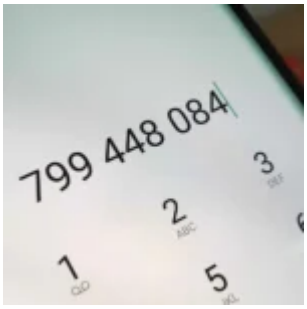
799 448 084 – ten numer trzeba znać



Numer +48799448084 to jeden z wielu, które warto zapisać w telefonie. Szczególnie w okresie wzmożonych ataków SMS-wych może się przydać w zasadzie codziennie. Przypominamy, dlaczego jest tak istotny i w jaki sposób z niego korzystać.

Numer 799448084 został uruchomiony przez CERT Polska specjalnie na potrzeby zgłaszania incydentów bezpieczeństwa. Każdy, kto dostanie podejrzaną wiadomość SMS (na przykład taką z wezwaniem do uregulowania rachunku za energię elektryczną) może ją przesłać do analizy. **SMS wystarczy przekazać w niezmienionej formie właśnie na numer +48799448084**, a trafi do specjalistów.

W CERT Polska wiadomość zostanie sprawdzona pod kątem bezpieczeństwa, co docelowo może poskutkować wydaniem dodatkowych komunikatów. W praktyce **wysłanie podejrzanego SMS-a na numer 799448084 może więc przełożyć się na stworzenie ostrzeżenia dla innych użytkowników**, którzy w danej chwili nie są świadomi, że ma miejsce atak SMS-owy. W ostatnim czasie najpopularniejsze są głównie te związane z energetyką i podszywaniem się oszustów pod dostawców prądu.

799 448 084 – jak przekazać wiadomość?

Aby przesłać podejrzaną wiadomość SMS do analizy CERT Polska,

wystarczy po jej otrzymaniu **przekazać ją na wspomniany numer 799448084**. Najłatwiej to zrobić, jeśli ten został wcześniej zapisany w kontaktach. Co ważne, **treść nie może zostać w żaden sposób zmieniona**. Należy po prostu użyć funkcji „przekaż dalej”, którą można znaleźć w opcjach wiadomości SMS w każdym telefonie.

Warto podkreślić, że co do zasady do analizy można przekazywać podejrzane SMS-y na przykład z nieznanymi linkami lub zachęcające do instalacji nieznanych aplikacji. Wiadomości SMS Premium nie zaliczają się do tych kategorii. **CERT Polska podaje, z jednego numeru można przesłać do analizy maksymalnie 3 SMS-y w ciągu 4 godzin.**

Oskar Ziomek

Będą zasiewać chmury nanocząstkami tlenku grafenu…

Nanocząstki tlenku grafenu 3D do zasiewania chmur: Patent US 2022/0002159 A1

*Niniejszy wynalazek dostarcza **cząstkę nukleującą lód do zasiewu chmur i innych zastosowań**, zdolną do inicjowania nukleacji lodu w temperaturze -8 stopni C. Ponadto **liczba cząstek nukleujących lód rośnie w sposób ciągły i gwałtowny wraz z obniżaniem się temperatury.** Cząstka nukleująca lód*

według niniejszego wynalazku ***jest porowatym nanostrukturalnym kompozytem trójwymiarowego zredukowanego tlenku grafenu i nanocząstek dwutlenku krzemu (PrGO-SN).*** *Niniejszy wynalazek dostarcza również proces syntezy PrGO-SN.*

US 20220002159A1

(19) **United States**

(12) **Patent Application Publication**

ZOU et al.

(10) **Pub. No.: US 2022/0002159 A1**

(43) **Pub. Date: Jan. 6, 2022**

(54) **3D REDUCED GRAPHENE OXIDE/SIO 2 COMPOSITE FOR ICE NUCLEATION**

(71) Applicant: **Khalifa University of Science and Technology**, Abu Dhabi (AE)

(72) Inventors: **Linda ZOU**, Abu Dhabi (AE); **Haoran LIANG**, Abu Dhabi (AE)

(21) Appl. No.: **17/422,994**

(22) PCT Filed: **Jan. 14, 2020**

(86) PCT No.: **PCT/IB2020/050259**

§ 371 (c)(1),
(2) Date: **Jul. 14, 2021**

Related U.S. Application Data

(60) Provisional application No. 62/791,927, filed on Jan. 14, 2019.

Publication Classification

(51) **Int. Cl.**
C01B 32/198 (2006.01)
C01B 33/12 (2006.01)

(52) **U.S. Cl.**
CPC ***C01B 32/198*** (2017.08); *B82Y 40/00* (2013.01); ***C01B 33/12*** (2013.01)

(57) **ABSTRACT**

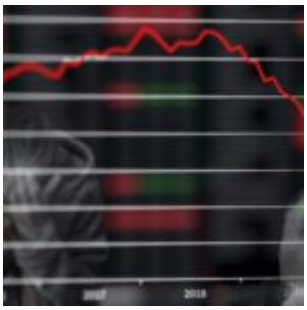
The present invention provides for an ice-nucleating particle for cloud seeding and other applications, which can initiate ice nucleation at a temperature of−8° C. Further, the ice nucleation particle number increased continuously and rapidly with the reducing of temperature. The ice nucleating particle in the present invention is a nanostructured porous composite of 3-dimensional reduced graphene oxide and silica dioxide nanoparticles (PrGO-SN). The present invention also provides for a process for synthesizing the PrGO-SN.

US20220002159A1Pobierz

3D-Reduced-Graphene-Oxide_Cloud-Seeding-CCN-US20220002159A1Pobierz

Naukowcy zwiększają możliwości zasiewania chmur za pomocą nanotechnologii: https://www.technologyreview.com/2022/03/28/1048275/scientists-advance-cloud-seeding-capabilities-with-nanotechnology/

Credit Suisse na krawędzi upadku. Potężny kryzys gospodarczy coraz bardziej prawdopodobny



Credit Suisse chyli się ku upadkowi. Obecnie jedną akcję tego znanego, szwajcarskiego banku można kupić za mniej niż 4 dolary, podczas gdy w lutym zeszłego roku trzeba było za nią zapłacić nawet ponad 14 dolarów. Sytuacja stała się tak zła, iż instytucja finansowa ogłosiła rozpoczęcie prac nad planem restrukturyzacji.

Credit Suisse, czyli szwajcarski bank z ogromnymi ambicjami

Credit Suisse Group AG jest szwajcarskiej bankiem, który pod względem wielkości ustępuje miejsca jedynie UBS AG. Jednakże zdaje się, że ambicje miał on znacznie większe od swojego krajowego rywala. **Credit Suisse** starał się stworzyć finansowy konglomerat zajmujący się między innymi zarządzaniem majątkami klientów, bankowością prywatną, świadczeniem usług w zakresie bankowości inwestycyjnej, który stałby się godną konkurencją dla banków inwestycyjnych z Wall Street. Jednakże obecnie jego zarząd musi porzucić to marzenie i zająć się ratowaniem banku, który znalazł się w naprawdę kiepskiej sytuacji ze względu na szereg złych decyzji inwestycyjnych, ale po kolei.

Szwajcarski bank dał się dwukrotnie nabrać

Na skutek wybuchu pandemii, wielu przedsiębiorców zdało sobie sprawę, jak ważne są sprawnie funkcjonujące łańcuchy dostaw. Jednakże **Credit Suisse** wiedział o tym już od dawna, gdyż lata temu rozpoczął on współpracę ze spółką **Greensill Capital,** która zajmowała się głównie sprzedażą usług związanych z finansowaniem łańcuchów dostaw. Łącznie uzyskała ona od niego pakiet funduszy o wartości 10 mld dolarów. Niestety dla banku okazało się, że Greensill nie prowadził swojej działalności zbyt uczciwie i w marcu 2021 roku upadł, jak informuje Financial Times, w wyniku zarzutów o oszustwa.

Co prawda, 7,3 mld ze wspomnianej kwoty udało się odzyskać, ale reszta pożyczonych spółce funduszy została praktycznie zakwalifikowana, jako strata. Co więcej, ze względu na ogłoszenie upadłości, bank został zmuszony do poniesienia dodatkowych wydatków między innymi na doradztwo prawe, restrukturyzacje, które łącznie wyniosły 10 mld dolarów. Co warto zaznaczyć, opisane tutaj koszty zostały przerzucone na inwestorów funduszu, którzy zostali do niego przekonani obietnicami o praktycznie zerowym ryzyku.

Przy czym **Credit Suisse** może się pochwalić tym, że zainwestował środki nie tylko w przedsiębiorstwo oskarżane o oszustwa, ale również w takie, którego właściciel skończył przed sądem federalnym Stanów Zjednoczonych. Otóż szwajcarski bank postanowił użyczyć swoich środków amerykańskiemu **Archegos Capital Management,** które zarządzało aktywami swego czasu znanego inwestora **Sung Kook Hwanga** znanego szerzej jako **Bill Hwang**. Przedsiębiorstwo to okazało się grać lekkomyślnie, inwestując znaczne środki w ryzykowne swapy. Jak się okazało strategia ta doprowadziła w końcu **Archegos** do ruiny. Przedsiębiorstwo w ciągu pierwszych 10 dni marca 2021 roku straciło 20 mld dolarów, a sam Hwang skończył z zarzutem o oszustwo przed federalnym sądem Stanów Zjednoczonych. Łącznie

ze względu na tę decyzję inwestycją, szwajcarski bank stracił ok. 4,7 mld dolarów.

Niektóre inwestycje okazały się wtopą. Do tego na bank nałożono kary

Do tego niektóre bezpieczne inwestycje banku, zamiast generować zyski, przyniosły straty. Choćby w 2000 roku **Credit Suisse** kupił bank inwestycyjny **Donaldson, Lufkin & Jenrette** za 11,5 mld dolarów. Jednakże od tamtego czasu, jego wartość nie tylko nie wrosła, ale spadła. Doprowadziło to do tego, że w 2021 roku szwajcarski bank obniżył jego wartość księgową łącznię aż o 1,75 mld dolarów. Jakby tego było mało, na **Credit Suisse** w ostatnich latach zostały nałożone różne kary. Na przykład w tym roku szwajcarski Federalny Sąd Karny uznał, iż przedsiębiorstwo zbyt niedbale przeprowadzał kontrole, dzięki czemu jeden z jego pracowników mógł aktywnie pomagać bułgarskiej mafii narkotykowej prać pieniądze. Za to przewinienie na bank został nałożony obowiązek uiszczenia grzywien i odszkodowań o łącznej wartości 22 milionów dolarów.

Credit Suisse na krawędzi upadku. Potężny kryzys gospodarczy coraz bardziej prawdopodobny

Wszystkie te czynniki w połączeniu z wysoką rotacją na stanowiskach kierowniczych (w ciągu ostatnich 25 lat prezes banku zmienił się aż siedmiokrotnie!) sprawiły, że wiara w przyszłość **Credit Suisse** spadła do historycznego minimum, co obrazują ceny akcji. Jak widać na zamieszczonym poniżej wykresie, w lutym 2021 roku, aby zakupić jedną akcję przedsiębiorstwa, trzeba było wydać nawet ponad 14 dolarów. Obecnie można bez problemu kupić ją za mniej niż 4 dolary.

