Libertatea ta începe unde se termină intimitatea mea

Cătălin VRABIE,
Facultatea de Administraţie Publică, SNSPA

vrabie.catalin@yahoo.com

Rezumat:

Printre cele mai importante invenţii ale secolului trecut se regăsesc: computerul (Damien, 2011) Internetul (Shuman, 2001; Castells, 2010) şi telefonul mobil (Hartmann et al., 2008). Acestea au schimbat lumea! Ei bine, înţelegându-se capacitatea acestora de a colecta date şi informaţii despre oricine şi orice, totodată ele s-au dovedit a fi şi instrumentele perfecte pentru supravegherea în masă (Wall Street Journal, 2011). Adesea mass-media prezintă articole scrise în urma unor scurgeri de date din cadrul serviciilor de informaţii internaţionale, ţintind totuşi cel mai mult spre cele americane, despre care se spune că supraveghează lumea. Acest articol intenţionează să prezinte câteva dintre cele mai notorii exemple care susţin afirmaţia precedentă.

Cuvinte cheie: securitate, supraveghere, digital.

În prima jumătate a anului 2013, Edward Snowden (fost angajat CIA şi contractor guvernamental în domeniul apărării pentru Booz Allen Hamilton) a dezvăluit public informaţii din interiorul agenţiilor de informaţii din America şi Marea Britanie – informaţii clasificate ca fiind *top secret* (Greenwald, 2014). Astfel, lumea a început să audă de proiecte precum PRISM, XKeyscore şi altele asemănătoare – exemple de programe pe care serviciile de informaţii americane le desfăşoară astăzi împotriva întregii lumi.

Dacă ne uităm puţin înapoi la predicţiile făcute de George Orwell asupra supravegherii (Orwell, 2012), ne dăm seama că acesta a fost un optimist. Astăzi suntem martorii urmăririi individului la o scară cu mult mai mare decât cea pe care Orwell şi-a putut-o imagina (Webb, 2007).

Fotografia următoare este făcută asupra clădirilor centrului de date al NSA (National Security Agency) din statul Utah, Statele Unite ale Americii, agenţie cunoscută ca fiind prima *Intelligence Community Comprehensive National Cyber-security Initiative Data Center*, care şi-a început activitatea pe 14 mai 2014 (Domestic Surveillance Directorate, 2015). Această bază, aşa cum este ea descrisă pe Web site-ul oficial, este atât un centru de calcul super performant, cât şi un depozit de date imens, capabil să stocheze până la un yottabyte – o mie de miliarde

de terabytes, fiind primul astfel de *data storage* din lume care dispune de un asemenea volum de stocare de date (Herbert, 2012).

Figura 1. Utah Data Center

Sursă: *https://nsa.gov1.info/utah-data-center/*

Imaginaţi-vă că este, de fapt, o suprafaţă enormă dedicată colectării şi analizei datelor. Când zic enormă, ei bine, conform Web site-ului oficial, doar clădirile ocupă o suprafaţă la sol de 140.000 m^2, din care 9.000 m^2 sunt ai centrului de date, restul fiind pentru suportul tehnic. Dacă această valoare nu vă spune mare lucru, atunci imaginaţi-vă o hală cu dimensiunea de două ori mai mare decât teren de fotbal plină cu hard disk-uri, iar celelalte, care însumate fac mai mult decât douăzeci şi cinci de terenuri de fotbal, sunt dedicate suportului tehnic. Ei bine, câte hard disk-uri puteţi depozita pe un stadion? Destul de multe, nu-i aşa? Doar factura de electricitate se ridică la suma de 40 milioane de dolari pe an (wired.com, 2012; defensesystems.com, 2011), întregul proiect costând peste 1.5 miliarde de dolari (Domestic Surveillance Directorate, 2015).

Asta înseamnă că organisme precum NSA pot colecta date despre fiecare dintre noi şi le pot stoca, practic, pentru perioade de timp nelimitate. Aceasta este ceea ce se numeşte „supraveghere en-gros a lumii întregi" (Nyst, 2014) – activitate care, evident, vine cu un set de noi riscuri, la acestea fiind cu toţii expuşi.

Statele Unite au dreptul legal de a supraveghea şi monitoriza străinii ale căror date şi informaţii ajung în, sau tranzitează, America (Department of Justice, 2001; DNI, 2013). În mod normal, supravegherea străinilor nu e un lucru atât de rău – asta până nu realizăm faptul că fiecare dintre noi este „un străin" în viziunea sistemului juridic american. Vorbim într-adevăr de supraveghere en-gros, permanentă şi a fiecăruia dintre noi – a noastră, a tuturor celor care folosim sistemele de telecomunicaţie şi Internet.

