

## Munkadokumentum a magánélet védelméről és a viselhető számítástechnikai eszközökről.

Végső változat, 57. ülés, Seoul, 2015. április 27-28.

### Az általános háttér és a hatály.

A viselhető számítástechnikai eszköz azt a számítógépi eszközt vagy berendezést jelent, amely meglehetősen kicsi, és a felhasználó testén vagy ruházatán helyezhető el.<sup>1</sup> Ezek az eszközök különféle képességekkel rendelkező érzékelőket tartalmaznak, és képesek, valós időben, információt gyűjteni a felhasználó testéről (életmód, szokások, fizikai tevékenységek, egészségi állapot, a helyváltoztatás sebessége, mobilitás), és a felhasználó környezetéről (képek, hangok, hőmérséklet, a levegő neveltség-tartalma, a felhasználó tartózkodás helye, a társadalmi környezet) is gyűjtenek számítógéppel generált adatokat, hogy azokból a felhasználót körülvevő világról gyűjtött tapasztalatokra következtessenek.

Sok viselhető eszközön egy kamerát is elhelyeznek. Ámbár a kamera a fentebb említett elemek közül csak néhányat rögzít, ezek is számos magánéletvédelmi aggodalomra adnak okot.<sup>2</sup> Ezek az eszközök képesek, esetleg állandóan és rejtett módon, adatokat rögzíteni a nem felhasználók magánéletére vonatkozóan, akik e rögzítés alanyai lehetnek.

Jelenleg a piacon a viselhető számítástechnika eszközök alábbi négy fajtája kapható:

- a) fitness, wellnes és életmód adatokat rögzítő eszközök (pl. intelligens ruházat és sport szemüvegek, tevékenységek adatait rögzítő monitorok, alvásérzékelők, stb.), amelyek vonzó kinézésűek, és az életmód sok módját követik nyomon;<sup>3</sup>
- b) informatikai és kommunikációs szolgáltatások felhasználóinak adatait gyűjtő eszközök (pl. intelligens órákkal, a kibővített valóság fülhallgatókkal, intelligens szemüvegekkel gyűjtött adatok);<sup>45</sup>

<sup>1</sup> A "viselhető számítástechnikai eszköz" különféle meghatározásait lásd pl. Steve Mann, (1996a): Smart Clothing: The Shift to Wearable Computing (Intelligens ruházat: átváltás az intelligens számítástechnikai eszközökre, lásd: Communications of the ACM, 39 (8) 23-24. oldalak továbbá: pp. 23-24. Mann, Steve (2014): Wearable Computing (Viselhető számítástechnikai eszközök). Soegaard, Mads and Dam, Rikke Friis (eds.), *The Encyclopedia of Human-Computer Interaction*, Az ember-gép kapcsolat enciklopédiája, 2. kiadás, Aarhus, Denmark: The Interaction Design Foundation. Hozzáférés: [https://www.interaction-design.org/encyclopedia/wearable\\_computing.html](https://www.interaction-design.org/encyclopedia/wearable_computing.html), hozzáférés: 2015. március 11. Lásd még: Webopedia, "wearable computing" ("a viselhető számítástechnikai eszközök", [http://www.webopedia.com/TERM/W/wearable\\_computing.html](http://www.webopedia.com/TERM/W/wearable_computing.html)) vagy a szótárban: "wearable computer", hozzáférés: <http://dictionary.reference.com/browse/wearable+computer>).

<sup>2</sup> Donald Melanson and Michael Gorman, "Our augmented selves: The promise of wearable computing." „Kibővítjük önmagunkat: a viselhető számítástechnikai eszközök üzenete), Engadget. 2012. december 12. Hozzáférés: 2013. július 8.

<sup>3</sup> Emily Waltz, "How I Quantified Myself: Can self-measurement gadgets help us live healthier and better lives" (Hogyan minősítem önmagam: segíthetnek-e nekünk az önminősítő eszközök abban, hogy egészségesebben és jobban éljünk? IEEE Spectrum, August 30, 2012. augusztus 30. Hivatkozva: Steve Mann. "Steve Mann: My "Augmediated" Life." (Az én „kibővített” életem. *IEEE Spectrum*. 2013. március 1. Hozzáférés: 2013. június 14.

<sup>4</sup> Examples of wearable devices in this category include Google Glass ([www.google.com/glass/start](http://www.google.com/glass/start)), Oculus Rift ([www.oculus.com](http://www.oculus.com), purchased by Facebook in ), Google Cardboard (<https://developers.google.com/cardboard/>), and Samsung's Gear VR ([http://www.samsung.com/global/microsite/gearvr/gearvr\\_specs.html](http://www.samsung.com/global/microsite/gearvr/gearvr_specs.html)).

