Dénes Tamás
matematikus-kriptográfus

email:
tdenest@freemail.hu

Van-(e)-választási lehetőség?!

Kriptográfusként[1] szeretném felhívni a közel 8 millió magyarországi és a több százezer határon túli szavazásra jogosult magyar állampolgár figyelmét a címben feltett (kettős)kérdés politikamentes, tisztán szakmai megválaszolására. A válasz egyben olyan megoldási javaslathoz vezet, amellyel bizonyítható, hogy a ma létező technikai lehetőségek mellett, az állampolgári alapjogok és a tökéletes információbiztonság tiszteletben tartásával, gyorsabban és gazdaságosabban lebonyolítható egy országos választás, mint az igen drága és sok biztonsági kérdést felvető papíralapú rendszerben.

1. Két kérdésre egy válasz

A címben feltett kérdés különös írásmódja azt sejteti, hogy több értelmezést rejt magában. Valóban, a kiolvasható két kérdés:

Van-e választási lehetőség? , illetve *Van e-választási*[2] *lehetőség?*

Amely kérdésekre a felkiáltójeles olvasat rögtön meg is adja a választ, vagyis:

Van e-választási lehetőség!

Ha tehát valóban a választási rendszerünk korszerűsítése, biztonságosabbá tétele, gyorsabb és gazdaságosabb lebonyolítása lenne a cél, akkor van valódi választási lehetőség, amely a már meglévő népességnyilvántartási rendszerhez természetes módon csatlakoztatható.
Az e-választási rendszer tehát a meglévő rendszer szerves továbbfejlesztése lenne, amelynek költsége az igen drága papíralapú rendszer jelentős költségmegtakarításából fedezhető. Különösen, ha figyelembe vesszük, hogy a papíralapú rendszer minden választásnál, ismételten jelentős költséggel jár, míg az egyszer létrehozott elektronikus rendszer újabb költség nélkül újra (és a valódi demokrácia gyakorlásának számtalan egyéb céljára) felhasználható.

Az e-választás esetén külön kiemelendő az adat és információbiztonság maximális szintre növekedése, valamint a korszerű technikai lebonyolítás lehetősége, amely a pénzben nem kifejezhető demokratikus jogok szabad, biztonságos és rendszeres gyakorlását teszi lehetővé.

[1] A *kriptográfia* eredeti ógörög jelentése: *rejtett írás*. A történelem folyamán az üzenetek, információk titkosításának tudományává vált. E tudomány elméleti és gyakorlati művelői a *kriptográfusok*.
[2] Az *e-választás* jelentése, a napjainkban már a köznyelvben elfogadott e-levelezés, e-bankolás, stb.-hez hasonlóan, *elektronikus választást* (szavazást) jelent. Vagyis amikor nem papírra nyomtatott szavazólapon szavazunk, hanem valamilyen számítástechnikai, informatikai, azaz elektronikus rendszerben.

Az e-választás tehát nem csak mindenféle előzetes regisztrációt, illetve más (választások előtti) állampolgári cselekményt tesz teljesen feleslegessé, de magát a választást is *egyszerűbbé* és lényegesen *olcsóbbá* teszi.

Igen aktuális a biztonság kérdésének felvetése, amikor a választási törvény kapcsán valódi lehetőségként kerül szóba, az adatbiztonsági szempontból különösen megkérdőjelezhető *egyszerű levélben történő szavazás*! Már a felvetés is meglepő, amikor éles (és jogos) kritikák érik a kopogtató cédulákat, amelyek hasonló biztonsági problémákat vetnek fel, vagyis alapvető biztonsági feltételeknek sem tesznek eleget. Az *„egyszerű”* jelző szerepe igen fontos, mivel létezik olyan kriptográfiai protokoll, ami ezt az eljárást is biztonságossá teheti[3], azonban tartok tőle, hogy ennek alkalmazása a következő választásokon nincs betervezve. Ugyanakkor ezeket a problémákat egy jól megvalósított e-választási rendszer teljesen kiküszöböli.

