Katarzyna Chałubińska-Jentkiewicz*

Prawo do prywatności jednostki w czasach pandemii

Streszczenie

Prawodawca międzynarodowy wyraźnie przewiduje, że każdy ma prawo do poszanowania swojego życia prywatnego, rodzinnego, swojego mieszkania czy też swojej korespondencji. Polska konstytucja również chroni prawo do prywatności, stanowiąc, że każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. W dobie COVID-19 nabiera ono nowego znaczenia. Bezpieczeństwo zdrowotne w dobie pandemii jest tą wartością, która podlega szczególnej ochronie. W związku z zagrożeniem wynikającym z rozprzestrzeniania się wirusa SARS-CoV-2 zdecydowana część działalności społecznej, a także zawodowej została przeniesiona do cyberprzestrzeni. To tutaj prywatność obecnie jest szczególnie zagrożona.

Słowa kluczowe: pandemia, COVID-19, prywatność, cyberbezpieczeństwo

* Dr hab. Katarzyna Chałubińska-Jentkiewicz, prof. ASzWoj, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, kierownik Katedry Prawa Mediów, Własności Intelektualnej i Nowych Technologii, e-mail: kasiachalubinska@gmail.com.

Szybki rozwój nowoczesnych technologii przetwarzania i przekazywania informacji stworzył możliwości oferowania i świadczenia usług za pośrednictwem urządzeń teleinformatycznych. Próba ujęcia normatywnego niektórych kwestii związanych ze świadczeniem usług cyfrowych wiążących się z rozwojem cyberprzestrzeni i nowych technologii polegających na przetwarzaniu informacji napotyka trudności w ścisłym określeniu podstawowych pojęć, a także zakresu odpowiedzialności podmiotów świadczących takie usługi. Dynamiczny rozwój usług właściwych dla społeczeństwa informacyjnego wymaga ciągłej aktualizacji i procedur dostosowawczych. Niemniej jednak podstawowym pojęciem do określenia zakresu stosowania ustawy jest „usługa cyfrowa" – „usługa społeczeństwa informacyjnego". Ogólnie rzecz ujmując, termin ten obejmuje wszelkie usługi świadczone za pomocą systemów teleinformatycznych, bez konieczności jednoczesnej obecności podmiotów biorących udział w tym procesie. Przesyłanie danych pomiędzy tymi podmiotami – usługodawcą i usługobiorcą – odbywa się poprzez publiczne sieci telekomunikacyjne. Usługi cyfrowe obejmują długą listę działań gospodarczych, które realizowane są w trybie połączenia z siecią teleinformatyczną (online). W ramach tego przesyłu dochodzi często do przetwarzania informacji, także na temat osób prywatnych. Usługi cyfrowe stały się również sposobem na realizowanie zadań publicznych, także tych związanych z zapewnieniem bezpieczeństwa publicznego. Samo prawo do prywatności może być zagrożone atakami w cyberprzestrzeni, ale cyberbezpieczeństwo w kontekście prawa do prywatności ma dwojaki charakter. Z jednej strony zagrożeniem mogą być cyberprzestępstwa. Z drugiej, za zagrożenie można uznać nadmierną reakcję państwa, ale zagrożać prawu do prywatności może także działanie podmiotów publicznych w ochronie cyberbepieczeństwa czy w ogóle bezpieczeństwa. Pojęcie „życie prywatne" w rozumieniu art. 8 EKPCz jest pojemnym terminem, który nie daje się wyczerpująco zdefiniować. Koncepcja autonomii osobistej może uwzględniać wiele aspektów fizycznej i społecznej oraz indywidualnej tożsamości osoby. Podstawowym przedmiotem wspomnianego art. 8 jest ochrona jednostki przed arbitralną ingerencją ze strony organów władzy publicznej. Artykuł ten zmusza państwa do powstrzymania się od takiej ingerencji – oprócz tego negatywnego zobowiązania mogą zaistnieć pozytywne obowiązki wpisane w skuteczne poszanowanie życia prywatnego. Obowiązki te mogą obejmować przyjmowanie środków mających na celu zabezpieczenie poszanowania życia prywatnego nawet w sferze relacji zachodzących pomiędzy jednostkami. Określenie granicy pomiędzy pozytywnymi i negatywnymi obowiązkami państwa nie jest łatwym zadaniem. Ważne jest, żeby społeczeństwa demokratyczne

zdołały zachowywać swoje zasady wolności, na których zostały zbudowane, także w warunkach zagrożeń. Zamknięcie przez państwo obywatela w dobrze strzeżonej twierdzy, coraz to nowsze systemy monitoringu, inwigilacji i kontroli nie rozwiązują problemu. Oznaczałoby to utratę wartości, w tym właśnie prawa do prywatności. W zapewnieniu bezpieczeństwa publicznego należy przyjąć podejście akceptowalnego ryzyka i myśleć o nim w sposób innowacyjny, postrzegając je jako proces o wielu ogniwach, w tym rozwiązań prawnych i rozwiązań organizacyjnych.

