Ręka państwa na gardle

Wielu ludzi w Polsce, (i nie tylko) łudzi się, że pomimo olbrzymiej przewagi organizacyjnej i medialnej opresyjnego systemu władzy, jest jeszcze możliwe jeszcze prowadzenie jakiejś działalności opozycyjnej. Niestety, to, co było realne jeszcze 20 lat temu, teraz wydaje się już niemożliwe. Państwo i jego służby, a nawet poszczególne korporacje na skutek rozwoju technologicznego pozyskały obecnie możliwości dogłębnego inwigilowania każdego obywatela, a nawet wstępnej automatycznej analizy pozyskanych danych. Dzięki temu dany ośrodek siły może szybko reagować na powstające kryzysy i znajdować skuteczne rozwiązania. Sprawujący władzę, bowiem nie mogą sobie obecnie pozwolić na pozostawienie bez opieki żadnego zakamarka przestrzeni publicznej. Tam czai się potencjalne zagrożenie. Opozycja musi być wykryta i unieszkodliwiona.
Dlatego też najważniejszym zadaniem służb medialnych nie jest informowanie obywateli, ale wyławianie potencjalnych źródeł zagrożeń i konkurencyjnych narracji, oraz analiza danych i likwidacja rozpoznanych wrogów.

Ważna jest też stała praca polegająca na promowaniu własnych kanałów informacyjnych, swoich liderów i ekspertów, tak, aby w chwilach różnych przesileń politycznych i informacyjnych mogli skutecznie przejąć najważniejsze narracje.

Wydaję się, że drugą najważniejszą rolą funkcjonariuszy jest umiejętność szybkiej reakcji – w taki sposób, aby do opinii publicznej nie przedostały się informacji inne niż te pożądane przez władze. Gdyby nawet takie się pojawiły, to ważne, aby

istniał zespół medialny, aktorski, naukowy mogący odpowiednio je wytłumaczyć manipulowanemu społeczeństwu.

MASOWI MANIPULATORZY

Najważniejsi są masowi – przemysłowi nadzorcy– wyspecjalizowane media, które kontrolują organizacyjnie najważniejsze kanały przekazu- internet, telewizję, radio i prasę. Pomimo szczytnych deklaracji o służbie publicznej i zaangażowanym dziennikarstwie, stały się one ośrodkiem dezinformacji społecznej, które w sposób masowy fałszują rzeczywisty stan rzeczy. Ich wrogą i negatywną rolę ujawniła tzw. „pandemia kowid", gdzie widzieliśmy jak na polecenie zewnętrznych decydentów tworzyły fałszywe mity, które później posłużyły do masowego ogłupiania społeczeństwa. Na przykład w Polsce wprowadzono tzw. lockdown (zamkniecie całego państwa) po zaledwie 20 stwierdzonych tzw. „przypadkach kowida", co wówczas na pewno nie było żadną epidemią. Następnie te same media prawie dwa lata stale i sztucznie nakręcały terror miseczkowy i szczepionkowy. I robiły to dosłownie wszystkie – of TVP do Radia Maryja.

Obecnie, w czasie konfliktu na Ukrainie również dostrzegamy, że oficjalne narracje zupełnie rozmijają się z prawdą i nie służą informowaniu ogółu społeczeństwa, ale jakimś zewnętrznym celom politycznym czy też obcym korporacjom. Celowo spreparowane – fałszywe narracje przyczyniają się do poważnych szkód gospodarczych i de facto przeszkadzają zwykłym ludziom we właściwej ocenie sytuacji w swoim otoczeniu. Nie ma tutaj czasu na analizowanie przyczyn tego stanu rzeczy. Faktem jest, że sterowanie jak i finasowanie większości mediów jest zupełne oderwane od wpływu społeczeństwa, które nie dysponuje ono żadnymi mechanizmami ich kontroli. Społeczeństwo staje się wyłącznie przedmiotem, którym się manipuluje. Masowe media mają za zadnie urobić informacyjnie szerokie masy odbiorców – przeciętnych Kowalskich i narzucić większości zaprogramowane wcześniej narracje wyznaczone wcześniej przez decydentów.

Robią to bardzo skutecznie i niemal bez przeszkód. W Polsce nie ma żadnych procedur chroniących obywateli przez negatywnym wpływem sterowanych zewnętrznie mass-mediów.

SKANALIZOWANE ORGANIZACJE

Partie polityczne w Polsce to kolejne przymusowe kanały, do których zapędza się ludzi pragnących działać społecznie. Obserwujemy tutaj sytuację podobną do tej w mediach, jednakże z uwagi na wagę partii w procesie sprawowania władzy, kontrola zewnętrzna jest zwielokrotniona. Nadzorcy zewnętrzni ściśle selekcjonują grono osób dopuszczonych do rytuałów demokratycznych (elekcji). Fasadowość systemu wyraźnie widać na pierwszy rzut oka. Nic, bowiem nie rodzi się tutaj demokratycznie z dołu. Wszystko – zarówno idee jak i finasowanie jest narzucane z góry i przydzielane starannie dobranym funkcjonariuszom. Dla plebsu istnieje dosyć wąski zakres potencjalnych wyborów- tzw. lewica lub tzw. prawica. Ideologia jak najbardziej ogólna, z reguły – bez najważniejszych – ekonomicznych szczegółów. Krzykliwe hasła i 100 % populizmu. Zupełna gwarancja, ze absolutnie nikt nie przebije się z jakimś niewygodnym pomysłem. W zamian za pilnowanie interesu i nie zadawanie pytań, nadzorcy pozwalają kadrze intensywnie grabić miejscowych. Wydaje się, że nikt niezależny nie ma obecnie szansy, jako opozycja przebić się do głównego nurtu polityki. Ostatnim, któremu to się udało był Andrzej Lepper. Obecnie prawie wszystkie bez wyjątku partie to organizacje zrzeszające posłusznych, bezpruderyjnych funkcjonariuszy, którzy za obietnice o charakterze finansowym godzą się na wszystkie możliwe podłości i zdrady.

„MAGNESY” DLA OPORNYCH

Nie każdego da obłaskawić jakimś stanowiskiem lub przekonać bezmyślną mainsteamową propagandą. W każdym społeczeństwie istnieje grupa tzw. wiecznych opozycjonistów i osób, które są

ostrożne i nieufne, żyją w rozproszeniu – nie skupiają się w jakieś większe struktury. Dla tych pojedynczych „oporników" władza przygotowała zastępczych liderów, swego rodzaju „magnesy", które mają przyciągać wszystkie pozostałe jeszcze niezależne odpryski. Poznać ich można od razu, znają się na wszystkim i krzyczą najgłośniej. Ich rolą jest blokowanie, zagłuszanie tych wszystkich, którzy mogliby by stać się naturalnymi liderami środowisk niezależnych. „Magnesy" tak jak i wcześniej wymienione mechanizmy kontroli narzucane są z góry. Dysponują najczęściej znacznymi środkami finansowymi i przychylnością w mediach. Swoje prawdziwe poglądy ujawniają rzadko. Robią to tylko w razie zagrożenia dla całego systemu władzy.

RODZI SIĘ NOWE

Stary model państwa odchodzi powoli do lamusa. Stale rozwijany jest model totalitarny mający swój pierwowzór w hitlerowskich Niemczech. Inaczej się nie da. Tylko w ten sposób władza może zmobilizować wszystkie zasoby, którymi dysponuje, aby obronić się przez zewnętrza ingerencją i po prostu przetrwać. Dotyczy to nie tylko takich państw, jak Polska. Nawet tak silne kraje, jak Francja czy Niemcy mają obecnie potężne problemy, aby nie dać się do końca zdominować przez największych graczy. Zewnętrzna agresja wymaga skupienia wszystkich sił państwa. Dlatego też nie ma sensu udawać, że będą dalej istnieć jakieś reguły demokratyczne i fair play. To nieprawda. Zadecyduje brutalna siła i zewnętrzne poparcie grup interesariuszy. Kto ma większe zasoby zmobilizowanej siły – wygrywa i decyduje o życiu i losie przegranych. Będzie mniej tradycyjnych swobód i wolności a coraz więcej kontroli i inwigilacji. Dawni dziennikarze odeszli do lamusa. Nowi funkcjonariusze medialni będą jedynymi zarządcami obowiązujących narracji. Państwo zaproponuje także samo jedyne formy zrzeszania się i działalności partyjnej. Stosowne gremia wyznaczą także najlepszych opozycjonistów i bezpieczne dla władzy formy kanalizowanego oporu. Witamy w nowym wspaniałym świecie!

Piotr Panasiuk

Rząd USA planuje opracować sztuczną inteligencję, która zdemaskuje anonimowych internautów

Wirtualne „odciski palców”?

Biuro Dyrektora Wywiadu Narodowego ogłosiło, że organizacja IARPA pracuje nad programem mającym na celu zdemaskowanie anonimowych pisarzy poprzez wykorzystanie AI do analizy ich stylu pisania, który jest postrzegany jako potencjalnie tak unikalny jak odcisk palca.

> *Ludzie i maszyny codziennie produkują ogromne ilości tekstu. Tekst zawiera cechy językowe, które mogą ujawnić tożsamość autora.*

IARPA uważa, że jeśli się uda, program Human Interpretable Attribution of Text Using Underlying Structure (HIATUS) mógłby zidentyfikować styl pisarza na podstawie różnych próbek i zmodyfikować te wzorce w celu dalszej anonimizacji pisma.

Identyfikacja autora przez tekst

Kierownik programu HIATUS dr Timothy McKinnon oznajmił:

> *Mamy duże szanse na osiągnięcie naszych celów, dostarczenie bardzo potrzebnych możliwości Wspólnocie Wywiadowczej i znaczne poszerzenie naszego zrozumienia zmienności ludzkiego języka przy użyciu najnowszych osiągnięć lingwistyki obliczeniowej i uczenia głębokiego.*

Powiedziano, że HIATUS może mieć wiele zastosowań, w tym zwalczanie działań związanych z wpływami zagranicznymi, "ochronę autorów" oraz identyfikację zagrożeń dla kontrwywiadu. Według McKinnona program może zidentyfikować, czy tekst został wygenerowany przez maszynę, czy napisany przez człowieka.

Źródło

Izraelska firma od oprogramowania szpiegującego Pegasus przechodzi reorganizację biznesowo – wizerunkową

Niesławna izraelska NSO Group, która była wielokrotnie przyłapana na sprzedawaniu oprogramowania szpiegującego w celu hakowania elektroniki służbom wywiadowczym kilku krajów, ogłosiła, że w ramach reorganizacji na dużą skalę firma nie tylko zmieni prezesa, ale także zawęzi krąg potencjalnych nabywców jej rozwiązań. W lipcu ubiegłego roku śledztwo z udziałem dziennikarzy z całego świata ujawniło, że NSO sprzedawało agencjom wywiadowczym na całym świecie oprogramowanie Pegasus, które było następnie wykorzystywane do szpiegowania obrońców praw człowieka, dziennikarzy, polityków i działaczy różnych wyznań. Doszło do tego, że Stany Zjednoczone nałożyły na firmę surowe sankcje.

Według rzecznika NSO firma zostanie zreorganizowana, a jej szef Shalev Hulio odejdzie. Dyrektor operacyjny NSO Yaron Shohat przejmie zarządzanie. Podczas reorganizacji wszystkie aspekty działalności firmy zostaną ponownie ocenione. Oprogramowanie szpiegujące Pegasus służy do infekowania smartfonów, wydobywania z nich danych, zdalnej aktywacji kamer i mikrofonów. Grupa NSO twierdzi, że oprogramowanie jest sprzedawane departamentom rządowym w celu zwalczania przestępców i terrorystów, a przed sprzedażą wymagana jest zgoda władz izraelskich. Okazuje się, że oprogramowanie pomogło już uratować wiele istnień ludzkich w różnych krajach. Jednocześnie NSO podkreśla, że nie kontroluje dokładnie, w jaki sposób klienci korzystają z Pegasusa.

