11. září na steroidech

Když se sledování šíří jako virus

Všeobecný strach z pandemie umožnil poměrně bezbolestně po celém světě sbírat osobní data, která mají v první řadě pomoci v boji s nemocí, ale často jsou zneužívána. I tuzemská zkušenost s aplikací eRouška přitom ukazuje, že informace lze anonymizovat, a zachovat tak soukromí občanů.

HONZA ŠÍPEK

„Data! Potřebujeme spoustu dat. (…) Potřebujeme na chvíli kašlat na GDPR," burcovala iniciativa českých ajťáků Covid19cz, zformovaná v tažení proti koronaviru. Zprávy o globální epidemii se rychle měnily a u mnoha lidí se strach z ohrožení transformoval do horečnaté snahy něco podniknout. A sledovací technologie, budovaná zejména pro potřeby marketingu, hodnocení úvěrů a komerčního profilování lidí, byla první po ruce.

Zatímco za normálních okolností sledujeme ukrajování z občanských svobod velice obezřetně a každý ústupek z práva na soukromí, svobodu pohybu či vyjadřování je těžce vybojovaný, tentokrát jsme během pár dní přijali uzavření hranic a omezení pohybu, svobody shromažďování i podnikání. Ani jsme příliš neprotestovali. „Omezení některých základních lidských práv se šíří Evropou skoro stejně rychle jako virus samotný," varovala začátkem dubna Amnesty International.

Během karantény jsme si hromadně instalovali telekonferenční software Zoom plný bezpečnostních děr, před nimiž varovala FBI i tuzemský Národní úřad pro kybernetickou a informační bezpečnost. Když skupina Covid19cz analyzovala data z platebních karet, z nichž média poněkud mylně odvodila, že téměř polovina lidí, kteří se vrátili z lyžovačky v Itálii, nedodržela povinnou čtrnáctidenní karanténu, neptali jsme se, jak se k datům dostala ani co se s nimi děje za normálních okolností. Nepřekvapily nás ani grafy Googlu, který ze sledování mobilních telefonů odvodil, že lidé ve středních Čechách trávili v parcích o 37 procent času více, než je obvyklé, nebo že obyvatelé Pardubicka v práci tráví o 18 % méně času než za normálních okolností. „Potenciál ke zneužití moci je extrémní," řekl Guardianu Ron Diebert, vedoucí skupiny Citizen Lab na Torontské univerzitě, „je to tak trochu 11. září na steroidech."

Digitální roušky a obušky

Autoritářské státy už dávno nevládnou jenom za pomoci obušků, a aplikaci povinně či „doporučeně" instalovanou do mobilních telefonů občanů zavedly už desítky vlád. V Indii vás bez ní nepustí do letadla. Ve Spojených arabských emirátech chce aplikace přístup k vašim fotografiím, mikrofonu i kameře. V Číně je napojena na finanční a dataminingovou službu Alipay a její uzavřený algoritmus vám rovnou spočítá status: jste-li „zelení", můžete všude, pokud jste „oranžoví", můžete být požádáni, abyste zůstali doma, a když jste „červení", máte čtrnáctidenní karanténu. Některým lidem s nařízenou karanténou se dokonce přede dveřmi jejich bytu objevila kamera. Jiným ji úředníci přišli nainstalovat přímo dovnitř. BBC popsala případ studenta na Tchaj-wanu, kterému se nad ránem vybil telefon s povinnou sledovací aplikací: do hodiny mu volali čtyři úředníci, přišla mu esemeska, že při porušení karantény se vystavuje postihu. A pak u dveří zaklepala policie.

V Moskvě přišla vláda s bizarním řešením: před každou cestou z domu musí občan oznámit úřadům, kde přesně se bude pohybovat, přiložit IČO zaměstnavatele, poznávací značku auta a kopii občanky – a získá tak QR kód, kterým se na ulici prokazuje. Přetížené servery vydávaly kódy s několikahodinovým zpožděním, případně rovnou spadly, načež Rusko obvinilo Západ, že na ně útočí „zahlcovacím útokem" (DDoS). V situaci, kdy ve vestibulech moskevského metra zřízenci kontrolují QR kódy ručně nebo kamsi zmateně volají, zatímco dav se hromadí a potenciálně infikuje, Moskvané žertují, že Západ útočí za pomoci DDoS spíš na vestibuly metra.

Přestože se trasování sociálních kontaktů za pomoci telefonů nabízí jako moderní a efektivní řešení, narychlo spíchnuté sledovací aplikace měly celou řadu bezpečnostních děr. A tak v pákistánském Balúčistánu koluje po sociálních sítích tabulka se seznamem nakažených, z katarské povinně instalované sledovací aplikace bylo možné získat informace o statisících obyvatel, mapa nakažených unikla úřadům na Slovensku a některé balkánské státy dokonce seznamy osob v karanténě samy zveřejňovaly.

