Németh Eszter

Privacyvédjegyek pró és kontra

14. téma

1 Bevezető

Az információ hatalom. Az információáramlás döntő többsége a világhálón megy végbe. Egyre több felhasználó –leginkább a vállalatok, de már a magánszemélyek közül is sokan- ismeri fel, hogy fontos védenie az adatait.

Szükséges védenünk a személyes adatainkat, hiszen a rólunk megtudott információkat mások fegyverként is használhatják ellenünk. Elég csak arra gondolnunk, hogy amit most nem bánunk, hogy kikerül az internetre, az később már ránk nézve kellemetlen is lehet. Személyes adatnak pedig nemcsak a nevünk, címünk, születési dátumunk (stb.) minősül, hanem minden adat, ami velünk, mint természetes személyekkel kapcsolatba hozható, valamint olyan adat is, amiből levonható ránk (érintettekre) vonatkozó következtetés.[1]

Ma már számos lehetőség közül, választhatunk, hogy mivel védjük a személyes adatainkat. A privátszférát erősítő technológiák (PET) azok, amelyek erősítik egy információs rendszerben az egyén magánéletének védelmét úgy, hogy megakadályozzák a személyes adatok szükségtelen vagy jogellenes felhasználását, vagy olyan eszközöket, beavatkozási lehetőségeket kínálnak, amik növelik az egyén ellenőrzését a személyes adatai felett.

A privacyvédjeggyel ellátott weboldalak, szolgáltatások jelezik a felhasználóknak azt, hogy amit éppen látogat, használ, megbízható-e. Ezek a személyes adatokat az saját irányelveinek megfelelően kezelik. Így nemcsak azok a felhasználók szembesülhetnek privátszféra-barát technológiával, akik már hallották, hogy létezik ilyen**.** Hanem mindaz, aki már járt ilyen weboldalon, rákattintott a pecsétre, és elolvasta az aktuális privacyvédjegyről szóló tájékoztatást (általában az oldalon egy pecsét jelzi)

2 Mi is az a privacyvédjegy?

Először is, hogyan határozhatjuk meg a védjegy [2] fogalmát? A védjegy a kereskedelemben árujelzőt jelent, ami a termékek és szolgáltatások egymástól való elválasztását, megkülönböztetését segíti. Feladata, hogy bizalmat ébresszen a fogyasztókban, hogy törzsvásárlóként máskor is védjegyes árut válasszanak. Valamint védi a védjeggyel rendelkező tulajdonos piaci helyzetét a konkurens gyártókkal szemben. A privacyvédjegy egy ellenőrzési szervezet logója, pecsétje. A privacyvédjeggyel rendelkező weboldalak jelzik a felhasználóknak, hogy megfelelnek-e saját adatvédelmi irányelveiknek. Ez szintén bizalmat ébreszthet bennük, mint ahogy a kereskedelmi védjegy a vásárlókban. Vajon tényleg többet használják az emberek a „pecsétes" oldalakat a többinél? Ennek megkülönböztető szerepe is van, hogy kiemelkedjen a védjegy nélküli webhelyek közül. Valamint a különböző védjegyeket egymástól is elkülöníti (mivel több fajta privacyvédjegy létezik). Ilyen például a TRUSTe, a EuroPriSe, a BBB (BBBOnLine). A legismertebb pivacyvédjegy a TRUSTe, ami a piacon a legnagyobb részesedéssel bír. Ezen kívül az EuroPriSe is ismert, ami az EU-s szabványokra van specializálódva. [3]

2.1 TRUSTe

A TRUSTe egy non-profit szövetségből alakult 1997-ben abból a célból, hogy a felhasználók és vállalatok maguk tudják szabályozni a személyes adataik feletti ellenőrzést. [4]

A TRUSTe védjegyek 3 féle kategóriába sorolhatók: adatvédelmi pecsétek, biztonsági zárak, valamint a megbízhatóságot tanúsító pecsétek. Az adatvédelmi pecsétek biztosítják, hogy adott oldal tartja-e magát az adatvédelmi program követelményihez, és a saját irányelveihez, valamint, hogy a saját sebezhetőségét ellenőrzi-e és ezeket a réseket észre is veszi-e. A biztonsági zárak jelzik, hogy az oldal tulajdonosa megvizsgálja-e a weboldalon használt technológiát, ami védi a személyes adatokat és kiszűri a rosszindulatú szoftvereket. (Ezt a napi ellenőrzési rutinnak tartalmaznia kell.) Az oldalnak figyelnie kell a saját sebezhetőségét, sérülékenységét. [5]

