

KELETI ARTHUR

A magánélet nyílt titkai, avagy privát zóna az internet korában

A mikor Thomas Edison a szénzásas izzólámpáján dolgozott, azt mondta, hogy immár sok ezer kísérletet be tud mutatni, amelyek közül egyik sem működőképes. Több mint húsz évnyi kibevédelmi munka után én is elmondhatom magamról, hogy számtalan olyan módszert ismerek, amelyik nem nyújt megfelelő védelmet. Sosem gondoltam volna, hogy amikor a kibertitkok kutatása kapcsán belemertülök a téma társadalomtudományi vonatkozásaiba, a felfedezéseim jobban megrázzák a kibevédelemben vetett hitemet, mint korábban bármi. Azt kellett látnom ugyanis, hogy a digitális valóság megálíthatatlanul elszabadult, mint egy vad bika, és maga alá gyűr társadalmakat, államokat, cégeket és családokat, és kibevédelmi szakemberként még mi sem tudjuk garantálni az érintettek számára a védelmet.

Régen elég volt tartani magunkat a mondáshoz, hogy hallgatni arany. Ha barátainkban megbízhattunk és bizalmasaink nem fecsegték ki titkainkat, nyugodtan aludhattunk. Manapság már nem csupán a barátaink vagy bizalmasaink veszélyeztetik a titkainkat, hanem sosem látott, vadidegen emberek egy távoli ország kis lakásának számítógépei előtt. Titkaink őrzéséhez megfelelő technikai eszközökre és folyamatosan fejlődő szakmai tudásra van szükségünk, mert az évszázados, kipróbált módszerek mára használhatatlanná váltak.

A titok és az emberi agy

Mindnyájunknak vannak titkai. És mindig lesz valaki, akit pont a mi titkaink érdekelnek. A titok mibenlétét mégis nehéz meghatározni, hiszen rengeteg olyan dologra, jelenségre utalhat a fejünkben, melyek mindegyikét gyakran felülvizsgáljuk, vagy akár meg is változtatjuk. Bármi titokká minősülhet az egyik pillanatban, míg a másikban elveszíti titokjellegét. A meghatározásnak mégis van egy kulcseleme, ez pedig a védelem. A titkok ugyanis megvédenek minket. Biztonságot adnak.



A magánélet kialakításának és fenntartásának alapfeltétele, hogy önmagunkat, kapcsolatainkat, tulajdonunkat stb. biztonságban tudjuk. Nem akarunk aggódni, az otthonunkba térve nyugalomra vágyunk, hogy pihenhessünk, feltöltődhessünk, visszanyerjük energiánkat.

Amikor egyedül, vagy szűk családi körben vagyunk, olyasmiket is csinálunk, amiket nem szívesen vállalnánk fel nyilvánosan. A magánszféra biztosítja számunkra a szabadság érzését.

A kibertitkokkal azért kezdtem el foglalkozni, mert meg akartam érteni, hogyan működnek a titkok és milyen kapcsolatban állnak az emberi természettel. Egy kiváló szociológus, *Szvetelszky Zsuzsa* volt segítségemre, aki egy rendkívül érdekes kutatást végzett a pletykáról. A tagolt beszéd kialakulása után a pletyka a második helyen áll az emberi kommunikáció fejlődésében, mégpedig minden embercsoport körében, legyen az egy ausztrál bennszülött törzs vagy egy manhattani irodaház közössége. Fontos számunkra a többi ember, különösen azok, akiknek az arcát

gyakran látjuk és hangját gyakran halljuk. Evolúciós sajátosság, hogy róluk minél többet szeretnénk megtudni és a titkaikra is kíváncsiak vagyunk; valószínűleg ez magyarázza a pletykák hihetetlen gyors terjedését. A titkok napfényre kerülését, továbbadását, a pletykát ráadásul – szintén evolúciós sajátosság – nem valami rosszként, ártalmasként értelmezzük, hanem pozitívumként. A közösséget romboló rágalmozással vagy manipulációval szemben a pletykanak közösségépítő szerepe van, és az emberek közti beszélgetés 60%-át teszi ki.

