Digital rights crash course

Primii pași spre înțelegerea drepturilor digitale

Primul capitol din cursul introductiv despre ce sunt drepturile civile digitale este dedicat protecției vieții private. Explicăm ce înseamnă dreptul la viața privată, ce sunt datele personale, explorăm cum poți să controlezi mai bine datele pe care le dai despre tine online și ce unelte tehnice poți folosi ca să te protejezi.

Dreptul la viață privată – de ce?

Ți-ai posta numele și prenumele pe un site public? Dar adresa poștală de acasă? Numărul de telefon? Adresa ta de email? Lista cu bolile de care suferi? Câți copii ai și numele lor? La ce grădiniță merg? De la ce ore? Câți bani ai în fiecare cont? Numărul cardului? Pin-ul cardului?

Dacă ai răspuns nu la cel puțin una din întrebări, atunci înseamnă că ai stabilit limitele în care ești dispus să lași pe alții în viața ta privată. Dacă ai răspuns da la toate întrebările înseamnă că încă le cauți….dar tot ai dreptul la viață privată. :-)

Dar toate răspunsurile sunt normale. Așa cum atunci când mergi cu trenul poți să ai pe cineva lângă tine care să îți povestească toată viața sa, la fel poți să ai pe cineva care te ignoră complet. Și ambele sunt OK.

Pentru că dreptul la viață privată nu înseamnă dreptul de a te ascunde, ci dreptul de a decide. De a decide când, cum și cu cine partajezi informațiile personale. Înseamnă că nu te obligă nimeni să ieși în piața publică să strigi că te-a părăsit soțul/soția/logodnicul/logodnica. Și nici pe Facebook. Dar dacă vrei să faci, te lasă. Pentru că e decizia ta.

Calculatorul, Internetul și în general mediul digital pot colecta mai multe date personale despre tine. Despre unele poate știi, despre altele nu. De aceea, ApTI lansează o campanie de conștientizare și promovare a acestor drepturi.

Ce sunt datele personale? Ce să fac dacă cineva postează poze cu mine pe un site? Când pot da în judecată? Cine îmi ascultă telefonul? Cum pot să șterg cookie-urile? Acestea sunt tipurile de întrebări la care vrem să răspundem în următoarele luni. Și nu numai. Facem și acțiuni de advocacy pentru respectarea acestor drepturi.

Fii pe fază. Cunoaște-ți drepturile și cere ca ele să fie repectate.

Avem din ce în ce mai puțin control asupra datelor noastre personale și de obicei este netransparent modul în care acestea sunt prelucrate de operatori. Nu este întotdeauna clar explicat la cine ajung datele noastre, în ce scop sunt prelucrate, ce măsuri de protecție s-au luat și pentru ce durată se păstrează.

Ce sunt datele personale?

Definiția datelor personale poate părea complicată – definiția exactă o găsești în Legea 677/2001. Explicat într-un mod mai structurat, datele personale pot fi orice date:

• ale tale (nume, prenume, CNP, amprentă, ADN)

• despre tine (vârstă, sex, etnie, rasă, orientare sexuală, politică, religioasă, starea de sănătate)

• în legătură cu tine (adresa de domiciliu, reședința, adresa de e-mail, ocupația, venitul)

Care, singure sau cumulate, te-ar putea identifica ca persoană – adică orice alt tip de date care se pot corela pentru a duce la identificarea ta.

Aceste date sunt personale dacă te pot identifica în mod direct sau indirect, altfel le considerăm date anonime. De exemplu, dacă spun “un bărbat de 48 de ani din Constanța” – acestea sunt date anonime, pentru că este practic imposibil să putem identifica această persoană. Dar dacă zicem “un bărbat de 48 de ani din Constanța care conduce mașina CT-02-HYNNJJJ”, atunci îl vom putea identifica dacă îl vedem pe stradă sau dacă avem acces la datele din registrul poliției de înmatriculare a mașinilor.