Należy zauważyć, że w zależności od sytuacji geopolitycznej, społecznej i gospodarczej pojawiają się nowe wyzwania związane z regulacją środowiska internetowego. Przykładem tego typu wyzwań jest pandemia SARS-CoV-2 COVID-19. To zjawisko spowoduje istotne zmiany w realizacji zadań publicznych takich, jak: edukacja, ochrona zdrowia, obronność itd., a także w świadczeniu pracy, działalności gospodarczej oraz w ogóle funkcjonowania życia społecznego. Przykładem szczególnym tej zmiany są postanowienia dotyczące funkcjonowania w warunkach pandemii. Zgodnie z art. 3 ustawy z 2 marca 2020 roku o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych[1], pracodawca może polecić pracownikowi wykonywanie pracy poza miejscem jej stałego wykonywania (praca zdalna), zgodnie zaś z par. 3a rozporządzenia Ministra Edukacji Narodowej z dnia 11 marca 2020 roku w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19[2] zadania wskazanych jednostek systemu oświaty są realizowane z wykorzystaniem metod i technik kształcenia na odległość. Można zatem powiedzieć, że pandemia COVID-19 stała się pretekstem do rozwoju tzw. usług cyfrowych, ale jednocześnie stworzyła warunki do podsycania niepokoju społecznego, manipulowania opinią publiczną, tworzenia postprawdy, dezinformacji itd. Dla cyberprzestępców pandemia jest okazją do zwiększenia skuteczności ataków opartych na socjotechnice przy popełnianiu oszustw (fałszywe sklepy internetowe ze środkami ochrony osobistej czy elektroniką), kradzieży z włamaniem środków z rachunków klientów wielu banków z wykorzystaniem stron internetowych podszywających się pod agentów rozliczeniowych i banki oraz nieuprawnionego uzyskiwania danych w postali loginów

1 Dz.U. 2020, poz. 374.
2 Ibidem, poz. 410, z późn. zm.

i haseł do logowania do portali społecznościowych[3]. Warunki wzmożonej aktywności społecznej online w warunkach pandemii COVID-19 (operacje bankowe, prowadzenie telekonferencji, telepraca) stworzyły nowe możliwości działalności przestępczej. Sprawcy pozostają nieuchwytni z uwagi na stosowanie przez nich różnych metod ukrycia własnej tożsamości. Najczęściej sprawcy bezprawnie posługują się fikcyjną lub przejętą tożsamością przy rejestracji domen, kart SIM (podają dane osobowe innych osób, jako abonentów usług przedpłaconych), korzystaniu z usług świadczonych drogą elektroniczną, zakładaniu kont poczty elektronicznej, profili na portalach społecznościowych, kont na giełdach kryptowalut czy w kantorach internetowych. Najczęściej przy tego typu działalności wykorzystuje się nazwy domenowe z domeny *.pl lub domeny, gdzie rejestratorami (pośrednikami) są podmioty mające siedzibę na terytorium Polski. Jest to istotny argument za pilnym dokonaniem zmian w procesie pośrednictwa w rejestracji domen i nałożenia obowiązków weryfikacji tożsamości na podmioty rejestrujące domeny (abonentów). Aktualnie rejestratorzy przyjmują dane deklarowane przez wnioskodawców.

Dużym zagrożeniem dla ochrony danych osobowych usługobiorców jest zestawianie ich danych i tworzenie profilów osobowościowych, które mogą zagrażać ich prywatności. Ustawa o świadczeniu usług drogą elektroniczną pozwalała na zestawianie ze sobą tylko danych, o których mowa w art. 19 ust. 4 i 5, do celów reklamowych, badań rynku oraz zachowań i preferencji użytkowników, mających poprawić jakość świadczonych usług. Żeby zestawić inne dane osobowe, usługodawca musiał otrzymać zgodę usługobiorcy na przetwarzanie danych, które pozwoliłyby na jego identyfikację i dopiero wtedy mógł je zestawiać z innymi danymi. Ważne stało się wdrożenie do polskiego porządku prawnego regulacji art. 3 ust. 4 dyrektywy 2000/31/WE, zgodnie z którym państwa członkowskie mogą podejmować środki mające na celu odstąpienie od zakazu ograniczania swobody świadczenia usług społeczeństwa informacyjnego pochodzących z innego państwa członkowskiego z powodów wchodzących w zakres koordynowanej dziedziny, w odniesieniu do określonej usługi społeczeństwa informacyjnego, jeżeli zostaną spełnione warunki wskazane w art. 3 ust. 4 lub 5 dyrektywy 2000/31/WE. Obecnie, gdy panuje swoboda przepływu towarów i usług, których przedmiotem jest także informacja, bezpieczeństwo każdego demokratycznego państwa zależy od wypracowania

3 Zob. Uchwała nr 7 Rady ds. Cyfryzacji przy Ministrze Cyfryzacji z dnia 14 kwietnia 2020 roku w sprawie działań mających na celu zapobieganie kradzieży tożsamości, https://www.gov.pl/web/cyfryzacja/dokumenty-rady-kadencji-2019-2021.

mechanizmów, które pozwolą skutecznie zapobiegać i zwalczać zagrożenia bezpieczeństwa w cyberprzestrzeni. Ze względu na wzrost zagrożeń ze strony sieci publicznych, od których całkowita separacja jest niemożliwa, oraz rozproszenie odpowiedzialności za bezpieczeństwo teleinformatyczne konieczne staje się skoordynowanie działań w zakresie zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni. W ten sposób działania te umożliwią szybkie i efektywne reagowanie na ataki wymierzone przeciwko systemom, sieciom teleinformatycznym i oferowanym przez nie usługom. Celem strategicznym w polityce bezpieczeństwa państwa jest zapewnienie podstaw organizacyjno-prawnych oraz systemu skutecznej koordynacji i wymiany informacji pomiędzy administracją publiczną oraz innymi podmiotami i użytkownikami cyberprzestrzeni, w tym przedsiębiorcami. Do zadań takich zaliczyć należy: 1) zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej, w tym teleinformatycznej infrastruktury krytycznej państwa; 2) zmniejszenie skutków naruszeń bezpieczeństwa cyberprzestrzeni; 3) zdefiniowanie kompetencji podmiotów odpowiedzialnych za ochronę cyberprzestrzeni; 4) stworzenie i realizacja spójnego dla wszystkich podmiotów administracji publicznej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych; 5) stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za ochronę cyberprzestrzeni oraz przedsiębiorcami dostarczającymi usługi w cyberprzestrzeni i operatorami teleinformatycznej infrastruktury krytycznej; 6) zwiększenie świadomości użytkowników w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni.

