonimizacji, czyli ograniczenie możliwości identyfikacji konkretnej osoby,

— sprostowania danych,

— ograniczenie przetwarzania,

— przenoszenie danych,

— sprzeciw,

— wniesienie skargi do organu nadzorczego: każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego,

— skutecznego środka ochrony prawnej przed sądem przeciwko organowi nadzorczemu,

— skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu,

— odszkodowania i odpowiedzialność: każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę (Dz.U. z 2020 r. poz. 1842, z późn. zm.).

Zgoda na przetwarzanie danych osobowych

Każdy użytkownik aplikacji zdrowotnych musi wyrazić zgodę na przetwarzanie danych osobowych. Zgoda musi być:

— dobrowolna,

— konkretna,

— świadoma,

— udzielona na konkretne użycie danych (Dz.U. z 2020 r. poz. 1842, z późn. zm.).

Osoba, która udziela zgody, ma prawo do jej wycofania.

Ustawodawca zdefiniował także warunki uzyskania zgody na przetwarzanie danych osobowych. Zarządzający aplikacją zdrowotną (podmiot wykorzystujący aplikację zdrowotną, na przykład Ministerstwo Zdrowia, Główny Inspektorat Sanitarny, wojewódzka stacja sanitarno-epidemiologiczna) musi określić: tożsamość administratora/kontrolera danych,

— cele każdej operacji przetwarzania, typy pozyskiwanych i używanych danych, możliwość wycofania zgody oraz poinformować o ewentualnie podejmowanych automatycznie decyzjach, a także o ewentualnym przesyłaniu danych do krajów trzecich (Dz.U. z 2020 poz. 1842, z późn. zm.).

Wniesienie sprzeciwu

Wniesienie sprzeciwu, o którym mowa w § 7 ust. 1 pkt 3 dokumentu Polityka prywatności aplikacji Kwarantanna domowa, nie powoduje automatycznego zaprzestania przetwarzania danych osobowych użytkownika. Administrator może odmówić zaprzestania przetwarzania danych użytkownika ze względu na ważny interes publiczny, czyli obowiązek monitorowania odbywania przez użytkownika kwarantanny związany z przeciwdziałaniem sytuacji kryzysowej związanej z rozprzestrzenianiem się wirusa SARS-CoV-2 (www.gov.pl/web/koronawirus/polityka-prywatności-aplikacji-mobilnych).

Obowiązek korzystania z aplikacji

Zgodnie z art. 7e ust. 1 ustawy z dnia 2 marca 2020 roku o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, od 1 kwietnia 2021 roku aplikacja Kwarantanna domowa jest obowiązkowa.

Istnieją dwa wyłączenia osób, które nie podlegają obowiązkowi korzystania z aplikacji Kwarantanna domowa. Są to osoby z dysfunkcją wzroku oraz osoby, które złożyły oświadczenie, że nie są abonentami lub użytkownikami sieci telekomunikacyjnej lub nie mają urządzenia mobilnego umożliwiającego zainstalowanie tego oprogramowania.

Komisja Europejska opublikowała dokumenty, które umożliwią bezpieczne i efektywne wykorzystywanie nowoczesnej technologii między innymi do stopniowego znoszenia obostrzeń i izolacji osób zakażonych koronawirusem. Jednym z nich jest komunikat (2020/C 124 I/01) w sprawie ochrony danych osobowych dla aplikacji mobilnych, które wspierają walkę z koronawirusem. KE wraz z Europejską Radą Ochrony Danych opracowała wytyczne, które mają zagwarantować bezpieczeństwo i ochronę prywatności użytkowników.

Komisja Europejska 8 kwietnia opublikowała zalecenie i rekomendacje odnoszące się do opracowania unijnego podejścia do wykorzystania technologii i danych w celu zwalczania kryzysu wywołanego przez COVID-19; 16 kwietnia zaś opublikowała unijny zestaw instrumentów ułatwiających stosowanie aplikacji mobilnych do ustalania kontaktów zakaźnych i generowania ostrzeżeń, a także wytyczne w sprawie ochrony danych osobowych i prywatności dla aplikacji wspierających walkę z pandemią COVID-19.

Zaletą aplikacji jest znacznie większa efektywność w ustalaniu kontaktów zakaźnych w porównaniu z tradycyjnym systemem opartym na przeprowadzeniu wywiadu z osobą zakażoną. Aplikacje muszą być jednak zgodne z ogólnym rozporządzeniem o ochronie danych (RODO) i dyrektywą o prywatności i łączności elektronicznej. Ma to zagwarantować wiarygodność i prawidłowe działanie aplikacji w całej UE. Skuteczność działania aplikacji w dużym stopniu będzie opierała się na zaufaniu społeczeństwa. Jeśli użytkownicy będą pewni, że aplikacja jest bezpieczna, będą z niej korzystać masowo. KE podkreśla, że zapewnienie ochrony danych osobowych i ograniczenie ryzyka inwigilacji przy korzystaniu z aplikacji mobilnych związanych z COVID-19 jest priorytetem.