Po zeszłorocznej aferze okazało się, że jeszcze przed medialnym szumem i sankcjami USA wyniki finansowe NSO pozostawiały wiele do życzenia. Wcześniej w mediach pojawiły się dokumenty sądowe, zgodnie z którymi wierzyciele firmy

upierali się, aby firma nadal sprzedawała oprogramowanie do krajów o „wysokim ryzyku” łamania praw człowieka w celu utrzymania rentowności, a Berkeley Research Group (BRG), będący większościowym udziałowcem „matki” spółki NSO, zażądał zaprzestania podejrzanej sprzedaży, z powodu której deweloper był prześladowany w Stanach Zjednoczonych.

Według Julio firma „reorganizuje się, aby przygotować się do następnej fazy wzrostu”. Nazwał Shohat „właściwym wyborem” i stwierdził, że technologie firmy „będą nadal pomagać ratować życie na całym świecie”. Shohat z kolei powiedział, że NSO zadba o to, aby jej technologie były wykorzystywane do „uzasadnionych i godnych celów”.

W międzyczasie ujawniane są coraz to nowe fakty związane z użytkowaniem oprogramowania Pegasus. Pod koniec lipca Komisja Europejska poinformowała o wykryciu infekcji oprogramowaniem szpiegującym urządzeń niektórych czołowych liderów UE. Również w zeszłym miesiącu pojawiły się doniesienia, że narzędzia Pegasusa były wykorzystywane do szpiegowania aktywistów w Tajlandii podczas antyrządowych protestów.

Źródło

ArriveCan czyli narzędzie Wielkiego Brata

Aplikacja ArriveCan – jak się okazuje może zostać z nami na stałe. Rząd twierdzi, że jest to bardzo użyteczne narzędzie dla przyspieszenia procesu przekraczania granicy.

ArriveCan rzekomo sprawdza przyjeżdżających podróżnych pod kątem COVID-19 i śledzi stan szczepień. Odmowa użycia aplikacji może skutkować grzywną w wysokości do 5000 dol. na mocy ustawy o kwarantannie.

W raporcie federalnego audytora generalnego z grudnia 2021 r. stwierdzono, że aplikacja ArriveCan **poprawiła jakość informacji zbieranych przez rząd na temat podróżnych**. Jednak słaba jakość danych oznaczała, że prawie **138 000 wyników testu COVID-19 nie można było przypisać do przyjeżdżających podróżnych**, **a tylko 25 procent podróżnych, którym nakazano poddać się kwarantannie w zatwierdzonych przez rząd hotelach, zostało zweryfikowanych, że w nich rzerczywiście przebywało.**

W zeszłym miesiącu, z powodu błędu ArriveCan poinstruowała około 10 200 podróżnych, aby poddawali się kwarantannie przez 14 dni mimo, że nie musieli tego robić. Wielu krytykuje dlaczego te decyzje są zautomatyzowane i pierwszeństwo ma to co nakazuje aplikacja nie to co wynika z danych.

Ostatnie aktualizacje ArriveCan aplikacji skupiły się na rozszerzenie jej aplikacji, a nie na środkach zdrowia publicznego. Na lotniczych przejściach granicznych można teraz przy jej pomocy, wypełnić formularz zgłoszenia celnego przed przybyciem na lotnisko Toronto Pearson, Vancouver lub Montreal.

W zeszłym tygodniu rząd poinformował, że planuje rozszerzyć tę funkcję o przyloty do Calgary, Edmonton, Winnipeg, Ottawy, Quebec City, Halifax na lotnisko Billy Bishop Toronto City.

Elektroniczne gromadzenie danych związanych jest obowiązkowe na wielu granicach międzynarodowych, a formularze internetowe są coraz częściej wykorzystywane z powodów niepandemicznych. Australia obsługuje swoje elektroniczne zezwolenia na podróż

wyłącznie za pośrednictwem aplikacji online, podczas gdy od przyszłego roku będzie wymagany formularz zezwolenia online do odwiedzenia Unii Europejskiej .

Kanadyjscy urzędnicy mogą planować coś podobnego. Minister bezpieczeństwa publicznego Marco Mendicino powiedział dziennikarzom w czerwcu, że chociaż ArriveCan została stworzona dla COVID-19, *„ma możliwości technologiczne, aby naprawdę skrócić czas potrzebny na kontrolę na granicy”.*

Przed pandemią Kanada rozpoczęła już cyfryzację swoich usług granicznych za pomocą innych inicjatyw, w tym instalowania kiosków celnych na głównych lotniskach począwszy od 2017 r. i wprowadzenia w 2018 r. aplikacji eDeclaration.

Wysocy rangą przedstawiciele administracji federalnej przyznają wprost, że Ottawa wykorzystuje COVID-19 jako okazję do przyspieszenia przejścia na digitalizację obsługi kontroli przemieszczania się ludzi. Rząd federalny wykorzystuje kryzys zdrowia publicznego, aby przyzwyczaić ludzi do zmodernizowanej granicy.

Według Pierre’a St-Jacquesa, rzecznika Imigracji i Unii Celnej, **około jedna czwarta osób, które wjeżdżają do Kanady samochodem z USA, nie używa wcześniej ArriveCan.**

Kanadyjska Agencja Służb Granicznych potwierdziła, że **na granicy lądowej kanadyjsko-amerykańskiej obowiązuje jednorazowe zwolnienie dla podróżnych,** którzy „mogli być nieświadomi” przepisów. Z pięciu milionów przepraw między 24 maja a 4 sierpnia zwolnienie to zostało użyte 308 800 razy, podała CBSA.

Jest to tylko tymczasowe rozwiązanie, powiedział St-Jacques, ponieważ funkcjonariusze, którzy już czują się przeciążeni z powodu braków kadrowych, stają się „konsultantami IT” i rozwiązują problemy techniczne podróżnych, zamiast robić to, do czego zostali przeszkoleni. *„Jeśli celem aplikacji jest zwiększenie wydajności lub bezpieczeństwa podróży*

transgranicznych, to obecnie nie działa” – dodaje

Burmistrzowie miast przygranicznych, izby handlowe miast przygranicznych, a nawet sklepy wolnocłowe skarżą się, że ArriveCan, wraz z innymi ograniczeniami odstrasza amerykańskich turystów.

Tymczasowa przywódczyni federalnych konserwatystów Candice Bergen napisała we wtorek na Twitterze, że ArriveCan stworzył „niepotrzebne przeszkody” i „ szkodzi kanadyjskiej gospodarce i branży turystycznej”.

Kandydatka na konserwatywne przywództwo Leslyn Lewis twierdzi że jest to „eksperyment nadzorowania populacji”.

Komisarz ds. prywatności bada również skargę dotyczącą gromadzenia i wykorzystywania danych osobowych przez aplikację.

Źródło

Cyfrowa tożsamość czyli całkowita kontrola

Raport rządu federalnego Kanady informuje, że kolejnym krokiem w kierunku rozwoju cyfrowej infrastruktury jest wprowadzenie „Programu tożsamości cyfrowej”. Zostało to ujawnione w

rządowym raporcie opublikowanym 4 sierpnia zatytułowanym Canada's Digital Ambition 2022, o czym jako po raz pierwszy doniósł portal „True North".

Pandemia COVID-19 podkreśliła potrzebę, aby usługi rządowe były „dostępne w erze cyfrowej" – czytamy w raporcie. „Następnym krokiem w zwiększaniu wygody dostępu do usług jest federalny program tożsamości cyfrowej, zintegrowany z istniejącymi wcześniej platformami prowincyjnymi" – czytamy. „Tożsamość cyfrowa jest elektronicznym odpowiednikiem uznanego dokumentu potwierdzającego tożsamość (na przykład prawa jazdy lub paszportu) i potwierdza, że „jesteś tym, za kogo się podajesz" w kontekście cyfrowym".

Rząd Ontario ogłosił w zeszłym roku, że stworzy cyfrowe identyfikatory w ramach odpowiedzi prowincji na COVID-19 i ma na celu stać się „najbardziej zaawansowaną cyfrową jurysdykcją na świecie".

Zdaniem krytyków każdy rodzaj cyfrowego identyfikatora może prowadzić do chińskiego systemu kredytów społecznych, który ocenia obywateli w oparciu o wiarygodność wobec państwa.

Tymczasem rząd Alberty już w kwietniu opublikował ogłoszenie o pracę dla dyrektora wykonawczego platform do nadzorowania usług tożsamości cyfrowej.

Ankieta Digital Identity and Authentication Council of Canada przeprowadzona w grudniu 2020 r. wykazała, że 49 procent Kanadyjczyków zna pojęcie tożsamości cyfrowej, a 88 procent popiera tę koncepcję. Kolejne 83 procent respondentów stwierdziło, że ufa rządom w zakresie ochrony danych osobowych, a 76 procent Kanadyjczyków stwierdziło, że byliby skłonni udostępniać więcej danych osobowych online, gdyby oznaczało to większą wygodę.

Rząd ujawnił również, że współpracuje z liniami lotniczymi, aby wprowadzić posiadanie „cyfrowych dokumentów tożsamości" i wymóg danych biometrycznych, takich jak rozpoznawanie twarzy,

by móc wejść na pokład, informował w maju portal „True North”.

Autorstwo: Andrzej Kumor
Źródło: Goniec.net

Norwegia chce śledzić zakupy żywności obywateli

To już się dzieje. Norwegia zmierza w kierunku społeczeństwa całkowicie kontrolowanego, gdzie państwo chce wiedzieć wszystko, co robisz.

Wcześniej pisano o tym, że Norwegia jest wiodącym krajem, jeśli chodzi o cyfrowy dowód osobisty. Jest to niemalże konieczność, aby prowadzić nowoczesne życie. Ludzie muszą go używać do bankowości internetowej i wielu innych rzeczy. Teraz okazuje się, że Norwegia chce mieć jeszcze większą kontrolę nad obywatelami. Centralne Biuro Statystyki Państwowej (SSB) w Norwegii żąda obecnie wiedzy na temat zakupów żywności przez obywateli i śledzenia wszystkich płatności kartą.

Biuro to odegrało kluczową rolę w tworzeniu „rejestru ludowego” w Norwegii po drugiej wojnie światowej, dzięki czemu ludzie otrzymali unikalny numer identyfikacyjny zwany „numerem urodzenia”. Biuro to już wie, gdzie ludzie mieszkają i jakie mają dochody, ale teraz chce również śledzić dokładnie wszystko, co kupujesz w sklepie spożywczym. Chcą znać każdy

pojedynczy artykuł spożywczy, który kupujesz. Państwo norweskie chce dosłownie wiedzieć, co jadłeś na obiad!

To idzie za daleko. To ostatnie posunięcie jest w istocie bardzo daleko idącym krokiem w kierunku społeczeństwa kontrolowanego. Idziemy teraz pełną parą do przodu. Prawie wszystkie duże sieci sklepów spożywczych w Norwegii muszą udostępniać państwu dane dotyczące paragonów. Wymogły również na firmie obsługującej terminale kart płatniczych, zwanej Nets, udostępnianie państwu szczegółowych informacji o wszystkich transakcjach. Około 80% płatności kartą w sklepach spożywczych w Norwegii odbywa się za pośrednictwem tej właśnie firmy. „Sprzężenie z transakcjami płatniczymi dokonywanymi kartą debetową i paragonami sklepów spożywczych pozwala SSB [państwowemu biuru statystycznemu] połączyć transakcje płatnicze i paragony w ponad 70% codziennych zakupów spożywczych" – podało państwowe biuro w oświadczeniu na swojej stronie internetowej.