2. Az e-választás követelményei

Az elektronikus választás (e-választás, vagy e-szavazás) alkalmazása még gyerekcipőben jár az egész világon, mivel több nyitott kérdés nem egészen tisztázott. Ilyen a biztonság, a megvalósíthatóság, az ár, és a standardizálás. A biztonság kivételével, mind csupán politikai akarat és gazdasági döntés kérdése. Ilyen irányú politikai döntés esetén tehát Magyarország nemzetközi referenciává válhatna. Megmutatjuk, hogy a kriptográfia (és az azt megvalósító digitális technika) már ma is lehetővé teszi az e-választás biztonságos lebonyolítását.

Egy minden szempontból biztonságos választási rendszernek (függetlenül attól, hogy papíralapú vagy elektronikus) az alábbi feltételeket kell kielégíteni:

2.1. Választási jogosultság hitelesítése - *csak a bejegyzettek szavazhassanak*
2.2. Egyediség – *egy szavazó ne szavazhasson többször*
2.3. Helyesség (pontosság) – *a szavazási rendszer helyesen rögzítse a szavazatokat*
2.4. Verifikálhatóság (ellenőrizhetőség) – *ellenőrizhetőnek kell lenni, hogy minden szavazatot helyesen vett számba a rendszer, és megbízható (hiteles) a választói névjegyzék*
2.5. Titkosság – *senki sem azonosíthatja (a szavazón kívül) az egyéni szavazatot, vagyis nem párosítható a szavazathoz a szavazó*
2.6. Kényszeríthetetlenség – *a szavazót ne lehessen befolyásolni a szavazásban*

Továbbá, a választási hajlandóságot növeli, ha a szavazáshoz egyszerű eszközök állnak rendelkezésre és minimális készségek szükségesek, valamint a szavazási eljárás könnyen megérthető.

3. Rendszerbiztonsági megfontolások

Bármely e-szavazási rendszer a következő technikai alrendszerekből áll:

- szerverek és háttér rendszerek
- a hálózat
- felhasználói végpontok

[3] Angol elnevezése: *Zero knowledge protocol*, amely a korszerű digitális technikával egyre terjedő, igen nagy információbiztonságot nyújtó, úgynevezett *Zero knowledge proof*, azaz „*előismeret nélküli bizonyítás”* kriptográfiai módszerére épül.

A szerverek és háttér rendszerek biztonsága a hagyományos módon kezelhető, mivel a fenyegetettség hasonló az online pénzügyi szolgáltatásokéhoz. Azonban lényegesen eltér a pénzügyi alkalmazásoktól, hogy ott a tranzakciók mindegyik lépése jól dokumentált (naplózott), míg a titkos szavazási rendszereket úgy kell tervezni, hogy a szavazatokból ne lehessen visszakövetkeztetni a szavazókra (lásd a 2.5. pontot).
A felhasználói végpontok biztonságát nehéz megvalósítani, különösen, ha a szavazó az otthoni PC-jét használhatja. Mivel a szavazó jóhiszeműen is rákapcsolódhat egy illegális szerverre, így a szavazat titkossága sérülhet, azaz szándéka szerint az X szavazatot adja le, de a szerver az Y szavazatot rögzíti. Mire van tehát szükség?
Egy *személyes biztonsági egységre* (angol rövidítése: PSD=Personal Security Device), amelyik nem csak a digitális aláírás személyes kulcsát védi, hanem biztosít egy „védett kijelzőt" a szavazási eljáráshoz. Például a mai korszerű mobiltelefonok alkalmasak a PSD funkcióra, mivel jól egyesítik az intelligens kártya (chipkártya) és kijelző funkciókat, valamint szinte minden állampolgár rendelkezik ilyen eszközzel, tehát nem igényel plusz költséget.

4. Az e-szavazás kriptográfiai protokollja

Először azt gondolhatjuk, hogy lehetetlen egyszerre kielégíteni a személyes azonosíthatóság és a szavazat titkosságának kritériumait. Azonban ennek a problémának többféle nagy biztonságú megoldása is létezik, amelyek különböző kriptográfiai módszereken és az ezekre épülő, úgynevezett protokollokon nyugszanak. Íme egy magas szintű, mégis egyszerű protokoll, amely az úgynevezett „vakaláírás"[4]-on alapul:

P1. A *szavazó azonosítja magát*[5] a szavazat regisztrációs rendszerben.