Deci definiția datelor personale este foarte largă. Ceea ce este foarte bine pentru că în felul acesta se poate oferi o mai bună protecție. Datele personale sunt un lucru dinamic, tot timpul pot fi noi identificatori care spun ceva despre tine și care te pot identifica.

Nu există o listă completă cu exemple de date personale pentru că orice informații care pot duce la identificarea unei persoane pot fi considerate date personale. De exemplu, pe lângă nume, adresă, contul bancar, amprentă, fotografie, intră și orice date care, deși nu sunt intim legate de tine, pot fi folosite pentru a te repera. Cine ar fi crezut că niște simple cuvinte introduse într-un motor de căutare (cum ar fi Yahoo, Bing, Google) pot duce la identificarea unei persoane? Ei bine, se poate și s-a și întâmplat deja. Este interesant de citit despre cum o femeie din Lilburn, Georgia a fost identificată doar după căutări; există și o serie de scurt metraje despre asta, recomandăm I love Alaska.

Care sunt categoriile speciale de date personale?

- rasa
- etnia

- orientarea politică
- religia
- convingerile filozofice sau de natură similară
- apartenența sindicală
- date privind starea de sănătate
- date despre viața sexuală
- În plus sunt considerate date cu un regim special:
- date cu caracter personal având o funcţie de identificare de aplicabilitate generală, cum este codul numeric personal (CNP)
- date personale referitoare la fapte penale sau contravenții

Mai multe despre **regulile speciale de prelucrare a datelor din categoriile speciale** poți citi aici: https://privacy.apti.ro/date-sensibile/

Te-ai întrebat câte date dai despre tine online?

Să luăm exemplul Waze, o aplicație de navigare pe care o puteți folosi și pentru a evita traficul. Oare de ce o asemenea aplicație ar vrea acces la evenimentele din calendar, plus la informațiile confidențiale? Este asta esențial pentru funcționarea aplicației? Sau de ce vrea să poată citi și modifica contactele din agendă? Nu merge altfel? Sau Runkeeper, care vrea să aibă acces la lista de apeluri efectuate – pentru ce anume e de folos asta unei aplicații care măsoară câți kilometri ați alergat?

Încă un test ar fi prin Panopticlick.eff.org. Aici puteți vedea cât de unică este configurația browser-ului și câte informații se trimit la o simplă accesare a unei pagini. Deși unele par a fi doar niște detalii tehnice, aceste informații pot spune foarte multe despre dvs. și, implicit, conduc la o serie de concluzii despre comportamentul dvs. Vizionați și seria de videoclipuri scurte Do Not Track pentru mai multe informații.

Cum poţi controla mai bine datele pe care le oferi despre tine?

De obicei, când instalăm o aplicație nouă (vezi și cel mai recent exemplu cu Windows 10 sau cu Bing pe telefon), apar o mulțime de informații, bucăți foarte mari de text despre care nu ne dăm seama tot timpul exact la ce se referă. Totuși, în procesul de instalare, luați o serie de decizii importante pentru interacțiunea cu aplicația și pentru protejarea intimității. De exemplu, permiteți aplicației să vă cunoască locația? Acceptați să aibă acces la cameră și microfon sau la numerele din agendă? Vreți să primiți ultimele noutăți?

De cele mai multe ori, suntem tentați să nu fim atenți la ce scrie (cine citește termenii și condițiile?!) și pur și simplu acceptăm toate setările, ca să se termine mai repede instalarea și să putem folosi programul.

Așadar, câteva **sfaturi** ar fi:

> Umblă la „Setările avansate / Advanced settings”. De obicei, acolo găsiți setările mai aprofundate care vă oferă mai mult control asupra programului pe care îl folosiți.

> Verifică aplicațiile și setările și de pe calculator, și de pe telefon/tabletă. Mai ales dacă aveți programe care se sincronizează pe toate dispozitivele pe care le folosiți.

Online nu mai înseamnă doar calculator sau laptop, smartphone și tabletă. Înseamnă și televizor, jucării, frigider, mașină, contor inteligent și orice alt dispozitiv cu senzori, conectat la Internet (Internet of Things).