Totuşi, să nu fim înţeleşi greşit. Sunt tipuri de supraveghere cu care suntem de acord. Eu, spre exemplu, iubesc libertatea, dar până şi eu sunt de acord că

supravegherea este necesară în anumite situaţii. Atunci când forţele de poliţie încearcă să găsească un criminal ori să prevină un atac terorist, dacă au suspecţi sau indicii de orice fel, este justificat să le asculte acestora telefoanele şi să le intercepteze comunicarea pe Internet. În aceste situaţii nu există dubii privind moralitatea. Dar proiecte precum PRISM nu sunt dezvoltate pentru aşa ceva. Ele nu sunt pentru a supraveghea oameni pentru care există motive de a acţiona în această manieră. Nu, ele supraveghează oameni despre care se ştie că sunt inocenţi. Prezint în continuare câteva argumente care susţin cele spuse.

Primul şi probabil cel mai important este acela conform căruia atunci când începem să argumentăm injusteţea supravegherii, se găsesc voci care vor să minimizeze efectele pe care aceasta le are, zicând că „Ştiam, ştiam toate astea" sau „Nu e nimic nou în treaba asta". Aşa cum se vede în Figura 2 a acestui capitol, am întrebat pe profilul meu de Facebook dacă lumea ştie că atunci când căutăm ceva prin intermediul motoarelor de căutare consacrate, acele informaţii ajung, probabil, la serviciile de informaţii din Statele Unite. Nouă minute mai târziu, am primit un răspuns de la un fost student de-al meu, care-mi spunea că acest lucru nu este nici surprinzător şi nici nu reprezintă o noutate. Ba mai mult, un alt participant la discuţie răspunde că „Ar fi păcat să fie altfel".

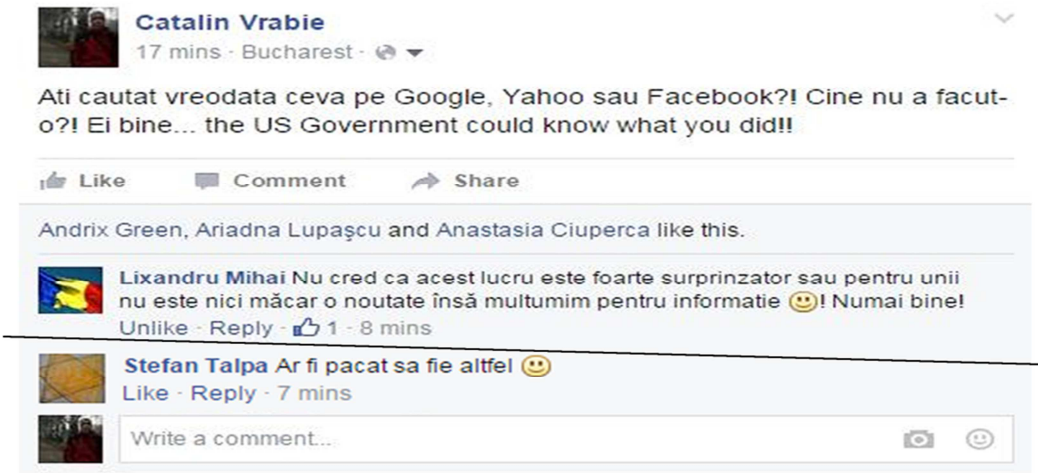

Figura 2. Discuţie pe Facebook privind supravegherea

Sursa: *Profilul personal de Facebook al autorului (decembrie 2015)*

Acest lucru nu este, însă, adevărat. Nu lăsaţi pe nimeni niciodată să vă spună că „se ştia asta deja", pentru că nu se ştia. Cele mai teribile gânduri ale noastre ar fi putut fi în această direcţie, dar nu ne gândeam că aşa ceva se va şi întâmpla. Acum ştim, este cert! Nimeni nu ştia nimic despre PRISM, nici despre XKeyscore sau oricare alt proiect condus şi întreţinut de agenţiile de informaţii americane. Acum se ştie (Washington Post, 2013; The Guardian, 2013a; ZDNet, 2013; Wall Street Journal, 2013a; The Guardian, 2014), însă nu am fi crezut că serviciile de informaţii americane vor merge până într-acolo încât să infiltreze un cod standardizat în

vederea sabotării algoritmilor de criptare (The Economist, 2013; The Guardian, 2013b; Der Spiegel, 2014; Reuters, 2014). Asta înseamnă că au preluat ceva ce era perfect securizat, un algoritm de securizare care era atât de sigur încât, dacă-l foloseşti pentru a cripta un fişier, nimeni nu-l poate decripta. Chiar dacă ar folosi fiecare computer din lume doar pentru a decripta acel fişier, i-ar lua milioane de ani (PGP, 2009). Practic, acel fişier este 100% sigur – uncrackable. A fost preluat ceva foarte bun şi slăbit intenţionat, clătinând astfel securitatea fiecărui cetăţean.

Echivalentul în lumea reală ar fi că serviciile de informaţii ar avea un cod PIN secret pentru fiecare sistem de alarmă din casele noastre pentru a putea intra nestânjenite oriunde, explicând asta prin faptul că răufăcătorii ar putea avea şi ei alarme acasă. Treaba asta, însă, ne face pe noi toţi mai vulnerabili. Existenţa unui astfel de viciu într-un algoritm de criptare este cel puţin surprinzătoare. Aşa ceva creează confuzie în mintea tuturor.