Spróbujcie to sobie wyobrazić! Norwegia zamierza połączyć szczegóły płatności dokonywanych kartą z paragonami ze sklepów spożywczych, aby dowiedzieć się dokładnie, jaki rodzaj żywności ludzie kupują i kto ją kupuje. Innymi słowy, Norwegia będzie śledzić dokładnie, jaki rodzaj żywności kupują obywatele. Mówimy tu o nowym poziomie kontroli państwowej.

Państwo będzie wiedziało, co jadłeś na śniadanie, obiad, kolację, wszystko. Cola, szynka, kurczak, stek, jak kto woli. Państwo będzie to wszystko widzieć. Państwo będzie śledzić wszystkie płatności Norwegii. Mówimy tu o ogromnych ilościach danych. Państwowy urząd statystyczny będzie zbierał 2,4 miliona paragonów KAŻDEGO dnia i jakieś 1,6 miliarda transakcji kartami rocznie. Aha, i jeszcze to. Te dane nie zostaną usunięte po ich zebraniu, jak podaje NRK.

Dane te zostaną następnie połączone z paragonami ze sklepu i wykorzystane do ustalenia, co dokładnie ludzie kupili. To jest przerażające!

Tak więc nie tylko państwo zbiera dane o wszystkich transakcjach kartą i łączy je z paragonami ze sklepów, aby dowiedzieć się, co dokładnie kupujesz, ale także będzie przechowywać te dane w nieskończoność. Państwo chce wiedzieć o tobie wszystko!

Jedna z sieci sklepów spożywczych o nazwie NorgesGruppen jest bardzo niezadowolona z tego nowego śledzenia, mówiąc, że złoży skargę w tej sprawie, ponieważ twierdzi, że jest to „bardzo inwazyjne w odniesieniu do danych osobowych naszych klientów, że nie możemy się na to zgodzić bez zwrócenia się o wskazówki do Datatilsynet [organu ochrony danych osobowych w Norwegii]".

Nawet Nets, firma zajmująca się płatnościami kartami jest krytyczna wobec tego procederu, twierdząc, że takie śledzenie może być „problematyczne i inwazyjne dla poszczególnych obywateli".

Urząd Statystyczny twierdzi, że informacje te mogą być wykorzystane między innymi przez władze zdrowotne do obliczenia rozwoju konsumpcji żywności w Norwegii i sprawdzenia, jak to się różni w poszczególnych obszarach geograficznych. Mówią, że jest to ważne, aby znaleźć „regionalne, demograficzne i społeczne różnice w konsumpcji żywności". Ponadto twierdzą, że te informacje o płatnościach mogą być wykorzystane do uzyskania statystyk o tym, którzy obywatele korzystają z prywatnej opieki zdrowotnej i ile pieniędzy na nią wydają.

Więc nie tylko zamierzają śledzić zakupy żywności przez obywateli, ale także śledzą inne rzeczy, takie jak osoby płacące za prywatną opiekę zdrowotną (w przeciwieństwie do korzystania z publicznej opieki zdrowotnej, która zresztą również sporo kosztuje w Norwegii). To jest torowanie drogi do społeczeństwa totalnej kontroli. (…) To, co widzimy obecnie, jest bardzo przerażające. Państwo próbuje zdobyć całkowitą kontrolę nad życiem ludzi i mikrozarządzać każdym drobnym szczegółem ich życia.

Jedynym sposobem na odrzucenie śledzenia zakupów przez państwo będzie użycie gotówki. Ale pytanie brzmi, jak długo będzie to dozwolone, ponieważ społeczeństwo bezgotówkowe jest coraz bardziej forsowane. A teraz może zaczniecie rozumieć, dlaczego to bezgotówkowe społeczeństwo jest forsowane… Aby państwo mogło kontrolować wszystko, co robicie. (…)

Źródło

Prawie wszystkie rządowe witryny informacyjne dotyczące COVID są tajnymi operacjami SZPIEGOWSKIMI

Europejscy naukowcy opracowali badanie ujawniające, że rządowe witryny informacyjne dotyczące (COVID-19 są koszmarem naruszającym prywatność – *niech opinia publiczna się strzeże*!

Dokument zatytułowany „Pomiar plików cookie w witrynach rządowych”, finansowany przez Europejską Radę ds. Badań Naukowych (ERC), Unię Europejską (UE) i rząd hiszpański, wyjaśnia, że witryny rządowe są zasadniczo wykorzystywane jako „pojedynczy punkt” monitorowania i śledzenia całej populacji kraju” za pomocą plików cookie.

Badacze przyjrzeli się trzem różnym rodzajom stron internetowych, w tym oficjalnym rządowym stronom internetowym krajów „G20” na całym świecie; strony internetowe organizacji międzynarodowych, takich jak ONZ; oraz popularne strony internetowe wykorzystywane przez społeczeństwo do śledzenia i informacji o Grypie Fauciego. Przyjrzeli się wykorzystaniu plików cookie w każdej witrynie i doszli do wniosku, że ponad 90 procent witryn rządowych „tworzy pliki cookie zewnętrznych modułów śledzących bez zgody użytkowników”.

„Ciasteczka internetowe były wykorzystywane do zbierania informacji o aktywnościach i zainteresowaniach użytkowników w Internecie” – wyjaśnia gazeta.

„Niesesyjne pliki cookie, które są tworzone przez moduły śledzące i mogą trwać przez kilka dni lub miesięcy, są powszechnie obecne nawet w krajach, w których obowiązują surowe przepisy dotyczące prywatności użytkowników. Pokazujemy również, że powyższe jest problemem dla oficjalnych stron internetowych organizacji międzynarodowych oraz popularnych serwisów, które informują opinię publiczną o pandemii COVID-19”.

Oto wskazówka: w pierwszej kolejności nie odwiedzaj żadnych rządowych witryn COVID, a nie będziesz śledzony

Innymi słowy, największe gospodarki świata angażują się w nieujawnione i potencjalnie nielegalne programy szpiegowskie i inwigilacyjne za pośrednictwem oficjalnych rządowych stron internetowych, z których społeczeństwo korzysta, aby dowiedzieć się o COVID i angażować się w inne formy konsumpcji propagandy.

Spośród 5550 rządowych witryn internetowych i ponad 118 000

adresów URL administrowanych przez rządy ponad 50 procent ich plików cookie należy do stron trzecich, podczas gdy od 10 do 90 procent pochodzi od znanych trackerów.

„Większość z tych ciasteczek ma żywotność dłużej niż jeden dzień, a wiele z nich wygasa rok lub dłużej" – ujawnia badanie.

Około 60 procent witryn rządowych używa co najmniej jednego pliku cookie stron trzecich, a 95 procent lub prawie *wszystkie* tworzy pliki cookie bez zgody użytkownika. Nawiasem mówiąc, pliki cookie stron trzecich są „znane z tego, że śledzą użytkowników w celu gromadzenia danych", wyjaśnia badanie.

Rządowe strony internetowe dotyczące chińskiego wirusa są najgorszymi przestępcami, ponieważ 99 procent zawiera ukryte pliki cookie, które zostały tam umieszczone bez zgody użytkownika.

„Na przykład bardzo popularna strona internetowa z globalnymi mapami dotyczącymi przypadków COVID-19, prowadzona przez *Johns Hopkins University*, dodaje pliki cookie z 7 trackerów" – czytamy dalej.

„Wszystkie pozostałe witryny Top 10 to oficjalne krajowe witryny informacyjne w krajach europejskich, które mają co najmniej trzy trackery. Amerykańskie Centra Kontroli i Zapobiegania Chorobom (CDC) również znajdują się w pierwszej dziesiątce, z plikami cookie powiązanymi z trzema trackerami".

Kiedyś tego typu rzeczy miały miejsce tylko w krajach jawnie komunistycznych, takich jak Chiny, które przodują w totalitaryzmie. Jednak ostatnio Stany Zjednoczone i inne mocarstwa zachodnie wydają się naśladować model Komunistycznej Partii Chin, narzucając w swoich krajach systemy typu „społecznej oceny kredytowej".

Grypa Fauciego szybko stała się powszechnym pretekstem do

naruszania prywatności ludzi, wymuszania pewnych restrykcyjnych zachowań, a nawet popełniania gwałtu medycznego w formie obowiązkowego maskowania i „szczepienia”.

Okazuje się, że nawet w sieci rząd łamie prawa ludzi i śledzi ich zachowanie bez pozwolenia. Pełny zakres powodów, dla których rząd chce śledzić zachowanie ludzi w Internecie, jeszcze nie został ujawniony.

Branża technologiczna opracowuje technologię AI czytającą w myślach, która jest w stanie mierzyć lojalność obywateli wobec rządu

Chińscy naukowcy twierdzą, że opracowali nową technologię sztucznej inteligencji (AI) zdolną do „czytania w myślach”.

The Sunday Times (Wielka Brytania) po raz pierwszy doniósł o dziwnej i niepokojącej technologii, która rzekomo zostanie wykorzystana do pomiaru lojalności obywateli wobec Komunistycznej Partii Chin.

Podobnie jak wiele innych technologii Orwellowskich, ta technologia AI kontroli umysłu prawdopodobnie przejdzie test w komunistycznych Chinach, by ostatecznie zostać udostępniona reszcie świata.

Usunięte wideo i powiązany artykuł z Chińskiego Kompleksowego Narodowego Centrum Nauki w Hefei wyjaśniają, że technologia AI może analizować mimikę twarzy i fale mózgowe ludzi narażonych na „myśli i polityczną edukację" KPCh, znaną również jako *propaganda*.

Jak wyjaśnili naukowcy, wyniki można następnie wykorzystać do „dalszego wzmocnienia ich pewności siebie i determinacji, aby być wdzięcznym partii, słuchać partii i podążać za partią".

Business Insider poinformował, że wideo i artykuł wyjaśniające to wszystko zostały usunięte z Internetu po publicznym oburzeniu chińskich obywateli, którzy już teraz zmagają się z tyranią oceny kredytów społecznych i cenzurą internetową.

Stany Zjednoczone usankcjonowały kilka chińskich firm w 2021 r. za opracowanie „rzekomej broni kontrolującej mózg"

W artykule, który napisał dla *Forbesa*, ekspert od sztucznej inteligencji i uczenia maszynowego, dr Lance B. Eliot, zasugerował, że bez znajomości specyfiki technologii nie można stwierdzić, czy naprawdę działa tak, jak się twierdzi.

„Z pewnością nie jest to pierwszy raz, kiedy w badaniach naukowych wykorzystano funkcję skanowania fal mózgowych na ludziach" – powiedział.

„Mając to na uwadze, wykorzystywanie ich do mierzenia lojalności wobec KPCh nie jest czymś, na czym można by się skoncentrować. Kiedy taka sztuczna inteligencja jest

wykorzystywana do kontroli rządowej, przekraczana jest czerwona linia".

Komunistyczne Chiny były jednak w przeszłości usankcjonowane przez Departament Handlu USA za próby stworzenia podobnych technologii, w tym systemu biotechnologicznego opisanego jako „rzekoma broń kontrolująca mózg".

KPCh już wykorzystuje sztuczną inteligencję i systemy rozpoznawania twarzy do śledzenia i kontrolowania ujgurskich muzułmanów przetrzymywanych w obozach koncentracyjnych w całych Chinach. Aż trzy miliony Ujgurów jest przetrzymywanych w niewoli, wielu z nich jest torturowanych przy użyciu systemów sztucznej inteligencji.

„Naukowe dążenie do biotechnologii i innowacji medycznych może uratować życie" – powiedziała sekretarz handlu USA Gina M. Raimondo w komunikacie prasowym po sankcjach nałożonych na chińskie firmy AI w 2021 roku.

„Niestety [Chińska Republika Ludowa] decyduje się na wykorzystanie tych technologii do kontrolowania swoich obywateli i represjonowania członków mniejszości etnicznych i religijnych".