Cum văd câtă informaţie este colectată despre mine?

Un prim pas ar fi citirea politicii de confidențialitate și verificarea termenilor și condițiilor site-urilor, dispozitivelor (vezi Smart TV sau Smart Barbie) sau ale programelor/aplicațiilor pe care le instalați (vezi Windows 10 sau Facebook sau Facebook Messenger). De obicei, anumite setări sînt selectate automat, iar pentru a le dezactiva trebuie să mergeți în meniu pentru a le personaliza în funcție de preferințele și nevoile dvs.

Apoi, Lightbeam arată, prin metode interactive de vizualizare a datelor, care e relația dintre diferite site-uri, cum interacționează site-ul primar pe care îl accesați cu site-uri terțe. Cel mai evident exemplu este atunci cînd sînt butoane de social media pe o pagină sau cînd există posibilitatea de a vă conecta la contul site-ului pe care îl vizitați prin Facebook sau Google; dar, în același timp, veți descoperi și relațiile mai puțin vizibile dintre site-uri. De exemplu, hotnews.ro e legat cu tradiționalele Facebook, Google, Twitter, dar și cu site-uri precum chargeplatform.com sau avandor.com. Ce fac site-urile acestea?

Cum să fim mai atenți la setările privind confidențialitatea?

Sunt câteva lucruri la care putem fi atenți pentru un control mai bun asupra programelor pe care le instalăm și asupra comportamentului online.

> Selectați atent aplicațiile sau site-urile pe care le folosiți. Citiți termenii și condițiile/permisiunile de care au nevoie aplicațiile pe care le instalăm (geolocalizare, microfon, cameră, fotografii, agenda telefonică). Cu atât mai mult dacă serviciul este gratuit, fiindcă modelul de afaceri este posibil să fie bazat chiar pe vînzarea de baze de date personale.

> Nu ziceți pe Internet ce n-ați scrie pe gard. Când postați informații sau comentarii pe Internet e ca și cum ați striga în gura mare în piață ca să vă audă toată lumea. Internetul este spațiu public, Facebook este spațiu public.

> Nu puneți excesiv de multe informații despre dvs. pe Internet. Toate check-in-urile pe care le dați, toate postările în care indicați locul unde sînteți sau ce urmează să faceți pot ajunge să ricoșeze împotriva dvs. Nu exagerați cu postările, e ca și cum chiar dvs. i-ați invita pe hoți să vă jefuiască.

> Nu presupuneți că sînteți în siguranță dacă anumite setări vin pre-bifate. Pachetul implicit nu înseamnă că acea configurare este cea mai bună pentru dvs.; de cele mai multe ori, opțiunile deja selectate înseamnă mai multe date despre dvs. transmise și mai puțină transparență față de ceea ce se întîmplă cu datele dvs. Cine știe exact la ce se referă „avem nevoie de informațiile personale colectate pentru a îmbunătăți serviciul livrat”? Adică cum…?

> Folosiți unelte care respectă viața privată – pentru browser, pe mobil sau pentru calculator. Există o serie de tutoriale și ghiduri care prezintă aplicații orientate către protejarea vieții private online pe care le puteți consulta. Aveți răbdare să testați aplicații în genul acesta pentru a identifica ce vi se potrivește mai bine.

> Luați în considerare folosirea sistemelor de operare și a programelor cu licență deschisă (open source). Fiind cu licență liberă, oricine poate avea acces la codul-sursă și verifica exact cum funcționează. Pe lîngă sistemele Windows și Apple, mai există și Linux. Pe lîngă Microsoft Office, mai există și Libre Office.

Modul implicit nu ar trebui să fie „Dă-mi datele tale personale pentru a-ți oferi un serviciu”. Nu ar trebui să încurajăm acest nou model de afaceri prin a fi nepăsători față de experiența digitală și a accepta absolut tot ce ni oferă. Ar trebui să avem întotdeauna o alegere și să fim foarte conștienți de cum anume se desfășoară totul. Altfel, o să întâlnim din ce în ce mai des derapaje și va fi poate prea tîrziu să le oprim.