Wskazane powyżej zasady pozostają wciąż aktualne w warunkach pandemii COVID-19. Cele te będą realizowane poprzez m.in. powszechne wdrożenie w jednostkach administracji publicznej oraz u podmiotów niepublicznych mechanizmów służących zapobieganiu i wczesnemu wykrywaniu zagrożeń bezpieczeństwa cyberprzestrzeni oraz właściwemu postępowaniu w wypadku stwierdzonych incydentów, a także powszechną edukację społeczną i specjalistyczną w zakresie ochrony cyberprzestrzeni Rzeczypospolitej Polskiej. Jednakże wydaje się, że to właśnie prywatność jednostki jest najbardziej narażona, a prawo do prywatności będzie najtrudniej przestrzeganym prawem spośród praw konstytucyjnie chronionych.

Wydaje się, że kluczem do zapewnienia ochrony prawa do prywatności i tożsamości jednostki jest wprowadzenie mechanizmów weryfikacji tożsamości z wykorzystaniem już istniejących narzędzi takich, jak: podpisy elektroniczne i pieczęci elektroniczne (jest mowa w tzw. e-IDAS), w tym w szczególności

podpisu kwalifikowanego, podpis osobisty (ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych, t.j., Dz.U. 2020, poz. 332), podpis zaufany, o którym mowa w ustawie z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j., Dz.U. 2020, poz. 346, z późn. zm.) lub innych mechanizmów takich, jak np. wideoweryfikacja[4], w szczególności z wykorzystaniem obrazu twarzy zapisanego w warstwie elektronicznej dowodu osobistego i paszporcie, przy zagwarantowaniu szerokiemu kręgowi podmiotów możliwości weryfikacji ważności tych dokumentów w rejestrach publicznych. Zdaniem Rady ds. Cyfryzacji, organu programowego działającego przy Ministrze Cyfryzacji, jawny rejestr domeny .pl powinien również zawierać dane do kontaktu z abonenta domeny (co najmniej adres e-mail). Aktualnie w bazie WHOIS nie są publikowane dane abonentów będących osobami fizycznymi. Bezpieczeństwo obrotu gospodarczego i zwiększenie bezpieczeństwa wydania certyfikatu kwalifikowanego wymagają tego, żeby istniała możliwość weryfikacji danych w rejestrze krajowym, tj. w rejestrze PESEL lub RDO. Mając pełną świadomość, że dawanie dostępu do tych rejestrów osobom trzecim może powodować ryzyka dla ochrony danych osobowych, Rada ds. Cyfryzacji zaproponowała, żeby wesprzeć te procesy mechanizmem, który już istnieje i jest dostępny, ale jego dostępność jest realizowana tylko i wyłącznie w oparciu o profil zaufany osoby mającej dostęp do swoich danych tylko i wyłącznie na portalu obywatel.gov.pl bez możliwości przedstawienia tych danych w e-usłudze wymagającej wiarygodnej identyfikacji. Polegałby on na tym, że osoba wnioskująca o rejestrację w usłudze kwalifikowanej może wykorzystać dane zapisane w warstwie elektronicznej dowodu osobistego, profil zaufany lub podpis kwalifikowany do zwrócenia się do rejestru RDO lub PESEL o swoje dane, niezbędne do potwierdzenia tożsamości w procesie wydawania certyfikatu kwalifikowanego, a te dane mogą zostać następnie udostępnione

4 Wideoweryfikacja – metoda, przy której pomocy może być potwierdzana tożsamość, zwłaszcza z wykorzystaniem obrazu twarzy zapisanego w warstwie elektronicznej dowodu osobistego, paszporcie, innych środkach oraz wsparciu przez rejestry państwowe. Zgodnie z art. 24 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (tzw. e-IDAS) potwierdzanie tożsamości może odbywać się: „przy użyciu innych metod identyfikacji uznanych na szczeblu krajowym, które zapewniają pewność równoważną, pod względem wiarygodności, fizycznej obecności. Równoważna pewność musi być potwierdzona przez jednostkę oceniającą zgodność". Jednakże z wideoweryfikacją wiążą się pewne zagrożenia, np. wykorzystywanie algorytmów twarzy użytkowników bez ich wiedzy i zgody – od Captchy przez FaceApp.