Unijny zestaw instrumentów ułatwiających stosowanie aplikacji mobilnych do ustalania kontaktów zakaźnych i generowania ostrzeżeń został opracowany przez sieć E-zdrowie. Toolbox określa następujące wymagania dotyczące aplikacji do ustalania kontaktów zakaźnych i aplikacji ostrzegających o zagrożeniu epidemiologicznym:

— bezpieczne i zgodne z unijnymi przepisami dotyczącymi ochrony danych i prywatności,

— zatwierdzone i wprowadzone do użytku za zgodą organów do spraw zdrowia publicznego,

— instalowane dobrowolnie,

— wykorzystujące funkcję Bluetooth do wykrywania innych urządzeń i użytkowników, a nie funkcję śledzenia lokalizacji,

— ostrzegające o zagrożeniu w sposób zanonimizowany, na przykład przez komunikat sugerujący wykonanie testu na obecność SARS-Cov-2 z powodu przebywania w bliskiej odległości z osobą zakażoną, bez ujawniania jej tożsamości,

— interoperacyjne i współpracujące z innymi aplikacjami tego typu, które działają w UE,

— dezaktywowane, gdy zostanie ogłoszone opanowanie pandemii COVID-19.

W komunikacie (2020/C124I/01) opublikowano wytyczne w sprawie ochrony danych osobowych dla aplikacji mobilnych wspierających walkę z koronawirusem z 17 kwietnia 2020 roku (Wytyczne dotyczące aplikacji pomocnych w walce z pandemią COVID-19 w odniesieniu do ochrony danych (2020/C 124 I/01)). Wytyczne uwzględniają doświadczenia Europejskiej Rady Ochrony Danych (art. 68) i odnoszą się do wszystkich dobrowolnie pobranych, zainstalowanych i wykorzystywanych aplikacji, które:

— dostarczają rzetelnych informacji o pandemii COVID-19,

— umożliwiają weryfikację objawów za pomocą kwestionariusza do samodzielnej diagnozy,

— ostrzegają o osobach zakażonych, miejscach i obszarach, na których występuje zwiększone zagrożenie epidemiologiczne, a także informują o konieczności poddania się samoizolacji lub przeprowadzeniu testu na obecność SARS-Cov-2,

— służą do utrzymywania kontaktu z lekarzem (telemedycyna).

Komisja Europejska określa zasady, których przestrzeganie jest niezbędne do prawidłowego korzystania z aplikacji mobilnych w świetle obowiązujących przepisów:

1) wbudowanie zabezpieczeń zapewniających poszanowanie praw podstawowych i zapobieganie stygmatyzacji,

2) preferowanie najmniej inwazyjnych środków, a także wykorzystywanie w miarę możliwości zanonimizowanych i zagregowanych danych,

3) istnienie wymogów technicznych dotyczących odpowiednich technologii (np. Bluetooth o niskim zużyciu energii) służących ustaleniu bliskości urządzenia, szyfrowania, ochrony danych, przechowywania danych na urządzeniu przenośnym, możliwego dostępu organów ds. zdrowia oraz przechowywania danych,

4) istnienie skutecznych wymogów w zakresie cyberbezpieczeństwa w celu ochrony dostępności, autentyczności, integralności i poufności danych,

5) wygaśnięcie zastosowanych środków i usunięcie danych osobowych uzyskanych za pomocą tych środków najpóźniej w momencie, w którym ogłoszone zostanie opanowanie pandemii,

6) wysyłanie danych dotyczących bliskości fizycznej w przypadku potwierdzonego zakażenia i stosowanie odpowiednich metod ostrzegania osób, które pozostawały w bliskim kontakcie z osobą zakażoną — która pozostaje anonimowa,

7) istnienie wymogów przejrzystości dotyczących ustawień prywatności w celu zapewnienia zaufania do aplikacji (Zalecenie komisji (UE) 2020/518 z dnia 8 kwietnia 2020 r.).

Kary za nieprzestrzeganie obowiązku korzystania z aplikacji mobilnych

Osoby, które wbrew ciążącemu na nich prawnemu obowiązkowi nie zainstalują lub nie będą używać aplikacji Kwarantanna domowa, mogą zostać ukarane karą grzywny lub nagany. Podstawa prawna: art. 116 § 1 ustawy z dnia 20 maja 1971 roku Kodeks wykroczeń (Dz.U. z 2019 r. poz. 821, z późn. zm.). Korzystanie z aplikacji nie zwalnia z przestrzegania obowiązków nałożonych przepisami na osoby poddane kwarantannie. W szczególności nieopuszczania miejsca odbywania kwarantanny oraz stosowania się do poleceń służb ustawowo powołanych do niesienia pomocy.

