

|  |  |
|--|--|
| Working Group on Data Protection in Telecommunications | Munkacsoport a Távközlési Adatok Védelmére |
|--|--|

## **A Távközlési Adatvédelmi Munkacsoport 27. ülése**

Seoul, 2015. április 27-28.

### **Az adat- és a magánéletvédelem átláthatósági jelentése.**

“Doverlyai, no proveryai.” Orosz közmondás, Ronald Reagan így értelmezi: “igaz, de bizonyítsd”.

“Ha minden részlet ismert, az ész is elégedett, és a képzelet szárnyaszegetten száll óhaja után.” Thomas Bailey Aldrich, amerikai költő és író.

“A biztonsági felügyelet titkos természete sokszor lehetetlenné teszi az igazságszolgáltatást, a joghatóságok és a közemberek pedig bírálják az államhatalmat. A felügyeletnek ez a hiánya önkényes és diszkriminációmentes.” Navi Pillay, Egyesült Nemzetek, az emberi jogok főmegbízottja.

#### **Hatály.**

Ebben a dokumentumban meghatározzuk az adat- és a magánélet-védelem átláthatósági jelentésének a céljait, amelyről egy jelentést a telekommunikációs vállalkozások és egyéb online szolgáltatók szövetsége tett közzé. Az átláthatósági jelentések hasznosak, mert támogatják azon szervezetek iránti bizalmat, amelyek személyes adatokat kezelnek, és azt is megkövetelik, hogy a közhatalmi hatóságok a gyakorlataikért és az általuk kezelt adatok jogszerűségéért felelősséget viseljenek, és az adatokhoz az adatvédelmi hatóságok felhatalmazása alapján.

Az adatkezelők- és feldolgozók átláthatósági jelentései statisztikákat, és a nem üzleti célt szolgáló, harmadik felek által kibocsátott személyes adatokkal kapcsolatos információkat is tartalmaznak. Ebben a dokumentumban elsősorban a jogérvényesítő szervek<sup>1</sup> és a

---

<sup>1</sup> A jogérvényesítő szervek: szabályozó testületek, valamint büntetőjogi szervek. Sok jogtóság szabályozó testületei, kormányzati osztályai és helyi kormányzati testületei is gyakran hozzáférnek a vállalkozások információihoz.

nemzetbiztonsági szolgálatok gyakorlatával foglalkozunk, egyéb, nem üzleti célt<sup>2</sup> szolgáló adattípusok kezelésének módjával viszont nem.

Ámbár elsősorban a jogérvényesítő vagy nemzetbiztonsági szervekhez a magánjogi szektorbeli, telekommunikációs szervezetek által intézett jelentéseivel foglalkozunk, az ajánlások és megfigyelések is hasznosak lehetnek a közhatalmi testületek és a távközlési szektorhoz nem tartozó vállalkozások számára is.<sup>3</sup> Ebben a dokumentumban nem foglalkozunk a jogérvényesítésre való felhatalmazással vagy a nemzetbiztonságnak a szervezetek által kezelt adatkezelési gyakorlatával sem, mert az azokhoz való hozzáférést a jogszabályok korlátozzák, és nem foglalkozunk a nyomozó testületek beavatkozó megfigyelési gyakorlataival sem.<sup>4</sup>

A Munkacsoport más dokumentumai is érintik ezeket a kérdéseket, és hasznosak lehetnek az e dokumentumban tárgyaltak tekintetében is. A Munkacsoport sok más dokumentumában is foglalkozik e kérdésekkel, és hasznos lehet ezeket is olvasni.<sup>5</sup>

A Munkacsoport támogatja az átláthatósági jelentések gyakorlatát, mert azok elősegítik a személyes adatok feldolgozását végzők felelősségre vonhatóságát. Az átláthatósági jelentéseket készítőknél gondoskodniuk kell arról, hogy a statisztikák megbízhatóak, informatívak és nemzetközileg összehasonlíthatók legyenek.

## Háttér.

A kormányzati szerveknek hozzá kell tudniuk férni a magánjogi szervezetek által kezelt adatokhoz abból a célból, hogy azok a közhatalmi funkciójukat támogassák.<sup>6</sup> Egy hagyományos példa erre, amikor egy vállalkozás rögzíti az adatokat, s így bizonyíthatja, hogy az adót pontosan befizette az adóhatóságnak. A kormányzati szervek évtizedek óta érzékelik, hogy a magánjogi szervezetek által kezelt adatok növekszik a polgárok és az üzleti vállalkozások aggodalmát a növekvő költséget miatt.

---

<sup>2</sup> Lásd pl.: beavatkozás a biztonságba vagy a sürgősségi helyzetben hozott intézkedésekbe.

<sup>3</sup> Pl. a pénzügyi szektor vagy a hiteleket jelentő ipar.

<sup>4</sup> Sok egyéb magánéletvédelmi politika tárgyalja ezt a jelenséget, pl. a Centre for Democracy and Technology, *Systematic Access to Government Data: A Comparative Analysis*, 2013. Earlier case studies on Systematic Government Access to Private-Sector Data available at <http://idpl.oxfordjournals.org/content/2/4.toc>.

<sup>5</sup> A Munkacsoport dokumentumait lásd: <http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdp/working-papers-and-common-positions-adopted-by-the-working-group>. Lásd továbbá a Munkacsoport munkadokumentumát is: [Human Right to Telecommunications Secrecy](#) (Berlin, 2013. szeptember), és [Granada Charter of Privacy in a Digital World](#) (Granada, 2010. április).

<sup>6</sup> A könnyebb érthetőség kedvéért ebben a dokumentumban a vállalkozás információira vagy rekordjaira utalunk, mégpedig azért, hogy az adatkezelő vagy –feldolgozó a kormányzati szervek igényeit kielégíthesse.