(za zgodą wnioskującego) kwalifikowanej usłudze zaufania w celu wydania kwalifikowanego certyfikatu na podstawie tych danych. Żeby to osiągnąć ze strony technicznej, funkcjonalność dostępna na obywatel.gov.pl powinna być dostępna w interfejsie API dla dostawców usług zaufania. Wniosek o udostępnienie własnych danych, w zakresie wymaganym polityką certyfikacji usługi zaufania, powinien móc być podpisany zarówno podpisem osobistym z dowodu osobistego, podpisem zaufanym (w oparciu o profil zaufany), jak i podpisem kwalifikowanym. Zdaniem Rady ds. Cyfryzacji, taki mechanizm rozwiązałby w znacznym stopniu obecny problem zdalnej identyfikacji. W uchwale Rada zaznaczyła: „Biorąc pod uwagę sytuację, w której zarówno obywatele, jak i przedsiębiorcy będą korzystali z dostępu do usług publicznych w celu nie tylko załatwiania spraw bieżących, ale także w celu składania wniosków o pomoc wynikającą z regulacji przyjętych w celu zmniejszenia skutków pandemii, należy pilnie umożliwić w systemach dostępowych do tych usług posługiwanie się nie tylko zaufanym profilem, jak obecnie w większości usług publicznych, ale także wykorzystanie w procesie dostępu do usługi publicznej danych zapisanych w warstwie elektronicznej dowodu osobistego i certyfikatu kwalifikowanego. Pomijanie w usługach publicznych kwalifikowanego certyfikatu jest naruszeniem rozporządzenia e-IDAS. Przykładem takiego prawidłowego i przez to bezpiecznego rozwiązania jest dostęp do platformy PUE w ZUS. Należy też zwrócić uwagę na fakt, iż wykorzystanie wyłącznie zaufanego profilu, którego funkcjonowanie zależy od prawidłowego funkcjonowania jednego systemu informatycznego, oraz brak innych metod dostępu do usługi publicznej jest z punktu widzenia bezpieczeństwa tych usług, czyli ich dostępności dla obywateli i przedsiębiorców, nieakceptowalnym ryzykiem". Jednym z zaleceń jest także odejście od weryfikacji tożsamości osób fizycznych opartej na znajomości numeru PESEL, który służy do identyfikacji danej osoby, ale jest też powszechnie dostępny online w rejestrach publicznych (księgi wieczyste, KRS itd.). Do podniesienia poziomu bezpieczeństwa i przeciwdziałania zjawisku kradzieży tożsamości celowe jest również wprowadzenie obowiązków dotyczących lepszej weryfikacji tożsamości podmiotów korzystających z usług podmiotów świadczących usługi cyfrowe. Aktualnie niemożliwe jest ustalenie danych osoby, która korzysta z konta poczty elektronicznej (np. podanego podczas rejestracji), a podmioty świadczące usługi drogą elektroniczną nie mają obowiązków związanych z gromadzeniem i przechowywaniem logów dostępowych użytkowników. Powoduje to nie tylko brak możliwości ustalenia, kto korzysta z konta poczty elektronicznej, ale znacząco utrudnia lub wręcz uniemożliwia przeprowadzenie postępowania dotyczącego uzyskania

nieuprawnionego dostępu (włamania) do takiego konta. Istotnym problemem jest również zakres danych gromadzonych i udostępnianych jako logi. Ze względu na to, że operatorzy powszechnie wykorzystują NAT i jeden publiczny adres IP, który może być przydzielony nawet kilkudziesięciu tysiącom użytkowników, uniemożliwia to ustalenie abonenta usługi.

Z jednej strony wskazana powyżej problematyka dotyka kwestii istotnych z punktu widzenia bezpieczeństwa obrotu gospodarczego, ale także realizacji zadań publicznych, np. w obszarze edukacji online. W tych okolicznościach pandemia COVID-19 stała się czasem weryfikacji reguł funkcjonowania jednostki w cyberprzestrzeni, a propozycje regulacji, rekomendacje legislacyjne odnoszą się do zmian związanych przede wszystkim z potrzebą cyberbezpieczeństwa. Im więcej eksploatacji cyberprzestrzeni, tym więcej regulacji podyktowanych względami cyberbezpieczeństwa. Wydaje się to oczywistą zależnością.

Pandemia COVID-19 pokazała, jak bardzo władza publiczna wkracza w obszar prywatności jednostki w związku z potrzebami ochrony dobra nadrzędnego, interesu publicznego. Przykładem tego działania jest aplikacja Kwarantanna domowa. Z pomocą polskim służbom, policji oraz w trosce o bezpieczeństwo polskich obywateli została utworzona, na zlecenie Ministerstwa Cyfryzacji, specjalna aplikacja, pomagająca sprawdzać, czy użytkownicy, którymi mogą być jedynie osoby objęte obowiązkową kwarantanną, spełniają swój obowiązek we właściwym miejscu. Aplikacja Kwarantanna domowa to narzędzie, które ułatwiało i usprawniało przeprowadzenie w warunkach domowych obowiązkowej izolacji. Umożliwiło potwierdzenie miejsca, w którym dana osoba aktualnie przebywała, ocenę stanu zdrowia oraz bezpośrednie zgłoszenie zagrożenia. Aplikacja ułatwiała również zaopatrzenie w najpotrzebniejsze artykuły osobom, które nie miały takiej możliwości samodzielnie. Aplikacja co do zasady była obowiązkowa, ale były przewidziane dwa wyjątki. Z obowiązku instalacji oraz jej użytkowania były zwolnione osoby z dysfunkcją wzroku, czyli osoby niewidzące lub niedowidzące, a także te, które złożyły specjalne oświadczenie właściwym służbom, że nie są abonentami lub użytkownikami sieci telekomunikacyjnej lub nie posiadają urządzenia mobilnego umożliwiającego zainstalowanie tego oprogramowania. Oświadczenie składało się policji lub państwowemu powiatowemu inspektorowi sanitarnemu właściwemu dla miejsca odbywania kwarantanny. Istniała również możliwość złożenia oświadczenia za pośrednictwem środków komunikacji elektronicznej. Warunkiem aktywacji aplikacji było otrzymanie SMS-u z informacją o utworzeniu konta użytkownika i konieczności pobrania aplikacji. Cały proces aktywacji sprowadzał się do: pobrania aplikacji i akceptacji regulaminu przez użytkownika;