A kutatásom során azzal kellett szembesülnöm, hogy amit a szakemberek felfedeztek a titkokról, vagy kibevédelemről, azt megtartották maguknak és a felfedezéseiket nem publikálták. Ki kellett hát dolgoznom a saját módszeremet: a kibertitkok kockázatelemzését.

A módszer az emberi agy titokkezelési működésén alapul, mely egy körkörös folyamat különböző állomásokkal. Az ember agya, amikor szembesül egy titokkal, mindig mérlegeli annak a környezetét. Majd

számba veszi az egyén szükségleteit és azok hierarchiáját (lásd: Maslow-piramis). Gondosan mérlegeli, hogy ha kiderül a titok, akkor az miként hat az alapvető fizikai szükségletek kielégítésére, ill. a többiére. Elménk mindemellett még mérlegeli a normákat is, vagyis azt, hogy a titokkal megtörünk-e valamilyen normát, legyen az vallási, társadalmi, törvényi, szokás alapú vagy esetleg belső, deklarált vagy hallgatólagos.

Minden titkunkat folyamatosan ezen az összetett koordináta-rendszeren vizsgáljuk, és arra próbálunk rájönni, hogy a titok nyilvánosságra kerülése kényelmetlenséget jelent majd csupán, vagy komoly gondot okoz. Meg tudjuk magyarázni, ki tudjuk menteni magunkat, vagy megállíthatatlanul felboríthatja az életünket?

A komoly gondok mögött általában súlyos, ún. fekete titok húzódik meg, például gyilkosság vagy egy jelentősebb céges pénzügyi csalás, de ilyen lehet egy céges leépítési hullám is, amelyet a főnökség az utolsó pillanatig titkol. Amikor viszont amiatt bukunk le, hogy hetekig hordjuk ugyanazt a zoknit anélkül, hogy kimosnánk, akkor fehér titokról beszélünk, ami kínos és kellemetlen, tehát komoly hatása lehet, de inkább kellemetlen, mint problémás. Vannak tehát fehér és fekete titkaink, illetve köztük a szürke szátmalan árnyalatába burkolódnak.

Elmondhatjuk tehát, hogy a közvélekedéssel ellentétben nem információink vannak, hanem titkaink. Titkaink, amelyeket összetett szerkezetű, a viszonyunk hozzájuk és a technológiai körülmények miatt egyre kevésbé vagyunk képesek megvédeni. A rendelkezésünkre álló idő is egyre rövidebb. 2020 már nagyon közel van.

Mik azok a kibertitkok?

Mielőtt folytatnánk a gondolatmenetet, végezzünk el képzeletben egy kísérletet. Idézzük fel a négy legmélyebbre elásott, legsötétebb titkunkat, amiket sosem akartunk még csak megosztani sem senkivel. Nem olyan csekélysegekre gondolkodunk, mint amikor ebéd előtt sütít loptunk a nagyitól, hanem azokra a nagy titkokra, amelyek, ha egy nap kiderülnének, fel tudnák borítani az eddig kialakított életünket. Például házasságunkat van egy titkos szeretőnk, vagy úgy alakítottuk a számokat a céges beszámolóinkban, hogy kedvezőbb fényben tűnjünk fel a főnökünk előtt, vagy valójában a saját nemünkhöz vonzódnak és erről senki sem tud, esetleg nem hiszünk Istenben, de ezt titkoljuk a rendkívül vallásos családunk előtt. Majd képzeljük el, hogy fel

kell mennünk egy körszínpadra, melynek minden oldalán emberek ülnek, akiknek a szemébe kell néznünk, és miközben egy kamera veszi az adást és élőben közvetíti a Facebookon, a négy legféltebb titkunkból hármát hangosan kimondva kell megosztanunk a nyilvánossággal.