- c) egészségügyi és orvosi adatokat gyűjtő eszközök (pl. folyamatos glukóz monitorok, viselhető bioérzékelő tapaszok; és
- d) az ipar, a rendőrség és a katonaság adatait gyűjtő eszközök (pl. kézben tartható terminálok, testre szerelhető kamerák, a kibővített valóság adatait gyűjtő eszközök);<sup>6</sup>

A c) és a d) pontban megjelölt kérdésekkel ebben a Munkadokumentumban nem foglalkozunk, és bár a c) pontban – egészségügyi és orvosi adatok –, el kell ismerni, hogy az a) pontban említett kérdések is – fitness, wellness és életmód követő adatok – egészségügyi adatoknak minősülhetnek.<sup>7</sup>

A viselhető számítástechnikai eszközök korszaka nem csak új kockázatokkal jár a magánélet védelme tekintetében, hanem fel is erősíti e kockázatok azáltal, hogy a mobil környezetből újabb, és valószínűleg érzékeny személyes információkat gyűjt, még hozzá feltűnés nélkül, titokban. Valakinek a divatos viseletére, fizikai vagy egészségügyi állapotára vonatkozó valós idejű információk valószínűleg személyes információnak minősülnek. Még egy egészséges személyre vonatkozó (pl. szívverésre) információk is érzékeny információnak tekinthetők. Egy intelligens telefon és a viselhető számítástechnikai eszközök közti különbségek is effélék, de vannak fontos, a magánélet védelméből adódó különbségek is.

A viselhető számítástechnikai eszközök megjelenésével, úgy látszik, a számítógépi teljesítmény eltűnik a ruházatról, a szemüvegekről, az órákról és esetleg a bőrről is, minek következtében egy egyéne tudomást szerezhetne arról, hogy efféle eszközök működnek rajta.

Ez az átláthatóság növekvő hiányával jár, és megnehezíti, hogy a felhasználók vagy más adatalányok tájékozott beleegyezésüket adják adataik kezeléséhez. Sok viselhető számítástechnikai eszközt kötelező a hardver, a mobil operációs rendszer vagy a számítástechnikai felhőhöz kapcsolódó eszközök gyártójának eszközeivel összekapcsolni. Ez azt eredményezheti, hogy az adatalány elveszti a gyűjtött személyes adatai felett gyakorolható ellenőrzés lehetőségét.

A magánélet védelmével kapcsolatos értelmes információk megválasztása kihívást jelent a mobil környezetben a kicsiny képernyőt váltakozó figyelemmel néző felhasználó számára. Az eszközök tervezésének ezek a jellemzői megnehezítik a felhasználók magánéletvédelmi jogaival kapcsolatos helyes tájékoztatását abban a formában, melyet megérthetnek, és megfelelő időben adják adataik kezeléséhez tájékozott beleegyezésüket. A viselhető számítástechnikai eszközök tovább növelek e kihívásokkal kapcsolatos veszélyeket.

## Ajánlások.

<sup>5</sup> Lásd: Vital Connect's [HealthPatch](#) (a vitális kapcsolat tapasza). Felkeresve: 2014. január 6.

<sup>6</sup> A Kopin's Golden-eszköz az életmód, az Internet hozzáférés, a helymeghatározás és a szabadkézi karbantartó munkások, a rendőrség, a paramedika és a tűzoltók adatait gyűjti. További információ:

[www.mygoldeni.com/home/](http://www.mygoldeni.com/home/).

<sup>7</sup> A 29. cikk szerinti Munkacsoport az életmódra és az egészségi állapotra vonatkozó személyes adatok három kategóriáját nevezte meg: (1) az egyértelműen egészségügyi adatokét, (2) személyes adatoknak esetleg minősülő vagy ilyenek nem is minősíthető adatokét, és (3) az egészségügyinek nem minősülő adatokét. Vö.: az 29. cikk szerinti Munkacsoportnak Az Európai Bizottsághoz intézett levele és annak melléklete, DG CNET, on mHealth of 05/02/2015;

[http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205\\_letter\\_art29wp\\_ec\\_health\\_data\\_after\\_plenary\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf)

[http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205\\_letter\\_art29wp\\_ec\\_health\\_data\\_after\\_plenary\\_annex\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf).