rejestracji użytkownika poprzez wprowadzenie numeru telefonu, pod którym użytkownik będzie dostępny podczas kwarantanny; wprowadzenie czterocyfrowego kodu autoryzacyjnego oraz realizacji inicjowanego zadania „Kwarantanna pełna informacji" w miejscu odbywania kwarantanny. Realizacja zadania „Kwarantanna pełna informacji" polegała na zapoznaniu się z informacjami dotyczącymi sposobu odbywania kwarantanny oraz wykonaniu zdjęcia, tzw. selfie w zadeklarowanym miejscu odbywania kwarantanny. Żeby aplikacja spełniała swoją funkcję, zdjęcie musiało być wykonane po uprzednim udostępnieniu funkcji lokalizacji GPS urządzenia. Usługa weryfikacji odbywania kwarantanny była powtarzana cyklicznie w ciągu dnia. Należało ją zrealizować w ciągu 20 minut od otrzymania SMS-u z informacją o pojawieniu się nowego zadania. Czas dostępu do aplikacji to 14 dni kalendarzowych, licząc od dnia decyzji służb sanitarnych o rozpoczęciu odbywania kwarantanny. Konto mogło być dezaktywowane wcześniej, jeżeli w trakcie trwania tego okresu wystąpiły okoliczności powodujące zakończenie kwarantanny. W tym przypadku nie ustalono okoliczności tego typu. Jedynym przykładem, jaki się nasuwa, była śmierć użytkownika[5]. Od 1 kwietnia 2020 roku instalowanie aplikacji było obowiązkowe dla osób odbywających kwarantannę domową.

Dodać należy, że w razie braku akceptacji regulaminu przez użytkownika uniemożliwiało aktywację aplikacji. W regulaminie ustalono, że minister informuje, że aplikacja do prawidłowego działania wymaga, żeby urządzenie mobilne umożliwiało jej w określonych sytuacjach dostęp do: 1) Internetu; 2) aparatu; 3) lokalizacji; 4) zdjęć. Minister udostępnia następujące usługi: 1) usługę weryfikacji przestrzegania kwarantanny przez użytkowników; 2) usługę wysłania formularza z zapotrzebowaniem do MOPS (posiłek, artykuły spożywcze, pomoc psychologiczna, kontakt); 3) usługę dostępu do komunikatów informujących o aktualnej sytuacji dotyczącej koronawirusa SARS-CoV-2; 4) usługę bezpośredniego kontaktu ze służbami odpowiedzialnymi za nadzór nad użytkownikami objętymi kwarantanną. Usługi dostępne w aplikacji świadczone są nieodpłatnie. Jednakże w związku z koniecznością zainicjowania połączenia internetowego w celu korzystania przez użytkownika z aplikacji operator zapewniający użytkownikowi połączenie internetowe mógł naliczyć opłatę za transmisję danych zgodną z cennikiem tego operatora. Usługa cyklicznej weryfikacji odbywania kwarantanny polega na wykonaniu następujących czynności: 1) potwierdzeniu

5 *Regulamin aplikacji Kwarantanna domowa*, https://www.gov.pl/web/koronawirus/kwarantanna-domowa.

przebywania w deklarowanej lokalizacji. Przy realizacji tego zadania automatycznie jest sprawdzana lokalizacja GPS, żeby zadanie zostało wykonane poprawnie; 2) zrobić zdjęcie typu selfie w miejscu deklarowanej lokalizacji; 3) zakończyć zadanie. Usługę, o której mowa w pkt 2, należy zrealizować w ciągu 20 minut od otrzymania SMS-u z informacją o pojawieniu się nowego zadania w aplikacji. Użytkownik jest zobowiązany do realizacji usługi zgodnie z przyjętym harmonogramem i przyjętymi zasadami realizacji usługi.

Podstawą prawną tego obowiązku był 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 (Dz.U. poz. 374, z późn. zm.). Niezrealizowanie usługi zgodnie z przyjętym harmonogramem i zasadami mogło skutkować powiadomieniem o tym odpowiednich służb, a w konsekwencji zastosowaniem przez nie środków przymusu określonych w ustawie oraz nałożeniem przez nie kary, o której mowa w art. 116 par. 1 pkt 1 kodeksu wykroczeń. Informacja o naruszeniu kwarantanny (tj. brak wykonania zadania, niezgodność zdjęcia lub próba oszustwa) była przekazywana automatycznie do odpowiednich służb. W razie wystąpienia objawów zakażenia SARS-CoV-2 użytkownik był obowiązany niezwłocznie powiadomić o tym odpowiednie służby, korzystając z funkcjonalności dostępnych w aplikacji. Podczas realizacji usługi zakazane było posługiwanie się oprogramowaniem mającym na celu zmianę danych lokalizacyjnych (szerokości i długości geograficznej). Dane były gromadzone wyłącznie w trakcie korzystania z usług wymienionych w regulaminie. Minister przechowuje dane osobowe (z wyjątkiem zdjęć, które usuwane są w momencie dezaktywacji konta) przez okres przedawnienia roszczeń określony w art. 118 kodeksu cywilnego (6 lat), który będzie liczony od momentu dezaktywacji aplikacji. Dane nie były przetwarzane w celach marketingowych. Użytkownik był zobowiązany poinformować odpowiednie służby o każdej zmianie jego danych, tj. imienia, nazwiska, lokalizacji odbywania kwarantanny lub numeru telefonu udostępnionych w ramach aplikacji. Podstawą prawną w tym przypadku jest art. 9 ust. 2 lit. i RODO.

Artykuł 9 ust. 1 wskazuje, że zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. W ust. 2 zostały wymienione warunki, z których spełnienie choćby jednego z nich sprawia, że

możliwość przetwarzania danych osobowych, o których mowa w ust. 1, jest całkowicie legalna.

Taka konstrukcja prawna pozwala, ze względu na wystąpienie szczególnych warunków wskazanych w rozporządzeniu, przetwarzać przez podmioty do tego uprawnione dane osobowe osób fizycznych w celu ich jednoznacznego zidentyfikowania. Właśnie jeden z tych szczególnych warunków, w którym wskazane podmioty mogą przetwarzać w ramach swoich obowiązków dane osobowe, reguluje art. 9 ust. 2 lit. i rozporządzenia. Możliwość przetwarzania danych w tym wypadku jest uzasadniona, jeżeli jest to niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego – bezpieczeństwo publiczne. Takimi czynnikami są m.in. ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych.

