

Ferenczy Endre*

AZ ADATVÉDELEM KÜLFÖLDI SZABÁLYOZÁSA

Bevezetés és kitekintés a nemzetközi szabályokra

Amikor arról írunk, hogy milyen az adatvédelem szabályozása külföldön, megtehetjük azt, hogy más országok szabályozását összehasonlítjuk a magyarral, de el is tekinthetünk ettől. Nem zárkozunk el eleve az összehasonlító jog – mint módszer – alkalmazásától, de először kísérletet teszünk a külföldi szabályozás önálló tárgyalására.

Az adatvédelem mint törvényi szintű szabályozás lelke a magánélet védelme, ezt előre kell bocsátani akkor is, ha a lehető legjobban koncentrálunk az adatvédelemre mint törvényhozási tárgykörre. Anélkül, hogy mélyebben bele akarnánk menni a *privacy* fogalmába, nem kerülhető meg, annak megállapítása, hogy a magánülethez való jog a tőlünk nyugatabbra fekvő demokráciáknak alapértéke volt, ezen belül az amerikai, jogi értékkel is felruházta azt, még a XIX. században (Warren–Brandeis, 1890). Az angol jogpolitika is magáévá tette ezt az értéket, noha sehol sem határozza azt meg a *statutory law*¹ (Calcutt, 1990: 7). Az ausztrál Privacy Charter preambuluma ünnepélyesen deklarálja, hogy „szabad és demokratikus társadalom tiszteletben tartja a személyiség autonómiáját és korlátozza, behatárolja az államhatalmi ágakat és a magánvállalatokat, hogy azok a magánélet szférájába ne léphessenek be. A magánülethez való jog az emberi méltóság kötőanyaga és alapjog általában a szabadsághoz és a vélemény szabadsághoz.”² A szabályozás mögötti megfontolás könnyen tetten érhető, valójában arra gondolnak, hogy az állampolgár legnagyobb ellenfele az *állam*, amely (egy amerikai bonmot szerint) „... őrült, akivel vigyázni kell, nehogy a fejünkre gyűjtsa a házat”. Természetesen az a körülmény, hogy létrejött a „házon belüli” terrorizmus, egészen új helyzetet teremtett a szabályozással szemben támasztott elvárásokot illetően. Az állam mint veszélyforrás a második helyre szorult vissza, de ez nem tette könnyebbé a jogvédők dolgát (közéjük tartozónak véelve a kodifikátorokat), mert kétfrontos harcot kell vívniuk. Ugyanezt a minősítést lehet alkalmazni az alkotmánybírákra is, ti. hogy azok is (a kodifikátorok mellett) jogvédők, tekintettel a *Bundesverfassungsgericht* 2008. február 27-én hozott ítéletére.³ A modern, globális terrorizmus, az általa felhasznált új eszközök, legfőképpen a számítógép és az általa elérhető világháló miatt, amit az utasítások továbbítására használnak, kivívta magának, az ún. távoli igazságügyi szoftver kifejlesztését, amely alkalmas az ún. online motozással való eljárás alkalmazására. Az ötlet, amelyet Wolfgang Schäuble nevével kötnek össze Európában, alkotmányossági vizsgálat alá került (ténylegesen Észak-Rajna–Vesztfália tartomány egy 2006. évi törvénye), ami Németországban, először tette lehetővé a fentebb említett módszert. Valójában arról van szó, amit a titkosszolgálatok koráb-

* tudományos főmunkatárs, Magyar Tudományos Akadémia – Budapesti Műszaki és Gazdaságtudományi Egyetem, Információs Társadalom Joga Kutatócsoport

ban is alkalmaztak valamilyen szivárgás elhárítására,; több információforrás lehallgatását igényelték a szükségesnél, miután nem tudták melyik az az egy, amelyik szivárogtat. A technika ugyanaz, amit matematikusok azzal a metaforával világítanak meg: „Hogyan fogjunk egy orosz-lánt? Fogjál százat, és engedj el kilencvenkilencet.”

A német Alkotmánybíróság nem engedte meg a szövetségi hatóságoknak a fenti eljárás egy az egyben való alkalmazását, mert a számítógépen való felderítést „tényszerű támpontokhoz” köti, először; másodsor pedig ahhoz, hogy „kiemelten fontos jogi tárgyak” legyenek veszélyben, úgymint az élet, a testi épség, illetve az állam működéséhez vagy a létfenntartáshoz szükségesek. Az ítélet lényege tehát: az állampolgárok számítógépeinek átkutatása nem korlátok nélküli opció a Szövetségi Bűnügyi Hivatal számára. Az ítéletből további korlátok is egyértelműen kiolvashatók, illetve következnek abból. Mindenekelőtt leginkább az, hogy az eljárást ún. nyomozati bírónak kell engedélyeznie, továbbá: a merevlemezeiről kinyert információk közül azonnal törölni kell azokat, amelyek az érzelmekre való következtetéseket lehetővé teszik.