Dar, bineînţeles, serviciile de informaţii îşi fac treaba. Acestea sunt sarcinile care le-au fost trasate: să monitorizeze comunicaţiile şi, de asemenea, traficul pe Internet şi să reacţioneze la semnalele depistate de-a lungul canalelor de comunicare. Asta e ceea ce încearcă să facă. Şi din moment ce cea mai mare parte a traficului pe Internet este astăzi criptat, atunci ele trebuie să găsească portiţe – cea mai la îndemână fiind să saboteze algoritmii de criptare. Acesta este un exemplu nemaipomenit despre cum agenţiile de informaţii americane pierd teren în lupta cu tehnologia. Practic, au pierdut controlul şi fac eforturi să reintre în posesia lui.

Ce se ştie, de fapt, despre scurgeri de informaţii? Toate au la bază fişierele puse la dispoziţie de Edward Snowden. În antetul primului slide al proiectului PRISM, care a fost făcut public de acesta în iunie 2013 (Figura 3, stânga), sunt detalii despre o suită de furnizori de servicii de Internet şi date, pe care proiectul este conceput să-i monitorizeze şi la care are acces.

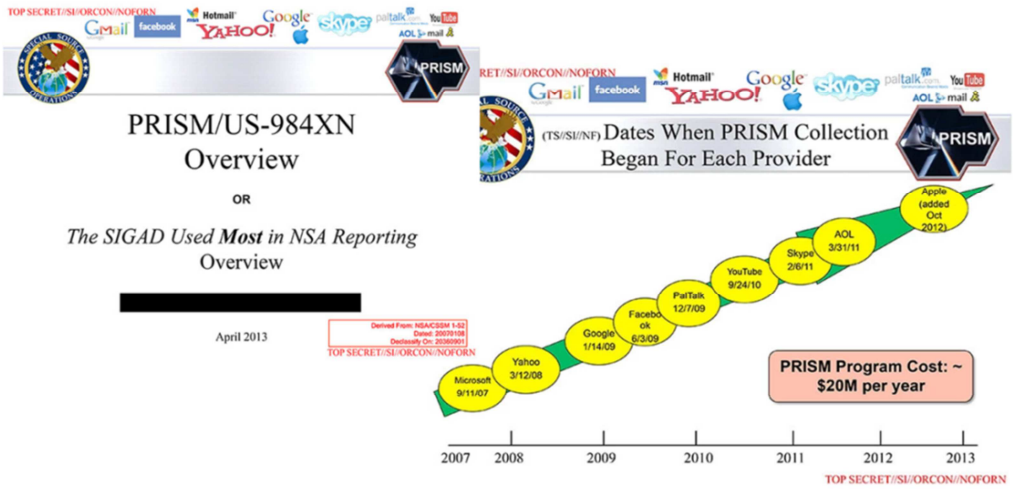

Figura 3. O parte din slide-urile puse la dispoziţie de Edward Snowden
Sursa:*http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/*

În plus, se poate observa (Figura 3, dreapta) că există informaţii exacte cu privire la data în care s-a început colectarea informaţiilor pentru fiecare furnizor al acestor servicii. De exemplu, este menţionată data de 11 septembrie 2007 ca debut al colectării datelor de la Microsoft, pentru Yahoo – 12 martie 2008, şi apoi alţii, precum Google şi Facebook, şi terminând cu Apple – octombrie 2012. Interesant este că fiecare dintre aceste companii neagă orice implicare – pur şi simplu spun că aşa ceva nu este adevărat, că ele nu dau acces nimănui la datele lor.

> *"Yahoo! takes users' privacy very seriously. We do not provide the government with direct access to our servers..." — Tim Bradshaw, June 7, 2013 (Yahoo, 2013)*
>
> *"Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government 'backdoor' into our systems, but Google does not have a 'backdoor' for the government to access private user data." (Bloomberg, 2013)*
>
> *"We do not provide any government organization with direct access to Facebook servers. When Facebook is asked for data or information about specific individuals, we carefully scrutinize any such request for compliance with all applicable laws, and provide information only to the extent required by law." (Techcrunch, 2013)*
>
> *"We [Apple n.a.] do not provide any government agency with direct access to our servers, and any government agency requesting customer data must get a court order." (Wall Street Journal, 2013b)*
>
> *"We [Microsoft n.a.] provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security program to gather customer data we don't participate in it." (The Verge, 2013)*

Această ipoteză contrazice existenţa fişierelor domnului Snowden, ceea ce înseamnă fie că cineva minte fie (ca explicaţie alternativă) că aceşti furnizori de servicii au fost sabotaţi. Asta ar explica totul. Ei nu cooperează cu guvernul Statelor Unite, ci sunt sabotaţi de acesta.