Administratorem danych osobowych przetwarzanych w aplikacji i systemie wspomagającym jej działanie jest Minister Cyfryzacji z siedzibą w Warszawie przy ul. Królewskiej. Zakres danych osobowych przetwarzanych w ramach realizacji usług dostępnych w aplikacji: 1) ID obywatela – techniczny identyfikator obywatela; 2) imię; 3) nazwisko; 4) numer telefonu; 5) deklarowany adres pobytu; 6) zdjęcie; 7) lokalizacja obywatela; 8) data końca kwarantanny. Odbiorcami przetwarzanych w aplikacji i systemie danych mogą być: 1) Komenda Główna Policji; 2) wojewódzkie komendy Policji; 3) wojewodowie; 4) Centralny Ośrodek Informatyki; 5) Take Task S.A.; 6) Centrum Systemów Informacyjnych Ochrony Zdrowia. Przetwarzanie przez administratora i podmioty, którym je udostępniono, danych osobowych przetwarzanych w aplikacji i w systemie obsługującym działanie aplikacji odbywało się ze względu na ważny interes publiczny, tj. zaistniałą sytuacją kryzysową związaną z rozprzestrzenianiem się wirusa SARS-CoV-2 (art. 9 ust. 2 lit. i RODO) oraz w związku z podpisanymi umowami powierzenia przetwarzania z podmiotami świadczącymi usługi wsparcia technicznego i utrzymywania technicznego dla aplikacji i systemu. Osobie, której dane dotyczą, przysługiwało w dowolnym momencie: 1) prawo dostępu do treści danych; 2) prawo ich poprawiania i sprostowania; 3) prawo do sprzeciwu do przetwarzania danych; 4) prawo do ograniczenia przetwarzania danych osobowych przez Ministra; 5) prawo do wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych. Prawo do poprawienia lub sprostowania danych było realizowane wyłącznie poprzez poprawienie danych znajdujących się w systemie teleinformatycznym zapewniających funkcjonowanie aplikacji oraz dotyczy danych, o których

mowa w par. 9 ust. 2 regulaminu. Przetwarzanie danych, w ramach realizacji zadań nałożonych na użytkownika w trakcie trwania kwarantanny, następowało w ramach realizacji obowiązków użytkownika na podstawie akceptacji regulaminu. Przetwarzanie danych następowało w celu wykonania przez użytkownika obowiązku wynikającego z art. 7e ustawy z dnia 2 marca 2020 roku o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, którego realizacja ma na celu wsparcie służb w monitoringu realizacji kwarantanny osób lub nadzoru epidemiologicznego przez osoby, co do których istnieje podejrzenie, że mogą być roznosicielami choroby zakaźnej COVID-19. W związku z celem przetwarzania, o którym mowa w ust. 8 tejże ustawy, Minister informował, że dane użytkownika są udostępniane służbom w celu realizacji ich ustawowych obowiązków związanych ze zwalczaniem zagrożenia epidemiologicznego wywołanego wirusem SARS-CoV-2 powodującym chorobę COVID-19. Dane te miały być gromadzone wyłącznie w trakcie korzystania z usług wymienionych w regulaminie aplikacji Kwarantanna domowa. Minister przechowuje dane osobowe (z wyjątkiem zdjęć, które usuwane są w momencie dezaktywacji konta) przez okres przedawnienia roszczeń określony w art. 118 kodeksu cywilnego (6 lat), który będzie liczony od momentu dezaktywacji aplikacji. Te zasady wzbudziły zastrzeżenia, czy przesłane przez obywateli zdjęcia i dane o lokalizacji nie powinny być usuwane natychmiast po ich prawidłowym zweryfikowaniu (tzn. ustaleniu, że objęta kwarantanną osoba przebywa pod swoim adresem). W odpowiedzi na wątpliwości Fundacji Panoptykon Ministerstwo Cyfryzacji doprecyzowało: „Nie tworzymy bazy zdjęć jako ustrukturyzowanego zbioru do przeszukiwania po identyfikatorze obywatela, np. PESEL. Składujemy je w celach określonych w regulaminie. Zdjęcia będą usuwane zaraz po odbyciu kwarantanny. Oznacza to, iż przez okres 6 lat będą przechowywane jedynie podstawowe dane, podawane przez użytkowników i użytkowniczki przy instalowaniu aplikacji, ale już nie raporty przez nich przesyłane". Jednakże w ramach analizy aplikacji w badaniu Fundacji Panoptykon okazało się, że aplikacja ma więcej uprawnień.

Po kliknięciu opcji „uprawnienia" w sklepie Google Play okazuje się, niestety, że aplikacja ma jednak większe uprawnienia, np.: 1) widzi, z którą siecią Wi-Fi łączy się urządzenie; 2) odczytuje zawartość pamięci urządzenia oraz ma możliwość modyfikacji lub kasowania jego zawartości; 2) odczytuje identyfikator urządzenia i informację o połączeniu; 3) ma dostęp do aparatu i mikrofonu (takie uprawnienie daje aplikacji możliwość nagrywania dźwięku i obrazu; 4) odczytuje lokalizację na podstawie danych z sieci komórkowej i GPS;

5) zapobiega przejściu telefonu w stan uśpienia; 6) może zmieniać ustawienia audio urządzenia; 7) może posiadać pełen dostęp do sieci oraz wyświetlać połączenia sieciowe; 8) posiada również kontrolę nad latarką.