Jeśli Chiny osiągną swoje cele, powstanie potencjalnie światowa „tokracja AI" , pogrążająca miliardy ludzi w technokratycznej tyranii.

Według analityków, Chiny wielokrotnie wskazywały, że chcą wykorzystywać sztuczną inteligencję, duże zbiory danych, uczenie maszynowe i inne zaawansowane technologie, aby „dostać się do mózgów i umysłów swoich obywateli". *VOA News* nazywa plan Chin „drakońską dyktaturą cyfrową".

„Wykorzystała najnowocześniejszą technologię, aby wzmocnić swoje państwo partyjne", mówi Hung Ching-fu, profesor nauk politycznych na *National Cheng Kung University* na Tajwanie, o najnowszym przedsięwzięciu KPCh w zakresie sztucznej

inteligencji.

„Chiny przeszły z wczesnego rozpoznawania twarzy na programy AI, które próbują dostać się do mózgów i umysłów (bardziej) niż na pierwszy rzut oka. Przyjęcie przez Chiny zaawansowanej sztucznej inteligencji wzmocni całkowitą kontrolę”.

Innymi słowy, państwo policyjne napędzane sztuczną inteligencją jest w programie komunistycznych Chin, jak również każdego innego kraju, który adoptuje lub jest zmuszony do przyjęcia tych metod.

Już teraz kraje, które skłaniają się ku autokracji, a nie demokracji, importują technologię sztucznej inteligencji do rozpoznawania twarzy z Chin. Wydaje się, że rośnie rynek dla tych orwellowskich systemów w krajach, które stają się lub już są napędzane przez totalitaryzm.

Źródła:

BusinessInsider.com

NaturalNews.com

VOAnews.com

Jak zadbać o swoją prywatność, używając Androida

Jak bardzo trzeba się postarać, by ograniczyć ilość danych zbieranych przez producentów urządzeń z Androidem i firmę Google, która regularnie wydaje nowe wersje systemu? Pokazujemy krok po kroku, co trzeba zrobić, by zapewnić sobie więcej prywatności.

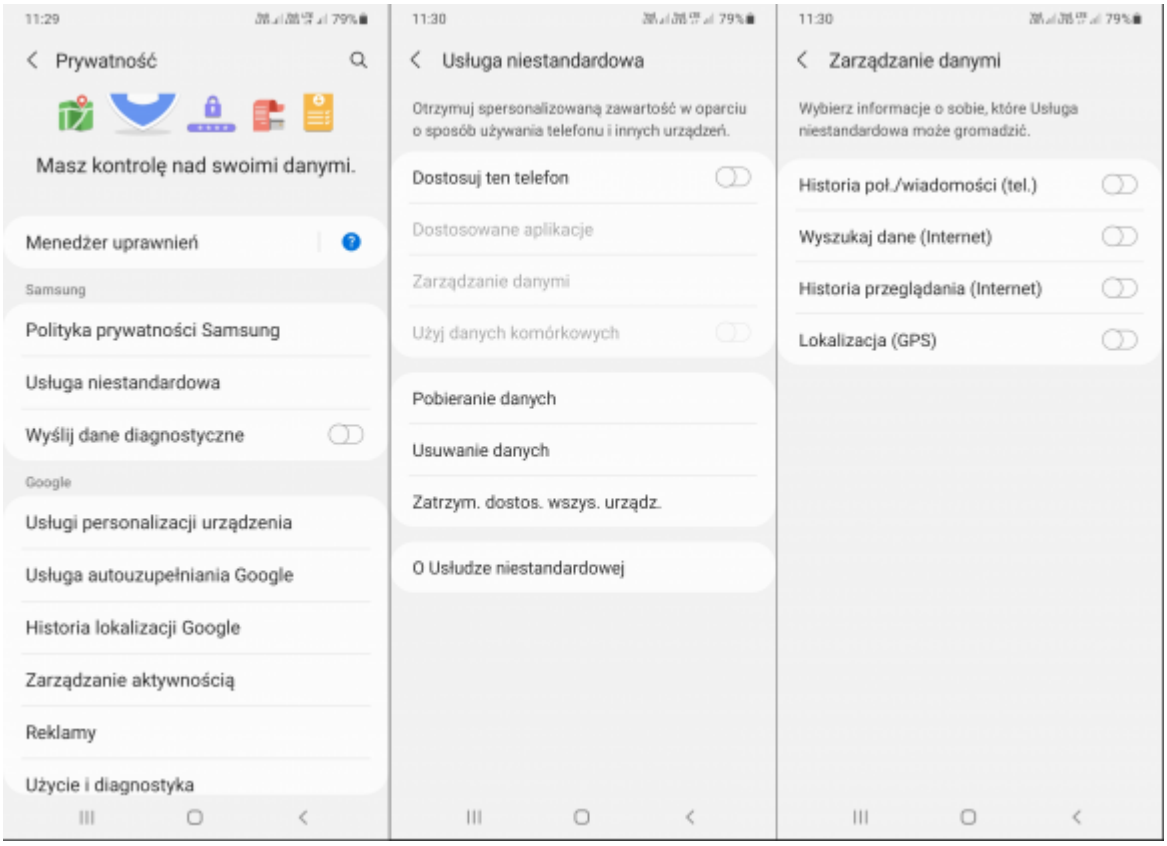
Twórcy Androida umieścili „Menedżera uprawnień" wśród ustawień mających wpływ na prywatność i rzeczywiście, szafując uprawnieniami na prawo i lewo, możemy nieopatrznie dać aplikacjom zbyt szeroki dostęp do naszych danych, tracąc tym samym część prywatności. Jak temu zaradzić, opisywaliśmy w jednym z wcześniejszych artykułów, w tym skupimy się więc na innych opcjach, które warto wziąć pod uwagę. Jak je skonfigurować, omówimy na przykładzie Galaxy M21 od Samsunga, działającego pod kontrolą Androida 11 z interfejsem One UI 3.1. Sprawdzimy też, co dodano w Androidzie 12 z One UI 4.1. Układ ustawień w telefonach z inną wersją systemu bądź nakładką innego producenta może odbiegać od tego, który pokazujemy, wiele opcji będzie jednak podobnych.

Jakie dane zbiera Samsung i co z tym zrobić

W polityce prywatności Samsung przyznaje, że „gromadzi informacje osobiste Użytkownika różnymi sposobami". Interesują go zarówno dane przekazywane bezpośrednio, np. podczas zakładania konta, zakupu którejś z płatnych usług czy kontaktu z obsługą klienta, jak i zbierane przez firmowe aplikacje, gdy korzystamy z naszego telefonu. W tym drugim przypadku chodzi nie tylko o podstawowe informacje o urządzeniu (jak model, IMEI, MAC, wersja systemu operacyjnego, numer telefonu czy adres IP), ale też o pliki cookie, dane pochodzące z logów, historię obejrzanych treści, nagrania naszego głosu (jeśli stosujemy polecenia głosowe), słowa wpisywane za pomocą klawiatury (gdy włączymy funkcję podpowiadania tekstu), informacje o lokalizacji itp. Jakby tego było mało, Samsung

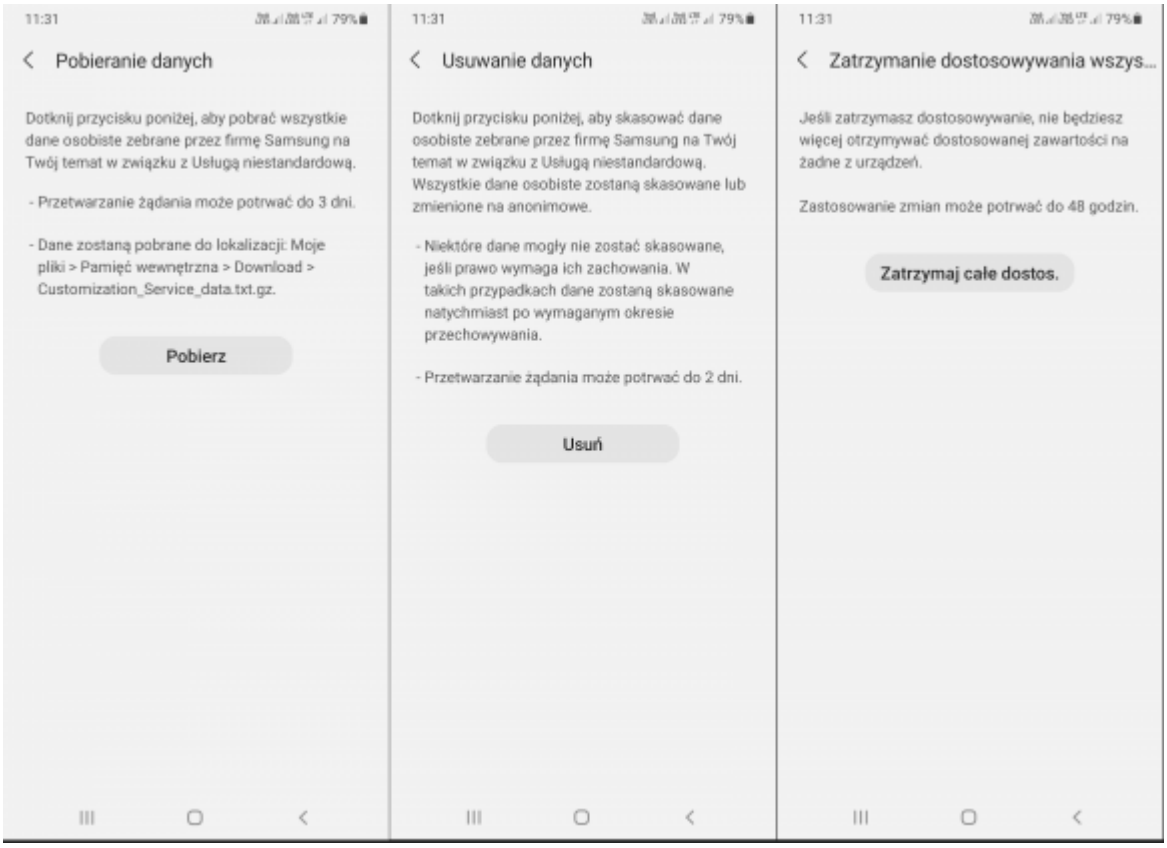
zbiera dane „dostępne publicznie lub za opłatą”, np. pochodzące z mediów społecznościowych – są one następnie łączone z innymi informacjami o użytkowniku danego smartfona. Firma nie stroni też od usług analitycznych zewnętrznych dostawców, jak Google Analytics.

Zgromadzone dane mogą być przekazywane licznym podmiotom, m.in. partnerom biznesowym Samsunga i współpracującym z nim usługodawcom, którzy dokonują napraw, przygotowują spersonalizowane reklamy itp. Informacje o konkretnych użytkownikach mogą być ujawniane „gdy wymaga tego prawo lub gdy jest to niezbędne do ochrony usług firmy Samsung”, jak również „na potrzeby organów ścigania, bezpieczeństwa narodowego, walki z terroryzmem lub innych kwestii związanych z bezpieczeństwem publicznym”. W polityce prywatności możemy przeczytać, że firma przechowuje dane użytkowników „Wyłącznie przez czas wymagany w celu, w jakim takie informacje zostały zgromadzone lub są przetwarzane, lub dłużej, jeśli wymaga tego jakakolwiek umowa, obowiązujące prawo, bądź w celach statystycznych, z zachowaniem odpowiednich zabezpieczeń”. Innymi słowy – nie wiadomo, jak długo i choćby z tego względu warto ograniczyć ilość przekazywanych Samsungowi danych. Dlatego sugerujemy np. nie używać dostarczanej wraz systemem przeglądarki, sugestywnie podpisanej jako „Internet” – lepszy będzie nawet Google Chrome (po włączeniu w ustawieniach „Piaskownicy prywatności”), ale można też pokusić się o zainstalowanie mobilnej wersji Firefoksa albo DuckDuckGo. Nie zaszkodzi też poszukać alternatywnych rozwiązań dla pozostałych narzędzi oferowanych przez producenta.