P2. A szavazó készít egy „elektronikus szavazatot" (e-szavazat), a 3. pontban leírt PSD személyes biztonsági egység segítségével. Így a szavazó tökéletes biztonságban lehet, hogy az általa kívánt szavazat fog a rendszerbe kerülni.

P3. A szavazó leadja e-szavazatát, amit *digitális aláírással*[6] lát el a rendszer.

P4. A P1. regisztrációs azonosítás ellenőrzi, hogy a szavazó nem küldött még szavazatot a rendszerbe, majd digitális „bélyegzővel" (vakaláírással) látja el a P3.-ban leadott szavazatát.

P5. A szavazó e-szavazata bekerül egy elektronikus szavazóládába, amely nem más mint a központi szerveren lévő (biztonságosan védett) adatbázis.

A szavazás leadása után a szavazó számára a határidő lezárul, a szavazat megszámláltatik, és egy adatbázisba kerül, ami ettől kezdve nyilvánossá válik. Bárki meggyőződhet arról, hogy minden szavazatnak van „bélyegzője" és minden szavazó meggyőződhet arról, hogy a szavazata bekerült az adatbázisba.

---

[4] A vakaláírás rövid ismertetése található a következő 5. pontban.

[5] Az azonosításnak biztosítania kell, hogy ne lehessen más helyett szavazni. Vagyis személyhez kötött azonosítót kell használni, ami lehet biometrikus azonosító (ujjlenyomat, hang, stb.), vagy olyan dinamikus kriptográfiai eljárás, amely nagy biztonsággal képes a személy azonosítására. Ilyen eljárások már az e-banki gyakorlatban is használatosak (dinamikus jelszó, zero-knowledge proof), amelyekről részletes ismertetés található jelen szerző több dolgozatában.

[6] A *digitális aláírás* az "elektronikus irat" tartalmát és az aláíró személyazonosságát igazolja úgy, hogy ezekből egy kriptográfiai eljárással speciális kódot hoz létre, amit az irathoz rendel.

5. Vakaláírás

A digitális aláírásnak egy különleges alkalmazási területe az úgynevezett vakaláírás. Ennek lényege az, hogy az aláíró (hitelesítő) anélkül ír alá, hogy az eredeti szöveget ismerné. Ez a közjegyzői gyakorlatban régóta ismert. A közjegyző hitelesítéskor ugyanis nem a dokumentum tartalmát igazolja, hanem csak az azon szereplő aláírást[7], így fogalma sincs arról, hogy mi áll a dokumentumban. A vakaláírás lényegét egy konkrét példával lehet egyszerűen megvilágítani:

Valaki egy végrendeletet ír, majd azt digitálisan aláírja[8], és az egészet rejtjelzi egy bizonyos algoritmussal. Ezután elmegy a közjegyzőhöz, és a közjegyzőnél nem az eredeti végrendeletet, hanem annak a rejtjelzett változatát helyezi letétbe oly módon, hogy a közjegyző a rejtjeles változatot, a rejtjelző kulcsot, és eljárást, digitális aláírásával hitelesíti anélkül, hogy a végrendelet szövegét ismerné (hiszen a rejtjelzés miatt el sem tudja olvasni).
A végrendelet kedvezményezettje a végrendelkező halála után bemutatja a végrendeletet, majd a közjegyző elvégzi az adott eljárással és kulccsal a végrendelet rejtjelzését. A rejtjelzett változatot összehasonlítja a letétbe helyezett változattal, illetve megvizsgálja a letétbe helyezett változat digitális aláírását, valamint az újonnan rejtjelzett változat digitális aláírását. Amennyiben ezek megegyeznek, úgy hitelesíteni tudja a végrendelet valódiságát anélkül, hogy a végrendelet szövegét eleve ismerte volna.[9]