A webes adatvédelmi követelmények meghatározzák, hogy a privacyvédjegyet igénylő weboldalnak, internetes szolgáltatásnak milyen jogokat és műveleteket kell biztosítania a felhasználónak. A felhasználótól beleegyezését kell kérnie, hogy az adatait hogyan kezelje. Csak beleegyezéssel lehet a személyes adatokat továbbadnia egy harmadik félnek. A felhasználó kérheti, hogy töröljék a honlaphoz tartozó levelezőlistákról,

hírlevelekről. Valamint a felhasználónak hozzá kell férnie az adataihoz, hogy azt frissíteni, javítani tudja. A webhely biztonságát is garantálnia kell. Az olyan oldalakon, amik kényes információkkal dolgoznak, működnie kell egyfajta titkosításnak, ami lehet Secured Socket Layers (SSLs) technológia alapú vagy egyéb, ezekhez hasonló. A webhelynek Malware mentesnek kell lennie, ami azt jelenti, hogy figyelniük kell arra, hogy semmilyen rosszindulatú szoftver ne épüljön be az oldal működésébe. A Malware szoftver illegálisan gyűjt adatokat azon az oldalon, ahova sikerül beépülnie. (A Malware rengeteg fajta lehet.) [6]

A TRUSTe adatvédelmi program magába foglalja a webes adatvédelmet, amely kötelezi a cégeket az adatvédelmi irányelveik betartására, ezzel védve a felhasználókat és személyes adataikat. Biztosítja, hogy az EU állampolgárok privátszférájának őrzését az EU Safe Harbor irányelv alapján, amely szerint az Európai Unión kívüli országokba korlátozva van a személyes adatok forgalma, hiszen például az USA-ban élőkre más adatvédelmi jogszabályok vonatkoznak, ami nem olyan erős intézkedéseket foglal magába, az EU-s jogokhoz képest. Az EU és az USA között külön megállapodás is született, ez az USA-EU Safe Harbor. Az e-mailezést is védelemben részesíti a program. Szükséges, hogy a felhasználó, ha akar, le tudjon iratkozni a vállalat, a honlap levelezőlistáiról, vagy egyéb listáiról. [6]

2.2 A TRUSTe és a Facebook [7]

A TRUSTe több nagyvállalatot, és nagylátogatottságú portált minősített biztonságosnak. 2010-ben egy adatvédelmi botrány kapcsán felmerült a TRUSTe neve is, mint akik többször vizsgálták már a Facebook adatkezelését. A Facebook egyes alkalmazásai személyes adatokat osztottak meg a felhasználókról, ami az adatvédelmi irányelveik megszegését jelentette. A Wall Street Journal írásából az derült ki, hogy a legnépszerűbb alkalmazások személyes adatokat továbbítottak egyes hirdetőkhöz, melyben a felhasználók neve is megjelen**t:** tehát a hirdetők számára fontos paraméterekhez hozzá volt párosítva a személy is. Akkoriban a TRUSTe valóban igazolta a Facebook.com adatvédelmi nyilatkozatát, de ez nem vonatkozott a mobil alapú szolgáltatásokra (egyébként a szervezet épp akkoriban fejlesztette ki a Mobil alapú adatvédelmi programját.) A Mobil App szolgáltatás meghatározza, hogy a mobil alkalmazások védik az egyén privátszféráját, személyes adatait. A TRUSTe segíti a Facebook-ot, hogy fejlessze az adatvédelmi politikáját.

2.3 EuroPriSe (European Privacy Seal) [8]

Az EuroPriSe privacyvédjegy tanúsítja, hogy egy informatikai termék vagy IT-alapú szolgáltatás megfelel-e az európai adatvédelmi előírásoknak, mennyire veszi figyelembe az EU-s jogszabályokat. Ha a termék teljesíti a vonatkozó jogszabályokat, és ezek betartását technológiailag is tudják biztosítani, akkor megkaphatják a szervezet adatvédelmi pecsétjét. Az odaítélés folyamata két lépcsős. Először egy jogi és informatikai szakértőkből álló csoport értékeli a weboldalt, a terméket. Ezt pedig egy független adatvédelmi testület (minisztérium, ügynökség…) megerősíti, ezzel érvényesítve a pecséthez való jogot. Két fajta jelentést állítanak ki a szolgáltatásról, termékről, az egyik hosszabb és bizalmas műszaki és jogi jelentés, a másik pedig egy rövid publikus, amihez bárki hozzáférhet. Privacyvédjegyet bocsátanak ki teljes termékre, szolgáltatásokra, vagy annak egyes részeire és technológiákra. Ezen belül

ilyen szolgáltatások, termékek kaphatnak EuroPriSe tanúsítványt: személyes adatokat feldolgozó szoftverek, honlapok, online banki szolgáltatások.