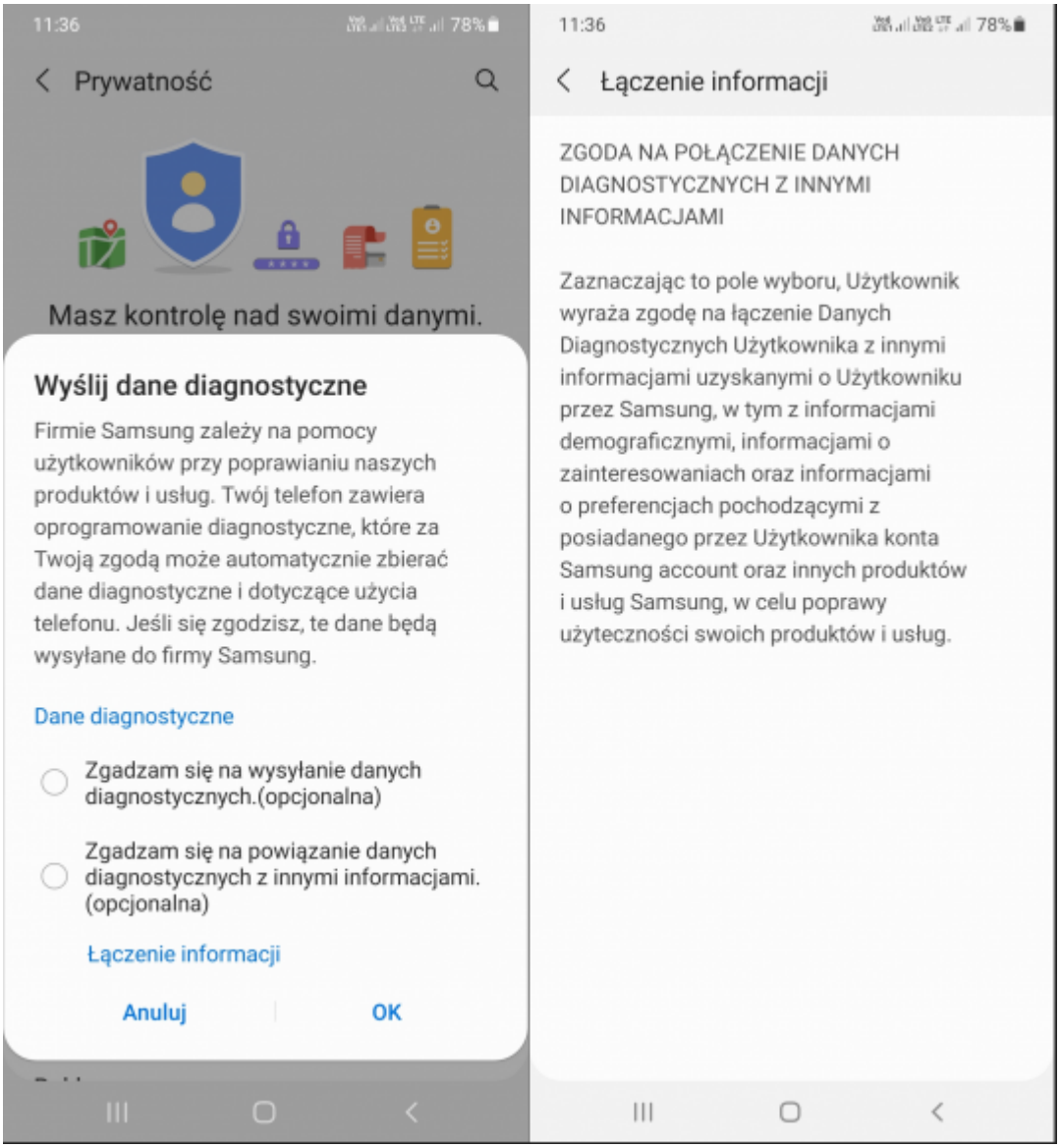
„Usługa niestandardowa” oferowana przez Samsunga

Po wejściu do ustawień telefonu w zakładce „Prywatność” znajdziemy ponadto pozycję „Usługa niestandardowa”, która odpowiada za dostarczanie reklam i innych treści w oparciu o nasze (rzekome) zainteresowania i odwiedzane przez nas miejsca w świecie rzeczywistym. Można ją skonfigurować po zalogowaniu się na założone wcześniej konto w usługach Samsunga. Jeśli opcja „Dostosuj ten telefon” zostanie aktywowana, to w sekcji „Zarządzanie danymi” będziemy mogli określić, czy usługa ma mieć dostęp do naszych połączeń i wiadomości, historii wyszukiwania i przeglądania oraz lokalizacji (ale nie są to jedyne zbierane przez nią informacje, o czym się przekonamy, zaglądając do odrębnej polityki prywatności). W sekcji „Dostosowane aplikacje” możemy z kolei wskazać, które z systemowych aplikacji będą z gromadzonych danych korzystać. Nasza rada? W ogóle tej usługi nie włączać.



Ujarzmianie „Usługi niestandardowej”

Jeśli nieopatrznie zrobiliśmy to wcześniej, możemy skorzystać z opcji „Pobieranie danych” i sprawdzić, czego dowiedział się o nas Samsung. Firma uprzedza, że przetwarzanie żądania może jej zająć nawet 3 dni, a interesujące nas informacje zostaną zapisane w folderze „Download” pod postacią pliku *Customization_Service_data.txt.gz*. Za pomocą opcji „Zatrzym. dostos. wszys. urządz.” możemy zrezygnować z otrzymywania spersonalizowanych treści, nie nastąpi to jednak od razu – zastosowanie zmian może potrwać do 2 dni. Podobnie mają się sprawy z usuwaniem gromadzonych przez usługę danych. Co gorsza, nie wszystkie zostaną skasowane z uwagi na bliżej nieokreślone wymogi prawne, o czym zostaniemy poinformowani przed naciśnięciem przycisku „Usuń”.



Zgoda na wysyłanie do Samsunga danych diagnostycznych

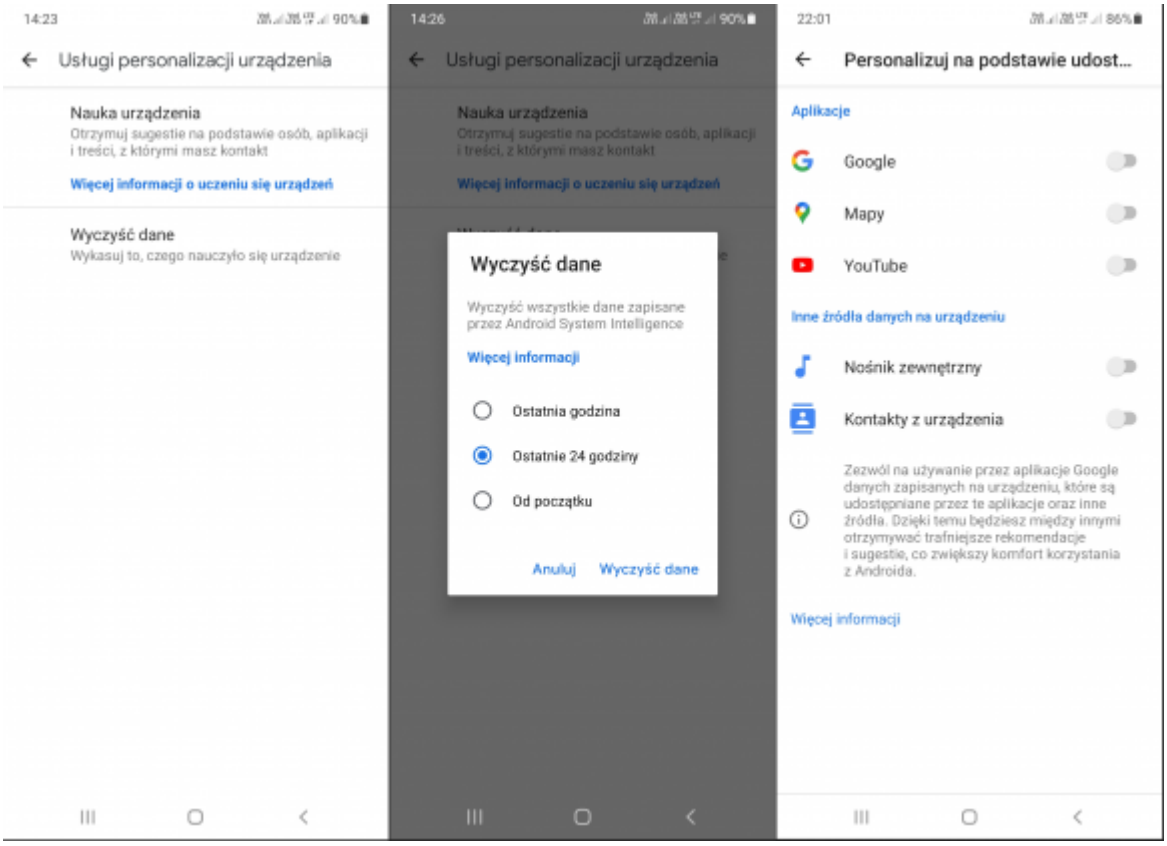
W zakładce „Prywatność” znajdziemy ponadto opcję wysyłania Samsungowi danych diagnostycznych, której również sugerujemy nie aktywować. Klikając w link „Dane diagnostyczne”, dowiemy się, że decyzja o nieprzekazywaniu firmie tego typu informacji nie wpłynie w żaden sposób na funkcjonalność telefonu. Producent zbiera je „w celu doskonalenia jakości produktów i usług oraz monitorowania przypadków i reagowania na przypadki niespodziewanych wyłączeń lub błędów systemu”. Jak widać na powyższym zrzucie ekranu, dane te za zgodą użytkownika mogą zostać powiązane z innymi informacjami o nim, które firma pozyskuje z różnych źródeł. Samsung zakłada, że cykl życia urządzeń przenośnych wynosi dwa lata i zapewnia, że po tym czasie informacje osobiste będą automatycznie usuwane (ale jak wiemy z polityki prywatności, nie brakuje od tej reguły

wyjątków).

Jeśli się zastanawiacie, czy inne firmy produkujące smartfony z Androidem gromadzą mniej danych albo obchodzą się z nimi lepiej, to odpowiedź brzmi „raczej nie”, o czym możecie się przekonać, zaglądając do ich polityk prywatności. Oto kilka przykładowych: Xiaomi, Huawei, Alcatel, Sony.