2020-ra pontosan ez az, ami történni fog velünk. A Gartner 2013. évi jelentése szerint addigra a négy legféltebb adatunkból három online elérhető lesz, vagyis legmélyebb titkunkból ennyi kerülhet nyilvánosságra. Kiberbiztonsági szakértőként kijelenthetem, hogy adataink 75%-ának nyilvánosságra kerülése nemcsak felkavaró élmény lesz, hanem igencsak fájni fog. Elsőre talán úgy tűnik, hogy egy furcsa apokaliptikus látomást vizionálok. De ezek gondolatok igencsak valószínűek például annak fényében, hogy 2010-ben *Mark Zuckerberg*, a Facebook alapítója és elnöke nem kevesebbet állított, mint hogy a magánélet magánjellege megszűnt általános társadalmi norma lenni. Az emberekben ugyanis feloldódott az az elvárás, hogy a magánélet kizárólag magánügy legyen.

A világ mára különböző kapcsolatok hálózatává vált, ami nagyrészt a számítógépeknek köszönhető. Számítógépek természetesen már elég régóta léteznek, de az elmúlt néhány évtizedet leszámítva, az informatikai szakmán kívül senki nem törődött velük, társadalmi hatásuk pedig egészen elenyésző volt. Mára viszont a számítógépek rendszereket alkotnak, és az emberekhez hasonlóan több szinten és rendszerben kapcsolódnak össze egymással. Az ilyen rendszerek kapacitásainak exponenciális növekedésével és a technológia fejlődésével pedig eljutottunk oda, hogy szükségtelennek látszik kiírni a stúdiókban, hogy „Csendet kérünk, felvétel zajlik!”, hiszen hang- és videófelvétel készülő folyamatosan szinte mindenhol és mindenről.

A számítógépek rengeteg információt tudnak közvetíteni. Ráadásul a minket körülvevő gépek adathordozó és -feldolgozó kapacitása is egyre növekszik. Az elektromos kenyérpírtónak a konyhában bonyolultabb számítógépes rendszere van, mint az embereket a Holdra szállító Apollo űrhajó irányítórendszerének volt. De hogyan tudjuk kiszűrni a modern gépek által kezelt hatalmas információfolyamból, hogy mi az, ami érdemes a figyelmünkre?

Az információ fontos vagy lényeges?

E kérdés eldöntése – bár különböző szinteken, de – általában a felhasználóra van bízva. Ki-ki keresse meg, szelektálja, rangsorolja a maga vagy a munkaadója számára szükségesnek és értékesnek tartott információkat. Egyes munkahelyeken ehhez esetleg kapnak még írásbeli instrukciókat meglehetősen nehezen emészthető szabályzatok és eljárások formájában. Az emberek viszont nem túl jók az adatok osztályozásában. Az átlagember például nem tud különbséget tenni a „szigorúan titkos” és a „különösen bizalmas” információ kategóriák között. Valószínűleg a törvényhozók, auditorok és a joggal foglalkozó szakemberek tisztában vannak a fogalmak pontos jelentéseivel, ám a szaknyelv árnyalatainak ismerete nem várható el. Vajon közölünk ki ejtett ki a száján vagy hallott már ilyen mondatot: „Anya születésnap ajándéka titkosított információ, korlátozott hozzáféréssel.” Nem hinném, hogy bárki is, hiszen nem így zajlik a hétköznapi életünk. Egy olyan mondat sokkal valószínűbb, hogy „Anya szülinapi ajándéka titok, ha bárki elárulja neki, nagyon mérges leszek.”

Emberi sajátosság, hogy az adatokat nem önmagukban, elszigetelten szemléljük, hanem szeretjük látni azok környezetét és összefüggéseit, vagyis a kontextus megha-



tározza a gondolkodásmódunkat, mi több, gyakran az adat értékét is. Kontextus alapján mérlegeljük azt is, hogy mi az, amit fontosnak tartunk és mi az, amit nem. Az információk osztályozását azok kontextusa – sőt annak szubjektív értelmezése – alapján végezzük, nem pedig azok tartalma alapján. Emiatt elképzelhető, hogy két szakember, azonos adatok alapján, két egymástól eltérő fontossági sorrendet állít fel vagy különböző következtetéseket von le.