Egy dokumentum rejtjelzett változatának a vakaláírása az ügyfél részére sokkal nagyobb biztonságot nyújt, mintha az eredeti végrendeletet helyezné letétbe, ugyanis ez utóbbi esetben ki van annak téve, hogy ha a közjegyző nem becsületes, úgy a végrendelet tartalmát meg tudja változtatni, illetve nem kívánt módon a kedvezményezettnek, vagy éppen a végrendeletből kizárt személynek a végrendelet tartalmát ki tudja szivárogtatni. Ugyanez a nemkívánatos jelenség sajnos előállhat becsületes közjegyző esetén is, ha őt zsarolással, vagy más életveszélyes fenyegetéssel kényszerítik.

6. Igazi-(e)-demokrácia?! avagy Az INFOSANCE a 21. század reménye

E pont címében elrejtett kérdés-válasz párt a főcím megfejtése után már rutinosan kezeli az Olvasó, azaz világos a feltett kérdés: *Igazi e demokrácia?*, amelyre a jelen sorok írójának válasza: *Igazi e-demokrácia!*
Míg e kérdés-válasz pár kifejtése egyben a fenti 1.-5. pontok rövid összefoglalása, addig a cím második felében még ismeretlennek tűnő INFOSANCE[10] több magyarázatot igényel, ám a 21. századi közös jövőnket rejti.

---

[7] Ezért szükséges a közjegyző előtt aláírni a dokumentumot.
[8] Az e-szavazás esetében, ez felel meg a digitális aláírással ellátott elektronikus szavazatnak.
[9] Az e-szavazás esetében, ez az eljárás felel meg a P4.-beli elektronikus szavazóládába került szavazatok „kibontásának", amelyeket aztán összesít a rendszer.
[10] A jelen szerző által az ezredfordulón bevezetett fogalom, az INFOSANCE mozaikszó, amely az INFOrmációs renaisSANCE-ból jött létre. Tömör definíciója: *Olyan társadalmi kor, amelynek lényege, a szabadon gondolkodó ember klasszikus képességeinek optimális egyesítése a mindent átszövő, globalizálódó e-technikával és az egyre teljesebb, biztonságosabb információ birtoklásával.*

A mai magyarországi választási rendszer szakmai szempontból többszörösen indokolhatatlan, nyomasztóan szubjektív politikai döntések sorát tartalmazza. Ezért talán még megdöbbentőbb az 1.-5. pontokban felvázolt *e-választási rendszer* pozitív tulajdonságainak látványa, egy csokorba fűzve:

- Az e-választási rendszerben a szavazás, a szavazó és a választási rendszer számára is *maximális biztonságot nyújtó*, úgynevezett szimmetrikus *egyenszilárdságú rendszer*.[11]
- Az e-szavazás lezárásának pillanatában, *azonnal rendelkezésre állnak a választási eredmények*. Nincs szükség órákon, esetleg napokon keresztül tartó és számos biztonsági kockázatot, valamint emberi tévesztési lehetőséget rejtő kézi összesítésre.
- Természetes módon alkalmazható az *online szavazás*. Így fel sem merül a technikai és biztonsági problémák sorát felvető, előzetes regisztráció és a postai (levélben történő) szavazás. Ugyanakkor teljesen azonos technikai és biztonsági feltételekkel szavazhat minden arra jogosult, az *ország, sőt a világ bármely részén*, ahol Internet hozzáférés van.
- Könnyen biztosítható a *kényelmes*, és egyre többek számára hozzáférhető, *otthoni szavazás!*
- Az online szavazás esetén alkalmazott protokollok *alkalmazhatók a helyi szavazókörzetekben* elhelyezett számítógépes felhasználói végpontokon is. Így az eddigi helyen, de az eddigieknél jóval egyszerűbben és biztonságosabban biztosított azoknak is az e-szavazás, akiknek nincs otthoni (számítógépes vagy okostelefonos) online hozzáférésük.
- Egy-egy *e-szavazás lebonyolítása és költségei minimálisak*, hiszen nem különböznek egy e-bank átutalási tranzakcióétól.