Să fii sabotat de propriul guvern poate părea, la prima vedere, greu de crezut, dar nu ar fi prima dată când se întâmplă aşa ceva dincolo de ocean. Ca exemplu, putem menţiona aplicaţia *malware* Flame, despre care se crede că a fost autorizată de guvernul Statelor Unite (GlobalResearch 2013; The Intercept, 2014) şi care, pentru a se răspândi, a subminat sistemele de securitate a reţelelor pentru Windows Update (ComputerWorld, 2012; C|net 2012; Arstechnica, 2012) – ceea ce înseamnă că Microsoft a fost sabotat de propriul guvern.

Şi sunt încă multe evidenţe care sprijină această teorie. Der Spiegel, din Germania, a publicat informaţii referitoare la operaţiuni întreprinse de echipe de hackeri de elită care funcţionează în interiorul agenţiilor de informaţii (Der Spiegel, 2013a). În NSA, această echipă se numeşte TAO – Tailored Access Operation (The Guardian, 2013c), în GCHQ (Government Communications Headquarters – Agenţia de Informaţii şi Securitate Britanică) se numeşte NAC – Network Analysis Centre (Der Spiegel, 2013b). În urma acestor scurgeri de informaţii, s-au putut identifica operaţiuni conduse de Agenţia de Informaţii din Marea Britanie – GCHQ, care au

avut ca ţintă o companie de telefonie mobilă belgiană – Belgacom. Această operaţiune a fost numită *Socialist* (Der Spiegel, 2013b).

Acest lucru înseamnă că o agenţie de informaţii a unei ţări europene sabotează, în mod intenţionat, securitatea unei reţele de telefonie dintr-un alt stat membru UE. În plus, conform materialelor devenite acum publice, întreprinde această acţiune cu nonşalanţă – *Business, as usual!*, „Aceasta este ţinta principală, aceasta este ţinta secundară [Figura 4, stânga], aceasta este echipa..." şi aşa mai departe – probabil aceste discuţii s-au purtat în cadrul unui team-building de weekend. Ba chiar au folosit Clip Art-uri specifice Power Point-ului, precum SUCCESS (Figura 4, dreapta), atunci când slide-ul prezintă paşii făcuţi şi în urma cărora au reuşit să obţină accesul la aceste informaţii.

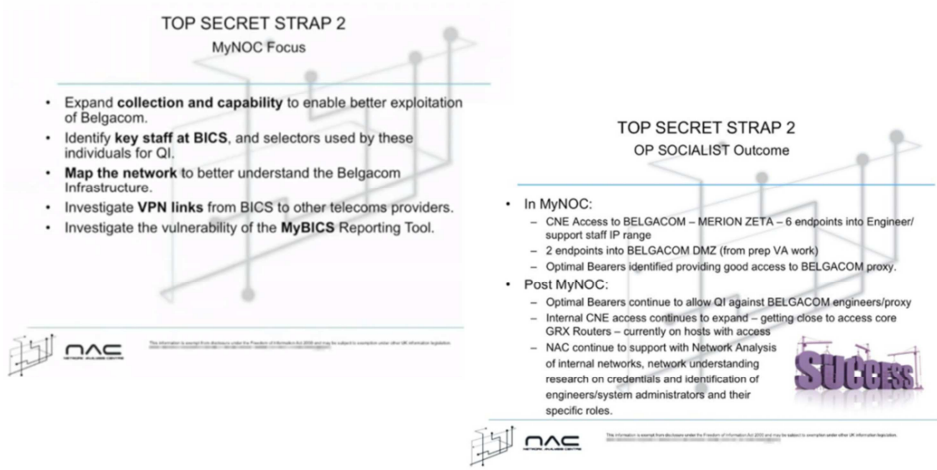

Figura 4. O parte din slide-urile postate de Der Spiegel despre atacul cibernetic asupra Belgacom – Operaţiunea *Socialist*

Sursa:*http://www.spiegel.de/fotostrecke/photo-gallery-operation-socialist-fotostrecke-101663.html*

Desigur, se poate contra-argumenta prin replici precum: „OK, este adevărat, dar şi celelalte ţări acţionează similar. Toate ţările spionează!". Şi, parţial, este adevărat. Cele mai multe ţări întreprind operaţiuni de spionaj. Să luăm, totuşi, exemplul ţării noastre. În ceea ce priveşte setul de norme juridice referitoare le protecţia datelor, acesta este cât de cât similar cu cel american, de care am vorbit mai sus. Când datele ajung în sau tranzitează România, Serviciul Român de Informaţii are dreptul legal de a le intercepta (Legea nr. 51 din 29 iulie 1991, în forma consolidată – 11 septembrie 2014, privind securitatea naţională a României, articolul 14, alin. 2, lit. a) – acesta ne spune: „Activităţile specifice prevăzute la alin. (1) pot consta în: a) interceptarea şi înregistrarea comunicaţiilor electronice, efectuate sub orice formă;"

Totuşi, se ridică aici o întrebare: Câţi oameni de afaceri, politicieni sau alţi oficiali români folosesc în fiecare zi servicii de date furnizate de companii din Statele Unite, precum Google, Yahoo, Facebook ori Linkedln, sau îşi stochează datele în sisteme *cloud* precum ICloud sau DropBox? Câţi dintre aceştia folosesc Amazon,

eBay sau platforme Web similare pentru transfer de valori – ca să nu mai vorbim de folosirea sistemului de operare Windows? Răspunsul este: toţi. Toţi liderii din mediul politic, social sau de business folosesc zilnic cel puţin un astfel de serviciu.