Az említett okok miatt már szinte ki is zárhatjuk egy társadalmi vagy akár szakmai konszenzus meglétét az információk fontosságáról. Ez viszont nem jelenti azt, hogy ne lennének olyan információk, melyek fontos-

ságát egy hivatal, egy cég vagy egy magán-személy deklarálja, és ennél fogva elvárja ezen információk bizalmas jellegének fenn-tartását és védelmét.

Miből áll a kibervédelem fegyvertára?

A védelemhez eszközök is kellenek. A fizikai harcászattól tudjuk, hogy a hatékony védekezéshez legalább olyan jó fegyverek szükségesek, mint a támadáshoz. Sőt, az igazán felkészült védelem folyamatosan új fegyverek kidolgozásán munkálkodik, mert bár ő van hazai terepen, de neki az egész várat és minden oldalról egyszerre kell védeni, míg egy sikeres támadáshoz elég egyetlen ponton koncentráltan áttörni a védelmet. Természetesen a támadók sem tétlenkednek, igyekeznek megtalálni a gyenge pontokat és az új fegyverek meglepetésszerű erejét kihasználni, így a fegyverek fejlesztése mindkét oldalon párhuzamosan történik, és a hatás-ellenhatás törvényének köszönhetően egyre bővül a fegyvertár.

Elég csak, ha eszünkbe jut az egész világon nemrégiben órák alatt végig söpört zsarolóvírus, amelynek hihetetlenül gyors terjedését az amerikai titkosszolgálatól kiszivárogtatott támadó programok tették lehetővé. Vegyük most sorra a védelem legfontosabb fegyvereit.



Titkosítás

Az első a titkosítás. A titkosítás a kibervédelem Szent Grálja. Pontosabban az lehetne, ám mivel nem tudjuk, hogy mit tekintünk fontos információnak, azt sem tudjuk pontosan, hogy mit védjünk vele, ennek következtében általában mindent igyekszünk titkosítani. Például a számítógépünk merevlemezének teljes tartalmát, beleértve az ideiglenes fájlokat is. Ha viszont mindent titkosítunk, akkor valójában semmit sem titkosítunk. Amikor pedig használjuk a számítógépeinket, különböző fájlokat nyitunk meg és dolgozunk azokban, akkor bár csak arra az időre, de feloldjuk a titkosítást, hogy el tudjuk végezni a kívánt feladatainkat, ám a titkosításnak ez az időleges feloldása pont olyan, mint amikor egy gyereksapat előtt felnyitjuk a játékokkal teli doboz fedelét: bárki rávetheti magát az ott talált információkra, jöhetnek a hackerek és szabadon ki-be pakolhatnak benne. A gépekre titokban feltelepített hátsó ajtók, kémprogramok és további ártalmas tartalmak „túlélnek” a titkosítást. Számukra a gép titkosítva is nyitott könyv. Láttam már valaki, hogy ilyen helyzetben a titkosítás visszatart egy hackert? Én bizony nem.

Mindemellett a titkosításnak vannak vitathatatlan érdemei, például hatékonyan megvédi adatainkat, amikor továbbítjuk azokat, vagy ha véletlenül elhagyjuk gépünket vagy pendrive-unkat.

A titkosításnak azonban van egy nagy hátránya is: megköti a törvény végrehajtó szerveinek a kezét, és sokszor ellehetetleníti vagy nagyon megnehezíti, hogy küzdjenek a terrorizmus vagy a gyerekbántalmazás ellen, mert nem feltétlenül férnek hozzá a nyomozás szempontjából elengedhetetlenül szükséges információkhoz.