A kormányzati szervezeteknek hozzá kell tudni férniük a vállalkozások információihoz, különösen azokhoz, amelyek egyénekkal kapcsolatosak, ezek a hatálya és volumene ugyanis 2001. óta lényegesen megnövekedett. Ez a növekedés azt tükrözi, hogy a kormányzati szervezetek számára a magánjogi szektor adatai egyre vonzóbbakká váltak, ide értve az alábbiakat is:

- *az adatok rendelkezésre állása:* az adatok tárolásának a költsége jelentősen csökkent, és továbbra is csökkenti fog, minek következtében nagy mennyiségű tranzakciós adatot lehet hosszú időn át tárolni;
- *a feldolgozási teljesítmény:* a nagy mennyiségű adat elemzése számos előnyt jelentett, mert a korrelációs folyamat elemzését és a nagy mennyiségű adat tárolását tette lehetővé, minek következtében a “nagy adatok” nagy üzletté váltak<sup>78</sup>.
- *a speciális technikák manapság a legfontosabbak:* ha néhány specializált, adatbázison nyugvó, olyan elemzési technikát alkalmazunk, amelyek az üzleti és a kormányzati körökben szabvánnyá váltak, úgy az előrejelző elemzés, a kapcsolatok láncolása, az adatok és a hálózatok vizualizálása számos előnyét élvezhetjük;
- *váltás az orálisról az írott formára:* az áttérés az analógról a digitális telefóniára kényelmes adatszolgáltatási szolgáltatásokra adott alkalmat, pl. az SMS-re, ami a fogyasztókat arra bátorította, hogy a nem folyamatos orális kommunikációról az írottra térjenek át, s így az adatokat hosszabb ideig megőrizhessék. A mobil telefónia és az intelligens telefonok széleskörű elterjedése csak siettették ezt a trendet;
- *a személyes adatok tömeges nyomai észrevehetetlenné váltak az érintettek számára:* az analóg telefóniáról való áttérés a digitálisra több forgalmi adatot generál, mint amennyit tárolni és elemezni lehet. Az intelligens mobil telefónia és a GPS geolokációs szolgáltatásokat tett lehetővé, s ez érzékeny, korábban nem létező információnyomokat generál, ráadásul a mindenütt jelenlévő érzékelők és a “dolgok Internete” az egyénekkal kapcsolatos adatokat generál, s ezek hozzáadódnak az érzékelők egyre növekvő univerzumához és a “dolgok Internete” konstrukciójához, ami az egyénekkal kapcsolatos adatokat generál, gyakran minden emberi beavatkozás nélkül.

---

<sup>7</sup> See IWGDPT Working Papers on [Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics](#) (Skopje, May 2014) and on [Cloud Computing – Privacy and data protection issues](#) (Sopot, April 2012).

<sup>8</sup> Lásd: az adat- és a magánéletvédelmi biztosok nemzetközi konferenciája határozatát a “nagy adat”-okról. Mauritius, 2014. és a konferencia 36-ik határozatát a “nagy adat”-okról, Mauritius, 2014. továbbá a konferencia 34. határozatát a számítástechnikai felhőről, Uruguay, 2012. “nagy adat”-okról: [www.icdppc.org](http://www.icdppc.org).

- *felhasználó-generált tartalom*: az Internet-szolgáltatások és újabban a közösségi média, megváltoztatta a fogyasztók viselkedését, s így sokan saját személyes adataikat és tranzakciós adataikat is közzéteszik, s így a kormányzati szervek könnyedén hozzájuk férhetnek a vállalkozások által rögzített adatokhoz még ellenőrzésük megkerülésével is.<sup>9</sup>

Ezek a technológiák és üzleti tényezők azonban önmagukban nem adhatnak magyarázatot a kormányzati szerveknek az adatokhoz való sűrűsödő hozzáférésnek. Az egyenlet kormányzati oldalán további tényezők jelennek meg:

- *közhatalmi-magánhatalmi kapcsolatok*: a magánjogi szektor határai elmosódtak, a magánszektor és a közhatalmi szektor gyakorlata egyforma. A korábbi, már privatizált közszolgáltatók hozzáférhetnek a közösség kulcsfontosságú adataihoz is. A kormányzati szervek szereplőivé váltak a magánjogi szektor adat-ecorendszerének, mint adatforrások és mint fogyasztói adatszolgáltatók. A magánjogi vállalkozások is főszereplőivé váltak a nyomozati és biztonsági munkának;
- *jogalkalmazás és nemzetbiztonság*: 2001. óta a közemberek, a jogalkotók és a bíróságok hajlanak arra, hogy a nemzetbiztonság aggodalmait a légiforgalmi<sup>10</sup> és egyéb vállalkozások adatai biztonsága tekintetében eloszlássák. A jogalkalmazás aggodalmait számos területen manifesztálódtak, s ezek közül kettő nagyon is ismert, az egyik a légiforgalmi, a másik a pénzügyi szolgáltatások területe.<sup>11</sup> A kormányzati szervek hagyományosan azon bűncselekmények elkövetésével gyanúsított egyének adatainak célzott kivizsgálására irányul, akiket ezért megfigyeltek, és adataikat elemezték abból a célból, hogy felfedjék tevékenységüket és más személyekkel ápolts kapcsolataikat is. A megfigyelésre adott felhatalmazás küszöbértékét több joghatóság területén csökkentették az információgyűjtés határainak bővítésével együtt, mert azok csak egyetlen nyomozás célját szolgálhatják. A hagyományos adatokat most már rutinszerűen gyűjtik több országban, feltéve, hogy egyáltalán léteznek, és ha a vállalkozások rendszerei képesek az adatokhoz hozzáférni;
- *a telekommunikációs rendszerek átalakítása abból a célból, hogy a kormányzati szervek igényeit kielégítsék*: a hagyományos kormányzati szervek a vállalkozásoknak csak azokhoz az adatrekordjaihoz igyekeztek hozzáférni, amelyekhez a vállalkozások rendszerei egyáltalán hozzáférést nyújtottak. A kormányzati szervek azonban az elmúlt években átszervezték kapcsolatukat a magánjogi szektor szereplőivel, és megegyeztek a hálózati szolgáltatókkal is, hogy, bár hatalmas költségráfordítással,