Během pár dní jsme přijali uzavření hranic a omezení pohybu. Ani jsme příliš neprotestovali. Ilustrace Bety Suchanová

Oficiální aplikace ze Severní Dakoty sdílejí své údaje s firmami Foursquare i Google – vzhledem k tomu, že se při vývoji aplikací často používají jejich vývojářské knihovny, které „volají domů", nebude jediná. Podle společnosti Top10VPN, která analyzovala 47 mobilních aplikací na epidemiologické sledování sociálních kontaktů z celého světa, 51 procent z nich obsahovalo přilepené štěnice od Googlu a Facebooku.

Pochybnosti Britů vzbuzuje plán spolupráce Národní zdravotní služby s dataminingovým obrem Palantir, který má zpracovávat všechny údaje o epidemii Covid-19. V Izraeli nejenže na sledování nakažených pracovala kontrarozvědka Šin bet, využívající údaje od operátorů, pozdvižení způsobil ministr obrany, který chtěl ke spolupráci přizvat i tamější firmu NSO Group, známou vývojem špionážního malwaru, nasazovaného do telefonů disidentů i novinářů po celém světě. Kyvadlo veřejného mínění se začalo pomalu vracet zpátky a izraelská parlamentní komise koncem dubna sledování telefonů neprodloužila. I tak bylo v jeho důsledku pro porušení karantény zatčeno 203 osob. Podobně rozhodl slovenský Ústavní soud, když pozastavil účinnost speciálního zákona, jenž měl právě sledování mobilů vládě umožnit.

Jak sledovat anonymně

V Evropě, citlivé na otázky soukromí a sledování, začali výzkumníci vymýšlet způsoby, jak provozovat aplikace, které zaznamenávají sociální kontakty nakažených, ale přitom zachovávají soukromí. Oba dva hlavní koncepty používají rozhraní Bluetooth na mobilním telefonu. Aplikace vysílá jedinečný pseudonymní identifikátor a současně zaznamenává identifikátory telefonů, které se vyskytly poblíž. Identifikátory nejsou nutně spjaté s fyzickou identitou uživatele a jeho osobními údaji, navíc se v pravidelných intervalech obměňují. Obě technologie se liší ve způsobu reakce v případě, že se u uživatele prokáže nákaza: model PEPP-PT nahraje na centrální server seznam všech kontaktů, s nimiž se nakažený potkal, a server posléze ostatní uživatele upozorní na nebezpečný kontakt. Druhý model, DP3T, jde v zachování soukromí ještě dál. Pokud se u uživatele prokáže nákaza, zařadí se jeho identifikátor na seznam, který si pravidelně stahují všechny ostatní telefony, a teprve ony vyhodnotí, zda se s kontaktem někdy setkaly. Ani centrální server tedy nevidí seznam našich setkání.

Hegemoni mobilního trhu Google a Apple přišli ve své rivalitě s nevídanou dohodou, že oba zapracují stejné rozhraní na sledování sociálních kontaktů přímo do svých operačních systémů. A zatímco jejich implementace se podobá spíše bezpečnějšímu modelu DP3T, česká aplikace eRouška, vyvinutá iniciativou Covid19cz, odpovídá spíše modelu prvnímu.

Přesto tato iniciativa IT firem ochromenému státu výrazně pomohla: vyvinula systém „vzpomínkových map" pro call centra hygieniků, kteří stopují kontakty nakažených, a její technická sekce za pomoci desetimilionové sbírky vyvinula plicní ventilátor CoroVent. Stát si od ní vypůjčil i název „chytrá karanténa" a sdružení pro něj nakonec vyvinulo i aplikaci eRouška. Aplikace má otevřené zdrojové kódy, které prošly nezávislými audity. Paradoxně jí nejvíce uškodil vládní epidemiolog Roman Prymula, který tvrdil, že bude použita ke kontrole dodržování karantény – nic takového podle autorů v plánu nebylo a není to ani technicky možné.

„Jednou z motivací, proč jsme chtěli pomoci a současně být u toho, bylo, abychom nedali vládě záminku pořídit si například izraelské řešení, které bez souhlasu sbírá lokační data uživatelů plošně," řekl na online konferenci Covid-ITe 2020 Petr Bartoš, jeden ze spolutvůrců takzvané chytré karantény. Zatím jsme tedy vyvázli, otázkou zůstává, na jak dlouho.

Autor je dokumentarista.

Text vznikl za podpory Nadace Rosy Luxemburgové