Să vedem cum stau lucrurile din celălalt punct de vedere. Câţi lideri americani folosesc serviciile de Webmail sau cloud românești? Răspunsul este: zero (sau foarte aproape de această valoare) – menţionez totuşi că nu am găsit nicăieri, în cadrul cercetărilor făcute, informaţii care să infirme această ipoteză, motiv pentru care putem considera că ea este adevărată. deci lipseşte echilibrul. Situaţiile nu sunt nici măcar pe departe comparabile.

Când avem totuşi, ocazional, poveşti de succes europene sau chiar naţionale, precum antivirusul RAV, produs de firma românească GeCAD Software, chiar şi acestea ajung să fie vândute marilor companii din Statele Unite – în acest caz, Microsoft (Ziarul Financiar, 2003). Aplicaţia Skype, creată de o echipă mixtă de programatori suedezi şi estonieni, care era foarte bine securizată la început – comunicarea fiind criptată de la un capăt la celălalt, a ajuns tot în proprietatea companiei Microsoft (BBC, 2011). Astăzi iată, avem toate motivele să ne îndoim şi de Skype – vă aduceţi aminte ce canale a folosit virusul Flame pentru a se răspândi? Deci, încă o dată, a fost preluat ceva sigur şi slăbit intenţionat, făcându-ne pe noi toţi mai vulnerabili.

Un alt argument este că Statele Unite luptă împotriva teroriştilor (The Guardian, 2013d). Acest motiv ar trebui să ne întărească încrederea în faptul că astfel de proiectele au menirea de a ne proteja. Totuşi, să ne gândim mai bine! O parte din existenţa acestor proiecte este justificată de actele de terorism la care am fost martori în ultimii ani – acte oribile, care adesea se soldează cu mulţi morţi şi cu şi mai mulţi răniţi, unii dintre aceştia rămânând invalizi permanent. Da, forţele aliate trebuie să lupte cu aceşti indivizi şi cu organizaţiile pe care le reprezintă. Dar în urma acţiunilor celor ca Edward Snowden sau ale jurnaliştilor de la Der Spiegel, ştim că serviciile de informaţii de care vorbim folosesc aceleaşi tehnici pentru a asculta telefoanele liderilor europeni (The Guardian, 2013e; Independent, 2013) sau pentru a intercepta email-urile cetăţenilor Mexicului şi ai Braziliei (USA Today, 2015). Ba mai mult, s-a ajuns până la citirea email-urilor schimbate în interiorul Parlamentului European (The Guardian, 2013d; CBSNEWS, 2015). Ei bine, în aceste cazuri nu cred că intenţia mai este aceea de a identifica teroriști. Unde? Sunt aceştia membri ai Parlamentului European? Nu, nu este vorba de un război împotriva terorismului. O parte, cum am mai zis, ar putea fi. Dar ne putem gândi la terorism ca fiind o ameninţare atât de mare încât să fie necesar să facem orice pentru a lupta cu el? Sunt cetăţenii americani dispuşi să-şi arunce la gunoi drepturile constituționale [ne referim aici la Primul amendament] doar pentru că există teroriști? De asemenea, valabil pentru cetăţenii europeni: sunt ei toţi de acord să arunce la gunoi Convenţia pentru Apărarea Drepturilor Omului şi a Libertăţilor Fundamentale [ne referim aici în special la art. 8 al Convenției.]; sau oricare alt cetăţean de pe planetă – este el de acord să fie ignorată Declaraţia Universală a Drepturilor Omului [ne referim aici în special la art. 12 al Declaraţiei]?

Este adevărat că cei mai mulţi oameni se tem de teroriști și, astfel, ei ar putea crede că această formă de supraveghere este legitimă pentru că nu au nimic de ascuns. Declaraţii precum „eşti liber să mă controlezi, dacă asta ajută” sunt întâlnite

adesea în rândul cetăţenilor. Însă oricine spune că nu are nimic de ascuns, pur şi simplu nu s-a gândit suficient de mult la acest aspect.

Avem ceea ce se numeşte intimitate. Şi dacă într-adevăr cineva crede că nu are nimic de ascuns, asta înseamnă că respectivului nu i se poate încredinţa nici un secret pentru că, în mod cert, nu îl poate ţine.