Po zainstalowaniu aplikacji okazuje się, że sprawdza ona również inne aplikacje zainstalowane na urządzeniu – czy nie ma wśród nich takiej aplikacji, która oszukuje lokalizację. W regulaminie aplikacji nie ma informacji na temat ukrytych funkcji, jakie ona posiada. Fundacja Panoptykon, która zajmuje się kontrolą społeczną nad praktykami nadzoru instytucji publicznych, zajęła się tą sprawą i wystąpiła z zapytaniem do Ministerstwa Cyfryzacji. W odpowiedzi Ministerstwo zapewniło Fundację, że aplikacja, mimo korzystania z dostępu do lokalizacji na podstawie GPS, sieci komórkowej i sieci bezprzewodowej, nie rejestruje, z której sieci korzysta obywatel, a także nie korzysta z pozostałych funkcji (latarki czy nagrywania dźwięku). Gdyby np. chciała uruchomić mikrofon, osoba korzystająca z aktualnego systemu Android albo iOS otrzymałaby analogiczne powiadomienie, jak w przypadku dostępu do zdjęć, multimediów i plików na urządzeniu. Nic takiego się nie dzieje, nie ma zatem powodów, żeby wątpić w zapewnienia Ministerstwa. Aplikacja nie sprawdza lokalizacji użytkowników przez cały czas, a jedynie podczas uruchamiania i wykonywania przez użytkownika zadania. Ministerstwo zapewniło też, że aplikacja korzysta z aparatu wyłącznie po to, żeby robić zdjęcia. Nie nagrywa krótkich filmików, czego obawiali się eksperci komentujący zabezpieczenia aplikacji przed typowymi próbami oszustw ze strony użytkowników. W regulaminie aplikacji znajduje się informacja o tym, że instalacja oraz używanie aplikacji jest ustawowym obowiązkiem osób, które zobowiązane są do poddania się kwarantannie w związku z podejrzeniem zakażenia wirusem SARS-CoV-2. Należy zaznaczyć, że każda strona internetowa, oprogramowanie czy też aplikacja, która w jakiś sposób przetwarza dane osobowe użytkowników, musi posiadać własną politykę prywatności. Taki dokument musi zawierać przede wszystkim informacje dotyczące przetwarzania danych osobowych użytkowników sieci, usług, serwisów, aplikacji; informację o administratorze danych osobowych; oraz jakie dane są przetwarzane oraz czy przetwarzanie tych danych jest niezbędne ze względu na usługi świadczone drogą elektroniczną przez dany podmiot; w jakim celu i na jakiej podstawie są przetwarzane dane; jak długo podmiot administrujący zamierza je przetwarzać; jakie prawa przysługują osobom, których dane dotyczą, oraz komu udostępniane są dane użytkowników. Polityka prywatności aplikacji Kwarantanna domowa zawarta została w regulaminie aplikacji w par. 9. W punkcie 1 polityki prywatności znajduje się informacja o tym, że administratorem danych osobowych przetwarzanych przez aplikację

i system wspomagający jej działanie jest Minister Cyfryzacji. Zgodnie z rozporządzeniem 2016/679, administrator danych osobowych jest zobowiązany do wyznaczenia inspektora ochrony danych osobowych – administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze wówczas, gdy przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości; główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę lub gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa (art. 37 pkt 1). W punkcie 3 polityki prywatności znalazł się enumeratywny katalog danych przetwarzanych w ramach realizacji usług dostępnych w aplikacji mobilnej dotyczących osób objętych kwarantanną. Dane zbierane przez aplikację to: ID Obywatela (techniczny identyfikator obywatela); imię; nazwisko; numer telefonu; deklarowany adres pobytu; zdjęcie; lokalizacja obywatela (system za pomocą odpowiednich algorytmów będzie sprawdzał i analizował, czy położenie GPS urządzenia mobilnego w trakcie realizacji zadania będzie zgodne z deklarowanym adresem pobytu) oraz datę końca kwarantanny. Ministerstwo zaznaczyło, że zgodę na dostęp do lokalizacji obywatel wyraża, akceptując systemowe powiadomienie. Takie powiadomienie jest widoczne w momencie pierwszego uruchomienia aplikacji. Podczas wykonywania pierwszego zadania w aplikacji system pyta nas o zgodę na dostęp do zdjęć, multimediów i plików na urządzeniu. Zgoda ta potrzebna jest do zapisania wykonanego zdjęcia i odczytania tego zdjęcia w celu przesłania do automatycznej weryfikacji. Ministerstwo poinformowało również, że aplikacja nie korzysta z pozostałych funkcji (m.in. latarki czy nagrywania dźwięku i video). Jeżeli aplikacja chciałaby uruchomić np. mikrofon, to osoba korzystająca z aplikacji dostałaby odpowiednie powiadomienie. Pozostaje tylko pytanie, po co w takim razie istnieje możliwość dostępu aplikacji do takich funkcji, skoro nie jest to potrzebne do jej prawidłowego działania? Fundacji udało się również ustalić, że wbrew podejrzeniom użytkowników oraz ekspertów aplikacja nie sprawdza lokalizacji użytkownika przez cały czas. Ma to miejsce jedynie podczas uruchamiania i wykonywania przez użytkownika zadania. Aplikacja nie nagrywa również filmów, aparat wykorzystuje jedynie do zrobienia zdjęcia w celu wykonania

