**RZECZNIK PRAW OBYWATELSKICH**

**Adam Bodnar**

Warszawa, 15-04-2020 r.

**VII.501.75.2020.KŁ**

**Pan**
**Jan Nowak**
**Prezes Urzędu Ochrony Danych Osobowych**

ePUAP

Szanowny Panie Prezesie!

Do Rzecznika Praw Obywatelskich docierają **głosy zaniepokojonych obywateli, którzy mają wątpliwości co do tego, czy korzystanie z aplikacji „Kwarantanna domowa" nie narusza ich prawa do ochrony danych osobowych**. Jest to szczególnie istotne teraz, kiedy zgodnie z art. 7e ust. 1 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz. U. poz. 374 ze zm.) został wprowadzony obowiązek zainstalowania i używania aplikacji przez osoby poddane kwarantannie.

Jako Rzecznik Praw Obywatelskich nie kwestionuję obowiązku przestrzegania kwarantanny, jednak w mojej ocenie konieczne jest zapewnienie, aby narzędzia wykorzystywane w tym zakresie przez państwo mieściły się w konstytucyjnym standardzie ochrony prywatności i autonomii informacyjnej jednostki, a także spełniały wymogi przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy

95/46/WE (Dz. U. UE L. 119.1 ze sprost.; dalej: RODO). Należy wskazać, że stosowanie technologii mobilnych do kontroli obywateli wiąże się z coraz większymi zagrożeniami związanymi z rozwojem nowych technologii przetwarzania danych. Dobrze znane są Panu Prezesowi na przykład wyzwania związane z analityką *big data.* Jak zauważa się w literaturze, możliwość, korelowania wielu informacji, pochodzących z różnych baz danych, tworzy przestrzeń do ujawniania nowych, nie występujących w danych źródłowych informacji[1]. Należy więc z dużą ostrożnością podchodzić do wprowadzania nowych instrumentów zakładających przetwarzanie danych na szeroką skalę. Należy również, ze względu na różny poziom kompetencji cyfrowych obywateli, dołożyć jak największych starań, by prawa i obowiązki związane z korzystaniem z aplikacji były przystępnie wyjaśnione i żeby stosowne komunikaty dotarły do wszystkich zainteresowanych.

W chwili obecnej w parlamencie trwają prace nad ustawą z dnia 9 kwietnia 2020 r. o szczególnych instrumentach wsparcia w związku z rozprzestrzenianiem się wirusa SARS-CoV-2 (druk senacki 101/X kadencja), której art. 72 pkt 13 wprowadza do ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych przepis art. 11f, który nakłada na operatorów, podczas stanu zagrożenia epidemicznego, stanu epidemii albo stanu klęski żywiołowej, obowiązek udostępniania ministrowi właściwemu do spraw informatyzacji danych o lokalizacji, obejmujących okres ostatnich 14 dni, telekomunikacyjnego urządzenia użytkownika końcowego chorego na chorobę zakaźną COVID-19 lub objętego kwarantanną, na żądanie oraz w sposób i w formie ustalonej przez ministra właściwego do spraw informatyzacji (ust. 1). Operator jest również obowiązany na żądanie ministra właściwego do spraw informatyzacji do przekazania w sposób i w formie ustalonej przez tego ministra, w celu przeciwdziałania COVID-19, podczas stanu zagrożenia epidemicznego, stanu epidemii albo stanu klęski żywiołowej zanonimizowanych danych o lokalizacji urządzeń końcowych użytkowników końcowych (ust. 2). Zgoda użytkownika końcowego na przetwarzanie i udostępnianie danych, o których mowa w ust. 1 i 2, nie jest wymagana (ust. 3).

[1] M. Rojszczak, *Definicja i granice prawnej ochrony prywatności w epoce analityki big data*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny", nr 1/2019, s. 120.