Ce unelte tehnice putem folosi pentru a ne proteja viaţa privată?

> Folosește motoare de căutare care nu păstrează date despre căutări. De exemplu Startpage.com sau DuckDuckGo.com
> Folosește browsere care nu sunt legate de firme mari deja aflate pe alte piețe din zona digitală – Firefox, Abrowser sau Icecat sînt variante mai bune.
> Folosește plug in-uri suplimentare pentru a evita profilarea online și a bloca reclamele inutile, gen: Ghostery, Privacy Badger, Adblock Plus, Disconnect sau HTTPs everywhere.
> Pentru un chat securizat pe telefon și desktop, folosește Signal, Wikr, Wire
> Învățați să vă criptați fișierele sau întregul calculator ori telefon.
> Folosește doar e-mail-uri cu conținut criptat dacă trimiteți chestiuni sensibile prin e-mail.
> Învață să folosești browser-ul ToR și sistemul de operare Tails pentru soluții complexe și aproape perfecte de protecție a vieții private pe Internet.

Te-ai întrebat cum se realizează supravegherea în era digitală?

Viaţa privată nu înseamnă ceea ce vrei să ascunzi. Ci mai degrabă ce informaţie personală decizi să dezvălui, cui şi în ce context. Până şi cei care spun că nu au nimic de ascuns reacţionează imediat în mod negativ dacă le ceri datele cardului de credit. Sau gîndiţi-vă doar la ultima informaţie legată de sănătatea dvs. – cu cine aţi împărtăşit această veste şi cînd? Aţi fi preferat să vă puneţi această informaţie pe frunte, pentru ca oricine să o poată citi?

În al doilea rând, există viaţă privată în era digitală. Doar că dezvoltarea tehnologică, odată cu cea a modelelor de business din ultimii zece ani – care îţi dau un serviciu ce pare gratuit, dar de fapt îl plăteşti cu datele tale personale – face ca, în practică, să ai diferite grade de viaţă privată în funcţie de uneltele digitale pe care le foloseşti. Partea bună este că există soluţii şi alternative pentru majoritatea problemelor referitoare la acest subiect. Partea proastă este că ele sînt extrem de puţin folosite sau chiar deloc şi că marele public foloseşte aplicaţiile cele mai intruzive, dar şi cele mai promovate.

Supravegherea privată în era digitală

Îmi zicea un amic din SUA, cu un zâmbet de tipul ce ironie are viaţa asta, că serviciile secrete americane s-au chinuit încă de la înfiinţare să strîngă cît mai multe date personale despre cetăţenii americani. Iar apoi a venit Facebook şi toţi le-au dat de bunăvoie…

Această mirobolantă şi atotcuprinzătoare reţea socială a reuşit performanţa demnă de invidiat de a avea 1,5 miliarde de conturi (e încă neclar cîţi oameni sînt pe Facebook şi câte conturi nu sunt reale) prin oferirea unei infrastructuri tehnice care le permite oamenilor să comunice unii cu alţii.

Ceea ce uită Facebook să îţi explice în detaliu la înscriere este că serviciul pare gratuit, dar plăteşti cu vârf şi îndesat cu datele tale personale. Şi nu doar cu cele pe care le dai când îţi deschizi contul, cu lista de prieteni, cu like-urile pentru subiectele tale de interes, cu identificarea gratuită a prietenilor din poze sau cu orice altă acţiune pe care o faci în mod vizibil. Ci şi cu datele şi informaţiile pe care le dai fără să-ţi dai seama. Cea mai simplă dintre ele ar fi faptul că Facebook ştie cînd vizitezi orice site care are implementat butonul de Like, chiar dacă tu nu îl apeşi. Mai mult, studii recente (2015) ale cercetătorilor de la Universităţile din Cambridge şi Stanford demonstrează că un calculator poate determina personalitatea ta mai bine decît cei mai buni prieteni de familie doar prin analiza a mai mult de 150 de like-uri din Facebook. Dacă are peste 300 de like-uri pe care le poate analiza, dă rezultate mai bune decît propria ta soţie (sau soţ).