Ujarzmianie usług Google

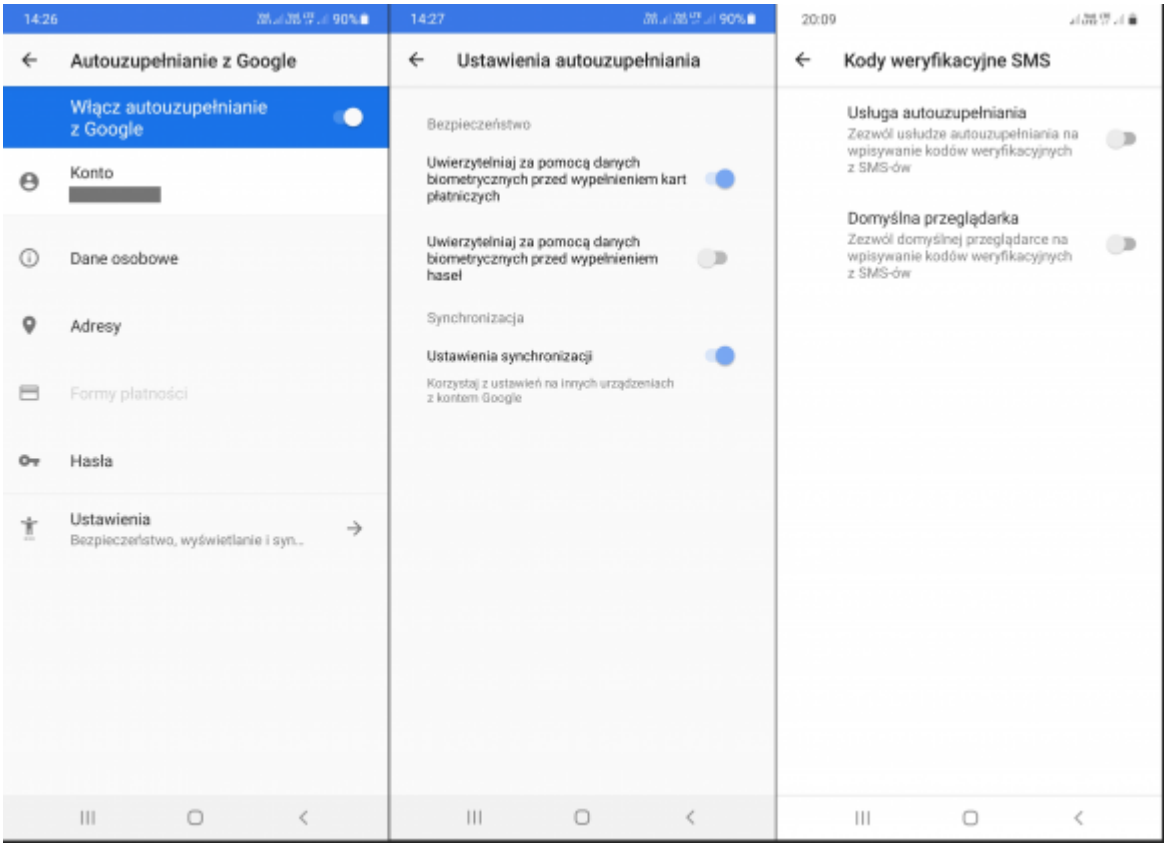
Przegląd ustawień prywatności związanych z usługami Google zaczynamy od możliwości personalizacji urządzenia i akurat w tym przypadku nie chodzi o wyświetlanie reklam, tylko o podpowiadanie użytkownikowi na podstawie jego wcześniejszych działań, co może w danej chwili zrobić. Jeśli np. zaznaczymy jakiś tekst, a Google rozpozna, że jest to nazwa restauracji, to możemy otrzymać sugestię otwarcia aplikacji Mapy i wyznaczenia trasy dojazdu. W zakładce „Prywatność” po wybraniu „Usług personalizacji urządzenia” możemy uzyskać więcej informacji na temat tej funkcji, a także usunąć zgromadzone dotychczas dane. W Androidzie 12 omawiana funkcja kryje się pod nazwą „Android System Intelligence” i pozwala dodatkowo włączyć inteligentne podpowiedzi w pasku sugestii klawiatury. W obu przypadkach, jeśli chcemy coś skonfigurować (czyli wskazać lub wykluczyć jakieś źródła danych), musimy się udać do zakładki „Google” i wybrać opcję „Personalizuj na podstawie udostępnionych danych”.



Usługi personalizacji urządzenia

Kolejna warta uwagi pozycja w zakładce „Prywatność” to „Usługa autouzupełniania Google” umożliwiająca automatyczne wpisywanie danych do formularzy, co jest – i owszem – wygodne, ale dostarcza producentowi Androida sporo wrażliwych informacji o użytkowniku. Jeśli włączymy tę funkcję, to po kliknięciu w „Dane osobowe” przeniesiemy się do sekcji zarządzania osobistymi informacjami na koncie Google, „Adresy” pozwolą nam ustawić adres domowy i służbowy w aplikacji Mapy, „Formy płatności” będą aktywne tylko po ich wcześniejszym skonfigurowaniu (w sekcji „Google” » „Ustawienia aplikacji Google” » „Google Pay”), a „Hasła” dadzą dostęp do wbudowanego menedżera haseł. Wybierając „Ustawienia”, będziemy mogli określić, czy chcemy uwierzytelniać się za pomocą biometrii przed wypełnieniem danych kart płatniczych i/lub haseł, a także zezwolić na synchronizację ustawień tej usługi na innych urządzeniach. Jeśli natomiast przejdziemy do sekcji „Autouzupełnianie” w zakładce „Google”, to znajdziemy tam m.in. opcję „Kody weryfikacyjne SMS”. Ze względów bezpieczeństwa nie powinniśmy zezwalać na wpisywanie kodów weryfikacyjnych z SMS-ów ani usłudze autouzupełniania, ani

domyślnej przeglądarce.

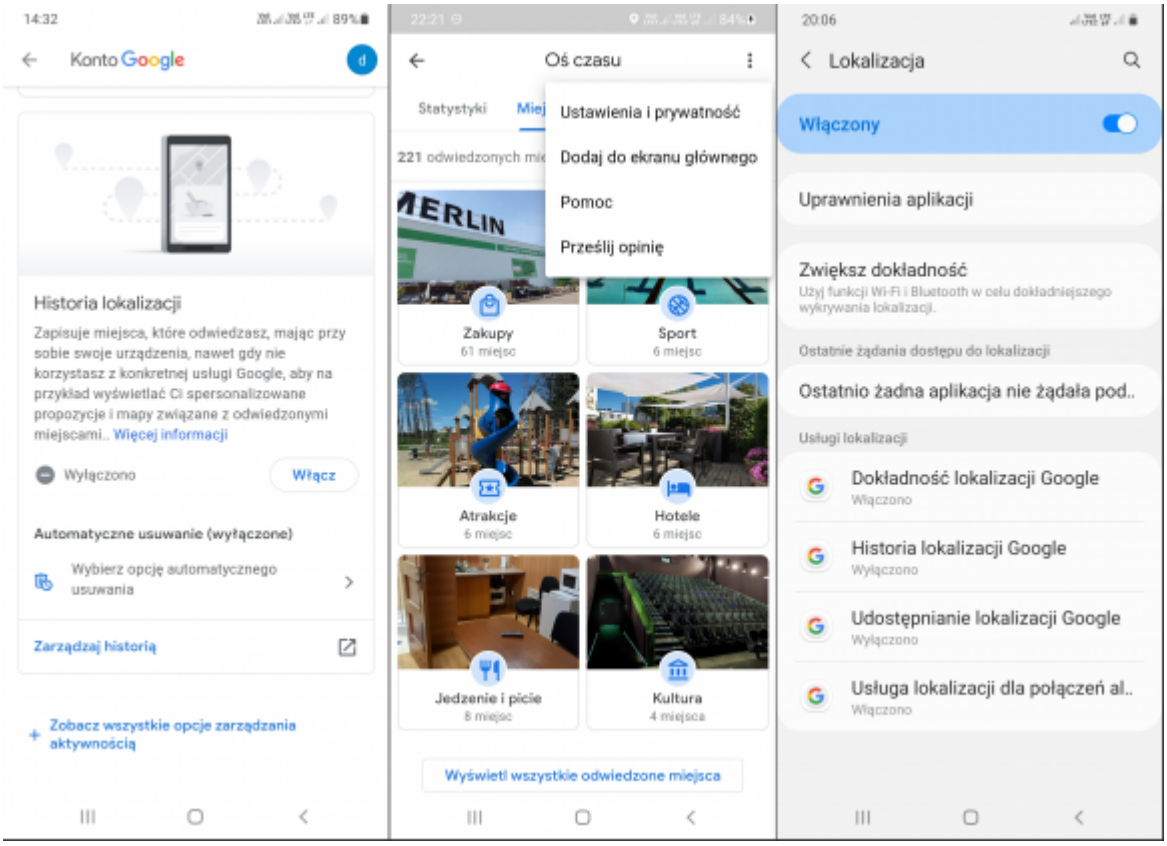


Ustawienia autouzupełniania

Przejdźmy teraz w zakładce „Prywatność” do sekcji „Historia lokalizacji Google”. Możemy ją od razu wyłączyć, lepszym pomysłem będzie jednak skorzystanie z opcji „Zarządzaj historią” i przejrzenie zapisanych przez firmę informacji o naszym przemieszczaniu się w świecie rzeczywistym. Klikając w trzy kropki widoczne po prawej stronie ekranu i wybierając „Ustawienia i prywatność”, uzyskamy m.in. możliwość usunięcia całej historii lokalizacji lub pewnego jej zakresu, a także skonfigurowania automatycznego usuwania gromadzonych danych – możemy w ten sposób na bieżąco kasować aktywność starszą niż 3, 18 lub 36 miesięcy.

Dodatkowe opcje znajdziemy w odrębnej zakładce „Lokalizacja”, dostępnej bezpośrednio z głównego menu ustawień smartfona. W sekcji „Uprawnienia aplikacji” możemy zobaczyć, jakim aplikacjom przyznaliśmy ciągły dostęp do danych lokalizacyjnych, jakie mają do nich dostęp tylko podczas używania i jakim nie daliśmy dostępu, choć o niego prosiły. W

przypadku pomyłki istnieje oczywiście możliwość skorygowania wcześniejszych wyborów. Standardowo lokalizacja urządzenia jest wykrywana za pomocą GPS, możemy jednak aplikacjom zezwolić na korzystanie z Wi-Fi i Bluetootha w celu dokładniejszego jej określania (co może się przydać, jeśli na fali sentymentu nadal gramy w Pokemon Go albo skonfigurowaliśmy zaufane miejsca w funkcji Smart Lock – zob. *Biometria i inne sposoby ochrony Androida przed niepowołanym dostępem*). Udostępniając swoją lokalizację innym osobom, powinniśmy pamiętać, że mogą się one dowiedzieć nie tylko, gdzie jesteśmy obecnie, ale również gdzie byliśmy przedtem, w jaki sposób się przemieszczamy (jedziemy czy idziemy), jaki jest stan naszego urządzenia, w tym np. stopień naładowania baterii i parę innych rzeczy – dlatego sugerujemy korzystać z tej opcji z rozwagą. Warto natomiast aktywować „Usługę lokalizacji dla połączeń alarmowych (ELS)". Jak tłumaczy producent systemu: „Gdy zadzwonisz lub napiszesz SMS-a na numer alarmowy, może zostać wysłana również lokalizacja Twojego telefonu, aby ratownicy mogli szybko Cię odnaleźć. Numer alarmowy w Stanach Zjednoczonych to 911, a w Europie 112".