Oznacza to, jak powiedział szef działu badań w **Goldmoney Alasdair Macleod**, iż:

> *Rynki mówią, że [Credit Suisse] jest niewypłacalny i prawdopodobnie upadnie.*

Cena akcji Credit Suisse wyrażona w dolarach

Oczywiście zarząd banku nie zamierza do takiej sytuacji dopuścić. Już ogłoszono, rozpoczęcie prac nad planem restrukturyzacji, który zostanie przedstawiony szerszej publiczności w październiku. Z zapowiedzi przedstawicieli przedsiębiorstwa wynika, że zapewne tysiące ludzi straci pracę, działalność inwestycyjna banku zostanie ograniczona, przy czym niewykluczone, iż bank całkowicie zaprzestanie działalności w Stanach Zjednoczonych. Czy takie zmiany są w stanie uratować Credit Suisse przed upadkiem? Trudno ocenić, ale jedno jest pewne. Jeżeli okażą się one nietrafione, prawdopodobieństwo wybuchu globalnego kryzysu finansowego znacznie wzrośnie.

Źródło

Naukowcy wynaleźli mikroroboty z własnymi mózgami, które mogą wejść do Twego ciała.

Technologie wyprzedzają nasze wyobrażenia. Chyba, że oglądaliśmy filmy science fiction, w których owe technologie były nam zaserwowane, ale w takim razie te filmy przestają być fikcją.

Naukowcy z Cornell University zainstalowali **elektroniczne „mózgi”** w zasilanych energią słoneczną mikrorobotach o rozmiarach od 100 do 250 **mikrometrów** – mniejszych niż głowa mrówki – aby mogły poruszać się autonomicznie, bez kontroli z zewnątrz..

Chociaż naukowcy z Cornell i innych uniwersytetów opracowali wcześniej mikroskopijne maszyny, które mogą czołgać się, pływać, chodzić i składać, urządzenia te zawsze miały dołączone „struny”; w celu wygenerowania ruchu użyto przewodów do dostarczania prądu elektrycznego lub wiązek laserowych, które musiały być skierowane bezpośrednio na określone obszary robotów.

„Wcześniej musieliśmy dosłownie manipulować tymi „strunami”, aby uzyskać odpowiedź od robota. Ale teraz, gdy mamy te mózgi „na pokładzie”, to jak przecinanie sznurków marionetek. T**o tak, jak wtedy, gdy Pinokio zyskał świadomość**” – powiedział

Itai Cohen, profesor fizyki w College of Arts and Sciences

„Mózg” nowych robotów składa się z komplementarnego obwodu zegarowego CMOS, który zawiera tysiąc tranzystorów oraz szereg diod, rezystorów i kondensatorów. Układ scalony CMOS generuje sygnał, który wytwarza szereg przesuniętych w fazie częstotliwości prostokątnych, które z kolei określają ruchy robota. Nogi robota to siłowniki na bazie platyny. Zarówno obwód, jak i nogi zasilane są energią fotowoltaiczną.

„Ostatecznie zdolność do przekazywania poleceń pozwoli nam wysyłać instrukcje do robota, a wewnętrzny mózg wymyśli, jak je wykonać. Następnie rozmawiamy z botem. Robot może nam coś powiedzieć o swoim otoczeniu, a my możemy zareagować mówiąc: „OK, idź tam i spróbuj dowiedzieć się, co się dzieje” – powiedział Cohen.

Nowe roboty są około 10 000 razy mniejsze niż roboty w skali makro, które mają na pokładzie elektronikę CMOS i mogą poruszać się z prędkością większą niż 10 mikrometrów na sekundę.

(…)

Co jest interesujące badania były wspierane przez Biuro Badań Naukowych Sił Powietrznych; Biuro Badań Armii; oraz Instytut Kavli na Uniwersytecie Cornell w Nanoskali.

Źródło

Śmiertelna pułapka internetu

czyha na dzieci. Pornografia. Uzależnienie. Cyber-przemoc. Gry śmierci. Uwodzenie.

Sidła zastawione! Śmiertelna pułapka internetu czyha na dzieci. Pornografia. Uzależnienie. Cyber-przemoc. Gry śmierci. Uwodzenie.

Dzieci, które nie umieją jeszcze bezpiecznie korzystać z internetu, mogą wpaść w śmiertelną pułapkę.

Bardzo aktualnym przykładem jest tu tragedia 12-letniego Archiego Battersbee, który stał się ofiarą igrania ze śmiercią podczas tzw. internetowego wyzwania, zwanego „Blackout Challenge" (w polskim tłumaczeniu „utrata przytomności"). Do tej pory ta demoniczna zabawa kosztowała życie już siedmioro dzieci. A to nie jedyny „wilczy dół", do którego mogą wpaść nasze pociechy, kiedy bez żadnej kontroli, swobodnie serfują w sieci.

7 kwietnia 2022 roku rodzice znaleźli Archiego w stanie nieprzytomności. Leżał, bez oznak życia, na podłodze w rodzinnym domu. Zabrano go do szpitala, gdzie lekarze stwierdzili, iż mózg nastolatka uległ bardzo poważnym uszkodzeniom wskutek niedotlenienia. Dziecko podłączono do aparatury podtrzymującej życie. Po jakimś czasie dyrekcja szpitala podjęła decyzję o odłączeniu Archiego od tej aparatury, gdyż zdaniem lekarzy **pień mózgu umarł i chłopca nie da się uratować.** Rodzice nie zgadzali się z decyzją szpitala.

Podali sprawę do sądu, który rację przyznał jednak lekarzom. Archiego 7 sierpnia odłączono od aparatury, niedługo po tym przestał oddychać.

Rozpoczęło się dochodzenie jak doszło do tej tragedii. Ostatecznie ustalono, że nastolatek dał się namówić do udziału w tzw. „wyzwaniu", upowszechnionym na portalu społecznościowym Tik Tok. Wyzwanie to, zwane z angielska „Blackout Challenge" (utrata przytomności) polega na możliwie najdłuższym wstrzymaniu oddechu. Wówczas to w mózgu pozbawionym tlenu powstają halucynacje, podobne do wizji narkotycznych. Kiedy jednak człowiek zbyt długo nie oddycha, wówczas najpierw traci przytomność, a potem umiera.

Do tej pory, na całym świecie, ujawniono co najmniej 7 przypadków zgonów dzieci, które „bawiły się" w „Blackout Challenge". Ich rodzice złożyli pozwy do sądów przeciwko platformie Tik Tok, oskarżając ją o nie zablokowanie śmiercionośnego challengu. Szefowie Tik Tok bronią się podając, iż zablokowano możliwość wyszukiwania hasła Blackout. Gracze znaleźli jednak tzw. „obejście". Wyzwanie „utrata przytomności" nie jest bynajmniej pierwszym takim igraniem ze śmiercią za pośrednictwem internetu. Wcześniejsze grupowe „wyciskanie" adrenaliny w mediach społecznościowych, też miało tragiczne skutki.

Uzależnienie

Internet jest pełen pułapek i sideł zastawionych na dzieci, nieświadomych czyhających tam na nie niebezpieczeństw. Samo długotrwałe przebywanie w odrealnionym, cyfrowym świecie prowadzi do uzależnienia. Dziecko uzależnione od internetu, traci kontakt z rzeczywistością, a kiedy pozbawi się go dostępu do sieci, staje się agresywne. Czasem tak bardzo, iż potrafi zranić, albo nawet zabić. Świeża jest tragedia, do której doszło w tym roku, w domu położonym niedaleko hiszpańskiego miasteczka Elche. Kiedy rodzice, z powodu złych

wyników w nauce, odcięli dostęp do internetu swojemu 15-letniemu synowi, ten wpadł w szał i zastrzelił całą swoją rodzinę – rodziców i brata.

Skala problemu uzależnienia od bycia w sieci widoczna jest chociażby bo gwałtownie rosnącej liczbie psychiatrycznych oddziałów odwykowych od interentu na całym świecie, również w Polsce. Ministerstwo zdrowia uruchomiło niedawno program „Terapia dla dzieci i młodzieży uzależnionych od nowych technologii cyfrowych". Już 12 dużych ośrodków zdrowia psychicznego w całej Polsce bierze udział w tym programie. Ośrodki te znajdują się na ogół w dużych miastach, takich jak m.in. Warszawa, Wrocław, Białystok, Szczecin, Łódź, Toruń czy Siemianowice Śląskie.

Pornografia

Jednym z największych niebezpieczeństw grożących dzieciom, poruszających się w sieci, jest wszechobecna tam pornografia, która bardzo mocno degeneruje młode umysły i szybko je uzależnia. Według badań naukowych mózg dziecka nie jest przygotowany na zmierzenie się z treściami pornograficznymi, które czynią w nim wielkie spustoszenie. Te przedwczesne i nieuporządkowane doznania seksualne, mają bardzo negatywny wpływ na późniejsze – życie dorosłe. – *Osoby, które miały wczesny kontakt z pornografią, np. w wieku 12 lat bądź wcześniej, o wiele częściej wskazują na problemy związane z czerpaniem satysfakcji w związku małżeńskim* – powiedział podczas jednego z wykładów wybitny specjalista – dr hab. Piotr Rzymski z Zakładu Medycyny Środowiskowej na Uniwersytecie Medycznym w Poznaniu. Niestety te problemy są częstym powodem rozbicia małżeństwa. Z danych statystycznych wynika również, że osoby uzależnione od pornografii o wiele częściej, niż osoby nie uzależnione, dopuszczają się gwałtów i przemocy wobec kobiet.

Rozwiązaniem dla rodziców są na pewno odpowiednie programy,

które blokują strony pornograficzne oraz tego rodzaju reklamy. Jedną z najskuteczniejszych takich zapór są przeglądarki internetowe, produkowane przez firmy profesjonalnie zajmujące się tworzeniem programów antywirusowych. Pomysłowość naszych dzieci jest jednak ogromna i potrafią one skutecznie poradzić sobie z różnego rodzaju blokadami stron, dlatego nieodzowna jest rodzicielska kontrola. Co jakiś czas trzeba zasiąść do komputera naszej pociechy i sprawdzić czy wszystko jest w porządku, bo bez tego zdrowego monitoringu, nasza pociecha może stać się dla nas ciężkim utrapieniem. Wystarczy, że same naturalne przemiany rozwojowe w wieku nastoletnim są dla rodziców poważnym wyzwaniem, po co więc sobie jeszcze dokładać. Pewien mądry i wesoły człowiek powiedział „Kto przeżyje trudy wieku nastoletniego swoich dzieci – temu czyściec będzie darowany". I tej nadziei się trzymajmy.

Gry śmierci

Inną „toksyną" związaną z komputerem, grasująca nie tylko w przestrzeni internetu, są agresywne gry komputerowe. Pełno w nich przemocy, krwawych i brutalnych scen. Oglądnie, a do tego jeszcze uczestnictwo w zabijaniu na ekranie, wulgarny język gier, nie może pozostać bez negatywnego wpływu na umysły graczy. Cyfrowe gry są coraz bardziej nasycone wszelkiego rodzaju dewiacjami i agresją. Ich bohaterowie to przeważnie seryjni mordercy, psychopaci, zombi, wampiry i demony. Godziny, które gracze spędzają w takim ciemnym towarzystwie, na pewno im nie służą. Jak mówi stare, mądre przysłowie „Z kim przestajesz takim się stajesz".