De asemenea, dacă scopul Facebook ar fi doar să vândă reclame pe baza profilului tău, poate nu ar fi o problemă atât de gravă. Doar că utilizările datelor Facebook merg dincolo de această metodă de a face bani şi merg în direcţii pe care nimeni nu le poate prezice. Un studiu al Facebook de anul trecut, care a stîrnit un scandal imens, ne oferă o mică previzualizare a potenţialului viitor: în acest studiu secret, realizat pe 689.000 de utilizatori care nu au fost informaţi, lista însemnărilor prietenilor a fost modificată pentru a arăta mai mult conţinut pozitiv sau negativ. Astfel, potrivit acestui studiu, s-a influenţat comportamentul utilizatorilor pentru „prima demonstraţie experimentală de contagiune emoţională la scară mare, prin reţelele sociale“.

Şi problema scopului ascuns (sau neintuibil uşor de o persoană neavizată) nu se limitează doar la Facebook sau alte servicii de pe Internet. În fond, ce trebuie să facă o păpuşă Barbie din era digitală? Să fie mai inteligentă cînd se joacă cu copilul tău? Sau să se conecteze la Internet ca să-i spună producătorului ce profil are copilul care se joacă cu ea? Şi ce trebuie să facă un TV inteligent (Smart TV)? Să folosească „inteligenţa“ pentru a consuma mai puţină energie? Sau pentru a deveni un fel de receptor ambiental care poate înregistra tot ce se vorbeşte în acea cameră? Puteţi înlocui păpuşa Barbie sau Smart TV-ul din întrebările de mai sus cu alt frigider, maşină, contor inteligent de electricitate sau, extrapolînd, cu orice alt dispozitiv cu senzori, conectat la Internet sau care transmite informaţii în alt mod.

Supravegherea statului în era digitală

Cele trei decizii ale Curţii Constituţionale din România din ultimul an care au privit în mod direct sau indirect acest subiect (legile legate de stocarea datelor de trafic, de înregistrarea obligatorie a cartelelor PrePay şi conexiunilor WiFi şi, respectiv, de securitatea cibernetică), cît şi decizia Curţii Europene de Justiţie în cazul directivei privind stocarea datelor de trafic, ar fi trebuit să fie baza discuţiei pentru criteriile oricărui sistem guvernamental ce implică colectarea, păstrarea sau accesarea unui sistem informatic care colectează datele personale ale cetăţenilor.

Trei noi măsuri propuse sau aplicate de diverse entităţi din Guvernul României ne arată că baza de discuţie nu există, iar noţiunile legate de viaţa privată, cît şi cerinţa ca asemenea decizii să fie adoptate doar prin legi, sînt ignorate în mod constant de autorităţi:

● O nouă ordonanţă stabileşte un sistem naţional de înregistrare a datelor tuturor pasagerilor care zboară cu avionul. S-a creat deja o nouă structură în MAI (Ministerul Afacerilor Interne) pentru a supraveghea aceste date. Scop: prinderea teroriştilor;

● O propunere de hotărîre de guvern creează un sistem naţional de evidenţă în care toate datele personale ale turiştilor vor fi înregistrate pentru o perioadă nedeterminată într-un sistem informatic integrat naţional (şi nu descentralizat şi pe hîrtie, ca pînă acum – cînd, oricum, unităţile hoteliere trimiteau zilnic Poliţiei, potrivit uzanţei comuniste, evidenţele lor cu turiştii cazaţi). MAI va avea acces la baza de date în temeiul unui simplu protocol de colaborare. Scop: prinderea teroriştilor;

● ANAF se pare că a accesat anumite baze de date ale altor instituţii publice cu date personale pe baza unor simple protocoale. Deşi scandalul a apărut odată cu lista marilor îmbogăţiţi care nu îşi pot demonstra averile, povestea este mai veche, ajungînd deja în faţa Curţii Europene de Justiţie, unde Avocatul General şi-a exprimat opinia în iulie 2015.