Kockázatelemzés

A kibervédelem varázserejű kardja a kockázatelemzés. Amikor kockázat-elemzünk, azt mérlegeljük például, hogy milyen kockázati tényezők veszélyeztetik adatainkat, mekkora eséllyel férnek hozzá adatainkhoz, milyen gyakorisággal léphet fel egy-egy kockázat, az adatok feltérzése milyen mély hatással lehet a cégünk működésére stb. Mivel mi magunk, vagyis a

nyos védelmet használnak. Sőt, a lehető legjobb terméket használják a kockázatokkal arányos védelem biztosítására. És valóban, én még sosem talákoztam olyan gyártóval, aki nem a legminőségibb és legfejlettebb rendszerrel állt volna elő. Mindenki a saját portfékáját dicséri, és ahogy a jelmezbálban nehéz kihirdetni a győztest, mert minden gyermek ötletesen választott kosztümöt és mind a tündér, mind lovag tökéletesen hozza saját karakterét, úgy a kockázatokkal arányos védelmi rendszereket is nehéz rangsorolni. Hiszen megfelelnek az alapvető követelményeknek, ráadásul mindegyik tartalmaz olyan extrát, ami a többieknél nincs, vagy nem pont úgy jelenik meg.

Azt azért nem érdemes szem elől tévesztünk, hogy a gyártók szinte a lehetetlenre vállalkoznak, ugyanis a számtalan hibával, pontatlansággal, becsléssel meghatározott kockázatokra kínálnak minden kétséget kizáró és teljes körű biztonságot szavatoló védelmet, és ezzel igencsak közel állnak az önellentmondáshoz.

Ha az említett fegyverek jól működnek, nem történének újabb és újabb hacker támadások, ám azok mégis bekövetkeznek.

Milyen lehetőség áll még előttünk? Végző soron, fordulhatunk az emberek felé. Az embereket ugyanis könnyű hibáztatni, mert nem elég óvatosak vagy felkészültek. A biztonság-tudatosság növelése olyan téma, amit bármikor elővehetünk, ha kibervédelemről esik szó. Az emberek azonban mindig csak emberek maradnak, ezért természetüktől fogva a békességet keresik és első reakciójuk nem az, hogy megakadályozzák mások információszerzését. Nem véletlen, hogy a lakosságnak csak egy kis része lesz katona vagy biztonsági őr.

Az OPM (Office of Personnel Management) már 2004 óta tart biztonságtudatosságot fejlesztő tréningeket. Ez azonban nem tartotta vissza például a kínai hackereket, hogy megszerezzék az amerikai katonaság és az államigazgatás több mint 20 millió tagjának az adatait.

A gép és az ember

A titkokat nehéz megragadni, ennél fogva megvédeni sem könnyű. Amit ugyanis mi valóságnak tartunk és amit mások valóságnak tartanak, az nem feltétlenül esik egybe. Ráadásul a kibertitkok folyamatosan változnak. Sajátos értékeik, minőségeik vannak.

Milyen megoldásokat látok szakemberként?

1. Fel kell ismernünk a titkokat.
2. Folyamatosan terítéken kell tartanunk a magánügy vs. biztonság témáját.
3. Mindehhez pedig gépekre, mesterséges intelligenciára (MI) lesz szükségünk, mégpedig egyre többre.

Egy dolgot tudunk csak biztosan kijelenteni a jövőről: az emberek egyelőre jelen lesznek benne. „Egyelőre”, hiszen az egyre összetettebb elektronikus eszközök és intelligens számítógépek feltűnésével több szakember is rámutatott az ember és gép párosításának előnyeire. Egyes kutatók, professzorok ebben az esetben már transzhumanizmusról beszélnek, értve ezalatt az emberi képességek növelését és kiterjesztését a gépek segítségével. Tisztább hallást, élesebb látást, gyorsabb és pontosabb memóriát, erősebb testet is elérhetünk számítógépes rendszerek és programok bevonásával. Elég, ha csak a DARPA által kifejlesztett agyvezérelt robotikus karra gondolunk, vagy az exoskeletonra, mely mozgásérült embereknek adta vissza a mozgás lehetőségét. Azt tehát, hogy milyen formában és alakban lesznek jelen az emberek a jövőben, még nem látjuk előre. De a változások minden bizonnyal nem csupán a fizikai testünket, hanem a gondolatainkat, önképünket, társas szokásainkat is érinteni fogják.