---

<sup>9</sup> Ebben a dokumentumban csak azokkal az aggodalomra okot adó kérdésekkel foglalkozunk, amelyek a vállalkozások adatkezelési problémáiból adódtak. Egyéb magánéletvédelmi és felelősségre vonhatósági kérdésekkel, köztük azokkal, amelyek a kormányzati szervek információhoz való hozzáféréssel vagy a vállalkozások jogszerűtlen adatkezelésével foglalkoznak nem foglalkozunk.

<sup>10</sup> Az utasok tranzakciós információi (melyekre gyakran, mint az utaslistákra hivatkoznak) védelmére hagyományosan hangsúlyt fektetnek. Lásd: a CDPPC 2007-ik évi, a [safeguarding of passenger data](#)-ra vonatkozó határozatát.

<sup>11</sup> A hangsúly különösen a pénzmosásra és a terrorizmus finanszírozására helyeződik.

egy „hátsó ajtót” nyitnak, hogy e szervek hozzáférjenek azokhoz a rendszerekhez, amelyekhez egyébként nem lenne szükséges, legalábbis üzleti célokból, hozzáférni<sup>1213</sup>;

- *kormányzati terhek áthárítása a vállalkozásokra:* a hagyományos keresési szolgáltatások, míg a nyomozás lényeges részét képezik, nagy adminisztratív terhet rónak az államokra, és új jogeszközöket igényelnek, amelyek a helymeghatározás, az adatgyűjtés és a dokumentáció céljait szolgálják, és a kormányzat terheit áthárítják a vállalkozásokra<sup>14</sup>;
- *a kormányzati szervek érdekeit szolgáló adattárolási követelmények ismételt elrendelése:* a kormányzati szervek nem csupán azért követelték meg a vállalkozásoktól, hogy gyűjtsék és dokumentálják az adatokat abból a célból, hogy a kormányzati szervek azok jogszerű gyűjtését felülvizsgálják, de azért is, hogy a vállalkozások a dokumentációt hosszabb időperiódus során megőrizzék, még ha üzleti célokra is szükséges, mely esetben a szerveknek szükségük lehet arra, hogy egy nyomozás érdekében az információhoz hozzáférjenek.<sup>15</sup>

Ezek a tényezők a magánszektor efféle információforrásait még vonzóbbá tették a kormányzati szervek számára, mint korábban. Óriási, a korábbinál lényegesen nagyobb mennyiségű információ állt a kormányzati szervek rendelkezésére, pedig korábban ilyesmi nem létezett vagy az információ nem volt hozzáférhető.

A kormányzati szervek szempontjából az információk tárolása az informatikai és hálózati szolgáltatók véleménye szerint is gyakran kényelmesebb volt, bár az elszigetelt egyedi vállalkozások szerint nem. Az értékes információk összekapcsolása további információkkal

---

<sup>12</sup> Több országban megkövetelik, hogy a digitális telefóniai rendszerek által nyújtott közszolgáltatásokat tegyék képessé a beavatkozásra, ami világos példája a kormányzati szervek érekeire, hiszen prioritásuk van a kommunikációs adatokhoz való hozzáférés bizalmas volta esetében. Számos országban ugyancsak ellenőrzik a telefonszámlák adatait.

<sup>13</sup> Vitatható, hogy az állam „hátsó ajtó” iránti igénye új jelenség, és nem létezett már korábban is postai, a távirati és az analóg rendszerekben. Efféle hozzáférés különösen megkönnyítette a kormányzati szervek dolgát azokban az államokban, ahol a távközlési rendszerek állami vagy egyetlen monopólium tulajdonában voltak. Ez a trend azonban nagyon költséges változások végrehajtásával járt, ami befolyásolhatta a vállalkozások viselkedését, és olykor a vállalkozás jogos, biztonságos hálózatok létrehozására irányuló érdekeivel is szemben álltak.

<sup>14</sup> Erre a hatalomra olykor, mint „termelésre vagy segítségnyújtásra vonatkozó kötelezettségre hivatkoznak”.

<sup>15</sup> For example, in the telecommunications sector, many countries impose retention requirements for storage of call traffic records beyond their need for business purposes. In the banking sector, most countries require long term storage of copies of customer account identification documents as part of anti-money laundering ‘know your customer’ requirements while in the telecommunications sector some countries outlaw anonymous cell telephone accounts and require retention of customer account identification documents.

megnövelte azok értékét. A hatalmas adatmennyiség leküzdhetetlen akadályát képezi az adatok hasznosításának és időben történő elemzésének. A számítógépi teljesítmény növekedése és a feldolgozási technikák fejlődése azonban lehetővé teszi a kormányzati szervek számára nagymennyiségű adatok gyűjtését is.