Zakończenie

Zdrowotne aplikacje mobilne służyły w czasie pandemii COVID-19 działaniom prewencyjnym, zapobiegającym rozprzestrzenianiu się wirusa. Generowały pod-

stawowe dane osobowe wraz z adresem zamieszkania, stanem zdrowia i numerem telefonu. Liczne normy prawne gwarantują wolność obywatelską i ochronę danych osobowych, korzystających obligatoryjnie i nieobligatoryjnie ze zdrowotnych aplikacji mobilnych. KE wskazuje, że poszanowanie praw podstawowych powinno uwzględniać ograniczone przetwarzanie danych osobowych. Powinno służyć jedynie do walki z koronawirusem, tak aby wykluczyć wykorzystywanie danych do innych celów. Nie powinny być wykorzystywane do celów komercyjnych lub nadzoru obywateli.

Bibliografia

Europejska Rada Ochrony Danych. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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) (RODO). Stan prawny na dzień 3 października 2021 r. Data dostępu: 30.07.2021, https://www.uodo.gov.pl/pl/131/224.

Goban-Klas, T. (red.). (2014). *Komunikowanie w ochronie zdrowia — interpersonalne, organizacyjne i medialne*. Warszawa: ABC a Wolters Kluwer business.

Goban-Klas, T., Sienkiewicz, P. (1999). *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*. Kraków: Fundacja Postępu Telekomunikacji.

Kotecka-Kral, S. (2021). Informatyzacja usług publicznych: założenia konstrukcyjne. W K. Flaga-Gieruszyńska, J. Gołaczyński (red.), *Prawo nowych technologii*, Warszawa: Wolters Kluwer, 13–51.

Ustawa z dnia 20 maja 1971 roku — Kodeks wykroczeń, Dz.U. z 2019 r. poz. 821, z późn. zm. Data dostępu 30.07.2021, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190000821.

Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych. Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 30 sierpnia 2019 roku w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie danych osobowych. Data dostępu: 30.07.2021, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190001781.

Ustawa z dnia 4 kwietnia 2019 roku o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, Dz.U. 2019 poz. 848. Data dostępu: 30.07.2021, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20190000848.

Ustawa z dnia 2 marca 2020 roku o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, Dz.U. z 2020 poz. 1842, z późn. zm., art. 7e ust. 1 w zw. z art. 6 lit. e i 9 ust. 2 lit. i RODO. Data dostępu: 2.10.2021, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20200000374/U/D20200374Lj.pdf.

Źródła internetowe

GIODO Generalny Inspektor Ochrony Danych Osobowych. Prawo. Reforma unijnych przepisów. Data dostępu: 2.10.2021, https://archiwum.giodo.gov.pl/1520143/j/pl. Data dostępu: 2.10.2021, https://techinfo.uodo.gov.pl/definicje-rodo/.

https://cyberpolicy.nask.pl/wykorzystanie-aplikacji-mobilnych-i-danych-o-lokalizacji-do-walki-z--covid-19/.

https://eurlex.europa.eu/legalcontent/PL/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN.

https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20200000374/U/D20200374Lj.pdf.

https://www.dzp.pl/files/shares/Publikacje/Prawo_Automatyka_9_2020_v2.pdf.

https://www.gov.pl/web/koronawirus/kwarantanna-domowa.
https://www.gov.pl/web/koronawirus/protegosafe.
Komunikat Komisji. Wytyczne dotyczące aplikacji pomocnych w walce z pandemią COVID-19 w odniesieniu do ochrony danych (2020/C 124 I/01). Data dostępu: 30.07.2021, https://eur-lex.europa.eu/legalcontent/PL/TXT/?uri=uriserv%3AOJ.CI.2020.124.01.0001.01.POL&toc=OJ%3AC%3A2020%3A124I%3AFULL.
Olesch. A. (2019). 241 aplikacji zdrowotnych. *Czasopismo OSOZ Polska*. 8, Data dostępu: 30.07.2021, ttps://osoz.pl/static_files/kom-linki/aplikacje_2019_03.pdf.
Projekt ustawy o ochronie danych osobowych. Data dostępu: 2.10.2021, https://legislacja.rcl.gov.pl/projekt/12302950.
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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). Data dostępu: 2.10.2021, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32016R0679:PL:NOT.
Wersja skonsolidowana Traktatu o funkcjonowaniu Unii Europejskiej. Data dostępu: 2.10.2021, https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=OJ%3AC%3A2010%3A083%3ATOC.
Zalecenie Komisji (UE) 2020/518 z dnia 8 kwietnia 2020 roku 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 C/2020/3300. Data dostępu: 30.07.2021, https://eur-lex.europa.eu/legalcontent/PL/TXT/?qid=1587153139410&uri=CELEX:32020H0518.