Sokan felvetik, hogy talán túl nagy gondot jelent az emberiség számára, hogy számítógépeink és okostelefonjaink jobban ismernek bennünket, mint mi magunkat. Hiszen nemcsak méri, azonosítja és elemzi életvitelünket, fizikai reakcióinkat, fogyasztási szokásainkat, érdeklődési körünket, hanem megjegyzi és tárolja gondolatainkat, cselekedeteinket. Ezzel egyidejűleg rendkívül hálások is vagyunk nekik pontosan ugyanazekért a tulajdonságaikért. Sokkal kényelmesebbé teszik az életünket, már nem kell telefonszámokat megjegyeznünk, vagy nem kell azzal foglalkoznunk, hogyan érjük el barátainkat és munkatársainkat, mert a gép felkínálja a leghatékonyabb lehetőséget, ahogy az autónk célba juttatásakor is teszi. Kedvenc márkánknak vagy stílusunknak megfelelő termékeket kínál fel az online vásárlás során, s így nem kell felesleges köröket megtennünk, hogy elérjük célunkat. A gépekkel való kapcsolatunkat áthatja ez az örökös ellentét, egyszerre rajongunk értük és undorodunk tőlük, pont mint amikor kedvenc nagymamánk odakozmált levesét kanalazzuk.

Mindezzel együtt megfigyelhető, hogy társadalmunk egyre toleránsabb lett és az átláthatóság igénye is egyre nagyobb tért nyert. Többet fedünk fel magunkból, mint régebbi korokban, és kevésbé szűgyelljük magunkat. Mark Zuckerberg is rámutatott erre, amikor hét éve így fogalmazott: „Az emberek kellemesen érzik magukat, amikor nemcsak egyre több és különböző fajta információt osztanak meg magukról, hanem teszik ezt egyre nyíltabban és egyre több emberrel... Ez egy olyan társadalmi norma, ami folyamatosan alakulóban van.” Őt sokan kritizálták e mondatokért, végül vissza is vonta azokat. De nem lehet nem egyetérteni vele. A minket körülvevő nyilvánosság egyre nagyobb és összetettebb, és e tény kihatással van a magánéle-

tűnkre is. Miközben a társadalom lineárisan, az információéhség és informatikai képesség exponenciálisan növekszik, s ezzel a ténnyel még elég nehezen tudunk bármit is kezdeni. Marad-e egyáltalán bármink, ami teljesen a sajátunk? Lehetnek-e titkaink? Meg tudjuk-e őrizni azokat?

Miközben a titkok és tabuk száma csökken, az információ iránti vágy növekszik, a társadalomnak nincs más lehetősége, mint alkalmazkodni a megváltozott feltételekhez. A magánélet első szintje mellett (értve ezalatt a személyes kapcsolatokat) megjelent a második szint is, melynek nem feltétele a személyes találkozás, hiszen olyan technológiai zónák is lehetővé teszik a magánélet virtuális irányú kiterjesztését és a titkok megosztását, amelyekhez elegendő néhány korlátozott hozzáférésű projektor, vagy titkosított hang- vagy képi kapcsolat. A magánélet ilyen irányú kiépítésének és fenntartásának alapfeltétele, amit Marcus J. Ranum amerikai IT biztonsági szakember úgy nevezett: tárgyas bizalom, vagyis a hálózatok és gépek iránti bizalom.