A Munkacsoport az alábbiakat ajánlja:

a személyes adatok feldolgozásának és a viselhető számítástechnikai eszközök alkalmazásának, amennyire csak lehet, átláthatónak kell lennie a felhasználók számára, és azok számára is, akinek az adatait feldolgozzák. Rejtett vagy miniaturizált eszközök esetében az átláthatóságok egyéb, nem vizuális módon kell biztosítani. Ez felöleli az olyan további eszközöket is, mint az intelligens telefonok;

a személyes adatokat, jobb híján, a viselhető számítástechnikai eszközt viselő hozzájárulásával szabad csak feldolgozni, s ezeket az eszközöket a hardver vagy a szoftver gyártójának eszközeivel, platformjaival vagy a számítástechnikai felhő szolgáltatásokat nyújtók eszközeivel össze kell kapcsolni;

a viselhető számítástechnikai eszközökkel rögzített adatok kiszolgáltatása vagy továbbítása az eszközöket viselő adatalany tájékozott és kifejezett hozzájárulását követeli meg;

az adatalany jogait, nevezetesen adatai kezeléséhez való hozzájárulásához, helyesbítéséhez és törléséhez fűződő jogait tiszteletben kell tartani. Az egyéneknek módot kell adnia arra, hogy a viselhető számítástechnikai eszközök által generált adataik helyességét kétségbe vonják, vagy azokat elemezzék;

bármely terméknek és/vagy szolgáltatásnak biztosítani kell a felhasználó ellenőrzéséhez fűződő elvek érvényesülését, ami, többek között az alábbiakat öleli fel:

az eszköz funkcionalitása módosításának a lehetősége (pl. a hallható beszélgetés átkapcsolása olvasható szöveggé (a felhasználó dinamikus ellenérzése));

a személyes adatok gyűjtésének időleges vagy esetről esetre való korlátozása (pl. bizonyos időtartamra és/vagy akkor, ha a személyes nem kívánja hogy viselkedését nyomon kövessék); és

a feldolgozott adatok részletezettségének megválasztása, vagy azoknak harmadik feleknek való továbbítása;

az egyéneknek képeseknek kell lenniük arra, hogy adataik kiszolgáltatásához való hozzájárulásukat bármikor visszavonhassák (pl. ha azokat intelligens telefonokkal vagy más, a felhasználó ellenőrzése alatt álló eszközökkel gyűjtötték), és hogy azokat háttértárra

mentsék;

biztosítani kell az adatok hordozhatóságának eszközeit;

a viselhető számítástechnikai eszközök használata a munkáltatók szektorban további kérdéseket vet fel az alkalmazottak szabad választása tekintetében. Azokat az alkalmazottakat, akik nem kívánnak részt venni semmiféle, a viselhető számítástechnikai eszközök alkalmazását célzó programban, ezért a döntésükért nem érheti hátrány;

ha a viselhető számítástechnikai eszközökkel feldolgozott adatok egészségügyi adatoknak minősülnek, úgy az adatok további feldolgozásához az adatalanyok kifejezett hozzájárulására van szükség;

a fenti ajánlásokon túlmenően a Munkacsoport ajánlja, hogy a dolgok Internete új keletű fejlesztéséről szóló, a 29. cikk szerinti Munkacsoport 8/2014. számú, valamint a 223. munkadokumentumban foglalt ajánlásokat is, ha egyáltalán szükséges, vegyék figyelembe.<sup>8</sup>

### **Az ajánlások háttere.**

A viselhető számítástechnikai eszközök jellemzői.

<sup>8</sup> Letölthető: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf); 21. és következő oldalak.

Sok, a piacon kapható viselhető számítástechnikai eszköz technológiáját jelenleg fejlesztik ki azért, hogy kinézésüket vonzóbbá tegyék, s így növekvő számú felhasználó viselje azokat. Azért például, hogy

- a) vizuális kinézésük legyen,
- b) varrás nélkül elhelyezhetőek legyenek a ruházaton vagy a testen;
- c) a felhasználó igényeihez igazodjanak, és visszacsatolást is biztosítsanak;
- d) viselőjének értelmezhető visszacsatolással szolgáljanak valós időben vagy nem, és közvetlenül vagy egy másik intelligens eszköz (tipikusan egy intelligens telefon) által;
- e) kiegészíthessék a felhasználó fizikai vagy értelmi képességeit;
- f) áruk, előnyeikhez képest, viszonylag alacsony legyen;
- g) személyes és munkahelyi környezetben is rugalmasan használhatók legyenek, és széles körben alkalmazhatók legyenek; és
- h) viszonylag egyszerűek legyenek, hogy a felhasználó könnyedén működtesse őket.