Több európai irányelv alapján végzik a vizsgálatokat. A Data Retention naplózási feltételeinek is alávetik magukat, valamint a követelményrendszerük összhangban van az ePrivacy Directive-el (Elektronikus Hírközlési Adatvédelmi irányelv). Ez az irányelv a szabályozás fontos kérdéseivel foglalkozik: bizalmas információk, forgalmi adatok kezelése. 2007-beni alapításuk óta többször kellett módosítaniuk a követelményrendszerükön. (Pl.: a cookie-król szóló adatvédelmi újítások érvénybe lépése). Követelményeik között hangsúlyt kap, hogy a szolgáltatásoknak milyenek a naplózási szokásaik. Ez egy érdekes terület, hiszen az EU-s jogszabályok szerint kötelező a naplózás, ami viszont a személyek megfigyelhetőségét teszi lehetővé. Ez pedig a privacyvédjegy lényegét veszélyezteti, ugyanis a védjegynek a személyes adatok védelmét, biztonságát, ezzel pedig a személy védelmét, anonimitását kell garantálnia. A EuroPriSe vizsgálja, hogy hogyan történik a személyes adatokhoz való hozzáférés, ki tud egyáltalán hozzájutni. Mivel az oldalakra és a termékekre szükséges a regisztráció. A bejelentkezési mechanizmust és a személyes adatokat tartalmazó fájlokat a szervezet minden szolgáltatásnak ellenőrzi, aki szeretne ilyen adatvédelmi pecsétet, hiszen ezt kötelezővé tették. Az adatkezelési területre a termékek továbbfejlesztésekor is figyelni kell, hogy az új verzióban továbbra is biztosítva legyen a személyes adatok védelme. A „fejlettebb" termék ugyanúgy teljesítse a követelményeket, mint az eredeti. A szolgáltatások ellenőrzésekor felmerül, hogy milyen naplózási technikát használ, tudja-e nyomon követni, hogy mikor módosítottak, helyesbítettek az adatokon. Fontos kérdés, hogy továbbítja- e az adatokat egy harmadik félnek, és ezt milyen módszerrel teszi, valamint, hogy rögzíti-e a felhasználó személyazonosságát. A tárolt adatokhoz való hozzáférést is vizsgálják, hogy kinek van joga az adatbázist olvasni. Az adatok őrzését is meg kell oldania valahogy a terméknek, hogy az ne ütközzön az adatvédelmi irányelvekkel és közben a jogszabályokat is betartsa. Ennek a kérdésnek az egyik megoldása, hogy a tárolt adatokat egy bizonyos idő elteltével törlik. A szolgáltatásnak ügyelnie kell a hálózati és infrastrukturális biztonságára. Megbízható szállítási és továbbítási mechanizmus, útvonal kell. Az adatokat csakis megfelelő címzettnek szabad továbbadni. A címzett személye ellenőrizhető tanúsítvánnyal, valamint az adatot védheti jelszó is. A szolgáltatásnak védelmet kell nyújtania a kártékony programok ellen is, mert ha kémprogramok, vírusok beépülnek a személyes adatok biztonsága veszélybe kerül. [9]

A felhasználóknak joguk van tájékoztatást kapni az adataik felhasználásáról, ezért a EuroPriSe fontosnak tartja, hogy a felhasználók mindig megkapják az aktuális információkat, amiket tudniuk kell, hogy az adataikat biztos helyen tudhassák. A szervezet ezt a szempontot is figyelembe veszi, mikor értékel egy honlapot, vagy szoftvert, hogy a felhasználóknak vannak-e lehetőségeik arra, hogy megtudják mi is történik az adataikkal, ehhez pedig elengedhetetlen a hatékony kétirányú kommunikáció, szolgáltató és felhasználó között.
Az eredmények értékeléséhez szükséges, hogy nyomon lehessen követni az adatvédelmi intézkedések hatékonyságát. Az új Cookie-jogszabály érvénybe lépésével a tárolt információ csak akkor válik elérhetővé, ha erre a felhasználó megadja az engedélyt. A privacyvédjegyek egyik célját ez az intézkedés részben elősegítheti, hogy a felhasználó irányíthassa a személyes adatainak kezelését, feldolgozását. (Azért csak részben, mivel a cookie-k által a felhasználók tevékenységei nyomon követhetők, ezzel sajnos a privátszféra védelme sérül.)