Az a környezet, amelyben ilyen projekteket lehetett kezdeményezni, mind jobban elősegítette a kormányzati érdekek érvényesítését. A terrorista támadások miatt növekedett az emberek félelme és igazolta, hogy a nemzetbiztonsági és jogérvényesítő szervek projektjeinek a kiszélesítését, hogy a kormány a vállalkozások által gyűjtött adatokat még fokozottabban ellenőrizhesse. 2001. óta sok olyan rendelkezést iktattak törvénybe, amelyek a jogérvényesítő hatóságoknak bővebb hozzáférést biztosítottak a vállalkozások által kezelt információkhoz. Ezek a rendelkezések hagyományosan pontosan korlátozzák az adatokhoz való hozzáférést, és a törvényes folyamatokat is. A múltban jogi igazolás kellett ahhoz, hogy a vállalkozások által kezelt adatokhoz hozzáférjenek, míg az elektronikus környezetben új paradigma merülhet fel az állami hatalmat illetően. Míg a jogalkotók gyakran a tradicionális normákra hagyatkoztak, a jogszabályok számának folyamatos növekedése és a "future proofing" rugalmasabb koncepciókat hozott létre, és ezáltal változatlanul kibővítette az adatokhoz való hozzáférés lehetőségeit.<sup>16</sup>

A jogalkalmazó és a nemzetbiztonsági szervek az adatokat gyakran titkosan gyűjtik. Ha azonban a nyomozás véget ér, az átláthatóság, amit a jogalkalmazó szervek vezettek be, egy szabad társadalomban is alkalmazható. A jogalkalmazó hatóságok általában vádat emelnek a gyanúsított személlyel szemben, és bemutatják a dokumentumokat a bíróságnak. A nemzetbiztonsági szervek mindig is titkosan gyűjtötték az adatokat, mert az eljárás nem szükségképpen járt eredménnyel, és a titkosságot nem lehetett feloldani.

Egy demokratikus társadalomban az állami hatóságok aktivitása titkos, és rendszerint gyanakvással és bizalmatlansággal nézik.<sup>17</sup> Azok a kísérletek, amelyek a közvéleménynek a

---

<sup>16</sup> A példák kevésbé szigorú követelményeket szabnak meg a meta-adatokhoz való hozzáférés esetében, és új dinamikus adatkörnyezetet a való időben. Felettébb valószínű, hogy míg a hatóságok rugalmasabb nyelven fejezik a korlátozás elvét, a legtöbb jogalkotó szerv alig érti, mit is engedett meg.

<sup>17</sup> Lásd: az Európai Parlament jelentése az amerikai megfigyelési programjáról, a tagállamok megfigyelő testületeiről és azoknak az európai polgárok alapvető jogaira gyakorolt hatásairól, valamint a tengeren túli igazságügyi és a belügyi szervek együttműködéséről. 2014. február.

nemzetbiztonsági szervekbe vetett bizalmának növelését szolgálták, sikertelennek bizonyult, még a felügyelő testületek tekintetében is.<sup>18</sup>

Ennek megfelelően, míg a kormányzati szervek, amelyek a vállalkozások által kezelt személyes adatokhoz egyre növekvő tömegéhez férhetnek hozzá, korábban nem ez volt a helyzet, mindazonáltal a hozzáférés lehetősége kissé bizonytalan maradt. Ebben az összefüggésben az átláthatósági jelentés hasznos lehet.

### **Az átláthatósági jelentés.**

Ha a kormányzati szervek minden esetben hozzáférhetnek a vállalkozások által kezelt azokhoz az adatokhoz vagy információkhoz, amelyek nem üzleti célokat szolgálnak, úgy egy kormányzati ügynökség férhet hozzá azokhoz és egy társaság fogadja a hozzáférési kérelmeket és tesz eleget nekik. Ebben a dokumentumban elsősorban azoknak a vállalkozásoknak az átláthatósági jelentéseivel foglalkozunk, mely vállalkozások efféle kérelmeket kapnak. Ámbár e dokumentumban nem erre összpontosítunk, hangsúlyoznunk kell, hogy a közhatalmi testületek átláthatósága és felelősségre vonhatósága a vállalkozásoktól azt is megköveteli, hogy az általuk kezelt adatokat e testületek számára kiadják. A Munkacsoport korábban már hangsúlyozta az átláthatóságnak, mint a felelősségre vonhatóság egyik elemének a fontosságát.<sup>19</sup>

A kormányzati szervek növekvő igénye a vállalkozások által kezelt személyes adatokhoz való hozzáférésre nem csak az egyéneket és a magánéletet védő egyesületeket aggasztja, hanem a vállalkozásokat magukat is. A vállalkozások aggodalmainak egy része a megfelelő adatkezeléssel kapcsolatos költségekkel kapcsolatos, mely költségek meglehetősen nagyok lehetnek.

A vállalkozások aggodalmi prózaiak, legalábbis a megfelelésséggel kapcsolatos, esetleg magas, költségeket illetően. Más jellegű aggodalmak azokkal az etikai nehézségekkel kapcsolatosak, amely szerint a bizalmas személyes adatoknak nem üzleti célokra való kiszolgáltatása csökkenti az ügyfelek és egyéb üzleti partnerek bizalmát.

Mások aggodalma a vállalkozások jogi felelősségével kapcsolatos, ha a vállalkozások jogi felelőssége versenyez a biztonsággal és a bizalmassággal, valamint egy közhatalmi hatóság

---

<sup>18</sup> Lásd pl.: az amerikai szenátus bizottságának jelentése a titkosszolgálatok tevékenységéről, 2014. december.

<sup>19</sup> Lásd: IWGDPT munkadokumentum, [Telecommunications Surveillance](#) (Auckland, 2002) és IWGDPT közös álláspont: [Public Accountability in relation to Interception of Private Communications](#) (Hong Kong, 1998).

hozzáférési igényével. A jogi komplexitás megsokszorozódik, ha egy multinacionális vállalkozás több országban is működik, és összeütközésbe kerül a jogszabályokkal vagy egy adatfeldolgozó arra irányuló kérelmével, hogy titkosan adja ki neki egy másik adatfeldolgozó adatait. Vannak azonban egyéb, a határátlépő adatáramlással kapcsolatosan, vagy a kölcsönös segítségnyújtásra vonatkozó egyezményekkel összefüggésben is.<sup>20</sup>

E probléma megoldása lehet, ha a vállalkozások egy világos és szigorú politika szerint teljesítik a kormányzati szerveknek az arra irányuló kérelmét, hogy az adatkezelést kompetens módon és a jogszabályok szerint végezzék, és a hibákat elkerüljék.