A felhasználó és a számítógép közötti folyamatos interakció során, a számítógép „megtanulja”, mit tapasztalt a felhasználó, amikor a viselhető eszközt használta, és ebből további információkra is következtethet, ami a viselhető számítástechnikai eszközök napjainkban folyó fejlesztésének a célja.

#### **A magánélet védelmére gyakorolt hatások.**

Egy, ipari területen folytatott közvélemény-kutatás szerint a viselhető számítástechnikai eszközökkel kapcsolatban feltett kérdésekre az Egyesült Királyságban és az Amerikai Egyesült Államokban a válaszadók 51%-a az ilyen eszközök viselésének akadályát azoknak a magánélet sérthetetlenségére gyakorolt hatásában látta, és 62%-a gondolta úgy, hogy a Google Glass és egyéb viselhető eszközök használatát valamilyen formában szabályozni kellene, míg a válaszadók 20%-a úgy vélte, hogy ezeknek az eszközöknek a használatát be kellene tiltani. A Forrester Reserch (közvélemény-kutató intézet) szerint a felhasználóknak az ilyen eszközzel gyűjtött adatainak a kezelését az ő ellenőrzésük alá kell helyezni, hogy eldönthessék, megosztják-e őket vagy sem.

#### **A jelenlegi hozzájárulás módjával kapcsolatos veszélyek.**

Az egymással összefüggésbe hozható adatokat gyűjtő érzékelők, függetlenül attól, hogy az egyének magukkal viszik, vagy csak ruhájukon viselik, óriási mennyiségű adatok rögzíthetnek, amelyek analizálhatók és megfelelő átláthatóság, felelősség vagy egyértelmű hozzájárulás hiányában is kezelhetők.

Ez a fejlődés, az egész világon, alapvető kihívást jelent a magánélet védelmének kereteit illetően. A cél korlátozásának elve például a személyes információk gyűjtésének mennyiségét kellett korlátoznia, mert azok csak akkor gyűjthetők, ha az érintett adatalany e specifikus célok alkalmazásához hozzájárult, ami felettébb nehézzé teszi ezeknek a mindenütt jelenlévő és mobil eszközök használatát.

Mi több az egyértelmű hozzájárulás a mobil eszköz gyűjtötte információ használatához, továbbra is kihívást jelent. Többet kell tenni ezért, hogy a felhasználót tájékoztassuk arról, éppen mi történik személyes információikkal.

#### **Újabb megfigyelési lehetőségek.**

Néhány viselhető számítástechnikai eszköz fényképek és videofelvételek, adatait, valamint helymeghatározó adatokat gyűjt az eszközt körülvevő környezetről, ide értve a közelben tartózkodó emberek adatait, valamint az egyéb eszközök által rögzített adatokat is. Az efféle eszközön elhelyezett kamera használata sok magánéletvédelmi aggodalomra ad okot, mert sokféle mindennapi esemény adatait rögzítheti, pl. a kosárlabda, az MP3 lemezjátszók és az inggombok adatait, mert a kamera ezeket folyamatosan és rejtetten képes rögzíteni.

A kamerán túlmenően azonban a fitness adatokat nyomon követő technológia újabb generációja az egészségbiztosító intézeteknek és munkáltatóknak lehetőséget nyújt arra, hogy megfigyeljék egészségi állapotunkat és magatartásunkat is. Számos észak-amerikai biztosító intézet és munkáltató pénzzel jutalmazza, ha a lehetőséget nyújtanak neki a fizikai állapot megfigyelésére. Az európai biztosító intézetek pedig hasonló szerződéseket kezdenek ajánlani.

Sokféle ilyen természetű fejlesztésnek nézhetünk elébe. A „physiolytics” a viselhető számítástechnikai eszközökkel gyűjtött adatokat össze fogja kapcsolni a „nagy adat” elemzésével, és a viselkedés megváltozásával kapcsolatos adatokat visszacsatolja az adatokat kezelő rendszerhez.