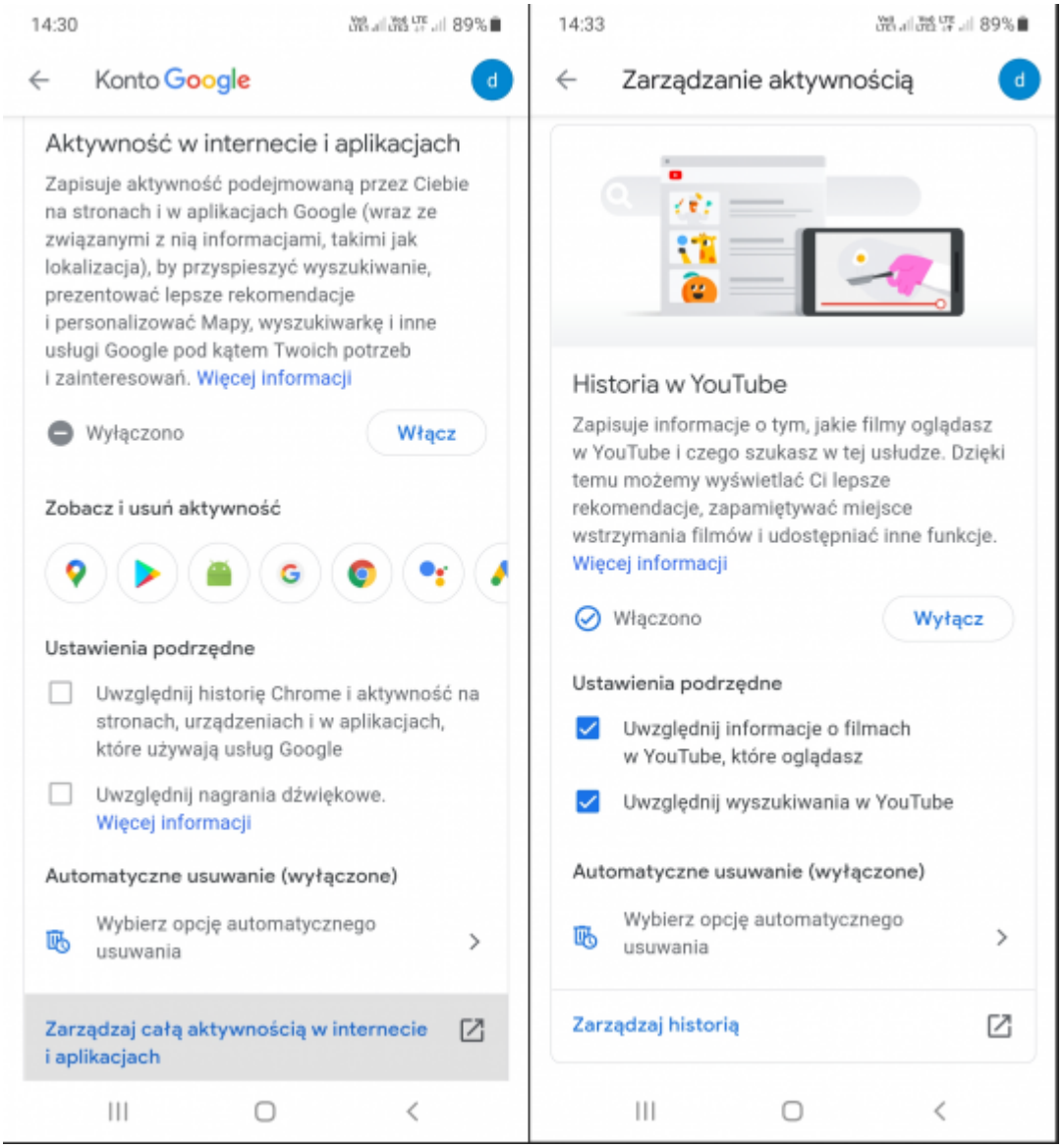


Zarządzanie lokalizacją

Wróćmy jednak do zakładki „Prywatność” i wybierzmy „Zarządzanie aktywnością”. Zobaczymy cztery sekcje: „Aktywność w internecie i aplikacjach”, ponownie (omówioną już) „Historię lokalizacji”, „Historię w YouTube” i „Personalizację reklam”.

Decydując się na zapisywanie naszej aktywności w internecie i aplikacjach, dowiemy się, że gromadzone dane „pomagają personalizować usługi Google, np. pozwalają szybciej wyszukiwać informacje oraz zwiększają trafność rekomendacji i reklam – zarówno w usługach Google, jak i innych firm”. Wniosek? Nic złego się nie stanie, jeśli wyłączymy tę funkcję. Jeśli tego nie zrobimy, możemy ograniczyć ilość zapisywanych informacji poprzez nieuwzględnianie historii przeglądarki Chrome i nagrań dźwiękowych generowanych podczas interakcji z wyszukiwarką Google, Asystentem i Mapami. Klikając w link „Więcej informacji”, przeczytamy, że ustawienie to „nie ma wpływu na dane dźwiękowe zapisane na Twoim urządzeniu i w innych usługach Google ani na sposób, w jaki Google przetwarza, transkrybuje i wykorzystuje do nauki Twoje dane w czasie rzeczywistym”. Tak jak w przypadku historii

lokalizacji, możemy skonfigurować automatyczne usuwanie zebranych danych. Wybierając „Zarządzaj całą aktywnością w internecie i aplikacjach”, otrzymamy także możliwość wyszukiwania i filtrowania zapisanych treści według dat i usług. Podobnie wygląda zarządzanie historią serwisu YouTube.

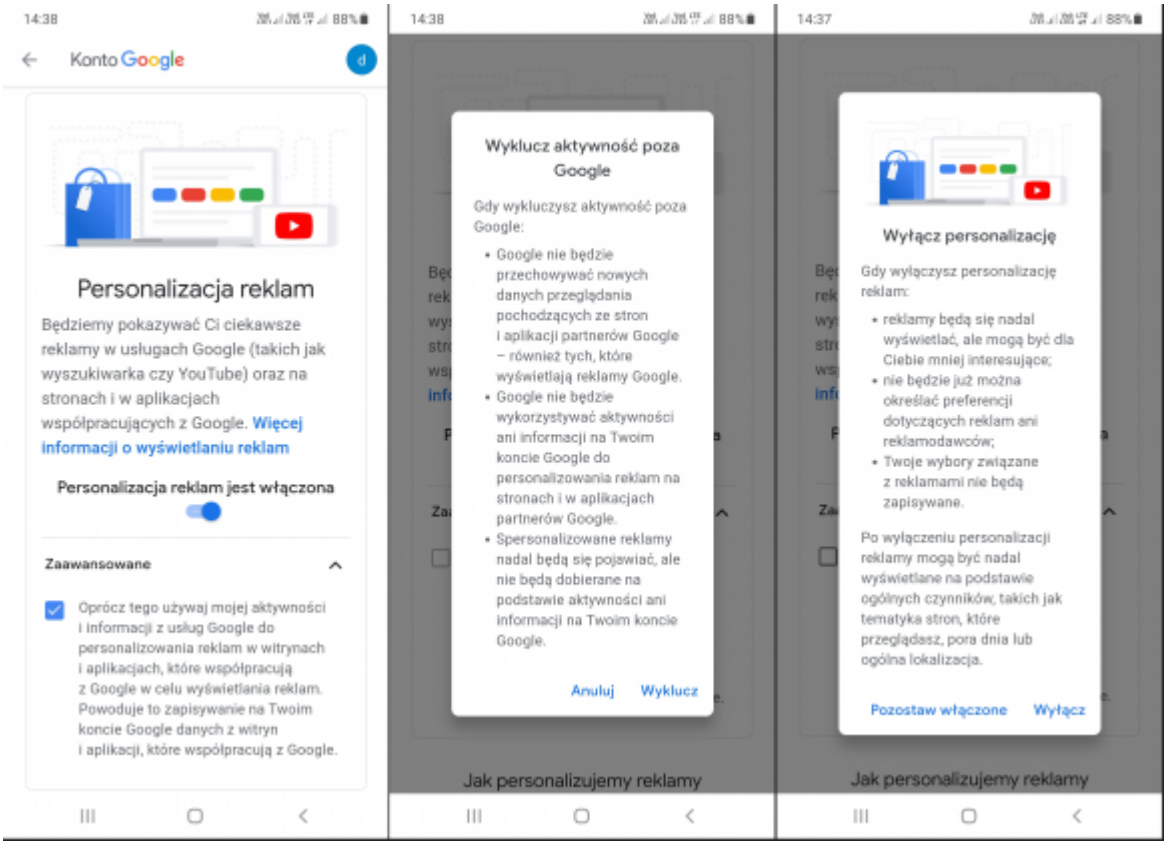


Zarządzanie aktywnością

Inaczej mają się sprawy z funkcją „Personalizacja reklam”. Jeśli jest ona włączona, to w sekcji „Jak personalizujemy reklamy” zobaczymy, na podstawie jakich danych osobowych Google dopasowuje do nas przekaz reklamodawców (przykładowe pozycje: „45-54 lata”, „Mężczyzna”, „Język: polski i jeszcze 1”). Każdą z uwzględnionych informacji możemy zaktualizować, a w przypadku profilowania na podstawie naszych zainteresowań – wyłączać te, z którymi się nie utożsamiamy i przywracać

wyłączone przez pomyłkę. W sekcji „Reklamy o charakterze kontrowersyjnym w YouTube” możemy ograniczyć wyświetlanie reklam dotyczących alkoholu i hazardu, a od pewnego czasu także randek, ciąży i rodzicielstwa czy nawet odchudzania. Na dole widnieje link „Twoje dane i reklamy”, pod którym znajduje się zapewnienie Google, że nigdy nie sprzedaje danych osobowych i nie używa informacji poufnych do personalizowania reklam. Sami musicie zadecydować, czy w to wierzycie. Bloomberg donosi, że z 68 mld dolarów całkowitych przychodów firmy w kwartale zakończonym 31 marca br. około 54 mld pochodziło z usług reklamowych.

Aby zapewnić sobie więcej prywatności, możemy usunąć zaznaczenie jedynej, niezbyt jasno opisanej opcji w zakładce „Zaawansowane” – dzięki temu Google nie będzie używać naszych danych do personalizowania reklam wyświetlanych na stronach i w aplikacjach firm trzecich, które z nim współpracują. Nie będzie też zapisywać informacji o naszych działaniach na stronach i w aplikacjach należących do zewnętrznych usługodawców. Jeszcze lepszym pomysłem jest całkowite wyłączenie personalizacji. Twórcy Androida uprzedzają, że reklamy nadal będą się nam wyświetlać, ale mogą być mniej interesujące – niewielka strata. Potwierdzając swój wybór, zobaczymy komunikat o możliwości wyłączenia personalizacji reklam Google wyświetlanych bez logowania oraz reklam z ponad 100 innych internetowych sieci reklamowych – da się tego dokonać w serwisie Your Online Choices (chociaż nie jest to rozwiązanie bez wad, bo opiera się na ciasteczkach).