Omawiany przepis wprowadza istotne kompetencje Ministra Cyfryzacji do żądania danych o lokalizacji w formie niezanonimizowanej w wypadku osób chorych i poddanych kwarantannie oraz zanonimizowanych danych dotyczących osób zdrowych. Należy wskazać, że jest to kolejne wkroczenie w prywatność obywateli po uczynieniu aplikacji "Kwarantanna domowa" obowiązkowym prawnie narzędziem. Jak można wnioskować, dostęp do danych osób chorych i poddanych kwarantannie będzie wykorzystywany do "uszczelnienia" systemu, tj. weryfikacji, gdzie znajdują się osoby które nie zainstalowały aplikacji. Dane osób zdrowych zapewne będą wykorzystywane w ramach wspierania działań służb. Należy wskazać, że decyzja o sięgnięciu po takie dane rodzi dużą odpowiedzialność po stronie władz. Trzeba podkreślić, że dostęp do danych telekomunikacyjnych był już wielokrotnie przedmiotem analizy z punktu widzenia wpływu na prywatność, w szczególności w sprawach dotyczących retencji danych telekomunikacyjnych (w Unii Europejskiej i w Polsce). Oczywiście w tym wypadku cel przetwarzania jest inny, w związku z tym inaczej będzie badana adekwatność danych osobowych do celów dla których są przetwarzane (art. 5 ust. 1 lit. c RODO), czy też realizacja konstytucyjnej zasady proporcjonalności ograniczeń prawa do prywatności. Należy jednak wskazać, że Prezes UODO, jako organ właściwy w sprawie ochrony danych osobowych oraz organ nadzorczy w rozumieniu RODO powinien badać te rozwiązania i zabierać głos w debacie publicznej. Trzeba bowiem zauważyć, że zgodnie z art. 57 ust 1 lit. c RODO organ nadzorczy doradza, zgodnie z prawem państwa członkowskiego, parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie aktów prawnych i administracyjnych środków ochrony praw i wolności osób fizycznych w związku z przetwarzaniem. Byłoby w mojej ocenie cenne, gdyby Pan Prezes zajął stanowisko w sprawie rozważanych i proponowanych rozwiązań i ich wpływu na ochronę danych.

Biorąc pod uwagę wspomniane wyżej wątpliwości obywateli, pozwalam sobie zasygnalizować Panu Prezesowi jeszcze jedną kwestię. W dniu 3 kwietnia 2020 r. na stronie Ministerstwa Cyfryzacji pojawiła się informacja, że rozpoczęły się prace nad aplikacją, która pozwoli kontrolować i zahamować rozprzestrzenianie się koronawirusa. Zgodnie z zapowiedziami Ministerstwa Cyfryzacji: „ProteGO to aplikacja projektowana na czas wychodzenia z najpoważniejszych obostrzeń wdrożonych do walki pandemią koronawirusa. Celem tego rozwiązania jest kontrola nad rozprzestrzenianiem się choroby. Chcemy to osiągnąć budując - poprzez technologię Bluetooth - swoistą sieć połączeń pomiędzy

użytkownikami telefonów komórkowych. Aplikacja nie będzie gromadzić ich danych, ani śledzić ich położenia”[2]. Z uznaniem należy przyjąć starania oparcia nowych technologii na rozwiązaniach, które chronią w wysokim stopniu prawo jednostki do prywatności, jednak również ta aplikacja powinna w trakcie jej projektowania podlegać ocenie z punktu widzenia skutków dla ochrony danych.

Na koniec należy wspomnieć, że swoje aplikacje związane z epidemią wprowadzają również Wojska Obrony Terytorialnej: https://www.cyberdefence24.pl/aplikacja-wot-ulatwi-dostarczenie-pomocy-osobom-w-kwarantannie.

Mając na względzie powyższe, działając na podstawie art. 12 pkt 2 ustawy z 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2020 r., poz. 627) zwracam się do Pana Prezesa z uprzejmą prośbą o zbadanie rozwiązań przyjętych lub planowanych w wypadku wspomnianych aplikacji pod kątem ich zgodności z prawem ochrony danych osobowych. Ścisła współpraca Urzędu Ochrony Danych Osobowych z między innymi Ministerstwem Cyfryzacji w zakresie przeprowadzenia oceny skutków dla ochrony danych jest tu w mojej ocenie kluczowa. Będę również zobowiązany za sformułowanie przez Pana Prezesa opinii na temat innych, przyjętych w postępowaniu ustawodawczym, rozwiązań mogących mieć wpływ na prywatność jednostki.

Łączę wyrazy szacunku
Adam Bodnar
Rzecznik Praw Obywatelskich
/-podpisano elektronicznie/

Do wiadomości:
**Pan Marek Zagórski**
**Minister Cyfryzacji**
ePUAP

[2] Życie po kwarantannie – przetestuj ProteGO, https://www.gov.pl/web/cyfryzacja/zycie-po-kwarantannie--przetestuj-protego