### **A viselhető számítástechnikai eszközökkel rögzített adatok aggregálása.**

A magánéletet veszélyeztető technikai eszközök új generációi kifejlesztésének vagyunk a tanúi, mely veszélyek a személyes információ látszólag ártalmatlan és nem érzékeny bitjeinek a kezelősből származnak, amelyek betekintést engednek a személyes viselkedés módjába. Azt is tudjuk, hogy a sok forrásból gyűjtött információ különálló bitjeinek a kombinálása az egyéneket azonosító, részletes profilképzésre ad lehetőséget. Már az is kihívást jelent az egyének számára, hogy tájékozott hozzájárulásukat adják személyes információik kiszolgáltatásához, hiszen nincsenek abban a helyzetben, hogy teljesen megértsék, információkat hogyan lehet kombinálni, és felhasználni a jövőben. A viselhető számítástechnikai eszközök folyamatosan gyűjtik, dolgozzák fel és továbbítják az általuk rögzített adatok, s a problémát valószínűleg éppen ez okozza.

### **A „szövegekörnyezet összeomlása”.**

Az egyének megkísérik, hogy életük különböző szféráit megkülönböztessék aszerint, hogy különböző társadalmi körökhöz tartoznak-e, vagy csupán életmódjuk vagy munkakörük különbözi-e egymástól. A közmédia és az on-line környezet általában aláássa arra irányuló szándékukat, hogy ezt a különbséget fenntartsuk. Erre a különbségre a társadalomtudósok mint a „szövegekörnyezet összeomlására” hivatkoznak, ami az érzékelők használatának a következményeképpen felgyorsulhat, és mert egymással állandó interakcióban vannak, azokat mindig ruházaton vagy a testen kell viselni. Ez a felbomlás, amit a társadalomtudósok a „szövegekörnyezet összeomlásának” neveznek, felgyorsulhat azoknak az érzékelőknek a hatására, amelyeket az emberek a ruházatukon viselnek, és állandó interakcióban vannak a felhasználó testén, vagy a környezetében elhelyezett eszközökkel.

### **Új feljogosítási módszerek, újfajta személyes információk.**

A viselhető számítástechnikai eszközök úgy konfigurálhatók, hogy a személyes információkat oly módon kezeljék, hogy a magánélet védelme biztosítva legyen. Ha például egy kutatás során az egyéneknek az érzékelők által generált adatait a zsebükbe dugott intelligens telefonok által gyűjtött, mindennapi tevékenységükkel kapcsolatos adatokkal kombinálják, például azért, hogy őket azonosítsák és feljogosítsák az adataikhoz való hozzáférésre.

Ez azt jelenti, hogy ha a zsebünkben az intelligens telefonnal sétálunk, kocogunk, hegyet mászunk, akkor esetleg a biometrikus aláírásunkat hozzuk létre. Minthogy ez valószínűleg fokozza a felhasználó feljogosításának biztonságát, ugyancsak a magánélet veszélyeztetésével jár.

### **Az eszközök tervezésével kapcsolatos megfontolások.**

#### Dinamikus felhasználói ellenőrzés.

A magánélet védelmének koncepciójáról jelenleg azt gondoljuk, hogy az egy dinamikus feltétel, mert az egyéneket körülvevő társadalmi és kulturális környezet folyamatosan változik. További lehetőségeket kell teremteni arra, hogy a hozzájárulás megfelelő legyen, alkalmazkodják a változó körülményekhez és preferenciákhoz, valamint hogy minimalizálja a döntéseket, elkerülve így a viselhető számítástechnikai eszközök környezetének túlterhelését. Többek között törekednünk kell arra, hogy

- a) olyan dinamikus kalibrált magánéletvédelmi szabályokat alakítsunk ki, amelyek kielégítik az adatalanyok magánéletét védő szükségleteket és elvárásokat;
- b) a viselhető számítástechnikai eszközöket olyan egyszerűnek tervezzük, hogy azok megfeleljenek az egyének magánéletét védő preferenciáinak;
- c) felszólítsuk a szervezeteket arra javítsanak magánélet védelmi politikáikon abból a célból, hogy a dinamikus és interaktív adattérképek és infografikák megmutassák a viselhető számítástechnikai eszközöket körülvevő ekorendszerrel való viszonyaikat.

A viselhető számítástechnikai eszközök egymással folytatott interakciói hatással vannak a felhasználó magánéletére. Ha egy ilyen eszköz például, amely hangüzeneteken alapszik, hasonló magánéletvédelmi veszéllyel jár, mintha telefonon, kiabálva beszélgetnénk egymással a piacon. Az egyén képessége viselkedésének megváltoztatására irányuló képessége a beszélgetést esetleg írásbelivé alakítja át, ami a magánélet védelmét szolgáló tervezés érdekes módja lehet.