Kiedy któregoś razu odwiedzałem kuzyna, wszedłem do pokoju jego nastoletnich synów, żeby się z nimi przywitać. Obaj grali właśnie na komputerze w bardzo drastyczną grę. Gdy zobaczyłem na ekranie monitora skalę okrucieństwa i przemocy, aż zimny pot mnie oblał. Poczułem się jakbym znalazł się nagle w przedsionku piekła. Zapytałem chłopaków jak mogą na to patrzeć i to wiele godzin. Jeden z nich odpowiedział ze spokojem „To

tylko gra”. Jak muszą być znieczulone sumienia osób uczestniczących w tych cyfrowych igrzyskach śmierci? Jak stępiona ludzka wrażliwość?

Uwodzenie

Dla pedofilów sieć internetowa stała się siecią, którą łowią dzieci. Te szatańskie łowy doczekały się nawet swojej anglojęzycznej nazwy – grooming. Pedofil tworzy profil na ulubionym portalu społecznościowym upatrzonej ofiary. Podaje się tam za dziecko, najlepiej rówieśnika osoby małoletniej, którą chce skrzywdzić. Zwyrodnialec obserwuje ofiarę, stara się zdobyć jej zaufanie poprzez przyjazne rozmowy, wysyłanie swoich fałszywych zdjęć. Wszystko to, aby wyłudzić od dziecka jego adres zamieszkania lub szkoły. Kiedy mu się to uda, wówczas może już uderzyć.

Cyberprzemoc

Agresja w internecie przejawia się na wiele sposobów i ma wiele imion. Trollowanie to różnego typu nieprzyjazne zachowania wobec innych użytkowników portali społecznościowych, prowadzone w celu rozbicia ich dyskusji. Flamingiem nazywa się sprowadzanie rozmowy do tonu jak najbardziej agresywnego i wulgarnego. Doskonale znany hejt to obraźliwe, nienawistne wypowiedzi kierowane wobec innych osób. Można by tu jeszcze długo wymieniać te angielskie imiona nienawiści, obecnej w sieci. Ale może lepiej sobie tego oszczędźmy. Dość powiedzieć, że przemoc w internecie nie jest wirtualna, ale realna. Do tego stopnia, że potrafi zabić.

Mój przyjaciel, opowiedział mi historię dziewczyny o bardzo kruchej psychice, która po zawodzie miłosnym, targnęła się na swoje życie. Odratowano ją. Przeszła terapię, stanęła na nogi. Zdawało się, że poukłada sobie życie. Niestety internetowi hejterzy przypuścili na nią atak. Jeden z tych nienawistników napisał „jest nieudacznikiem, nawet samobójstwa nie potrafi

popełnić”. To było jak kamieniowanie. Policja podała w komunikacie, że druga próba samobójcza była niestety skuteczna. Ale tak naprawdę to nie ona się zabiła – zabiła ją ludzka nienawiść, zwana internetowym hejtem.

Nie pozostawiajmy dzieci samych z cyfrową hydrą

Najnowsze badania wskazują, że współczesny rodzic jest bardzo często nieobecny w cyber świecie swojego dziecka. W 60 proc. domów rodzice nie stawiają dzieciom żadnych granic w korzystaniu z internetu, a wiadomo, że dzieci same sobie tych granic nie postawią. Siedzą, czy leżą godzinami ze wzrokiem utkwionym w ekran monitora lub smartfona. Trwanie w takim bezruchu jest częstym powodem nadwagi, lub innej skrajności – niedowagi, gdyż dziecko urzeczone wirtualną rzeczywistością, nie da rady oderwać się od niej, nawet na posiłek. Brak ruchu, świeżego powietrza prowadzi do utraty zdrowia, osłabienia odporności. Wady wzroku to obecnie wśród dzieci i młodzieży prawdziwa plaga, a to też efekt obciążania wzroku gapieniem się w ekran z bliskiej odległości. Kolejnym „efektem ubocznym” braku ograniczania przez rodziców czasu, które dzieci spędzają przy monitorach, jest brak snu naszych pociech. Niewyspanie odbija się niezdrowa czkawką w postaci braku zdolności koncentracji, co prowadzi do słabych wyników w nauce i wzmożonej nerwowości, a nawet depresji i nerwic.

Warto więc znaleźć czas dla dziecka. Nie wykręcać się sianem, że muszę dużo pracować, zarabiać, mam inne obowiązki. Jeżeli nie znajdziemy czasu dla dziecka, to możemy je – stracić. Cóż wówczas będą znaczyły nasze pieniądze, praca i obowiązki? Przecież czas przeżyty z osobą bliską, to czas najlepiej przeżyty. Postarajmy się więc wyrwać swoje dziecko, choć na krótki czas, ze świata wirtualnego i zainteresować go światem realnym, który jest bez porównania piękniejszy i ciekawszy. Mogą w tym pomóc wspólne spacery, sporty, gry, zabawy na

świeżym powietrzu, w otoczeniu przyrody. Dobrze jest też pomóc dziecku w odkrywaniu jego talentów i zachęcić, aby je rozwijało. Wspólne, dobre spędzanie czasu razem z dzieckiem buduje zdrową relację, która jest podstawą, do tego, aby dziecko nie bało się nam powiedzieć o swoich problemach i radościach, również do tego, aby wysłuchało naszej opowieści o Stwórcy, świecie i prawdziwym sensie życia.

Adam Białous

Wielu przypuszcza, że cyberataki nie mogą zabijać ludzi. To nieprawda

Cyberataków nie należy lekceważyć i traktować jako niewinnej zabawy młodych ludzi. To poważne przestępstwa, które mogą prowadzić również do śmierci.

- Grupa ekspertów ostrzega, że □□Korea Północna mogłaby wykorzystać techniki groźnych cyberataków.
- Cyberprzestępcy mogą na przykład przejąć kontrolę nad oczyszczalnią wody i zmienić mieszankę chemiczną, aby była toksyczna…
- …albo przeniknąć do systemów komputerowych elektrowni jądrowej, powodując poważne awarie.

Koreański dziennikarz Jung Min-ho pisze:

> *Jednym z najbardziej niedocenianych zagrożeń bezpieczeństwa pochodzących z Korei Północnej są jej możliwości cyberataków. Wielu przypuszcza, że □□hakerzy nie mogą zabijać ludzi. Ale mogą.*

Cyberprzestępcy mogą przejąć kontrolę nad oczyszczalnią wody i zmienić mieszankę chemiczną, aby była toksyczna, lub mogą przeniknąć do systemów komputerowych elektrowni jądrowej, powodując poważne awarie. W ostatnich latach w wielu częściach świata podejmowano próby takich cyberataków, niektóre z nich zakończyły się pośrednio śmiercią lub obrażeniami.

Grupa ekspertów ostrzega, że □□Korea Północna mogłaby wykorzystać takie techniki, gdyby wybuchła wojna na Półwyspie Koreańskim, w raporcie RAND Corporation zatytułowanym "Charakterystyka zagrożeń związanych z północnokoreańską bronią chemiczną i biologiczną, impulsem elektromagnetycznym i zagrożeniami cybernetycznymi".

Choi Kang, prezes Asan Institute for Policy Studies i jeden ze współautorów wspólnego raportu napisanego z think tankiem RAND Corporation, powiedział na konferencji prasowej w instytucie w Seulu we wtorek.

> *Infrastruktura w Korei Południowej wydaje się być bardzo podatna na cyberataki Północy. Widzieliśmy kilka przypadków w systemach bankowych… Ale co z inną infrastrukturą, taką jak zaopatrzenie w wodę lub elektryczność? To spowodowałoby chaos.*

Możliwe scenariusze

Jednym z możliwych scenariuszy może być wykolejenie pociągów załadowanych śmiercionośnymi chemikaliami. Inne możliwe cele obejmują tamy, szpitale, lotniska i sieci energetyczne,

których wiele systemów komputerowych zostało już wcześniej przenikniętych przez Koreę Północną.

Raport mówi, że domniemane rozmieszczenie wirusa Stuxnet przez Stany Zjednoczone i Izrael w celu uszkodzenia irańskich wirówek do wzbogacania nuklearnego oraz rosyjski program złośliwego oprogramowania towarzyszący inwazji na Ukrainę w tym roku mogą służyć jako przykłady do naśladowania i rozwijania przez Koreę Północną.

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

Strzelanina w Uvalde a dostęp do broni

„Mianem barbarzyństwa określam silną rasę, rasę gotową się bić. Drapieżnik leży, gotowy do skoku, w duszy ludzkiej” (Oswald Spengler)

Strzelanina w teksańskim Uvalde gdzie z rąk młodocianego mordercy zginęło 21 osób, ożywiła ponownie debatę nad dostępnością broni, tym razem wzbogaconą o wątek obrony Ukraińców przed rosyjską agresją. Wydaje się, że w dyskusji tej warto zabrać głos, gdyż ścierające się w niej stanowiska częściowo jedynie dotykają problemu i są przez to niezadowalające.

Abolicjonizm

Zacznijmy od abolicjonistów, bo wyjaśnienie jest tu bardziej oczywiste. Ilustracją tej postawy może być papież Kościoła rzymskokatolickiego Franciszek. W ostatnim czasie duże

kontrowersje wzbudziła jego wypowiedź wzywająca strony wojny na Ukrainie do natychmiastowego wstrzymania działań zbrojnych a blok atlantycki do natychmiastowego wstrzymania dostaw broni dla Ukraińców. Nawet jeśli praktyczne skutki takich wypowiedzi w postaci upadku Ukrainy i zwycięstwa Rosji byłyby z eurazjatyckiego punktu widzenia pozytywne, nie powinno nam to zamykać oczu na kryjącą się za nimi bałamutną współczesną katolicką „teologię wojny".

Wypowiedzi Franciszka można by bowiem sprowadzić do tez, że walka jest zawsze – niezależnie od okoliczności i powodów – zła, zawsze trzeba dążyć do jej przerwania, negocjacje zaś i dialog zawsze są dobre i pożądane. Do tego dochodzi jeszcze teza, że broń jest zła, bo prowadzi do wojny, należy więc dokonać powszechnego rozbrojenia i zaniechać produkcji broni.

O tym czy zła jest walka i agresja można by napisać odrębny tekst. W tym miejscu ograniczmy się jedynie do krótkiej uwagi przeciwstawiającej ją w większości nadal zachowującym aktualność ustaleniom w zakresie współczesnej wiedzy przyrodniczej poczynionym przez etologa **Konrada Lorenza** oraz prymatologa **Michaela Ghiglieri**. Ten drugi wskazuje w swojej książce „Ciemna strona człowieka" że agresja po prostu „jest", na podobnej zasadzie jak grawitacja. Stosunki społeczne zawsze regulowane są przez siłę lub groźbę jej użycia i faktu tego nie powinno zaciemniać w naszej świadomości życie w „kryształowym pałacu" (określenie filozofa **Petera Sloterdijka)** nowoczesnego zachodniego państwa z jego policją i armią oraz współczesnej Europy z jej jankeskim protektorem pacyfikującym wszystkie konflikty wewnętrzne i zewnętrzne jak i całą strategię w ogóle.