A politikák általában a kérelmek, a szabványos adatkezelési kritériumok szerinti végzését írja elő, továbbá a belső auditot, a nyomkövetést és a menedzsment tájékoztatását pedig a szenior és tapasztalt alkalmazottaknak kell végezniük. A belső audit, a nyomkövetés és a jelentéstétel a szenior menedzsmentnek szokásos követelmények. A vállalkozások, mielőtt egy adatrekordot kiszolgáltathatnának a nyomozóknak erre felhatalmazással vagy más hasonló jogi eszközzel kell rendelkezniük. A helyes gyakorlat, az ügy etikai vonatkozás és a vállalkozás hírneve sok vállalkozást arra indított, hogy mindezekről tájékoztassa a közvéleményt.

A Google az első átláthatósági jelentését 2009-ben publikálta, amit számos távközlési és internetszolgáltató követett a következő három év folyamán.<sup>21</sup> Ez a gyakorlatot azonban csak kb. tucatnyi vállalkozás követte, pl. Észak-Amerikában, Európában, Ázsiában és Ausztráliában.<sup>22</sup>

A vállalkozások általában nem adnak részletes magyarázatot arra, hogy miért tesznek közzé átláthatósági jelentéseket, ámbár sokuk szerint a magánélet védelmi fontos számukra. Minthogy efféle jelentések közzétételéről jogszabály nem rendelkezik, a motiváció valószínűleg a hírnév iránti aggodalomból adódik, továbbá abból, hogy a vállalkozás felelősnek tartja magát alkalmazottaiért, és ennek olykor a hírnév az oka. Egy jelentés közzététele kísérlet lehet arra, hogy a vállalkozás megőrizze a belé vetett bizalmat, és hogy megmutassa, hogy mindent meg tesz azért, hogy a jogszabályi követelmények

---

<sup>20</sup> Lásd pl: Global Network Initiative, [Data Beyond Borders: Mutual Legal Assistance in the Internet Age](#), 2015. január.

<sup>21</sup> Legalább 12 vállalkozás tett közzé on-line átláthatósági jelentést 2012-ben. Forrás: Újzéland magánéletvédelmi biztosának irodája.

<sup>22</sup> Mintegy 27 vállalkozás tett közzé átláthatósági jelentést on-line 2013-ban. Forrás: Újzéland magánéletvédelmi biztosának irodája.



megtartásáért, valamint az adatok biztonságáért és bizalmas voltáért viselt kettős felelősségének eleget tegyen. A kezelt adatokhoz való hozzáférésre vonatkozó kérelmek megfelelő kezelése, és, ezzel összefüggésben, tevékenysége jellemzőinek közzététele nem más, mint az ügyfelekkel, üzleti partnerekkel és a szélesebb közvéleménnyel kapcsolatos nagyrabecsülésének kifejeződése.

Ebben az értelemben a vállalkozások átláthatósági jelentése a magánjogi szektort képviselő testületek kísérlete arra, hogy a közhatalmi testületeket tartsák felelősségre vonhatónak, hiszen éppen ők a felelősek azokért a hozzáférési kérelmekért, amelyek kényelmetlenek vagy ellentétesek az ügyfelei elvárásaival, és mégis a vállalkozásoknak kell kiszolgáltatni az információkat. A vállalkozások viselkedésével kapcsolatos jelentések kísérletek arra, hogy a közhatalmi testületeket tegyék felelőssé saját viselkedésükért. A vállalkozásoknak az arra irányuló kísérlete, hogy a közhatalmi testületek is felelősséget viseljenek viselkedésükért némi előnnyel is jár, ugyanis, ha többen kérnek hozzáférést az adatokhoz, úgy ennek költségeit a vállalkozások viselik. Ha egy vállalkozás csak gyengén tesz eleget kötelezettségeinek, úgy azt mint „gyengét”-t jelölik meg a hatóságok, minek következtében a vállalkozás a könnyedén hozzáférhető információk kedvelt forrásává válik. Az átláthatósági jelentés közzététele segítheti a hatóságokat, hogy több gondot fordítsanak hatáskörük arányos és jogos gyakorlására. A vállalkozások esetleg megkísérik a „nyílt kormány” etikájának a helyreállítását, az ugyanis a kormányzati szerveke megfigyelési gyakorlata következtében e területen lényegesen csökkent.

Ha a vállalkozások az információikat nem üzleti célra egy harmadik fél rendelkezésére bocsátják az érintettek hozzájárulása nélkül, sőt valószínűleg az ő szándékukkal és érdekeikkel ellentétesen, úgy az nyilvánvalóan veszélyezteti az adatok védelmét. Ez azonban nem mindig van így, a jogérvényesítő szervek ugyanis általában felismerik a nyomozás érdekeit, és az adatok kibocsátásával kapcsolatos jogos kivételeket. A jelenlegi helyzet a vállalkozások által kezelt információkhoz való, egyre szélesedő hozzáféréssel kapcsolatos, és nem a kivételes nyomozási technikákkal, az adtok tömeges kiszolgáltatásával és a vállalkozások által kezelt információk kiadásával megfigyelési célokra.