#### Újabb átláthatósági modellek.

A viselhető számítástechnikai eszközök alkalmazásának vannak újabb lehetőségei is, amelyek azonban veszélyeztetik az átláthatóságot. Ha például ezek a viselhető eszközök látványt, hangot vagy valami mást érzékelnek, úgy az ezekkel az eszközökkel gyűjtött adatokat szoros kapcsolatba lehet hozni a felhasználó adataival, s így némileg könnyebbé válik a felhasználó azonnali figyelmeztetése az adatait fenyegető veszélyekre. A viselhető számítástechnikai eszközök tervezése során, ily módon, a hozzájárulást és az intelligens telefonok által okozott veszélyekre vonatkozó figyelmeztetést „zsigerivé” teszik. Egyes viselhető számítástechnikai eszközöket úgy terveznek, hogy egyáltalán ne legyen szükségük képernyőre, s így az új modellek képesek legyenek arra, hogy a felhasználó magánéletét veszélyeztető kérdéseket vele megvitassák.

A felhasználó magánélete és a felhasználót körülvevők magánélete is ilyen kérdés, és ráadásul sokkal bosszantóbb. Nagyon nehéz tudomást szerezni arról, hogy valaki egy intelligens telefonnal vagy más eszközzel rögzíti hangunkat vagy arcvonásainkat. Hogy a viselhető, a számítógépekhez sokkal szorosabban kapcsolódó, észrevehetetlen eszközökkel, például a közönséges szemüvegkeretekkel gyűjtött adatokról is tudomást lehessen szerezni, ezeket az eszközöket úgy kell megtervezni, hogy a felhasználó ismerhesse és ellenőrizhesse a rá vonatkozó információk gyűjtését.

### **Az adatokhoz való hozzáférés és a helyességükkel kapcsolatos kihívások az automatizált döntéshozás során.**

Az átláthatósággal közvetlen kapcsolatban van a személyes információkhoz való hozzáférés. Nem nyilvánvaló, hogy az egyének meghatározhatják egy viselhető eszközzel gyűjtött adatok fajtáját, hogy kik gyűjtik, mire fogják használni, és kiknek fogják kiszolgáltatni azokat. A felhasználóknak lehetőséget kell adni arra, hogy személyes információik gyűjtését és a szervezetek által való felhasználásának módját megkérdőjelezzék, hiszen ez képezi döntéseik alapját, jóllehet azok helyességére nincs garancia.

Egy újabb keletű tanulmány szerzői megkérdőjelezzik a kis intenzitású, fitness jellemzői adatait gyűjtő, viselhető számítástechnikai eszközök megbízhatóságát, mert kis intenzitású tevékenységek, például az állás vagy tisztálkodás, adatait gyűjtik, ráadásul alacsony energiaráfordítással. Az ilyen eszközökkel gyűjtött adatok valóban pontatlanok lehetnek, és hatást gyakorolhatnak az egyének viselkedésére. Ezeknek az adatoknak a hibás felhasználása például csökkenti az Alzheimer kór korai diagnosztizálásának lehetőségét, ide értve a beteg mozgásának egy accelerométerrel gyűjtött adatainak hibás értékelését is, ráadásul mindez befolyásolhatja a kór diagnózisát és a beteg ápolásának módját. A hibásan leolvasott mérési adatok a munkahelyen is problémákat okozhatnak, ha a munkáltatónak az alkalmazottak termelékenységére értékelését illetően az ilyen eszközökkel gyűjtött adatokra kellene támaszkodnia. Az egyéneknek lehetőséget kell adni arra, hogy az így generált, a viselhető számítástechnikai eszközökkel gyűjtött adatok helyességét vagy elemzésének eredményét kétségbe vonják. Mindezt az eszköz tervezésekor fontos figyelembe venni.

### **A biztonság veszélyeztetésének esetei.**

Megfelelő biztonsági és feljogosítási rendszerek hiányában a viselhető számítástechnikai eszközök támadásnak vannak kitéve. A kompromisszumos viselhető számítástechnikai eszközök nem csak az egyének személyes információit és hírnevét kockáztatják, hanem egészségi állapotukat is. Ha például egy, az inzulinadagolást szabályozó, viselhető eszköz lehallgatása vagy személytelenítése iszonyú következményekkel járhat az egyének egészségi állapotára nézve. Egy kommentátor ezt így fejezte ki: „az Ön személyes adataink biztonsága olyan gyenge, mint az Ön kvantifikált ekorendszerének leggyengébb láncszeme”.

\*\*\*\*\*