Ten drugi w książce „Tan zwane zło" udowadnia z kolei, że agresja jest rewersem indywiduacji i osobowej natury: ławice nieróżniących się od siebie ryb nie znają wewnętrznej agresji, skrajnie kolektywistyczne społeczności mrówek i szczurów znają jedynie agresję międzygrupową – agresja międzyosobnicza pojawia się wraz z wyodrębnieniem osobniczego „ja". Jeśli więc

chcemy pozostać ludźmi aktualizującymi pełnię swojego osobowego potencjału, nie możemy pozbyć się agresji, gdyż byłoby to równoznaczne z wyrugowaniem osobowej autonomii ludzkiego indywiduum. Agresji nadać możemy formy społecznie konstruktywne – na przykład pojedynki na śmierć i życie zastępując sportowymi walkami na ringu itp.

Tezy papieża Franciszka mają jednak głębokie teologiczne umocowanie w chrześcijaństwie, będąc rozwinięciem zaleceń Jezusa o „miłowaniu nieprzyjaciół" i „nadstawianiu drugiego policzka" oraz biblijnego proroctwa o „przekuciu mieczy na lemiesze a włóczni na sierpy". Jest to próba ustanowienia radykalizmu ewangelicznego, przez większą część historii chrześcijaństwa ograniczanego do społeczności zakonnych, ogólnocywilizacyjnym standardem. O ile przy tym Kościół rzymskokatolicki wraca dziś takimi tezami do „cnót ewangelicznych" po wiekach „ulegania mentalności pogańskiej", o tyle bliższy związek z rzeczywistością zachowuje teologia wojny Rosyjskiego Kościoła Prawosławnego przedstawiona w wystąpieniu patriarchy Cyryla.

Dla kwestii dyskutowanej w tym tekście najistotniejsza jest jednak teza papieża iż **„broń jest zła, bo prowadzi do walki, by zapewnić pokój należy więc się rozbroić"**. Warto przywołać tu pionierkę badań nad uważanymi za najbliższych ewolucyjnych krewnych człowieka szympansami **Jane Goodall**. W swojej głośnej książce „Przez dziurkę od klucza" jeden z rozdziałów poświęciła zwyczajom wojennym szympansów. Małpy te nie znają oczywiście i nie używają żadnej broni. Pomimo tego, Goodall opisuje, gdy pewnego razu jeden z szympansich szczepów wkradł się niepostrzeżenie na terytorium sąsiedniej grupy, po czym zabił bez powodu oddalonego od stada osobnika, rozrywając go na koniec na strzępy.

Niewiele różniące się wyprawy urządzały oczywiście również podobne liczebnie do grup szympansów archaiczne grupy ludzkich łowców-zbieraczy, za jedyną broń mając niekiedy zebrane w lesie kije i kamienie. Wojna i agresja są więc zjawiskiem

poprzedzającym zbrojenia i powstanie broni, będąc integralną częścią ludzkiej natury. Z drugiej strony, antropolog **Jared Diamond** opisuje w swoich wspomnieniach z Nowej Gwinei, gdy zabrany na pokład samolotu członek archaicznej grupy ludzkiej, gdy maszyna przelatywała nad sąsiednią wioską innego szczepu, poprosił by zawrócić, by mógł zrzucić na jej mieszkańców kamienie – zbrojenia są zatem równie stare jak ludzkość i żadna pacyfistyczna utopia tego nie zmieni.

Libertarianizm

Przejdźmy teraz do zwolenników powszechnego dostępu do broni, którzy nader często wywodzą się w Polsce ze środowisk libertariańskich. Powielają oni ideologię jankeskiego liberalizmu, w której powszechny dostęp do broni palnej jest miarą wolności i równości jednostek. Charakterystyczne jest w tym kontekście powtarzanie z lubością w tych kręgach, że „broń palna wyrównuje szanse" i że zaprawionego w walce i znacznie silniejszego przeciwnika może przy jej pomocy zabić choćby staruszka, kobieta lub dziecko. Takie postrzeganie broni palnej jako instrumentu zaprowadzającego egalitaryzm widać przy tym doskonale na „westernach" USA, gdzie jedynym przymiotem różnicującym przeciwników jest umiejętność szybkiego wyciągania rewolweru z kabury.

Te egalitarna ideologia stworzona została w Ameryce Północnej w ramach kontestacji stanowego porządku Europy, gdzie prawo do noszenia broni (białej) przysługiwało tylko szlachcie, tak więc z założenia stanowi wojowników. Również szlachta wolna była od budzących strach wśród amerykańskich kolonów zależności feudalnych właściwych stanowi trzeciemu. Stany Zjednoczone Ameryki założone zostały przez ludzi stanu trzeciego, którzy po osiedleniu w Ameryce Północnej przestawali tym zależnościom podlegać. Rewolucja 1776 r. miała za swe źródło głęboką niechęć kolonów do tego rodzaju obciążeń. Nowa Anglia, która historycznie okazała się ośrodkiem tożsamości USA, socjologicznie nie znała przy tym

niemal szlachty jako wyodrębnionego stanu wojowników.

Etos wojownika

Trójstanowa struktura społeczna, jak zauważył **Georges Dumezil**, charakteryzuje jednak niemal wszystkie ludy indoeuropejskie i tworzone przez nie cywilizacje. Nie tylko zresztą indoeuropejskie, by wspomnieć choćby feudalną Japonię z jej kastą samurajów i ich bunty w drugiej połowie XIX wieku, których bezpośrednią przyczyną był zakaz noszenia broni białej przez zdegradowanych w reżymie Meji dawnych rycerzy i przyznanie go jedynie oficerom formowanej spośród plebsu armii rządowej. Przywileje szlachty w zakresie posiadania i posługiwania się bronią miały swoją wewnętrzną logikę: tylko wojownik uformowany jest w etosie, sprawiającym że broń w jego rękach jest elementem społecznie konstruktywnym. Wojownik wie bowiem jak i kiedy jej używać – użyje jej więc umiejętnie i odpowiedzialnie, nie robiąc krzywdy sobie ani innym.

Prawdą jest bowiem do pewnego stopnia, jak twierdzą zwolennicy powszechnego dostępu do broni, że oswojenie z nią, uczy odpowiedzialnego posługiwania się nią. To trochę jak ze znajomością języka obcego – ten, kto zna jakiś język naprawdę dobrze, nie odczuwa pokusy by wplatać obcojęzyczne słowa do swoich wypowiedzi. Ten, kto jednak danego języka się dopiero uczy, ma pokusę „bawienia” się nim i demonstrowania swojej jego znajomości nawet w sposób nieadekwatny. Również osoba mająca jedynie okazjonalny kontakt z bronią, jest nią nienaturalnie podekscytowana, podczas gdy ktoś dla kogo broń jest codziennością, traktuje ją jako coś bardziej naturalnego i w sposób bardziej zrównoważony.

Uzbrojony tłum

Zwolennicy powszechnego dostępu do broni mylą się jednak twierdząc, że danie możliwości nabycia broni wszystkim jest tożsame z wychowaniem do cnót wojowniczych. Cywile, którym

rozda się broń, są po prostu uzbrojonym tłumem. Jego wartość bojowa nie jest równa zeru, jest jednak niewiele od niego większa.

Dotyczy to zresztą również armii z poboru, co ilustruje obecna wojna na Ukrainie. Z 900-tysięcznej armii rosyjskiej jedynie 200 tysięcy to żołnierze zawodowi – i tylko ci nadawali się do wysłania na front ukraiński, podczas gdy poborowi okazali się całkowicie bezużyteczni. Pochodzące z poboru armie donbaskich republik ludowych ponoszą dziś największe straty w ludziach. Naprędce mobilizowane rezerwy rosyjskie posiadają równie nikłą wartość bojową. Również po stronie ukraińskiej, gdy wczytać się uważnie w doniesienia, znaczenie w walce posiadają wcale nie rolnicy na traktorach, Romowie, babcie ze słoikami ogórków ani cywile jeżdżący samochodami, lecz profesjonalna armia.

Autorami cyklicznie powtarzających się w USA strzelanin w większości nie są zawodowi policjanci, żołnierze, najemnicy ani członkowie żadnych podobnych grup zawodowo posługujących się bronią palną, dających się więc z pewnym przybliżeniem określić mianem wojowników**, lecz uzbrojeni cywile, którym dano broń, nie formując ich jednak w etosie wojowniczym ani nie wychowując do cnót rycerskich**. Broń traktują jako zabawkę, z niezdrową ekscytacją, jako sposób na gorączkowe i frenetyczne demonstrowanie swojej dominacji, nadużywają jej niczym członkowie gangów lub dawni rewolwerowcy, dla których był atrybutem statusu na który nie zasługiwali, ale który przy pomocy broni starali się wymuszać.

Uzbrojony plebs zawsze jest zdemoralizowany i podatny na zachowania przestępcze. Dotyczy to zarówno plebsu w USA, któremu pozwolono nabywać swobodnie broń (nieprzypadkowo Dziki Zachód miał tak wysoki odsetek zabójstw, a miasta USA notują w tej dziedzinie rekordowe wskaźniki do dziś), jak i plebsu z różnych grup chuligańskich i nacjonalistycznych, który uzbraja się i używa go w różnych konfliktach na obszarach dawnego bloku wschodniego – od dawnej Jugosławii, przez Ukrainę, po Zakaukazie. To właśnie uzbrojony plebs dokonuje przy użyciu

broni przestępstw, rozbojów, zbrodni i gwałtów, broń bowiem jest dla niego dźwignią gwałtownego awansu, na który nie był mentalnie przygotowany odpowiednią formacją ani wychowaniem.

Mentalność koszarowa

Receptą jaką starają się niekiedy do dziś stosować państwa europejskiego kręgu cywilizacyjnego jest swego rodzaju „system koszarowy", którego jednak jedynym faktycznym produktem jest typ mentalny nazywany w Polsce pogardliwie „trepem". Taka „cywilizacja koszarowa", oparta na ślepym posłuszeństwie i bazująca na odwołaniach do najniższych, sprzed indywiduacji, warstw osobowości, napiętnowana została przez **Juliusa Evolę** jako „militaryzm". Jej ideą jest powstrzymanie u rekruta indywiduacji, by pozostawić go w stadium swoistego niedorozwoju, jako „klocek" do wepchnięcia do odpowiedniego „okienka" kolektywnej „foremki". Tego rodzaju militaryzm reprezentowały nowoczesne państwa epoki demokratycznych wojen totalnych, a do dziś jego elementy żywe są w armiach państw przestrzeni dawnego ZSRR.

Słabości tego „subindywidualnego", mechanistycznego modelu ciekawie opisał jankeski pisarz fantastyczno-naukowy **Mel Brooks.** W swojej doskonałej powieści „Zombie Survival" (2003) kreśli scenariusz światowej pandemii zombizmu. Niepotrafiące opanować kolejnych ognisk zarazy Niemcy decydują się radykalnie „skrócić front" wycofując się do „reduty" na pograniczu z Danią by ratować niewielką część populacji, pozostałych zaś pozostawiając własnemu losowi. Porzucona ludność oczywiście protestuje, następnie zaś ginie w męczarniach. Wychowany w ślepym posłuszeństwie rozkazom oficer dawnej armii NRD, nie wytrzymując presji psychicznej, strzela sobie w głowę. Uformowany w duchu brania odpowiedzialności moralnej za własne decyzje i postępowaniu w zgodzie z własnym sumieniem oficer dawnej NRF dźwiga etyczny ciężar decyzji i zdaje egzamin w chwili próby, na śmierć słabszego moralnie towarzysza prychając „mięczak". Siła materialna jest bowiem

zawsze jedynie zewnętrznym wyrazem stabilności wewnętrznej „osi” czy też „pionu” duchowego i moralnego.