Amikor például Barack Obama amerikai elnök felvetette, hogy terrorizmusgyanú és veszély miatt a szakembereknek olyan titkosító algoritmus kifejlesztésén kellene dolgozniuk, amely csak egy bizonyos szűkebb csoport számára tenné elérhetővé az adatok elérését a titkosítás feloldásával. Ennek kapcsán azonnal felvetődött: ki választaná ki ezen szakembereket és milyen szempontok alapján, ill. ki ellenőrizné őket és kinek tartoznának elszámolással? Egy ilyen lépés megtételének alapfeltétele egy olyan technológia létrehozása, mely képes arra, hogy csak bizonyos szakemberek előtt fedje fel a titkosítást, vagyis ilyen esetekben a megoldást a mesterséges titokfelismerő vagy viselkedés-elemző eszközök bevetése jelentheti. Amikor például terrorizmus vagy egyéb bűntény elkövetésének gyanújába keveredünk, akkor elfogulatlan gépek segíthetnek a helyzetünk tisztázásában, amikor részrehajlás nélküli kereső algoritmusokkal át tudják fésülni adatainkat, ki tudják gyűjteni az összes releváns és a tárgyra vonatkozó információt, és azokat – de csak azokat – át tudják adni az illetékes szerveknek. Emberek

nem tudnák elvégezni ezt a feladatot anélkül, hogy ne sértenék meg számtalan egyéb személyes adat titkosságát, és ne hoznák napvilágra, hogy például minden áldott este a szeretőkkel chatelünk miközben tisztázunk minket a terrorizmus vádjai alól.

Még ránk vár

Természetesen néhány „kisebb” technikai problémát még meg kell oldanunk ahhoz, hogy mindez valóban megbízhatóan működni tudjon. Például bizonyos esetekben az alapoktól újra kell írni némelyik informatikai rendszert (akár teljes operációs rendszereket is), miközben a jelenlegi memória- és tárhelykapacitást növelnünk kell. És még tisztázásra vár az a kérdés is, hogy mi történik azzal az adattal, amit például megfosztunk a védelmétől.

Az emberiség történetében azonban nem ez az első lehetetlennek tűnő feladat, mely megoldásra vár, és nem is a legbonyolultabb. Az 1960-as, 70-es évek űrprogramjainak eszközei egyszerűbbek voltak, mint egy mai elektromos borotvácé, az űrhajók memóriakapacitása pedig 1000-szer kisebb, mint ami 2016-ban szükséges volt ahhoz, hogy el tudjunk kapni egy Pokémont. John F. Kennedy mondta híres beszédében: „Nem azért döntöttünk amellett, hogy még ebben az évtizedben a Holdra szálljunk és véghezviszünk más dolgokat is, mert azok könnyűek, hanem mert nehezek...”

Stephen Hawking szerint ugyanakkor nem fogjuk korlátozni a gépek használatát, hiszen az emberek folyamatosan fejlesztik azokat, azért hogy megkönnyítsék saját munkájukat és életüket kényelmesebbé tegyék. A kényelmünket pedig nem adjuk. Alapvetően csak a gépek képesek arra, hogy gyorsan és hatékonyan elemezzék az ember előtt álló lehetőségeket és kockázatokat, és a szükségleteinek megfelelő automatizált válaszokat adjanak.

A titkaink megbízható és pontos kezeléséhez és védelméhez gépekre van szükségünk. A gépek meg tudják őrizni a magánéletünk magánjellegét, ugyanakkor eleget tudnak tenni a társadalmi vagy egyéni biztonság fenntartásához szükséges adatszolgáltatási kritériumoknak. A gépek a jövőben meg tudják oldani a magánélet vs. biztonságok ezt a nagy emberi dilemmáját, amelyet egymás közt nem voltunk képesek kezelni.

Érdemes tehát új szemmel tekintenünk magunkra, a gépekre és a digitális információkra: az embereknek ugyanis nem adataik vannak, a cégeknek pedig nem információik, hanem titkaik. 