Din păcate, după cum se vede, o luăm de la capăt cu aceleaşi probleme şi întrebări, fără a dezbate public întrebarea-cheie: este acceptabil să supraveghem toată populaţia României (sau o categorie anume a ei) pentru a-i prinde pe X sau Y? Şi, dacă da, care este supravegherea maximă admisă?

Trebuie colectate toate datele de trafic din comunicaţii şi de pe Internet pentru toţi cetăţenii? Putem cere tuturor celor care cumpără o cartelă PrePay să îşi dea datele din cartea de identitate? Pentru siguranţa noastră, nu ar fi mai bine ca ADN-ul nostru să fie colectat de la naştere şi pus într-o bază de date? Dacă tot ne dăm amprentele pentru paşapoartele biometrice, nu ar fi logic ca ele să fie stocate într-o bază de date comună care să fie folosită pentru identificarea infracţiunilor de omor? Şi, în fine: în aceste condiţii, nu pare absolut normală şi justificată măsura de a duce maşina de scris la serviciul de securitate pentru înregistrarea ei?

Este evident că poziţia noastră este clară: orice supraveghere în masă, care nu îl priveşte pe X sau pe Y (unde există indicii sau suspiciuni că ar comite o infracţiune), este pur şi simplu disproporţionată din start şi nu vedem cum o astfel de măsură ar putea să fie acceptabilă în sistemul actual de protecţie a dreptului la viaţă privată. Partea şi mai complicată este că statul are acces, în anumite condiţii care uneori sînt neclare, la toate datele colectate de privaţi, deci s-ar putea ca în majoritatea cazurilor să ne semnăm singuri deciziile de supraveghere.

Putem face ceva cu supravegherea în era digitală?

Da. În cazul acestei supravegheri private mai există soluţii: de la decizia de a nu cumpăra un produs sau aplicaţie de mobil care pare prea invaziv(ă) pînă la soluţii sau alternative tehnice. Vezi mai sus.

În cazul supravegherii publice, este mult mai complicat. Acţiunile noastre de a explica de ce este nevoie de o analiză serioasă a acestui domeniu înainte de adoptarea unor astfel de acte normative se lovesc de cele mai multe ori de un zid al prejudecăţilor şi dorinţei de securitate cu orice preţ. În cele mai rele cazuri, am primit şi o replică de genul „Staţi liniştiţi şi nu vă mai zbateţi, oricum în cîţiva ani vom fi cu toţii cipaţi“.

Şi atunci, soluţia de a demonstra că astfel de măsuri sînt excesive şi încalcă drepturile fundamentale este găsită de obicei, în mare parte din cazuri, spre finalul traseului: publicare informaţii şi conştientizare publică – participare dezbatere publică – (după caz) atacare act normativ la Avocatul Poporului, instanţe de drept comun, Curtea Constituţională, CEDO sau Curtea Europeană de Justiţie.

Hai sa trecem la mituri.

#1. Sunt prea neimportant ca să-i pese cuiva.

Am auzit de multe ori zicându-se: „Și ce dacă mă ascultă? Cui îi pasă de conversațiile mele banale zilnice?”

Dacă tu crezi că ești neimportant, atunci nici drepturile tale nu contează. Nu doar dreptul la viață privată. Ci și cel la viață, la muncă sau la sănătate. Dacă nu îți pasă de drepturile tale, atunci să fii sigur că nici altora nu le pasă.

Da, programele de supraveghere secrete sunt ilegale și încalcă drepturile și libertățile. Să mai amintesc că nu toți ne-am născut în democrație și că s-a luptat și se luptă pentru drepturi? Să mai amintim că nu ai cum să știi în ce context (de cine, cum, pentru ce?) vor fi folosite aceste conversații banale în viitor?

Și exact – sunt neimportante. Atunci de ce să inteceptezi pe toată lumea, când ai pericole reale de care trebuie să te ocupi? De ce nu previi atacurile de la Boston Marathon, de la Londra sau mai recent, cele din Paris? Când targhetezi pe toată lumea, nu mai ai cum să fii eficient. Așa că măsurile de supraveghere în masă nu numai că îți încalcă drepturile, dar nici nu dau rezultatele pe care contăm atunci când vine vorba de siguranță.