Takiemu koszarowemu „militaryzmowi” Julius Evola przeciwstawiał wywierającego na społeczeństwo konstruktywny wpływ „ducha militarnego”. Rozumiał pod nim wspominane tu kilkukrotnie wychowanie do cnót rycerskich, formowanie w etosie wojownika, oraz przewagę i promieniowanie tego ducha na całe społeczeństwo. „Ducha militarnego” można by więc utożsamić ze słusznie podnoszoną w ostatnich latach w polskich środowiskach narodowych ideą „militaryzacji narodu”. Ideę tę rozumieć należałoby jednak nie prostacko – jako po prostu „rozdanie ludziom broni”, bo jedynym tego efektem będą powracające strzelaniny takie jak w USA. „Militaryzacji narodu” nie należy mylić ze stworzeniem uzbrojonego tłumu, czyli daniem cywilom przywilejów należnych jedynie wojownikom.

„Militaryzację narodu” rozumieć należy tak , jak rozumiał „ducha militarnego” baron Evola: jako zwieńczenie społeczeństwa warstwą ludzi uformowanych w cnotach rycerskich, którzy byliby ośrodkiem wokół którego grawitowałoby całe społeczeństwo, oraz których rycerski etos nadawałby temu społeczeństwu formę. Powstaje oczywiście pytanie, jak szeroki zakres społeczny taka formacja mogłaby przybrać?

Wszyscy jesteśmy wojownikami

Sięgnąć by tu należało do bardziej elementarnych warstw ludzkiej natury, niż akcydentalne formacje społeczno-cywilizacyjne – pochodne okoliczności historycznych i warunków geograficzno-klimatycznych. Pamiętajmy, że feudalizm jak i cała gospodarka agrarna były zjawiskami historycznymi i taki też traktować należy opisywaną przez Georgesa Dumezila trójstanową strukturę społeczną ludów indoeuropejskich. Rewolucja neolityczna i gospodarka agrarna to przemiana sprzed kilku tysięcy lat. Człowiek na Ziemi istnieje od co najmniej 200 tysięcy lat, a jego bezpośredni ewolucyjni przodkowie

nawet od ok. 2 mln lat. To, kim jesteśmy, jaka jest nasza natura, uformowało się więc nie w ciągu ostatnich kilkuset lat historii Zachodu czy kilku tysięcy lat cywilizacji po rewolucji neolitycznej, lecz przez sto kilkadziesiąt tysięcy lat życia na afrykańskich sawannach. Chcąc odpowiedzieć na pytanie „kim jesteśmy?", przyjrzeć musimy się znanym nam społecznościom łowców-zbieraczy.

Społeczności takie były relatywnie niewielkie i wojownikami-łowcami byli w nich wszyscy dorośli mężczyźni. Potencjał do stania się łowcą i wojownikiem tkwi więc w naturze każdego mężczyzny i ani cywilizacja agrarna zamieniająca niektórych mężczyzn z muły pociągowe ani współczesne „terapeutyczne" państwo poprawności politycznej podające chłopcom żeńskie hormony by osłabić w nich instynkt agresji, tego nie zmieniły. Dojrzewanie ku cnotom rycerskim to nie tylko potencjał ale też potrzeba każdego zdrowego mężczyzny. Niezaspokojenie tej potrzeby tworzy neurotyków oraz fizyczne i psychiczne kaleki, w niektórych zaś przypadkach nawet niebezpiecznych zwyrodnialców. W społecznościach archaicznych chłopca ku cnotom wojowniczym wychowywały męskie bractwa inicjacyjne, o czym pisali religioznawca Mircea Eliade, antropolog **Jared Diamond** i odnowiciel narracji mitycznej i idei męskiej inicjacji **Robert Bly**.

Jak militaryzować naród

Konkretyzacja tego wniosku to już odrębny temat, kilka punktów nasuwa się jednak natychmiast. Po pierwsze zatem, przywrócenie zasadniczej służby wojskowej. Zwróćmy uwagę, że jej pierwszymi przeciwnikami byli w Polsce libertarianie, zarazem domagający się ułatwień w dostępie do broni palnej. **W świetle tego co dotychczas powiedzieliśmy, libertarianizm jawi się więc jako ideologia chłopców a nie mężczyzn: to ideologia „zabawy bronią" przy histerycznym wręcz odrzuceniu instytucji inicjujących ku męskości i przynajmniej w założeniu mających formować w etosie wojownika**. Zwróćmy też uwagę, że w USA gdzie

regularnie dochodzi do strzelanin, powszechny pobór do wojska wprowadzano jedynie akcydentalnie na okoliczność najbardziej wymagających konfliktów. Współcześni europejscy młodzi tożsamościowcy, jak **Markus Willinger** z Austrii i **Marcus Follin** ze Szwecji, podkreślają zaś formacyjny i inicjacyjny (w sensie inicjacji w męskość) wpływ służby wojskowej.

Po drugie, niezależnie od obciążeń ideologicznych i politycznych, na wsparcie zasługują tego rodzaju inicjatywy obecnej władzy jak formacje obrony terytorialnej. Docelowo powinny one dążyć do objęcia całej męskiej populacji, a prawo do posiadania broni i w ogóle pełnia praw publicznych, jak w Izraelu, powinny być uwarunkowane odbyciem zasadniczej służby wojskowej i przynależnością do tego rodzaju formacji. Na wsparcie zasługują również obecne „klasy mundurowe" i takie formy ich popularyzacji jak znany w naszym kraju przypadek syna **Edyty Górniak** który podjął naukę w takiej właśnie klasie, czy znany z Anglii przypadek syna aktora **komediowego Rowana Atkinsona,** który odbył służbę w jednostkach specjalnych i dołączył do formacji Gurkhów. I ponownie: docelowo należałoby dążyć do odbudowy edukacji zróżnicowanej i zastąpienia „zwykłych" lekcji wychowania fizycznego w szkołach męskich zaprawą militarną. Póki co zaś, znowu – niezależnie od wiadomych obciążeń ideologicznych i politycznych – na poparcie zasługują wszelkie inicjatywy w postaci organizacji paramilitarnych Jak i oczywiście, ogólniejsze propagowanie sportu, sprawności fizycznej i zdrowego stylu życia.

Bardziej problematyczna jest kwestia przysposobienia militarnego kobiet. Wspominana Jane Goodal opisuje, że niekiedy w wyprawach wojennych szympansów brały udział młodociane i niezwiązane wychowaniem potomstwa samice, były to jednak sytuacje rzadkie. W archaicznych społecznościach ludzkich kobiety w wyprawach wojennych, łowieckich ani łupieskich nie uczestniczą. W tradycyjnych społecznościach Azji też jest to raczej nieznane. W sytuacji napaści na osadę czy na grupę kobiet, starały się one jednak przed takimi

napaściami bronić. Przygotowanie kobiet w zakresie sztuki przetrwania i samoobrony byłoby więc zasadne w świetle idei przeniknięcia społeczeństwa „duchem militarnym”.

Figura „Damsel in distress” jest bowiem raczej groteskowym przejaskrawieniem patriarchatu – w zakresie dostępnych sobie możliwości i właściwego sobie potencjału, kobieta powinna oczywiście móc zadbać o siebie i obejście pod nieobecność mężczyzn lub też wspomóc ich w obronie. Predyspozycje kobiet dotyczą jednak „obrony ogniska domowego”, mając przez to charakter defensywny. Angażowanie kobiet do działań „ofensywnych”, to znaczy współczesnych odpowiedników wypraw wojennych, łowieckich i łupieskich, to przedrzeźnianie natury rodem z Rewolucji Francuskiej (słynny obraz Delacroix) i bolszewickiej Rosji.

Naród mężczyzn

Społeczeństwo przeniknięte „duchem militarnym” jak ujmował to baron Evola, czy też „naród poddany militaryzacji” jak chcą dzisiejsi polscy narodowcy, posiadałoby wartość obronną nawet nieuzbrojone. Posiadałoby też wartość nawet w okresie pokoju, na należne im naczelne miejsce wynosząc ponownie ducha męskości, cnoty rycerskie i etos wojownika, w świetle których zblaknąć musiałaby dzisiejsza inwersja wartości na szczyt wynosząca kapitalistyczną plutokrację i rozbuchany konsumpcjonizm oraz materializm. Uzbrojenie takiego narodu którego dusze uprzednio by „umundurowano”, nie stanowiłoby zagrożenia dla porządku społecznego, jak stwarza go „powszechny dostęp do broni” w USA. Byłby to bowiem naród mężczyzn dojrzałych do bycia wojownikami, a nie chłopców urządzających sobie „zabawy z bronią”.

Ronald Lasecki

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.

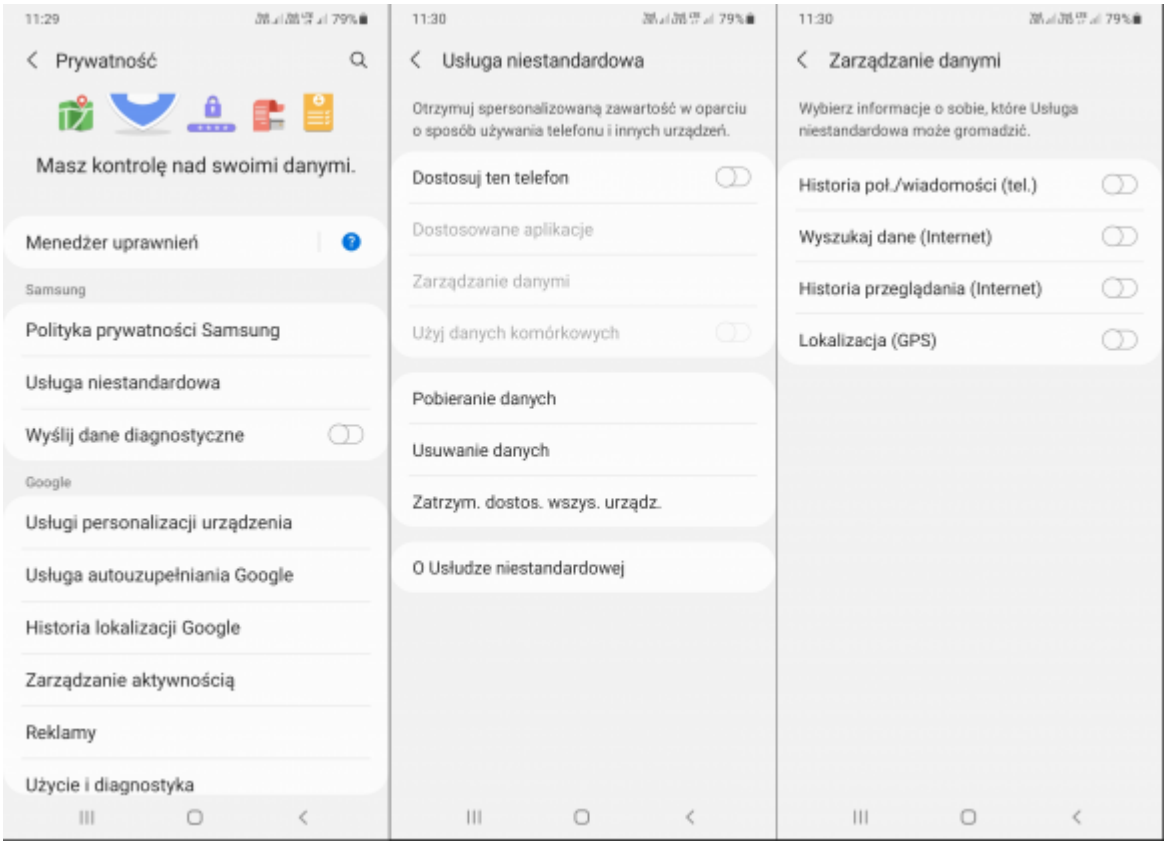
Jakie dane zbiera Samsung i co z

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.