A hagyományos adatvédelmi elvárásokkal szemben jelentkező kihívásokra válaszul nagyobb figyelmet kell fordítani az adatok védelmére mind a közhatalmi testületeknek, mind pedig a

vállalkozásoknak abból a célból, hogy igazolják, információkezelési gyakorlataikért felelősséget viselnek, hiszen az átláthatóság mindennek lényeges részét képezi, s az olyan társadalmi hatásnak tekinthető, amelyet a polgárok el is várnak mind kommunikációs gyakorlatuktól, mind pedig ügyeik titkos voltától, amelyet csak a jogérvényesítő és nemzetbiztonsági szervek arányos és megfelelő igényei esetén lehet áthágni, s nekik is csak akkor, ha gyakorlatukat független, megbízható hatóságok ellenőrizhetik. Az átláthatósági jelentés a közhatalmi szervek felelősségre vonhatóságát biztosítja. A jelentés a megszokott módon tájékoztatja a közvéleményt a közhatalmi hatóságok tevékenységéről. Az átláthatósági jelentéshez a testületek szabadon hozzáférhetnek és azok a nagy szereplők, akiknek a hozzáférést a felelősségre vonhatóságuk érdekében támogatni kell, ebben az esetben, ha azt a megfigyelésre vonatkozó jogszabályok megkövetelik, és a szabadságjogok érvényesítése érdekében is.

### **Az átláthatósági jelentések tartalma.**

A vállalkozások önkéntes átláthatósági jelentése sokféle statisztikát is tartalmaz, amelyek nem mindig összehasonlíthatóak egymással.<sup>23</sup> A részletezettség változó, a metrika különböző és az adatok meghatározása vagy meghatározásuk is hiányos.

Abból a célból, hogy a jelentési rendszer hatályát rendbe tegyük, az átláthatósági jelentéseket meglehetősen hasonlóvá kell tennünk. A jelentések statisztikát is tartalmaznak a vállalkozásoknak az információ kérelmére és e kérelmek teljesítésére vonatkozóan. A jelentések egyéb, az érintett vállalkozások által kezelt információra vonatkozó adatokat is tartalmazhatnak, pl. pl. az európai 'jog a felejtésre' vonatkozó kérelmekkel kapcsolatos Internet oldalon, de ezek a további jelentések e dokumentum hatályán kívül esnek.

A jelentések tipikus szempontjai a következők:

- *a joghatóság*: a több joghatóság területén működő vállalkozások általában különböző országok hatóságaitól fogadnak kérelmeket, ezért a jelentés szerkezetének ezt is tükröznie kell. Különböző országok a hasonló koncepciókat különbözően határozzák meg, és a vállalkozásnak kell eldöntenie, hogy a jelentéseiben az annak megfelelő szabványos terminológiát, vagy egy partikuláris joghatóság terminológiáját használja-

---

<sup>23</sup> A jelentések szabványosításából adódó problémákat Christopher Parsons világítja meg. Lásd: [Do Transparency Reports Matter for Public Policy? Evaluating the Effectiveness of Telecommunications Transparency Reports](https://ssrn.com/abstract=2546032), 2015, hozzáférhető: SSRN: <http://ssrn.com/abstract=2546032> vagy <http://dx.doi.org/10.2139/ssrn.2546032>.

e. Értékes lehet a szabványos terminológia használata, de a lábjegyzetekben meg kell magyarázni, hogy az melyik joghatóság területén alkalmazzák.

- *a jelentés periódusa*: az átláthatósági jelentés nem egyszeri gyakorlat, hanem folyamatos. míg az on-line jelentés megmarad a jövőben is, a vállalkozások gyakorlata eddigelé az volt, hogy évente tesznek jelentést, míg a nagyobb vállalkozások ennél gyakrabban, negyed- vagy félévenként. A jelentések rendszerint figyelik a trendek alakulását és ábrákat, magyarázatokat is tartalmazhatnak az előző periódusra vonatkozóan;
- *a kérelmek típusai*: a kormányzati szervek kérelmének formája különböző ugyan, de a legtöbb jelentés szabványos, ami megfelel a joghatóság és az ipar igényeinek is. A tipikus klasszifikáció a kérelmek jogi formájával azonos (pl. bírósági felhatalmazás vagy egy adminisztratív kérelem), a vállalkozás akciói (pl. hozzáférés a létező rekordokhoz vagy egy olyan eszköz elhelyezéséhez, amely nyomon követi egy számla alakulását és aktivitásra vonatkozó, valós idejű adatokat szolgáltat ki a kormányzati szerveknek) iránti kérelem a büntető- vagy a magánjogi rendelkezéseken alapszik, és a kérelem a hazai vagy a külföldi jogérvényesítő hatóságoktól érkezik.<sup>24</sup> Sokféle alkategória használata is értékes lehet. A vállalkozások hajlanak arra, hogy jelentéseikbe foglaljanak számos kérelmet, rendszerint azokat, a mely a hazai jogérvényesítő szervektől érkeztek.
- *a kérelmek száma*: a jelentésnek elsősorban a kormányzati szervek kérelmeire adott válaszokat kell tartalmaznia. Felettébb egyszerű azon kérelmek számának a jelentésbe való belefoglalása, amelyek elfedik a lényeges különbségeket, mindenek előtt a kérelmek természetére és terjedelmére nézve. Ennek megfelelően a legértékesebb jelentések mind az érkezett jelentéseknek, mind az egyéni rekordoknak, mind pedig azoknak a számláknak a számát is tartalmazzák, amelyekre a kérdések vonatkoznak;
- *az információ terjedelme vagy az érintett egyének száma*: egyes, de nem minden jelentés ábrákat is tartalmaznak, amelyek az információ terjedelmét és a kérelmek hatását ábrázolja; *a kérelmek eredménye*: az átláthatósági jelentések nemcsak egyszerűen azt tükrözik, hogy a kormányzati szervek milyen választ adtak a vállalkozások kérelmeire, hanem azt is, hogy a kérelmek milyen eredménnyel jártak, ámbár ez a vállalkozások jellegétől függ, valamint a jogszabályoktól. Az adatfeldolgozónak például hivatkozni kell a kormányzati szervek kérelmére, hogy az érintett adatkezelő is hozzáférhessen az általa kezelt adatokhoz, kivéve h az