Oamenii de astăzi sunt incredibil de oneşti pe Internet. Când scurgerile de informaţii – despre care vă vorbeam mai sus, au devenit subiectul de discuţie a tuturor ziarelor lumii, mulţi au reacţionat spunând că ei nu au nimic de ascuns, nu fac nici un rău nimănui sau nu întreprind nici o acţiune ilegală.

"Normally honest people would have no need to fear anything they have said, or written, could be used against them." — utilizatorul Inglenda2, 31/12/2013 (Der Spiegel, 2013-1)

"If it helps stop another 9/11, then I am very happy for the NSA to trawl through my e-mails." — utilizatorul Stelvio 28/12/2014 (Der Spiegel, 2014)

"As expected a long time ago. Key words being scrutinised." – utilizatorul allislost, 31/07/2013 (The Guardian, 2013)

"As a frequent traveler I am happy that someone from the land of the free is looking after my interests and the majority of normal peace loving citizens. Going back to the 1950's to a TV programe called Dragnet they started by saying Democracy might not be the best for all but its better than the rest.... yes before 9/11 the two Gulf Wars... it was a different world... thanks I feel safer knowing your on my side." – utilizatorul James Hamilton-Bird, 27/03/2015 (Washington Post, 2013)

"Majority of this information is as old as the hills. Majority of all American internet and most foreign internet users probably already knew this. Especially when you have internet crashes, hackers, etc and you have to have your computer fixed and your data drives cleaned. More power to NSA to use my email and data. Maybe they will catch real terrorists, would be terrorists, etc. I thankful they are working to keep the majority of the world safe." – utilizatorul Penny Middleton, 26/12/2014 (Washington Post, 2013)

Cu toate acestea, niciunul dintre cei în cauză nu are un subiect anume pe care să dorească să-l discute cu serviciile de informaţii (fiecare articol apărut în presă şi folosit în acest capitol ca sursă de documentare este însoţit şi de astfel de comentarii din partea cititorilor on-line, dar pe care din motive de spaţiu şi ca să nu obosesc, nu le mai reproduc aici), în special cele din afara ţării. Dacă într-adevăr avem nevoie de Big Brother, am prefera totuşi unul al nostru, naţional.

Trebuie, însă, să vorbim şi de intimitate. Ea nu se negociază, ci ar trebui implementată nativ în toate sistemele pe care le folosim.

Cu riscul de a ne repeta, trebuie să fie înţeles faptul că suntem excesiv de oneşti cu motoarele de căutare de pe Internet. Faceţi-vă public istoricul navigării pe Web a fiecăruia dintre voi şi veţi vedea că se vor găsi fie informaţii incriminatoare, fie jenante în mai puţin de zece minute. Suntem mult mai oneşti cu motoarele de căutare decât suntem cu familiile noastre. Acestea ştiu mai multe despre noi decât ştiu toţi ceilalţi din jur (Andrews, 2012). Aceste tipuri de informaţii le oferim guvernului Statelor Unite.

Supravegherea are puterea de a schimba cursul istoriei. Să luăm exemplul preşedintelui american Nixon – ce ar fi putut face el dacă ar fi avut la dispoziţie instrumentele de astăzi (Greenberg, 2012)! Sau, dacă vreţi, aduc în discuţie cazul

preşedintelui Braziliei, doamna Dilma Rousseff, care a fost ţinta NSA, email-ul domniei sale fiind interceptat şi citit de serviciile de Informaţii americane, şi care a spus: *In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy* (The Guardian, 2013). Despre asta este vorba – intimitatea este unul dintre pilonii pe care se construieşte şi se sprijină o democraţie.

Edward Snowden a fost acuzat de multe lucruri. Unii l-au acuzat că ar fi zdruncinat industria de software şi pe cea de cloud prin acţiunile lui. Dar acuzându-l pe el pentru aceste lucruri este ca şi cum i-am acuza pe ecologişti pentru încălzirea globală.

Ce se mai poate face? Ar trebui să fim îngrijoraţi? Scott McNealy, cofondator al companiei Sun Microsystems, le-a spus reporterilor într-o conferinţă de presă din 24 ianuarie 1999: *You have zero privacy anyway. Get over it!* (Manes, 2000). Stephen Manes, reporter pentru revista Forbes, i-a criticat declaraţia într-un articol al său, zicând: *He's right on the facts, wrong on the attitude. ... Instead of „getting over it", citizens need to demand clear rules on privacy, security, and confidentiality* (Manes, 2000). Într-adevăr, aşa cum şi autorii volumului *Privacy in the 21st Century* au spus, trebuie să fim furioşi pentru că ceea ce se întâmplă nu este bine. Aceste metode sunt barbare, lipsite de tact şi nu trebuiesc acceptate şi promovate (Adams et. al. 2005).