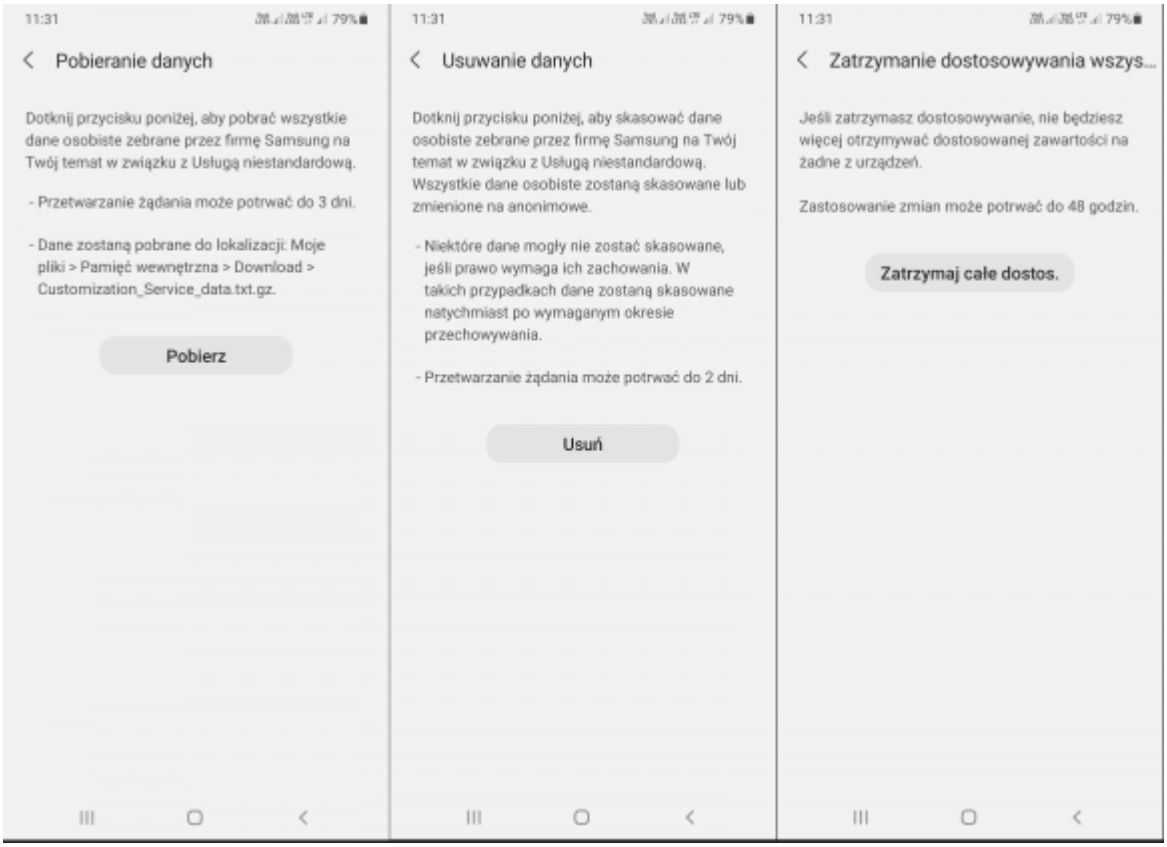
Dlatego sugerujemy np. nie używać dostarczanej wraz systemem przeglądarki, sugestywnie podpisanej jako „Internet” – lepszy będzie nawet Google Chrome (po włączeniu w ustawieniach „Piaskownicy prywatności”), ale można też pokusić się o zainstalowanie mobilnej wersji Firefoksa albo DuckDuckGo. Nie zaszkodzi też poszukać alternatywnych rozwiązań dla pozostałych narzędzi oferowanych przez producenta.



„Usługa niestandardowa” oferowana przez Samsunga

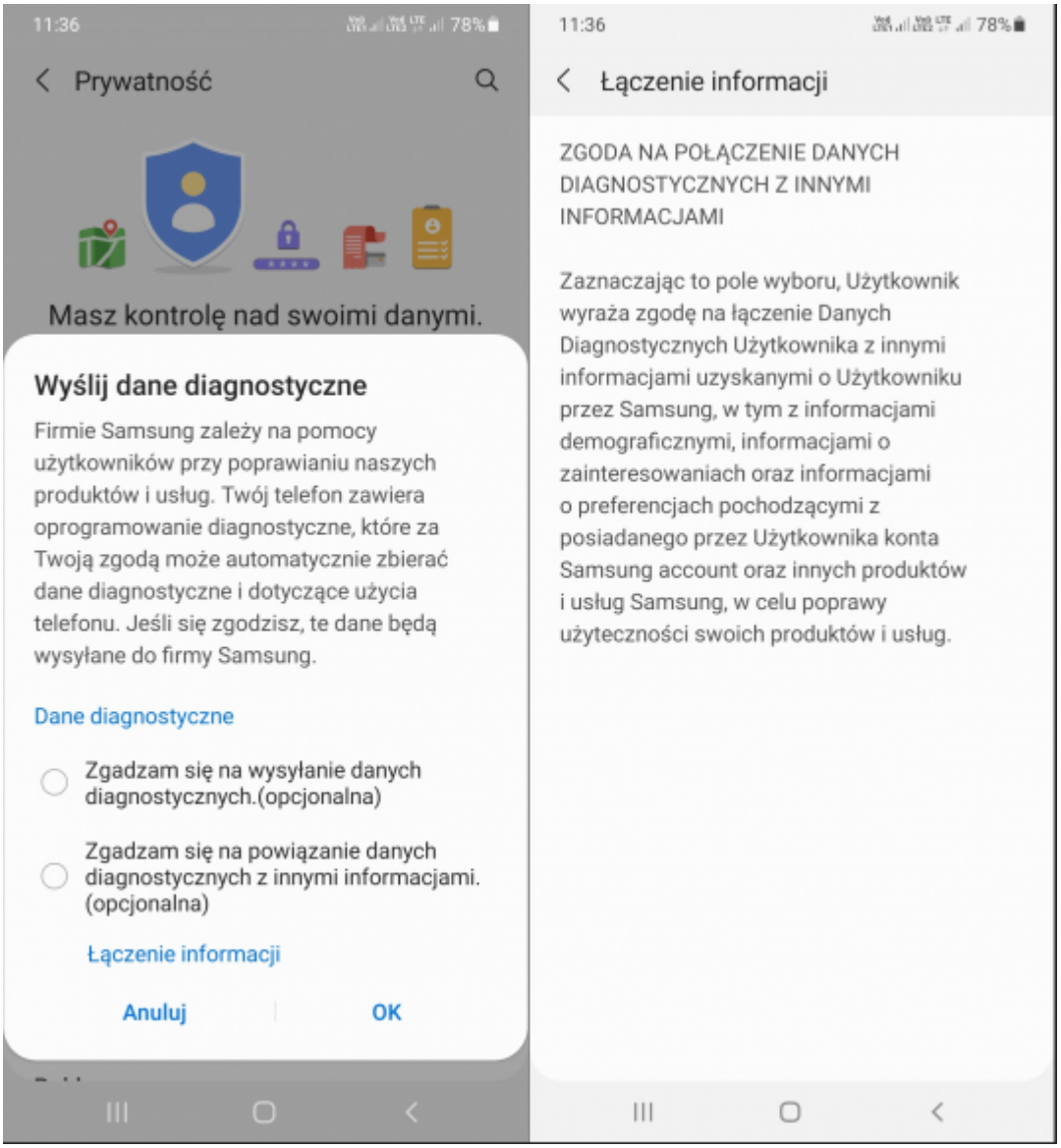
Po wejściu do ustawień telefonu w zakładce „Prywatność” znajdziemy ponadto pozycję „Usługa niestandardowa”, która odpowiada za dostarczanie reklam i innych treści w oparciu o nasze (rzekome) zainteresowania i odwiedzane przez nas miejsca w świecie rzeczywistym. Można ją skonfigurować po zalogowaniu się 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

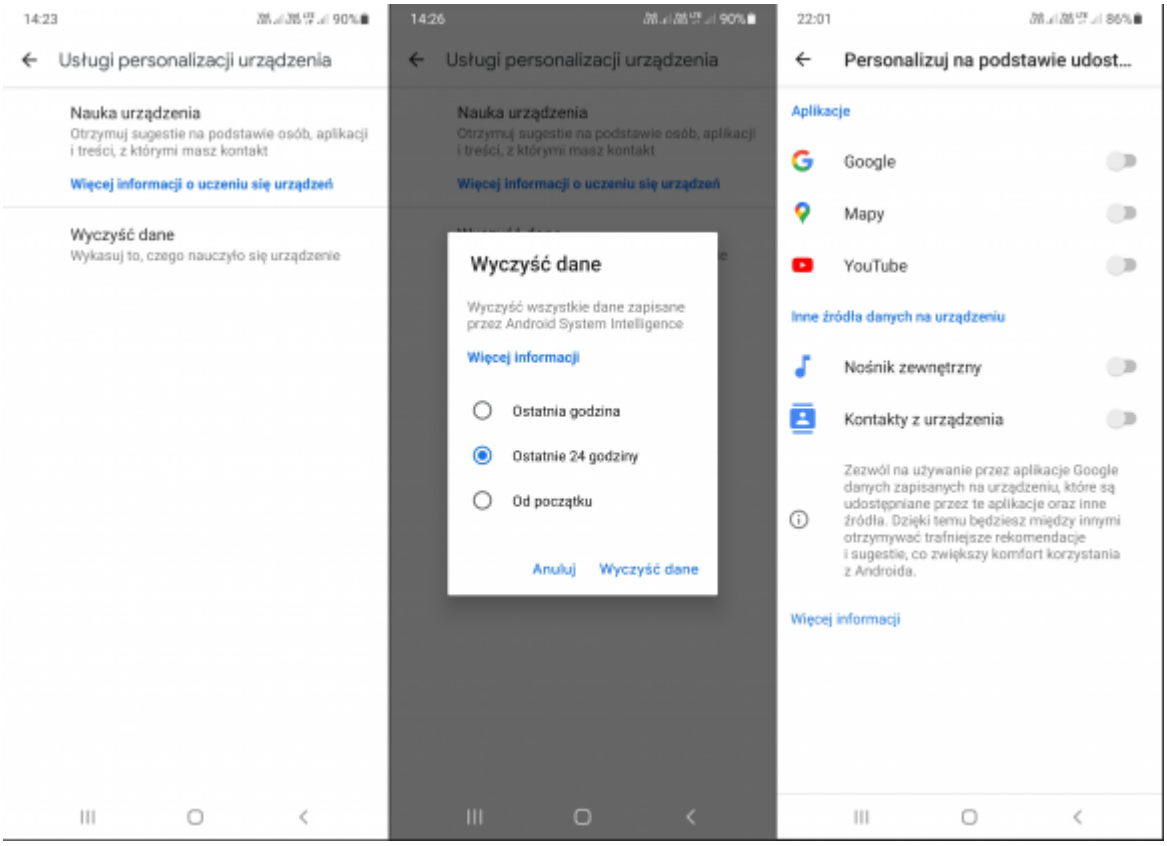
W zakładce „Prywatność” znajdziemy ponadto opcję wysyłania Samsungowi danych diagnostycznych, której również sugerujemy nie aktywować. Klikając w link „Dane diagnostyczne”, dowiemy się, że decyzja o nieprzekazywaniu firmie tego typu informacji nie wpłynie w żaden sposób na funkcjonalność telefonu. Producent 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