---

<sup>24</sup> A vállalkozások megtagadhatják a külföldi hatóságoktól érkezett kérelmek teljesítését, de ezek okait fel kell sorolniuk a jelentéseikben is.

adatfeldolgozó a kormányzati szervek kérelmének tesz eleget, és ha a jogszabályok megtiltják, hogy feldolgozó további lépéseket tegyen. Az adatfeldolgozó jelentésének ezért tartalmazhatja az adatkezelők ügyfelei azon ügyeinek a számát, melyekben a feldolgozó közvetlenül válaszolt a kérelmekre. A legtöbb bejelentett statisztika a kérelmek teljesítésére vagy elutasítására vonatkozik, és ha e kérelmet teljesítették, akkor a rekordok számát is részletezni kell és az érintett egyének jellemzőit és érintett számláinak tartalmát is. Egyes esetekben a jogszabályok korlátozzák vagy késleltetik a statisztikák közzétételét.

- *magyarázat*: a statisztikákat általában egy magyarázattal is ki kell egészíteni, a fogalmakat meg is kell magyarázni és a trendeket is figyelembe kell venni. Különleges magyarázatot kell adni a váratlan vagy kivételes számok esetében.

### **Az átláthatósági jelentés elvei.**

A Munkacsoport javasolja, hogy a magánélet- és adatvédelmi hatóságok ösztönözzék a vállalkozásokat, hogy az átláthatósági jelentés alábbi 'elveinek' eleget tegyenek:

1. **A felelősségre vonhatóság elve**: a vállalkozásoknak felelősségre vonhatóknak kelleneük azokért a cselekedeteikért, hogy miképp teljesítik a kormányzati szerveknek az arra irányuló kérelmeit, hogy az általuk kezelt információkat kiadják nem üzleti célokra is.
2. **Az átláthatóság elve**: a vállalkozásoknak általában teljesíteniük kell a kormányzati szerveknek arra irányuló kérelmét, hogy az általuk kezelt, nem üzleti célt szolgáló információk jellegét és mennyiségét időközönként közzétegyék;
3. **A megbízhatóság elve**: a vállalkozások átláthatósági jelentéseinek tartalmazniuk kell azokat a személyes információkat, amelyeket a kormányzati szervek kérelmére pontosan és teljes mértékben kiszolgáltattak;
4. **Az az elv, mely szerint a jelentés nem lehet félre vezető**: annak ellenére, hogy a jogszabályok olykor késleltethetik a jelentések közzétételét, vagy korlátozhatják annak hatályát, a vállalkozásoknak mégis közzé kell tenniük a jelentéseiket, és el kell kerülniük, hogy azokat helytelenül értelmezzék, és pedig a félrevezető statisztikák által.<sup>25</sup>
5. **Az összehasonlíthatóság elve**: a vállalkozásoknak biztosítaniuk kell, hogy a bejelentett statisztikák összehasonlíthatóak legyenek a korábban közzétett jelentésekben foglalt statisztikákkal, ide értve az egyéb átláthatósági jelentésekben foglaltakkal is.

---

<sup>25</sup> It is to be understood in offering these principles that companies need to be compliant with applicable national law in undertaking transparency reporting.

6. **A hozzáférhetőség elve:** az átláthatósági jelentéseket olyan formában és azon a helyen kell közzétenni, amilyen formában és amely helyen ahhoz mindenki hozzáférhet, ide értve a médiát és az érintett szereplőket is.

**Az elvek érvényesítésével kapcsolatos ajánlások:**

A jelentés eddigelé önkéntes kezdeményezés volt, amelyet a magánszektor a kormányzati szervek kérelmére válaszul fejlesztett ki, és amely megfelel minden egyéb, többek között a magán-életvédelmi követelményeknek is. A Munkacsoport ezért támogatja ezt a kezdeményezést, és ajánlja, hogy az átláthatósági jelentés hatályát több vállalkozásra és szektorra is kiterjessék. Az egyes vállalkozások már elkezdték az átláthatósági jelentések közzétételét, ezért gratulálunk nekik, mindazonáltal a cél nem változik, és a közzétett statisztikáknak összehasonlíthatóaknak kell lenniük. Egyetlen vállalkozás sem lehet átlátható egy egész szektorban, együttesen azonban csak azok a vállalkozások, amelyek ezt a gyakorlatot folytatják, és minél teljesebb a kormányzati szervek tevékenységéről alkotott kép, annál megfelelőbb lesz a vállalkozásoknak a személyes adatok feldolgozásával kapcsolatos gyakorlata. Ha a prominens vállalkozások közzéteszik átláthatósági jelentéseiket, úgy a versenytársaik is átláthatóbbakká válnak.

A Munkacsoport véleménye szerint a vállalkozásoknak és a részvényeseiknek támogatniuk kell az átláthatósági jelentések közzétételét, ezért ezek az ajánlások mind a vállalkozásokhoz, mind pedig a részvényeseikhez szólnak abból a célból, hogy az átláthatósági elvek alkalmazását hatékonyabbá tegyék.