#2. Nu am nimic de ascuns.

Ești foarte sigur? Dacă ești foarte sigur și nu ai nimic de ascuns, completează într-un comentariu: toate datele tale de pe buletin, cardurile bancare, contul IBAN și adaugă ultimele 5 investigații medicale făcute. Mai adaugă numele persoanelor cu care ai împărțit un pat în ultimii 3 ani și detalierea condițiilor în care s-a întâmplat acest lucru. Și adaugă și numărul de telefon. Și adresa. Hai și CNP-ul… :-D

Eu cred că avem cu toții ceva ce nu vrem să se afle față de anumite persoane, actori statali sau privați. Pentru că discuția nu este despre a ascunde ceva, ci despre libertatea de a decide cine, ce, cât, cum și când află informații personale despre tine. Este vorba de a avea control asupra vieții tale și a alege.

Și să fim serioși, mai devreme sau mai târziu tot o să faci o mică greșeală pentru care poți fi cu ușurință taxat. Și poate nici nu vei fi imediat luat la întrebări, dar nicio problemă – se adună acolo toate, numai bine de scos de la „dosar”.

Ce ar fi să existe totuși și garanția că suntem liberi – că nu suntem supravegheați de programe secrete, că activitatea noastră nu e monitorizată de companii, că avem într-adevăr puterea de decizie în ceea ce privește viața noastră și nimic din ce nu vrem nu e lăsat arbitrariului.

#3. Nu folosesc unelte privacy că mai rău mă expun.

S-a tot scris că dacă folosești Tor ai putea intra și mai rapid pe o listă de suspecți și că NSA tot te va urmări și va ști ce faci.

Informația se bazează pe puține informații despre cum funcționează Tor și pe poveștile legate de XkeyScore. NSA sau altă instituție similară ar putea să afle că ești interesat de Tor sau Tails, după

diverse informații pe care le lași pe Internet. De asemenea se pare că NSA are în fucțiune Tor exit nodes.

Dar aceasta nu înseamnă că atunci când intri să folosești Tor vei fi targhetat. Iar informația din exit nodes e mai importantă pentru a înțelege ce se face prin Tor în general și nu în particular (pentru că procesul de anonimizare nu este reversibil). Dar NSA nu este singurul pericol! Avem companii care colectează date despre tine, iar prin faptul că tehnologiile de supraveghere au devenit din ce în ce mai accesibile financiar – realmente oricine poate fi în stare acum să te supravegeze. Nu îți trebuie foarte mult.

Așa că vin și argumentez:

1) Dreptul la viață privată este un drept fundamental, iar dacă vrei să ți-l protejezi asta nu înseamnă că e un motiv de suspiciune. Exercitarea unui drept prin folosirea Tor (sau alte soluții privacy) nu e echivalentă cu sunt un infractor și vreau să mă ascund.

2) Pericolele nu vin doar din partea serviciilor secrete, ci și din partea marilor companii care pot începe să ia decizii arbitrare pentru tine (nu-ți mai dau asigurare de viață fiindcă am văzut pe Facebook că îți plac sporturile extreme), cât și din partea persoanelor din jur pe care poate le calci pe bătături. De fapt, în curând nu vei știi nici cine, ce date ar putea să aibă despre tine – și cum le-ar putea corela cu alte informații.

Ca să fim pe deplin informați, hai să vedem un pic și cum funcționează Tor, iar dacă vreți să citiți mai multe despre ce au de zis cei de la Tor, aveți aici o serie de articole și declarații. Plus, dacă folosești Tor de pe Tails o să ai și adresa IP și adresa MAC (de identificare a dispozitivului pe care îl folosești) schimbate.

Pentru mai multe mituri, citește și seria de articole **Digital Rights Mythbusting**: https://apti.ro/sites/default/files/Seria-mythbusting-drepturi-digitale.pdf