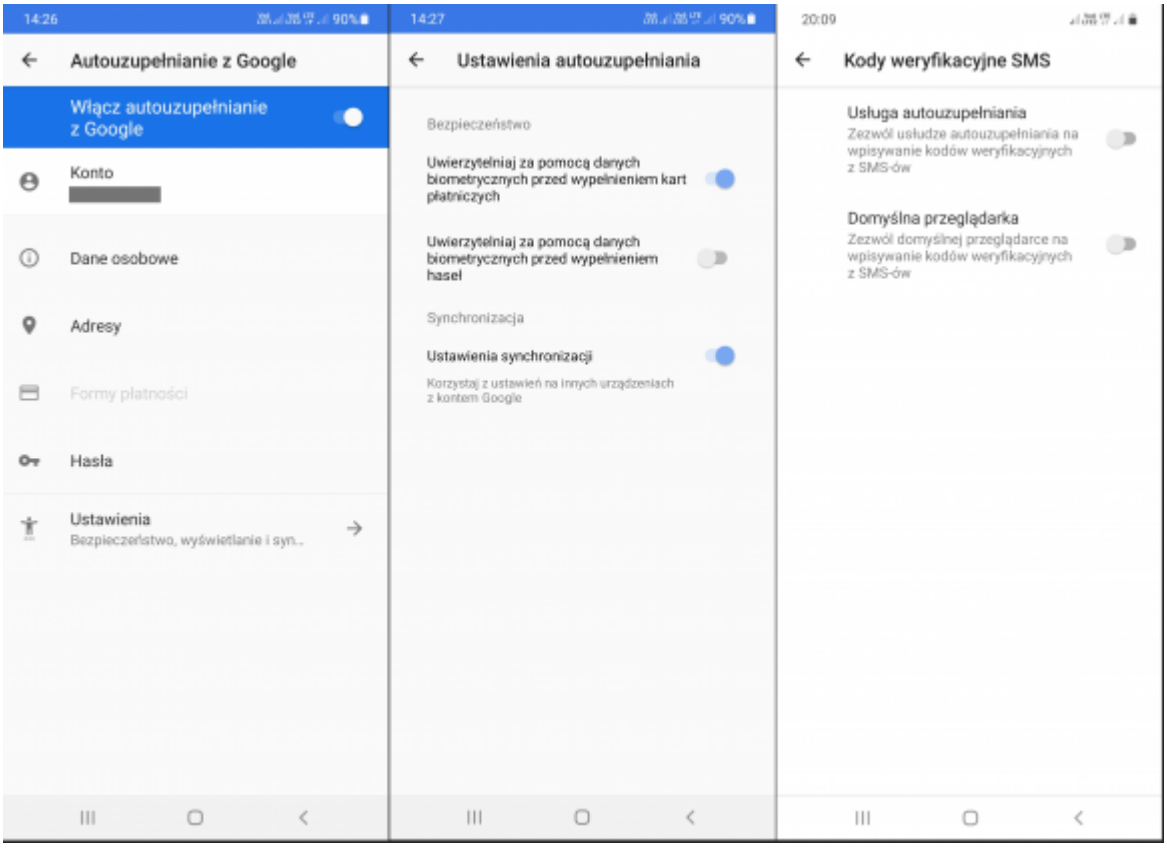
Przegląd ustawień prywatności związanych z usługami Google zaczynamy od możliwości personalizacji urządzenia i akurat w tym przypadku nie chodzi o wyświetlanie reklam, tylko o podpowiadanie użytkownikowi na podstawie jego wcześniejszych działań, co może w danej chwili zrobić. Jeśli np. zaznaczymy jakiś 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.

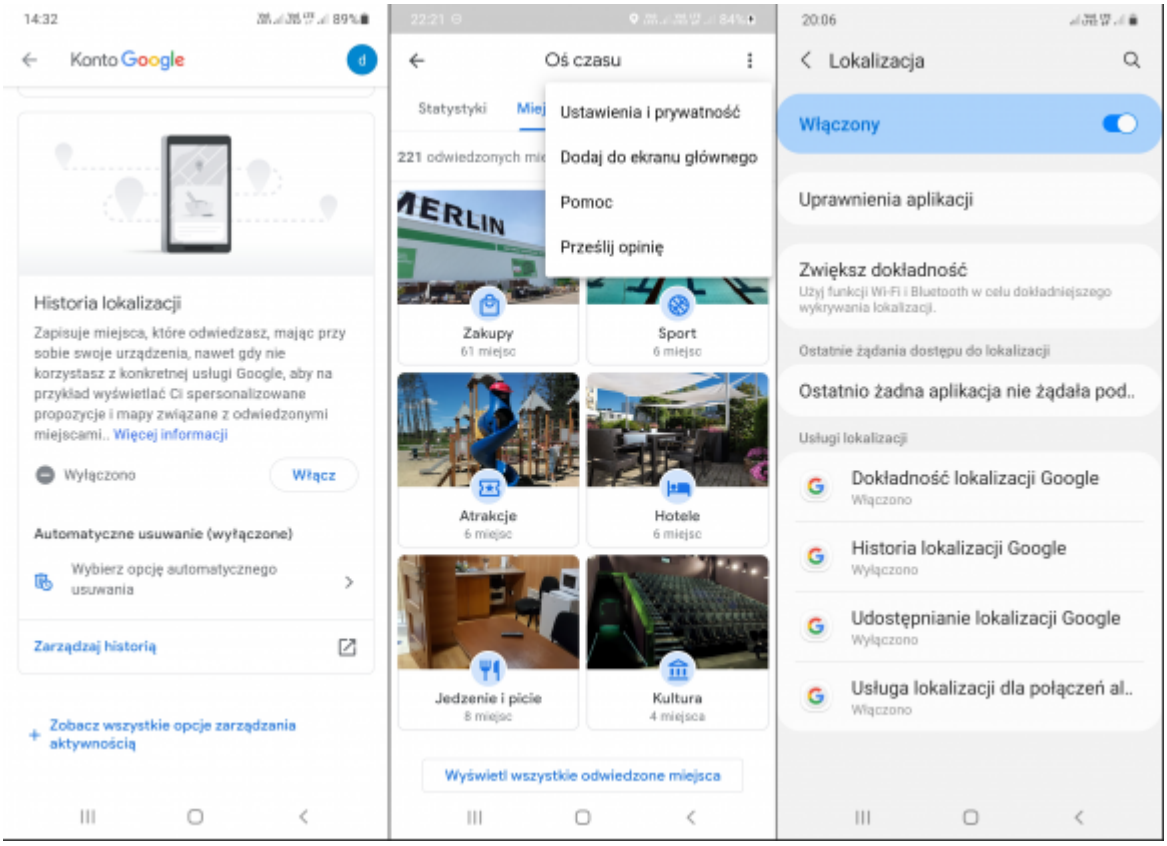


Ustawienia autouzupełniania

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".

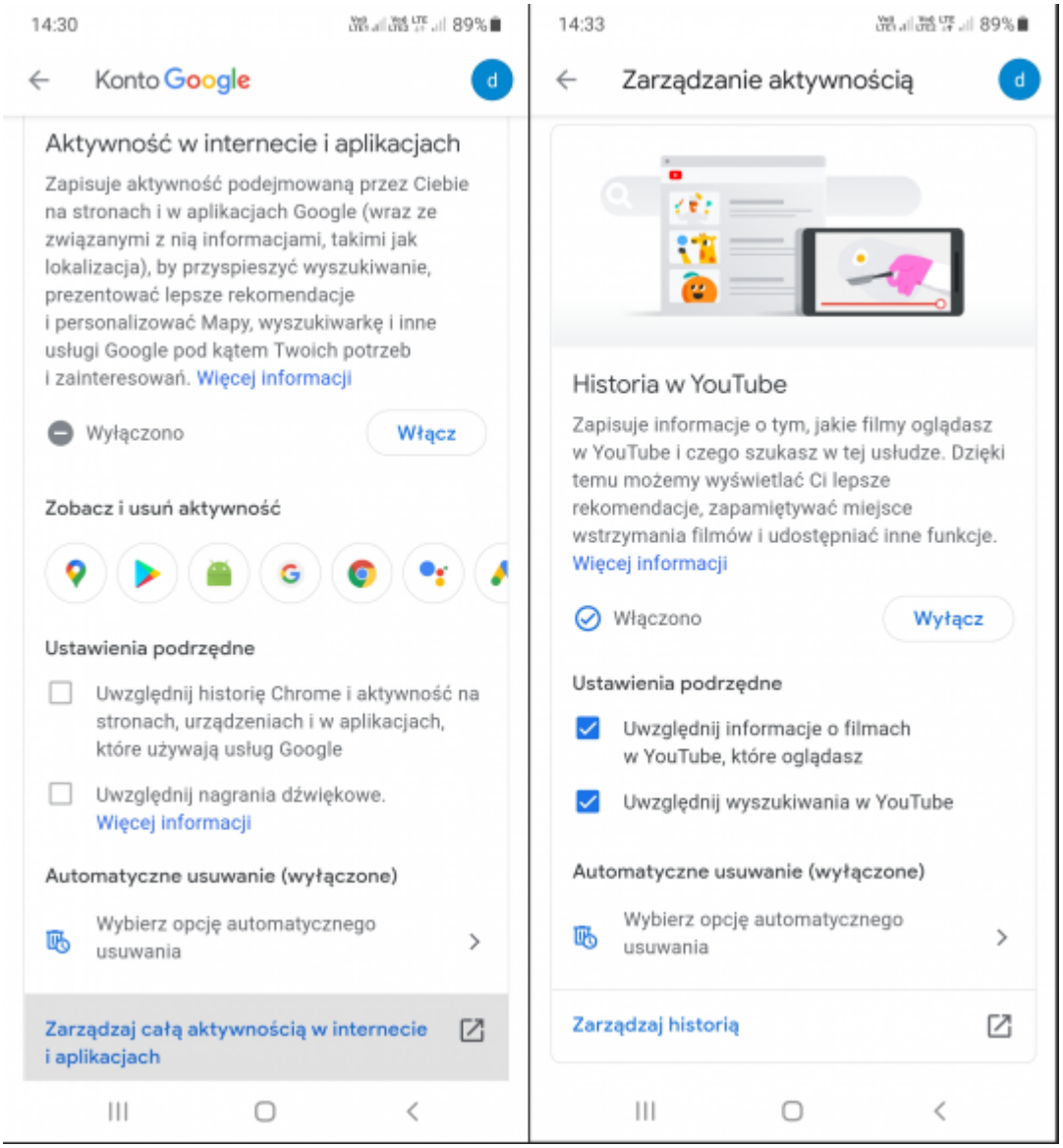


Zarządzanie lokalizacją

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.