Mindezek alapján nehezen értelmezhető, sőt érthetetlen a technikai fejlettségükre oly büszke, úgynevezett modern társadalmak húzódozása attól, hogy a mérhetetlen szellemi és anyagi befektetés eredményeként létrejött káprázatos technikában, ne csupán üzleti lehetőséget lássanak, hanem a ***közvetlen demokrácia****, az* ***emberi szabadságjogok*** *kiteljesedésének soha nem látott megvalósíthatóságát?!*

A címbeli felkiáltásként megfogalmazott kérdésre, ma sem lehet bölcsebb választ találni, mint amit több mint fél évszázada N. Wiener[12] így fogalmazott meg: *„A tipikus amerikai világban az információ sorsa az, hogy áru lesz, venni és eladni lehet. Nem az én dolgom, hogy azon akadékoskodjam, hogy ez a kereskedői álláspont erkölcsös-e vagy nem, durva-e vagy finom. Az én dolgom az, hogy kimutassam: ez az álláspont az információ és a vele kapcsolatos fogalmak félreértéséhez és félrekezeléséhez vezet."*

[11] Az *egyenszilárdság* az információbiztonság egyik kulcsfogalma. Az egyenszilárdságot a mérnöki tudományokból vették át metaforaként a biztonsági rendszerekkel foglalkozó tudományok. Ez annyit jelent, hogy hiába alkalmazzuk egy biztonsági rendszer bizonyos pontjain a legkorszerűbb eszközöket, ha van akár egyetlen eleme, amely alig védett. Ezen a kevéssé védett elemen keresztül az egész rendszer támadhatóvá válik.
A szimmetria azt biztosítja, hogy mindkét fél biztonsága azonos mértékben biztosított, ami általában nem teljesül, *főleg az állam és állampolgárok viszonylatában*.

[12] Norbert Wiener (1894-1964) a kibernetika atyja, az információelmélet nagy alakja.

Meg kell állapítanunk, hogy Wiener intelme nem használt. Az egyre globalizálódó információalapú társadalmakban, a tömeges információt és az azt kezelő óriási technikát, egyre inkább a hatalom birtokolja. *Rá kell tehát mutatni, hogy az információ és a vele kapcsolatos fogalmak, mint például a szimmetrikus információbiztonság, információs önrendelkezés, azaz magának az e-demokráciának tudatos félreértése és félrekezelése folyik!*

Ebből csak egy 21. századi *új renaissance kor* vezethet ki, ezért Jókai zseniális utópiáját megidézve azt állítom, hogy az INFOSANCE (http://www.titoktan.hu/_raktar/INFOSANCE.htm) a jelen század reménye.
A reneszánsz ugyanis szélesre tárta az ablakot a középkor csőlátásával szemben, amikor az egyház birtokolta a világról szóló információk jelentős részét, így a kezében volt az emberek gondolkodásának *„marionett-vezérlése”*. Mára ez átalakult a digitalizált, elektronikus technika csőlátásává, az Internet, az információs hálózatok fekete dobozává, amelynek „marionett-vezérlése” a hatalom, az adattárak és informatikai rendszerek tulajdonosainak kezében van.

Az INFOSANCE társadalom ígérete és nagy lehetősége tehát, a gondolkodó ember klasszikus képességeinek optimális egyesítése a mindent átszövő, globalizálódó e-technikával és az egyre teljesebb, biztonságosabb információ birtoklásával. A 21. századi INFOSANCE kor olyan e-társadalom képét rajzolja fel, amelynek középpontjában a felszabadultan gondolkodó és cselekvő új, *modern renaissance e-mber áll*.
Az INFOSANCE e-mber lehetősége *„új ablaknyitás”*, amely a felhalmozott óriási technika, a globális kommunikációs és informatikai rendszerek lehetőségeit egyesíti a renaissance mintájú szabad, szárnyaló, kreatív, emberi gondolkodással.

Az INFOSANCE tehát a 21. század elektronikus digitalizációjának emberközpontú felhasználásán nyugvó, közvetlen demokrácia társadalma.