Most két példát szeretnék említeni, akik megkapták a EuroPriSe pecsétet. Az egyik a Nugg.ad[10][11]. Ez a cég online reklámozással foglalkozik. Egy ilyen cég rengeteg adatot dolgoz fel, de ennek ellenére sikerült privátszféra-barátnak maradni, hogy az oldalt látogatók IP-címét elrejti a harmadik fél elől, így anonimak tudnak maradni. Az ügyfeleinek folyamatos és rendszeres útmutatást, tájékoztatást ad, így átlátható marad a rendszere a felhasználók számára. Valamint rendelkezik olyan funkcióval, amiből megismerhetik a látogatók, hogy milyen kategóriába lettek besorolva. Ez a topic monitor. (Az oldal PTN-technológiai megoldást használ, amely marketinges területen a prediktív viselkedést célozza meg.) Az oldal idén érvényesítette a védjegyét, hiszen először 2009-ben nyerte el a jogot, hogy viselhesse. (A EuroPriSe védjegyek 2 évig érvényesek, ha meg szeretnék hosszabbítatni, akkor már elég egy egyszerűsítő eljárásban résztvenniük. A másik weboldal, ami szintén rendelkezik EuroPriSe tanúsítvánnyal, az az Ixquick [12] holland meta-kereső, aminek még az a különlegessége, hogy elsőként szerezte az EuroPriSe védjegyét 2008-ban, amit azóta egyszer hosszabbíttatott meg, ami mára már sajnos elavult (2009-2011). Ez a kereső több kereső óriás általi találatokat egységesít, és ezekből a súlyozott átlagos találatot adja ki. A nyilvános jelentésben szerepel róla, hogy a személyes adatok és egyének védelmére nagyon koncentrál. A pozitívuma az adatminimalizálás, nem sok adattal dolgozik, a személyes azonosításra alkalmas adatokat például nem is tárolja. A nem keresésre vonatkozó információkat 14 naponta eltávolítja, tehát nem őrzi meg, ezzel is gondosan ügyel az adatgyűjtésre korlátozására. A harmadik fél csak minimális, szükséges adatokat kaphat, ezért és a személyes adatok nem raktározása által, a harmadik felek nem tudják azonosítani a felhasználót, ezért anonim tud maradni.

3 Pro és kontra

A privacyvédjegyeknek vannak előnyeik is. Felhívhatják a felhasználók figyelmét az adatvédelem fontosságára, azáltal is, hogy ha egy felhasználó találkozik egy ilyen pecséttel, akkor tájékozódik egy kicsit az adatvédelemmel kapcsolatban. Az nagyon jó, hogy a pecsétes weboldalak a saját adatvédelmi irányelveiket betartják, viszont sajnos így azt kell, hogy gondoljuk, hogy akik nem rendelkeznek ilyen bélyeggel, azok nem tartják be ezeket, vagy nem megfelelően védik a személyes adatainkat (az adatok kezelése nem biztonságos). A TRUSTe-nál nem garantálják, hogy az EU-s irányelvek megvalósulnak az általuk minősített szolgáltatásnál. Valószínűleg ez abból fakadhat, hogy a TRUSTe egy amerikai szervezet, és az USA-ban gyengébbek az adatvédelmi jogszabályok (amint az az EU Safe Harbor –ban ki is van fejtve).

A pivacyvédjegyek a felhasználók kezébe adják az irányítást a személyes adataik felett, tehát csak azt osztják meg, amit jónak látnak, így a felelősséget is a felhasználókra helyezik át.

A privacyvédjegy egyik céljának azt tűzték ki, hogy bizalmat ébresszen a védjegyes termékek szolgáltatások használóiban a termék iránt, ezért például piacserkentő hatása is van, mivel így növeli a versenyt a szolgáltatók között, a „pecsétesek” számára versenyelőnyt biztosítva, hiszen a személyes adataik biztonságáért aggódók sokkal szívesebben választják majd a védjegyes termékeket, akárcsak a kereskedelemben. Emellett új piaci lehetőségeket teremt, az új PET-technológiák is, ezáltal kelendőbbek lesznek. Egyéb pozitívuma a privacyvédjegyeknek, hogy a felhasználók körében egyre többen szembesülnek a jogszabályokkal és egyre többen meg is értik a privátszféra-védelem szükségességét és fontosságát.

