

T. Obrenovic, STRATEGIC CULTURE: ANONYMITA ONLINE - jak nezanechat stopu?

- CZ24 News | 18. dubna 2023

Tato celková informace může trochu po-osvětlit i jednu „záhadnou záležitost“, totiž jak například ukrajinské tajné služby (a samozřejmě nejen ony) získávají přehled o potenciálních osobách, které lze naverbovat, či prostě zneužít i jen pro jediný úkol – pozn.překl.) Teda kromě jiného, přemýšlivým to „další“ dojde samo sebou. Peter 008

Vzhledem k tomu, že podrobné sledování online (online surveillance) dnes začíná již v raném věku, je třeba o digitální hygienu dobře pečovat již od dětství.

Zdá se, že u nezkušených uživatelů internetu panuje iluze, že pouze někteří jedinci jsou pečlivě sledováni a tajně „sledováni“ online. Běžný uživatel má tendenci se domnívat, že tajně sledovat a odposlouchávat nic netušícího uživatele internetu je příliš nákladné a složité a že jeden konkrétní jedinec, on nebo ona, tj. prostý uživatel, není pro nikoho zvlášť zajímavý, aby byl vůbec odposloucháván nebo pečlivě sledován.

Fakta však nemají slitování, ukládání dat a informací je dnes poměrně dostupné a tzv. big data o každém uživateli se ukládají průběžně již zhruba osm až deset let, protože ti, kdo nás bedlivě sledují, nemohou přece vědět, čím a kým bude dnešní student za deset či patnáct let (například poslancem parlamentu, vysoce postaveným státním úředníkem, úspěšným podnikatelem nebo třeba jakou pozici bude současný zaměstnanec střední úrovně zastávat za tři až čtyři roky a s kým bude v budoucnu pracovat.

Důkladně sledovat stovky milionů uživatelů formou online sledování je dnes technicky možné a není to nijak přehnaně nákladné, takže to dělá mnoho jednotlivců v USA i ve světě.

Existují takzvané „markery“ – citlivé body, body zájmu – které se určují prostřednictvím automatických postupů hromadného zpracování dat. Analýza dat je v současné době poměrně levná. Jednotlivci, kteří provádějí podrobné sledování druhých, se ani nijak zvlášť nezajímají přesně o nějakého konkrétního člověka, ale pomocí převodu informací do jeho dopadu – na koho z obrovského množství uživatelů lze formou on-line sledování v průběhu let a let podrobného sledování shromáždit kompromitující údaje o vztazích této osoby, jejích slabostech, sklonech atd.

Na vlastní digitální hygienu by si tedy měl dávat pozor každý jednatlivec, zejména státní úředník, politik, manažer, podnikatel, osoba s vysokou reputací nebo celebrita a osoba s vysokou reputací v jakékoliv oblasti zájmu, tedy všichni ti, na které již lze pohlížet jako na rizikovou skupinu a kteří jsou již nyní podrobeni důkladnému sledování (dohledu) a ovlivňování. **Vzhledem k tomu, že důkladné sledování online (online surveillance) dnes začíná již v raném věku,** je třeba dobře dbát na digitální hygienu již od dětství, protože shromážděný kompromitující materiál o tom, že nějaké dítě má prostě sklony k nějakým lumpárnám typickým pro dítě, bude „cenný“ v jeho dospělém zralém věku, kdy se z dnešního dítěte stane dospělý, zralý člověk, který může časem změnit svůj vlastní pohled na svět.

Je zřejmé, že pečlivé sledování (dohled) významných osob na internetu je prováděno pečlivě a velmi podrobně, a to včetně podstrčení programů typu trojský kůň do počítače člověka tím, že se všechny

komunikační kanály spojí dohromady sledováním jeho bezprostředního digitálního okolí.

Tato nová digitální realita doslova totální viditelnosti a vysokého rizika vyžaduje nová pravidla digitální hygieny.

Anonymita: Je možné nezanechávat stopy?

Osoba 1. Dobrý den, je toto anonymní telefonní číslo FSB?

Osoba 2. Ano, Michail Petrovič, ano, je. Jsme tu pro vás. Co byste nám chtěl říct?