przez użytkownika zadania[6]. Jeżeli osoba podlegająca obowiązkowej kwarantannie nie będzie przebywała sama w miejscu deklarowanego pobytu, to jest zobowiązana podać imię, nazwisko, PESEL/numer dokumentu oraz numer telefonu wszystkich osób przebywających razem z nią w danym miejscu. Analizując część regulaminu, która reguluje kwestię podmiotów uprawnionych do przetwarzania pozyskanych danych osobowych przez aplikację, nasuwa się pytanie: czy na pewno tylko te podmioty mogą być odbiorcami przetwarzanych danych? Otóż, wydaje się, że katalog podmiotów uprawnionych do przetwarzania danych jest znacznie większy. Wydaje się, że okres przechowywania danych wskazany w regulaminie aplikacji byłby czynnikiem dodatkowo umacniającym przekonanie o znacznie szerszym zakresie korzystania z danych w przyszłości. Zgodnie z par. 9 pkt 11 regulaminu, dane osobowe użytkowników będą przechowywane przez Ministerstwo Cyfryzacji (z wyjątkiem zdjęć, które będą usuwane z systemu w momencie dezaktywacji aplikacji) od momentu dezaktywacji aplikacji – zgodnie z art. 118 kodeksu cywilnego – przez 6 lat, czyli okres przedawnienia roszczeń. Okres przechowywania danych osobowych użytkowników aplikacji przez Ministerstwo wydaje się być nieuzasadniony, ponieważ aplikacja miała służyć zweryfikowaniu, czy obywatel objęty kwarantanną przestrzega nałożonego na niego nakazu. W związku z tym na swoich serwerach Ministerstwo Cyfryzacji powinno przechowywać dane użytkowników tylko tak długo, jak jest to konieczne, czy dana osoba faktycznie przestrzegała zasad kwarantanny. Kwestią sporną jest również to, że dane użytkowników aplikacji będą przechowywane przez 6 lat. Wydawałoby się, że nie ma potrzeby magazynowania takich danych i powinny one być usuwane w momencie zakończenia kwarantanny. Niemniej jednak trzeba zastanowić się, czy dane pozyskane przez Ministerstwo są tak ważne do zapewnienia bezpieczeństwa ze względu na ważny interes publiczny.

Zdaniem ekspertów Fundacji Panoptykon, rozwiązanie zastosowane w aplikacji Kwarantanna domowa oznacza, że (mniej lub bardziej twarzowe) zdjęcia osób wraz ze szczegółami widocznymi w tle, które niekoniecznie chciałyby pokazywać, trafiają na serwery, skąd mogą trafiać dalej w bliżej nieokreślonym celu i być przetwarzane na różne sposoby. Zamiast wysyłać zdjęcia na serwery Ministerstwa, lepiej z punktu widzenia prywatności byłoby wykonywać analizę zgodności twarzy na urządzeniu. Taki algorytm (np. FisherFace) mógłby tworzyć lokalny model cech biometrycznych. Suma kontrolna takiego wzoru

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

mogłaby być przechowywana na serwerze, żeby weryfikować, czy wzór się nie zmienił w czasie. W przypadku nadejścia żądania weryfikacji lokacji oraz twarzy sprawdzane byłoby tylko to, czy lokalny wzorzec się nie zmienił, a następnie – również lokalnie – następowałoby porównanie twarzy ze wzorcem. Dodatkowym zabezpieczeniem byłoby wzbogacenie algorytmu o mechanizm atestacji urządzenia zdolny do pomiaru stanu zdrowia i tego, czy użytkownik czegoś nie kombinuje (tak wypowiedział się Mateusz Chrobok, entuzjasta biometrii behawioralnej, wiceprezes do spraw biometrii behawioralnej w Buguroo)[7].

Odpowiedź na pytanie o zakres możliwych ograniczeń w sferze prywatności jednostki w warunkach potrzeby zapewnienia bezpieczeństwa jest trudna. Problematyka ta obejmie bez wątpienia obszary, które stanowią nieprawdopodobną i dzisiaj jeszcze nieznaną sferę ludzkiego działania w cyberprzestrzeni. Z drugiej strony, konieczne są prawa do samostanowienia w zakresie informacji, czyli autonomia informacyjna, być może o znacznie rozbudowanych regułach monitorowania danych na swój temat – włącznie ze sztywno ustalonymi regułami dostępu do danych osobowych i ich przechowywania w warunkach niezbędności takich działań, do których możemy zaliczyć zasadę wykorzystywania danych zgodnie z ich przeznaczeniem; zasadę korzystania z prawa bycia zapomnianym przez użytkowników sieci, zagwarantowaną przez Trybunał Sprawiedliwości UE w 2014 roku, zasadę anonimizacji i pseudonimizacji, które powinny towarzyszyć wszystkim rejestrom, zwłaszcza rejestrom medycznym. To tylko początek niezbędnych ustaleń odnośnie do przyszłych regulacji, które stają się niezbędne zwłaszcza w sytuacjach, których nie byliśmy w stanie przewidzieć jeszcze rok czy dwa lata temu, w warunkach pandemii COVID 19, kiedy władze publiczne na całym świecie podejmują działania umożliwiające walkę z wirusem, ale wkraczające często w prywatność jednostek, na rzecz dobra publicznego.

Bibliografia

Rozporządzenie Ministra Edukacji Narodowej z dnia 11 marca 2020 r. w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, Dz.U. 2020, poz. 410, z późn. zm.

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, t.j., Dz.U. 2020, poz. 346, z późn. zm.

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

Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych, t.j., Dz.U. 2020, poz. 332.

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

The individual' right to privacy during the pandemic

Abstract

The international legislator clearly states that everyone has the right to privacy as regards their private and family life, residence or correspondence. The Constitution of the Republic of Poland also safeguards the right to privacy, stipulating that everyone has the right to enjoy legal protection of their private and family life, dignity and good name, and to decide about their personal life. However, during the COVID-19 pandemic, the right to privacy has acquired a new meaning. Health security is under special protection in the time of the pandemic. Due to the threats posed by the spread of the SARS-CoV-2 virus, a major part of the social and professional activity was transferred to cyberspace which is where privacy is particularly endangered.

Key words: pandemic, COVID-19, privacy, cybersecurity