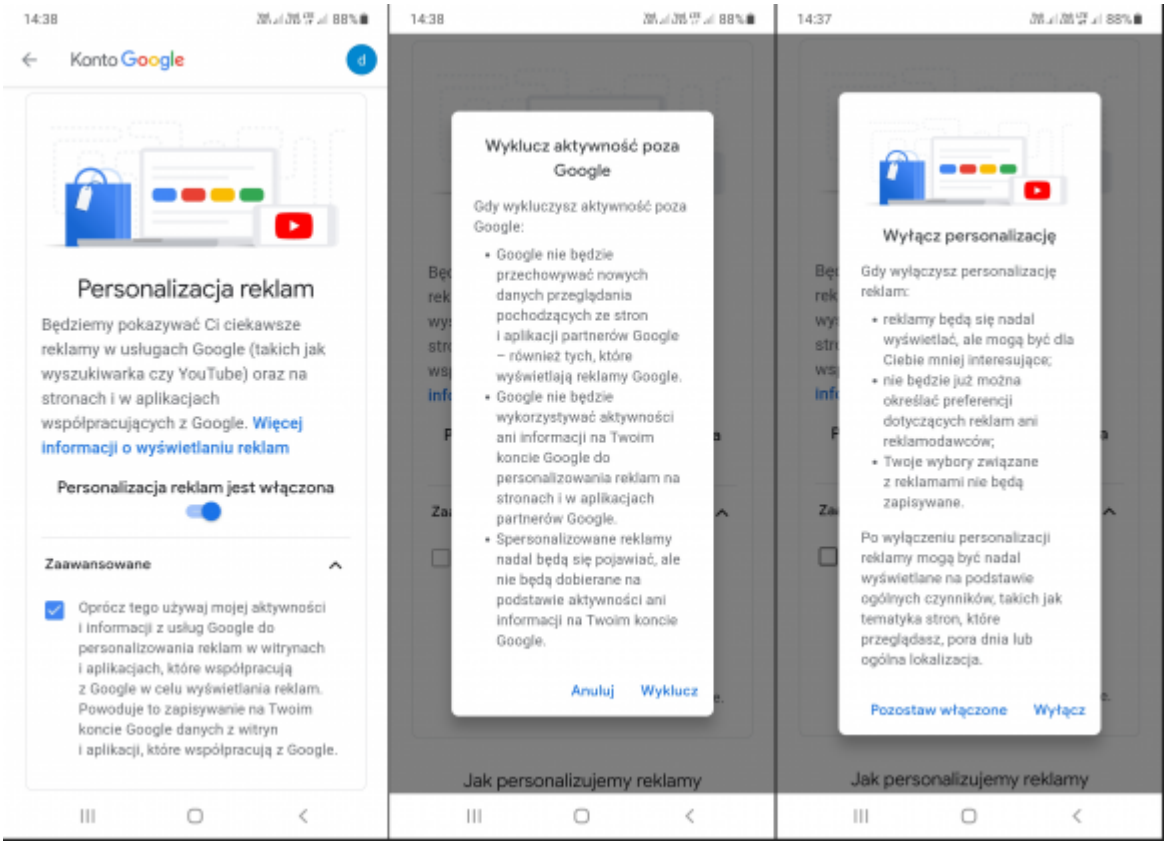


Zarządzanie aktywnością

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).

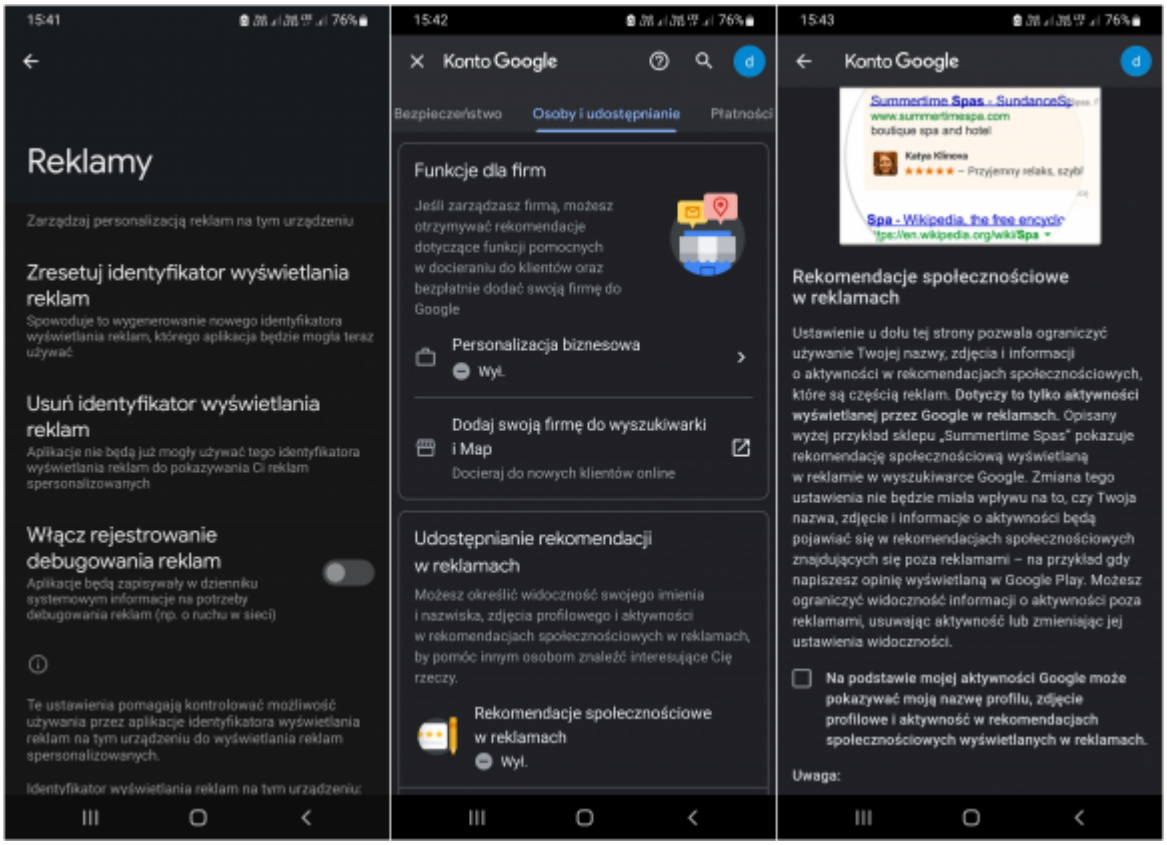


Personalizacja reklam

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.

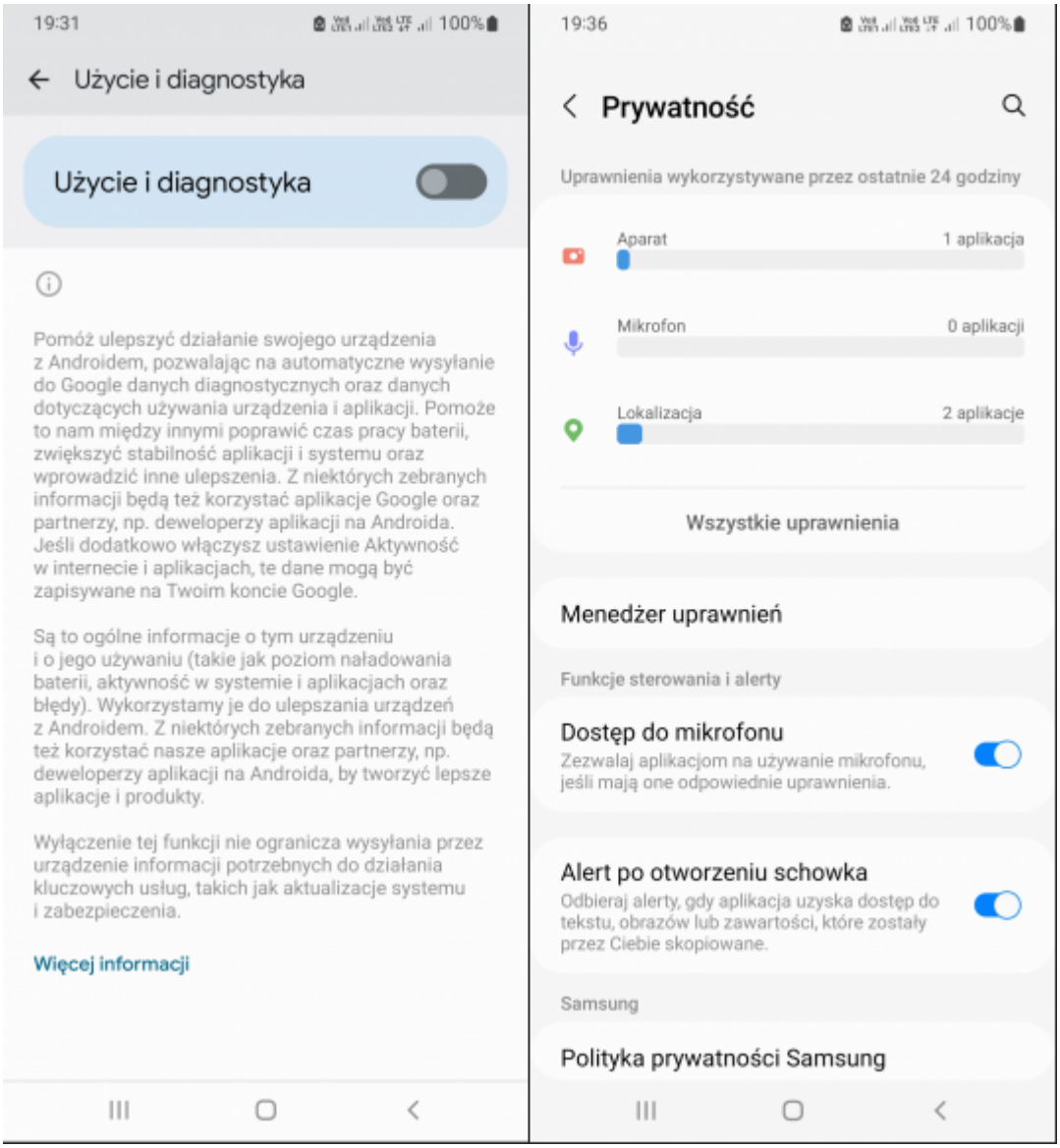


Reklamy i rekomendacje społecznościowe

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