Zdá se, že uživatelé internetu si myslí, že si mohou zachovat soukromí a zůstat anonymní a neviditelní, pokud si to přejí, vstupují do online sítě prostřednictvím anonymních účtů pod maskou svých avatarů a přezdivek, používají různé anonymizéry, které skrývají vlastní IP adresu, virtuální privátní sítě VPN, které skrývají vlastní IP adresu, soukromé virtuální adresy, vstupují na web prostřednictvím sítě TOR, aniž by policie nebo speciální služby mohly tohoto “mazaného” uživatele rozpoznat a/nebo pečlivě sledovat.

Částečně je na tom však něco pravdy. Je možné, aby člověk nepozorovaně existoval a působil v digitálním prostoru, pokud má znalosti a zkušenosti profesionálního hackera nebo digitálního špiona. Naštěstí, nebo ne, je tento soubor znalostí a návyků pro většinu uživatelů nedostupný.

Běžný uživatel neustále zanechává vlastní digitální stopu, kterou může využít pro svou určitou identifikaci, má-li o to zájem a disponuje-li vhodnými nástroji,

Podpis: Digitální otisky prstů

Používáním digitálních zařízení s přístupem k internetu neustále, v každém okamžiku, vytváříme jedinečné “digitální otisky prstů” a stopy svého jednání a svého digitálního prostředí. Ty se nazývají “podpisy” („signatura“ – z latinského jazykového kořene sign).

Například v geoanalytice existuje pravidlo čtyř bodů, na základě kterých se dá analyzovat, které z nich máte tendenci navštěvovat nejčastěji. Jeden bod, například stanici metra v blízkosti vašeho bydliště, navštěvují desítky tisíc lidí s chytrými telefony v kapse a zároveň dva body: jeden v těsné blízkosti vašeho domu a druhý bod v bezprostřední blízkosti vaší práce navštěvuje jen několik tisíc lidí. Tři body - dvě stanice metra a vaše oblíbená restaurace - nyní se počet zúží na pouhých několik desítek lidí s chytrými telefony v kapsách. A pokud k tomu přidají adresu vaší maminky, kam chodíte jednou nebo dvakrát týdně, nebo adresu vaší posilovny - budete jediným člověkem s touto kombinací geografických bodů, kam chodíte.

To je váš individuální geografický digitální podpis, váš vlastní “digitální otisk prstu”. Takových digitálních podpisů je spousta a ty se dostanou k dekódování obrovskému množství těch, kteří vás pečlivě sledují (online a digitální sledování osoby).

Historie vašeho prohlížení, tj. seznam webových stránek, které denně navštěvujete, tvoří váš jedinečný digitální “otisk” vašich prohlížečů (vyhledávačů), a to jak v logách (denících) vašich prohlížečů, tak v cloudu jejich výrobce a také v nesčetných marketingových a reklamních systémech a “počítadlech” na internetu.

Je možné, že pro vaši vlastní jedinečnou přesnou identifikaci nemusí být navštíveny čtyři webové stránky, ale například čtrnáct, ale to není až tak podstatné.

Obecně platí, že pokud je vektor, což je soubor číslic, složený ze stop, které za sebou zanecháváte (geografické body, navštívené webové stránky, stažené aplikace), dostatečně dlouhý, definitivně vás bez jakýchkoli pochybností dokonale identifikuje. Například pokud zveřejňujete statusy na sociálních sítích s anonymní přezdívkou, v takovém případě tvoříte minimálně vektor dat v čase a přesných časech jejich zveřejnění a komentářů, a to i bez ohledu na jejich obsah).

Z pohledu poskytovatele internetu tvoříte jeden konkrétní časový vektor = data a časy vstupu na internet.

První vektor znají uživatelé sociálních médií – platformy a dohledové programy pro pečlivé sledování sociálních médií. Druhý časový vektor zná váš domácí poskytovatel internetu nebo váš mobilní operátor, který sice nevidí vaše příspěvky na sociálních sítích, ale zpravidla zná vaši osobní identitu.

Prolínáním a křížením těchto vektorů například na formální žádost orgánů činných v trestním řízení (např. orgánů činných v trestním řízení, soudů atd.) lze poměrně snadno dekódovat údajně anonymní identitu člověka.