Viszont találhatunk visszásságokat is a privacyvédjegyekkel kapcsolatban. Az adatvédelmi irányelvek sokszor megjelenik az adatok gyűjtése (bár a továbbadásukban már fogalmaznak meg korlátozásokat). A védjegyek pontosan ezeknek az adatvédelmi irányelveknek való megfelelést jelölik. Sőt, mint azt már említettem, a Data Retention kötelezővé teszi a naplózást, amiből egyáltalán nem következik a személyes adatok védelme. A naplózás során több felhasználó internetezési, böngészési szokásait lehet rögzíteni, ami egy esetleges támadáshoz épp elég információt szolgáltathat az alanyról. Még ha ezt, a privacyvédjegyek követelményei enyhíteni is akarják (pl. azzal, hogy egy

4. Összefoglalás

A védjegyeket kiállító szervezetek a termékek és szolgáltatások vizsgálata során sok privátszférát erősítő technológiával találkoznak, amiket a weboldalak használnak. Ezekkel tudják a jogszabályokat alátámasztani. Önmagában a privacyvédjegy nem ad védelmet a támadások, illegális behatolások ellen, mert az oldalon használt mechanizmusok teszik ezt meg. Ezért a privacyvédjegyet ál-PET- nek nevezhetjük, hiszen nem önmagában adja a védelmet.

Véleményem szerint a privacyvédjegyek olyan PET-technológia, ami elég nagy felelősséget helyez a felhasználókra, hogy milyen szolgáltatásokat használnak, és milyen mechanizmusokat vesznek igénybe a privátszférájuk megőrzése érdekében, hiszen a privacy pecsét egy jelzés az oldalt látogatóknak, hogy az aktuális webhely a személyes adatokat az adatvédelmi irányelveknek megfelelően kezeli. Ez egyrészt jó, mivel fontos a felhasználóknak is tisztában lenniük azzal, hogy mennyire kell a személyes adataink biztonságára figyelmet fordítanunk, és a jogainkat is meg kell ezzel kapcsolatosan ismernünk, valamint tájékozódnunk kell, hogy milyen technológiákkal tudjuk biztosítani ezt a védelmet. Tehát ha az ember egy privacyvédjeggyel találkozik, remélhetőleg felfigyel rá és utána olvas a tudnivalóknak, így szembesül a problémákkal és a lehetőségekkel is. Másrészt pedig rossz, mivel nem egy konkrét technológiát biztosít védelemül a számunkra.

A privacyvédjegyek fejlesztése szerintem a jövőben is folytatódni fog, hiszen az új technológiák újabb és újabbakat generálnak, amiket a jogszabályoknak is utol kell érniük, így a privacy pecsétet kibocsátó intézeteknek is folyamatosan követni kell a fejlődés irányát mind technikailag, mind jogilag. A követelményeiket is hozzá kell igazítani a fejlődéshez. Viszont úgy gondolom, hogy vannak ennél gyorsabban fejlődő PET-technológiák, amik talán sokkal inkább esélyesek a jövő PET-technológiája címre.

Irodalomjegyzék

Forrás:

[1] http://hu.wikipedia.org/wiki/Szem%C3%A9lyes_adat

[2]http://iplaw.hu/wp-content/uploads/2012/01/v%C3%A9djegyt%C3%B6rv%C3%A9ny.pdf

[3] http://en.wiktionary.org/wiki/privacy_seal

[4] http://en.wikipedia.org/wiki/TRUSTe

[5] http://www.truste.com/

[6] http://www.truste.com/why_TRUSTe_privacy_services/privacy_best_practices

[7] http://www.siliconvalleywatcher.com/mt/archives/2010/10/truste_responds.php

[8] https://www.european-privacy-seal.eu/

[9]https://www.european-privacy-seal.eu/criteria/EuroPriSe%20Criteria%20May%202011%20final.pdf

[10] http://en.wikipedia.org/wiki/Ixquick

[11] https://www.european-privacy-seal.eu/awarded-seals/de-080001p

[12] http://www.nugg.ad/de/unternehmen/datenschutz/europrise