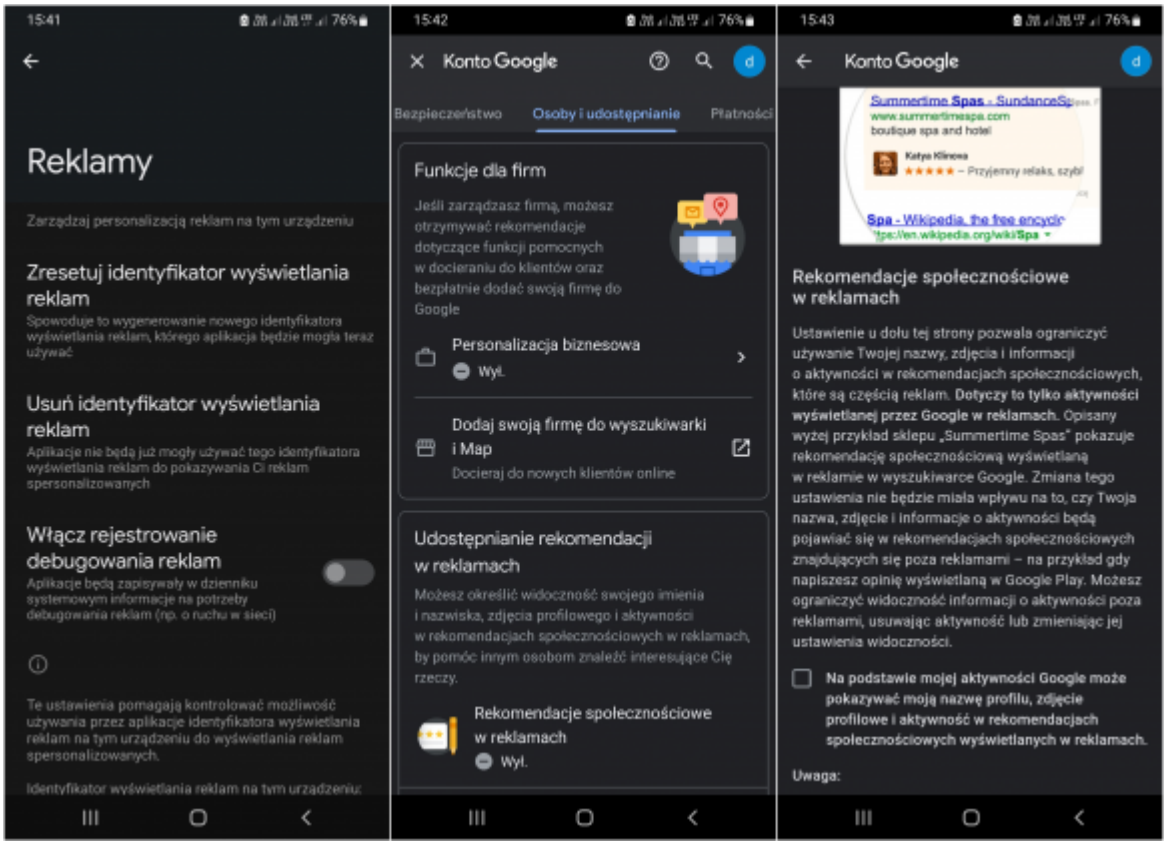


Personalizacja reklam

W zakładce „Prywatność” znajdziemy też odrębną sekcję „Reklamy”. W to samo miejsce trafimy, wybierając opcję o identycznej nazwie po wejściu z głównego menu ustawień do zakładki „Google” (czemu służy takie dublowanie ścieżek, nie wiadomo – może zamotaniu niedoświadczonego użytkownika, który dzięki temu coś przeoczy). W sekcji tej możemy zresetować unikalny identyfikator, który pozwala usługodawcom śledzić nasze zwyczaje i zainteresowania w celu lepszego dopasowania prezentowanych nam reklam. Identyfikator ten możemy również usunąć bez zastępowania go nowym. W Androidzie 12 stosowną opcję znajdziemy bez większych problemów, w starszych wersjach systemu kryje się ona natomiast pod nieco mylącą nazwą „Rezygnacja z personalizacji reklam”, którą dla odmiany trzeba włączyć.

Innej ukrytej funkcji musimy poszukać, wciskając w zakładce „Google” przycisk „Zarządzaj kontem Google”. Z górnego menu wybieramy „Osoby i udostępnianie”, przechodzimy do sekcji „Udostępnianie rekomendacji w reklamach” i klikamy w link „Zarządzaj rekomendacjami społecznościowymi”. Zobaczymy ścianę

tekstu wyjaśniającą, czym są wspomniane rekomendacje – w skrócie chodzi o możliwość wykorzystania w celach reklamowych naszej nazwy użytkownika, zdjęcia i informacji o aktywności (np. dodanej przez nas opinii o jakiejś restauracji). Aby temu zapobiec, trzeba zjechać na dół strony i usunąć zaznaczenie znajdującego się tam pola wyboru.

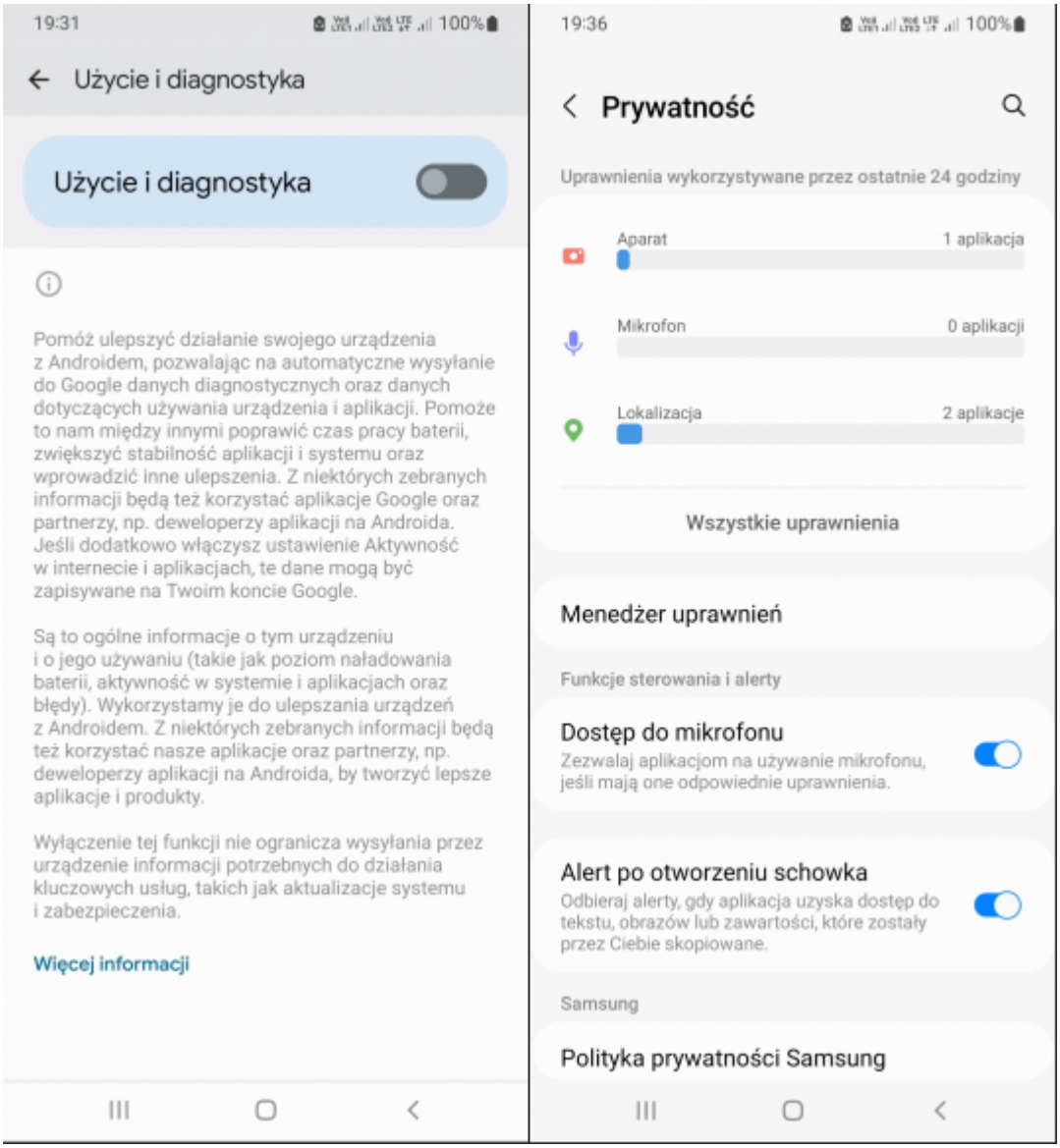


Reklamy i rekomendacje społecznościowe

Więcej sugestii dotyczących zarządzania kontem Google można znaleźć w naszych wcześniejszych artykułach z cyklu Podstawy Bezpieczeństwa: *Jak zadbać o swoją prywatność w usługach Google* oraz *Jak zadbać o swoje bezpieczeństwo w usługach Google*.

Ostatnią wartą uwagi sekcją w zakładce „Prywatność” jest „Użycie i diagnostyka”, która po włączeniu przesyła producentowi systemu informacje o jego działaniu i ewentualnych problemach. Ze strony pomocy technicznej Google możemy się dowiedzieć, że firmę interesują również takie dane, jak częstotliwość używania aplikacji, poziom naładowania baterii oraz jakość i czas trwania połączeń sieciowych. Są one

zapisywane na koncie użytkownika, co oznacza, że da się je przejrzeć i usunąć za pośrednictwem strony Moja aktywność. Przesyłanie tych informacji nie jest konieczne do poprawnego funkcjonowania Androida, możemy więc tę funkcję zdezaktywować.



Wysyłanie danych diagnostycznych i inne opcje

Spośród nowych opcji, które dodano w Androidzie 12, warto wymienić możliwość cofnięcia wszystkim aplikacjom dostępu do mikrofonu (wystarczy posłużyć się jednym suwakiem) oraz alerty po otworzeniu schowka. W kolejnej wersji Androida ma się pojawić także automatyczne usuwanie historii schowka, dzięki czemu aplikacje zostaną prewencyjnie odcięte od wcześniej skopiowanych, nieprzeznaczonych dla nich informacji. Wchodząc do zakładki „Prywatność”, możemy teraz zobaczyć statystyki wykorzystania aparatu, mikrofonu i lokalizacji w ciągu

ostatnich 24 godzin. Kliknięcie w którąkolwiek z tych funkcji umożliwia zapoznanie się z dokładną historią jej użycia. W Androidzie 13 liczba aplikacji wymagających dostępu do lokalizacji może ulec zmniejszeniu – nie trzeba będzie np. przyznawać tego uprawnienia, aby włączyć skanowanie Wi-Fi.

Na konferencji Google I/O, która odbyła się w maju, firma poinformowała o dostępności „trzynastki" w wersji beta 2, którą wyposażono w wymienione wyżej i sporo innych nowości. Można ją przetestować na smartfonach kilku różnych producentów, ale Samsung się do nich nie zalicza. Cóż, poczekamy… zwłaszcza że Android 12 ledwo zaczął zdobywać popularność. Według statystyk dostępnych na stronie StatCounter na razie używa go tylko 11,77% posiadaczy telefonów z tym systemem, a w Polsce jeszcze mniej, bo 9,78%. Niekwestionowanym liderem pozostaje „jedenastka", która na szczęście przykłada do prywatności użytkowników większą wagę niż poprzedniczki.

Dla zachowania pełnej przejrzystości: Patronem cyklu jest Aruba Cloud. Za opracowanie i opublikowanie tego artykułu pobieramy wynagrodzenie.

Źródło

Brytyjczycy nie ufają technologii opartej na danych

Zespół Ada Lovelace Institute przeanalizował dostępne publikacje dotyczące oczekiwań ludzi wobec wykorzystania ich danych. Wbrew lansowanej od lat tezie branży internetowej użytkownicy i użytkowniczki rozwiązań cyfrowych wcale nie pogodzili się z nieograniczonym eksploatowaniem informacji na swój temat.

Brytyjscy odbiorcy są zwolennikami innowacji opartych na danych, ale uważają, że powinny one być etyczne, odpowiedzialne i służyć dobru wspólnemu. Istnieją też liczne dowody na to, że Brytyjczycy i Brytyjki popierają pomysł lepszego uregulowania wykorzystania technologii opartych na danych. Oczekują też jaśniejszej informacji o tym, jak są wykorzystywane ich dane i jak wpływa to na prawa i wolności użytkowników. Potrzebne są jednak dalsze badania, żeby doprecyzować, jakie dokładnie wymagania mają wobec przepisów, a także co dokładnie rozumieją pod pojęciem wspólnego dobra.

Społeczeństwo opiera się stosowaniu wykorzystujących dane systemów, jeśli nie ma do nich zaufania. Raport Ada Lovelace Institute podpowiada, że nie należy ignorować niepokoju ludzi wobec wykorzystania ich danych, tłumacząc go brakiem wiedzy czy zrozumienia. Problemu nie rozwiąże samo oczekiwanie, że użytkownicy i użytkowniczki staną się bardziej ufni wobec technologii. Liczne publikacje wskazują, że kluczem do budowania zaufania jest regulacja. Dopiero przepisy zaprojektowane tak, by chronić ludzi przed nieprzejrzystą i niesprawiedliwą technologią, dadzą poczucie bezpieczeństwa.

Badania dotyczą Wielkiej Brytanii. A co polskie społeczeństwo sądzi o technologiach opartych na danych?