Conform zicalei *Without knowledge action is useless and knowledge without action is futile*, doar ştiind ce se întâmplă, situaţia nu se va schimba. Ea se va schimba dacă ne îndepărtăm de sistemele dezvoltate în Statele Unite. Cum? Dificil! Nici o ţară din lume nu poate dezvolta, peste noapte, sisteme care să le înlocuiască pe cele deja existente. Însă cooperarea poate aduce rezultate frumoase – mă refer aici la platformele *open source*. Acestea sunt dezvoltate în urma unor colaborări, de regulă internaţionale. Sunt sisteme deschise, gratuite şi bine securizate (InfoWorld, 2015). Astfel, sistemele de supraveghere existente vor putea fi ocolite.

Malcolm Gladwell, sociolog canadian, spunea că este suficient să se facă un mic val pentru că apoi, prin eforturi colective, acesta s-ar putea transforma într-un tsunami (Gladwell, 2004) care ar avea puterea să înlocuiască sistemele actuale. Un astfel de exemplu este platforma pentru e-learning Moodle, dezvoltată de un grup de zece australieni, dar care colaborează cu peste şaptezeci de case de dezvoltare software din întreaga lume (Moodle, 2015). Să-i luăm pe ei ca exemplu şi să acţionăm în consecinţă.

Criptare – metode şi tehnici folosite pentru securizarea informaţiilor şi a comunicării într-o reţea.

Scurgere de informaţii – acţiuni întreprinse cu scopul de a divulga informaţii confidenţiale.

Bibliografie

Adams, Helen R.; Bocher, Robert F.; Gordon, Carol A.; Barry-Kessler, Elizabeth, (2005). *Privacy in the 21st Century*, Libraries Unlimited.

Andrews, L., (2012), *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy,*Capitolul 2, *George Orwell... Meet Mark Zuckerberg*,Free Press, New York.
Arstechnica, (2012), *Flame malware hijacks Windows Update to spread from PC to PC*, *It's hard to patch a machine when the update mechanism is compromised*, http://arstechnica.com/security/2012/06/flame-malware-hijacks-windows-update-to-propogate/
BBC News, (2011), *Microsoft confirms takeover of Skype*, http://www.bbc.com/news/business-13343600
Bloomberg, (2013), *NSA Spying, The Companies' Lines on Prism,* http://www.bloomberg.com/bw/articles/2013-06-07/the-companies-lines-on-prism
C|net (2012), *Flame virus can hijack PCs by spoofing Windows Update,* http://www.cnet.com/news/flame-virus-can-hijack-pcs-by-spoofing-windows-update/
Castells, M. (2010), *End of Millennium. The Information Age. Economy, Society, and Culture,* Wiley-Blackwell.
CBSNEWS, (2015), *IN DEPTH. NSA surveillance exposed. A secret government surveillance program targeting phone calls and the Internet is revealed,* http://www.cbsnews.com/feature/nsa-surveillance-exposed/
ComputerWorld (2012), *Researchers reveal how Flame fakes Windows Update, Bogus certificates key, but espionage malware also spoofs Microsoft's update service on a network,* http://www.computerworld.com/article/2503916/malware-vulnerabilities/researchers-reveal-how-flame-fakes-windows-update.html
Damien, J., (2011), *Introduction to Computers and Application Software*, Jones & Barlett Learning.
defensesystems.com (2011), *Work commences on $1B NSA 'spy' center*, https://defensesystems.com/Articles/2011/01/07/NSA-spy-cyber-intelligence-data-center-Utah.aspx
Department of Justice (2001), *The USA PATRIOT Act: Preserving Life and Liberty,* http://www.justice.gov/archive/ll/highlights.htm
Der Spiegel, (2013a), *Inside TAO: Documents Reveal Top NSA Hacking Unit*, http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html
Der Spiegel, (2013b), *Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm*, http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html
Der Spiegel, (2014), *Prying Eyes: Inside the NSA's War on Internet Security*, http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html
DNI (Office of the Director of National Intelligence) (2013), *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf

Domestic Surveillance Directorate, https://nsa.gov1.info/utah-data-center/
Forma consolidată – 11 septembrie 2014, a *Legii nr. 51 din 29 iulie 1991, privind securitatea națională a României*, https://www.sri.ro/fisiere/legislatie/Legea51.pdf
Gladwell, M., (2004), *Punctul critic. Cum lucruri mici pot provoca schimbări de proporţii*, Ed. Andreco Educational, Bucureşti.
Global Research, (2013), *Digital Warfare: Stuxnet and Flame Viruses could have Three "Sister Viruses"*, http://www.globalresearch.ca/digital-warfare-stuxnet-and-flame-viruses-could-have-three-sister-viruses/5305160
Greenberg, I., (2012), *Surveillance in America: Critical Analysis of the FBI, 1920 to the Present*, Lexington Books, UK.
Greenwald, G., (2014), *Afacerea Edward Snowden: Cele mai șocante dezvăluiri despre spionajul global american,* publicat în română de Ed. Litera în 2015.
Hartmann, M., Rössler, P., Höflich, J., (2008), *After the Mobile Phone? Social Changes and the Development of Mobile Communication*, Frank & Timme, Berlin.
Independent, (2013), *NSA spying scandal: Merkel and Hollande demand talks as US is accused of listening in on phone calls of 35 world leaders*, http://www.independent.co.uk/news/world/americas/nsa-spying-scandal-merkel-and-hollande-demand-talks-as-us-is-accused-of-listening-in-on-phone-calls-8901065.html
InfoWorld, (2015), *The state of open source security*, http://www.infoworld.com/article/2901893/security/the-state-of-open-source-security.html
Manes, Stephen, (2000), *Private Lives? Not Ours!* PC World 18 (6): 312. ISSN 0737-8939.
Moodle official Web portal (2015), https://moodle.com/partners/?keywords=&sector=&country=&service
Nyst, Carly & Crowe Anna, (2014) *Unmasking the Five Eyes' global surveillance practices,* Global Information, Society Watch 2014, Communications surveillance in the digital age, Association for Progressive Communications (APC) and Humanist Institute for Cooperation with Developing Countries (Hivos), ISBN: 978-92-95102-16-3.
Orwell, G. (2012), *O mie nouă sute optzeci și patru*, publicat în română de Ed. Polirom în 2012.
PGP Corporation (2009), *An Introduction to Cryptography by Jon Callas*, https://symwisedownload.symantec.com/resources/sites/SYMWISE/content/live/SOLUTIONS/149000/TECH149738/en_US/introcrypto.pdf?__gda__=1450069900_622d724685e5df327ff5d4fb6460a357
Reuters (2014), *Exclusive: NSA infiltrated RSA security more deeply than thought – study*,http://www.reuters.com/article/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331#VDXbhGdgmf4IET4T.97
Serviciul Român de Informații – SRI (2015), *Legislația*, https://www.sri.ro/legislatia.html
Shuman, B., (2001), *Issues for Libraries and Information Science in the Internet Age,* Libraries Unlimited.

Techcrunch, (2013), *Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL And Apple Deny Participation In NSA PRISM Surveillance Program,* http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/

The Economist, (2013), *The NSA's crypto "breakthrough"*, http://www.economist.com/blogs/babbage/2013/09/breaking-cryptography

The Guardian, (2013), *Brazilian president: US surveillance a 'breach of international law'*. http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance

The Guardian, (2013a), *XKeyscore: NSA tool collects 'nearly everything a user does on the internet'*, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

The Guardian, (2013b), *Revealed: how US and UK spy agencies defeat internet privacy and security*, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

The Guardian, (2013c), *NSA 'hacking unit' infiltrates computers around the world – report.*http://www.theguardian.com/world/2013/dec/29/der-spiegel-nsa-hacking-unit-tao

The Guardian (2013d), *Codename 'Apalachee': How America Spies on Europe and the UN,* http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html

The Guardian, (2013e), *Angela Merkel's call to Obama: are you bugging my mobile phone?* http://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german

The Guardian, (2014), *Prism - The latest news and comment on Prism the national security electronic surveillance program operated by the United States National Security Agency*, http://www.theguardian.com/us-news/prism

The Intercept, (2014), *How the nsa plans to infect 'millions' of computers with malware,* https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/

The Verge, (2013), *Apple, Google, Microsoft, Facebook, Yahoo, and more deny providing direct access to PRISM surveillance program,* http://www.theverge.com/2013/6/6/4404112/nsa-prism-surveillance-apple-facebook-google-respond

Wall Street Journal, (2013a), – *U.S. Official Releases Details of Prism Program*, http://www.wsj.com/news/articles/SB10001424127887324299104578533802289432458

USA Today, (2015), *U.S. secretly tracked billions of calls for decades*, http://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/

Utah Governor Gary Herbert, 2012 Energy Summit, http://blog.governor.utah.gov/2012/02/2012-energy-summit/

Wall Street Journal (2011b), *Document Trove Exposes Surveillance Methods*, http://www.wsj.com/articles/SB10001424052970203611404577044192607407780

Wall Street Journal, (2013), *Tech Firms' Data Is Also Tapped,* http://www.wsj.com/articles/SB10001424127887324798904578529912280347482

Washington Post (2013), *NSA slides explain the PRISM data-collection program*,http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

Webb, M., (2007), *Illusions of Security: Global Surveillance and Democracy in the Post-9/11 World*, City Lights San Francisco.

Wired.com (2012), *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say),* http://www.wired.com/2012/03/ff_nsadatacenter/all/1

Yahoo (2013), *PRISM Companies Start Denying Knowledge of the NSA Data Collection Program*, http://news.yahoo.com/prism-companies-start-denying-knowledge-nsa-data-collection-004541590.html

ZDNet (2013), PRISM: *Here's how the NSA wiretapped the Internet*, http://www.zdnet.com/article/prism-heres-how-the-nsa-wiretapped-the-internet/

Ziarul Financiar, (2003), *Tranzacție istorică: Bill Gates cumpără un antivirus românesc,* http://www.zf.ro/prima-pagina/tranzactie-istorica-bill-gates-cumpara-un-antivirus-romanesc-2981166/