**A Munkacsoport további ajánlásai:**

(a) A vállalkozásoknak teljesíteniük kell a kormányzati szerveknek az általuk kezelt személyes információk rendelkezésre bocsátására irányuló kéréseit, és megbízható folyamatokat kell kifejleszteniük abból a célból, hogy az általuk kezelt személyes információkhoz a kormányzati szervek hozzáférhessenek, és ezek kezeléséért felelősségre vonhatóak legyenek, a kezelés pedig összhangban legyen a jogszabályok rendelkezéseivel és a vállalkozás politikáival;

(b) a vállalkozásoknak közzé kell tenniük a kormányzati szervek kérései teljesítésével kapcsolatos politikáikat;

- (c) ha a vállalkozások az általuk kezelt személyes információkhoz való hozzáférésre irányuló ismételt kérelmeket fogadják a kormányzati szervektől, úgy azokra az e dokumentumban meghatározott átláthatósági gyakorlatoknak megfelelően kell válaszolniuk;
- (d) a vállalkozásoknak biztosítaniuk kell, hogy az általuk közzétett átláthatósági jelentések megbízhatóan igazolják, hogy a statisztikák alaposak és igazolhatóak;
- (e) a vállalkozások jelentéseinek szerkezete és terminológiája támogatja a vállalkozások, szektorok országok és időperiódusok szerinti statisztikáit;
- (f) el kell kerülni azokat a gyakorlatokat, amelyek félrevezetik az olvasókat azáltal, hogy a számok nem teljesek, mert ezt a kormányzati szervek is észlelik;
- (g) a jelentéseket hatékonyabb módon kell támogatni, például azáltal, hogy a közös és a nemzetközi statisztikákat is közzéteszik;
- (h) a jelentéskészítés gyakorlatát érvényesíteni és, hatékonyságát növelni is kell.

#### **A kormányzati szervek jogszabályai.**

- (i) a kormányzati szervek olyan jogszabályokat és szabályokat alkossanak, amelyek biztosítják, hogy a vállalkozások az általuk kezelt személyes információkat közzétegyék;
- (j) a kormányzati szervek jogszabályainak és szabályainak ésszerű korlátok között rendelkezniük kell arról, hogy azok arányosan érvényesítsék az általános értékeket, megfelelő biztosítékokat írjanak elő, és rendelkezzenek a közhatalmi hatóságok felelősségre vonhatóságáról is;
- (k) a kormányzati szervek támogassák az átláthatóságot; és
- (l) távolítsák el az átláthatósági jelentések közzétételének felesleges korlátait.

#### **A közhatalmi hatóságok hozzáférése a vállalkozások által kezelt információkhoz.**

A közhatalmi hatóságok gondoskodjanak arról, hogy

- (m) a vállalkozások az információkat, jogszerűen, arányosan és felelősséggel kezeljék;
- (n) a vállalkozások információkezelési gyakorlata átlátható legyen;
- (o) a vállalkozások tegyenek eleget a titkosítási követelményeknek, de azok nem haladják meg azt az ésszerűen megkívánt mértéket, amelyet a jogérvényesítő és nemzetbiztonsági szervek megkívánnak;
- (p) vizsgálják felül az érvényes titkosítási követelményeket abból a célból, hogy az ne haladja meg a szabad társadalomban igazolható mértéket.

### **Az adatvédelmi hatóságok:**

- (q) támogassák a vállalkozásoknak a jelentések közzétételére irányuló törekvéseit; és
- (r) azokat a törekvéseket is, amelyek a felfedett információk hasznosítását célozzák.<sup>26</sup>

### **A nemzetközi kormányzati szervek:**

- (s) bátorítsák azokat a törekvéseket, amelyek egy nemzetközileg összehasonlítható metrika kifejlesztésére irányulnak abból a célból, hogy elősegítsék a magánélet védelmét és a személyes adatok határátlépő áramlását;
- (t) azonosítsák azokat a területeket, ahol a kormányzati szervezeteknek az adatokat titkosan kell kezelniük, és bontsák el az átláthatóság szükségtelen korlátait, és támogassák a jó gyakorlatokat, segítsék a nyíltságot és az on-line bizalom kialakulását.

### **A távközlési szabályozó hatóságok:**

- (u) támogassák és bátorítsák a távközlési szektorban működő vállalkozások átláthatósági jelentéseinek közzétételét.

### **Az ipari csoportok:**

- (v) ajánlják az ipari vállalkozásoknak az átláthatósági jelentések kidolgozásának legjobb gyakorlatát<sup>27</sup>.

### **A polgári társadalom jogalkotó szervei:**

w követeljük meg minden érintett jogalanytól a felelősségre vonhatóság érvényesítését (azoknak a kormányzati szervezeteknek az esetében is, amelyekre vonatkozó jogszabályok megengedik a vállalkozások által kezelt információkhoz való hozzáférést, és a kormányzati szervek arra irányuló kérelmét kezelő vállalkozások esetében is amelyek hozzáférhetnek a vállalkozások által kezelt, nem üzleti célt szolgáló információkhoz;

z ösztönözzék a vállalkozásokat átláthatósági jelentéseik közzétételére<sup>28</sup>;

---

<sup>26</sup> Egy ipari kezdeményezésre példa a távközlési ipar párbeszéde, amely tevékenységét a [UN Guiding Principles on Business and Human Rights](https://www.un.org/development/dpd/publications/2011/09/un-guiding-principles-on-business-and-human-rights/) szerint fejti ki, és igazodik a 21. elvhez (emberi jogok), amely arra bátorítja a vállalkozásokat, hogy az emberi jogokra hatást gyakoroló gyakorlatukat tegyék közzé. Lásd: [www.telecomindustrydialogue.org](http://www.telecomindustrydialogue.org).

x bátorítsák a vállalkozásokat arra, hogy hasznosítsák az átláthatósági jelentésekben foglalt statisztikai adatokat.

\*\*\*\*\*

---

<sup>28</sup> Kanadában, Hongkongban, Lengyelországban és az Amerikai Egyesült Államokban például a szokásos módon vagy egy Internet oldalon teszik közzé a jelentéseket, és a vállalkozások azokat kombinálják statisztikai adataikkal, vagy a jelentéseket kiegészítik kutatásaik összehasonlítható adataival is.