Ano, všechny vektory všech uživatelů internetu bude třeba podrobněji zkoumat a porovnávat s vektorem vašich příspěvků na sociálních sítích. Tento úkol je spíše technického rázu a s dnešními internetovými servery a jejich technickými možnostmi jej lze vyřešit poměrně snadno.

Celkově je třeba mít na paměti, že váš jedinečný digitální podpis se skládá z:

1. tovární identifikátor IMEI vašeho chytrého telefonu
2. seznamu aplikací a souborů ve vašem zařízení, jako je notebook nebo mobilní telefon, který je dostupný pro mnoho zařízení a aplikací, antivirový program, počítačové viry a trojské koně, prohlížeč, operační systém, kancelářské aplikace a všechny kancelářské aplikace vašich kolegů atd.
3. vaše prostředí Bluetooth – všechna zařízení, se kterými se vaše Bluetooth dostane do kontaktu za účelem sdílení dat nebo se kterými se kdy dostalo do kontaktu a digitálně se spojilo, vaše hudební zařízení doma nebo v autě, vaše sluchátka, vaše hlasové nástroje atd.
4. vaše prostředí Wi-fi – seznam všech zařízení Wi-fi v okolí vašeho pracoviště nebo domova.
5. historie vašeho prohlížeče – seznam webových stránek a internetových služeb, které pravidelně navštěvujete.
6. seznam vašich přátel na sociálních sítích – váš sociální dojem je jedinečný i v případě, že se rozhodnete na internetu používat pseudonym. Tento seznam existuje u platformy sociálních médií jako takové a u všech “monitorovacích” programů a také ve vašem prohlížeči.
7. váš lexikální podpis – skupina vašich oblíbených slov, frází a rčení, a dokonce i jedinečná kombinace vašich běžných překlepů.
8. váš obličej a obličej ostatních na vašich fotografiích a videích na sociálních sítích – kombinace všech obličejů, včetně toho vašeho mezi ostatními, je také jedinečným identifikátorem.
9. váš zeměpisný podpis – seznam vašich tras a zeměpisných bodů, které navštěvujete, ať už ve vašem městě, nebo mimo něj. Existuje ve vaší navigaci nebo v navigačních aplikacích.
10. váš hlasový podpis – vaše hlasová digitální stopa nebo “otisk”, který zanecháváte buď při používání mobilního telefonu, nebo mikrofону na vašem notebooku.

11. klíčová slova vašeho seznamu pro vyhledávání – kromě situačních klíčových slov pro vyhledávání v závislosti na situaci existují běžná klíčová slova, která často vyhledáváte a zadáváte, a jejich kombinace je jistě jedinečná, tj. vaše vlastní, a existuje ve vašem oblíbeném vyhledávači a prohlížeči.

12. Váš seznam oblíbených témat – například na zpravodajském portálu.

13. seznam zařízení ve vašem okolí – například váš poskytovatel internetu “vidí”, která další mobilní zařízení se běžně nacházejí v bezprostřední blízkosti, například členové vaší rodiny nebo blízcí kolegové.

A tento seznam může pokračovat dále. Všechny tyto podpisy jsou uloženy ve vašem chytrém telefonu a v obrovském množství těch nezávislých prohlížečů, které s vámi nesouvisejí (reklamní systémy, mobilní operátoři, poskytovatelé internetu, prohlížeče, vyhledávače, sociální média, online platformy, aplikace atd.)

Pokud by náhodou nějaký podpis chyběl, lze během procesu identifikace přidat další podpisy mezi výše uvedené, a pak bude tato kombinace určitě jedinečná: vaše vlastní kombinace.

To, co jsme právě naznačili výše, znamená, že **i anonymní uživatel na webu zanechává své jedinečné digitální stopy a “otisky”**. Pokud máte dva účty, jeden pro běžnou komunikaci pod svým skutečným jménem a druhý, který je anonymní, buďte si jisti, že je lze automaticky propojit analýzou jejich podpisů.

AUTOR: Tatiana Obrenovic

[ZDROJ](#)

Překlad: Peter 008/Pokec24