Megjegyezzük, hogy a német törvényhez hasonló jogszabály bevezetését tervbe vették Ausztriában, bár ott is nagyon vitatott. Az Egyesült Államokban a szövetségi ügynökség által alkalmazott keresőprogramot, állítólag, a számítógépekre telepített antivírusrendszerek nem érzékelik.⁴

A szabályozási tárgyköröket alapvetően a magánéletet mint tárgykört, megközelítő különböző aspektusok alakítják az egyes nemzeti jogokban, e helyütt is jelezve, hogy az adatvédelem egy kisebb halmaz a magánélet védelmét jelentő normák között. Az angolszásznak, de a kontinentális jogrendszernek is elsőnek nevezhető megközelítési iránya a személyes adatok védelme, amelyek között olyan adatokat tartanak számon, mint az egészségügyi adatok vagy a közigazgatás által vezetett nyilvántartásokban szereplők, de ide sorolják a magánpénzügyeket érintőket is, például a hitelezéssel összefüggőket. Ezek közül igen érzékenynek minősítve az állampolgárok adósságait tartalmazókat, nem is megengedve azt, hogy a hitelintézetek adataikat összekapcsolhassák és egy központi adóssadatbázist létesítsenek. Másik ilyen aspektus, amelyet figyelembe vettek a szabályozás tartalmánál és technikájánál, az a kommunikációhoz való jog. Tekintettel az emberek közötti szóbeli és írásbeli érintkezések lehetőségeinek hihetetlen mértékű kiszélesedésére, szinte minden egyes formára külön-külön született szabályok. A harmadik szempont, amelyre az adatvédelmi szabályok tekintettel vannak, az a magánterület védelme.

A tudományos megfigyelések szerint a jogalkotók többféle modellel⁵ (módszerrel) kísérleteznek, hogy a magánélet különböző területeit (jogi tárgyait) megfelelő védelemben részesítsék. (A szakirodalom megkülönbözteti a magánélet védelmében alkalmazott jogi módszerek között a „*comprehensive laws*”-t; a „*sectoral laws*”-t, a „*self-regulation*”-t és a „*technologies privacy*”-t.) Az egyik modell, amikor az adatvédelmi szabályok a köz- és magánszektorra nézve együtt jelennek meg. Európa szabályozását (pontosabban: az Európai Unióban lévő szabályozás modelljét) a külföldi szakirodalom ilyennek minősíti. Számon tartják még az „együtt-szabályozó (*co-regulatory*) modell”-t is, amelyet Kanada és Ausztrália szabályozási módszeréhez kötnek.

A másik modell, amelyet a szakirodalom először az Egyesült Államokat vizsgálva regisztrált, ahol külön szektorálisan (telekommunikáció, rendőrség, fogyasztói hitelezés területe) szabályoznak. Szintén az Egyesült Államokat illetően írják le az ún. ön-szabályozási modellt, amelyben a nagyvállalatok maguk alkotnak viselkedési kódexeket és alakítanak ki önálló adatvédelmi politikát, és ezt közzé is teszik.

A magánélethez való jog joganyaga, amint azt már jeleztük, az adatvédelem szellemi háttere, és ennek egyes részterületei nagyon közel állnak az adatvédelemhez, mert például az információhoz való hozzájutás akadályozását (illetve az erre reagáló, védekező álláspontot elfoglaló jogot) aligha lehet másként felfogni, mint az adatvédelem ellentétpárját, ahogy azt az Emberi

Jogok Európai Bírósága is tette a Leander-ügyben (Roberts, 2004: 11) hozott döntésében. Ebből következően a magánélethez való külföldi jog fejlődésének tanulmányozása nélkül a felületes szemlélő elveszti az intellektuális fonalat; az adatvédelem nem „*Ding an Sich*” (azaz önmagában vett dolog) sem a jogban általában, sem pedig az általános személyiségi jogban.

Az adatvédelem egy általános politikai és jogpolitikai szemlélet eredménye, amely például nem engedi meg, hogy a politika potenciális szereplőinek (a parlamenti képviselőjelölteknek) vallási szabályokat követő magatartásáról adatokat gyűjthessenek (ahogy azt egy másik kontinensen lévő ország szabályai nemhogy megengedik, de egyenesen kötelezővé teszik). Mindez megmagyarázza a Nagy-Britanniában élő muzulmánok egy részének kirohanását Rowan Williams, a Canterbury érsek ominózus kijelentésre reagálva.⁶ Ezzel csak azt akartuk érzékeltetni, hogy ma már az adatvédelemre való igény nem köthető az ún. nyugati civilizációhoz; bár biztos, hogy ott viselik a legjobban gondját.

Következésképpen, a témakör tárgyalása az általános személyiségi jog és az információhoz való hozzáférés joga nélkül részleges, bár története, a külföldi szakirodalom tanúsága szerint tárgyalható külön is.

Abban egyetértés van a szerzők között, hogy az adatvédelem mint önálló törvényhozási tárgykör megjelenésének döntő oka a számítógépek kapacitásának hihetetlen gyors növekedése. A történeti munkák először a magánélet védelmét szolgáló törvényhozást tárgyalják. Az első törvényhozási munkát Hessen német szövetségi tartománynak tudják be, 1970-ben. Ezt követték a svéd (1973),⁷ az egyesült államokbeli (1974) a német (1977) és a francia (1978) törvények. Ahhoz, hogy az öreg kontinensen az európai államok elfogadták az adatvédelem fontosságát nagyban hozzájárult az 1981. évi Egyezmény (*Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data*) és a *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data* (OECD, 1981). Ezek nyomán két közösségi irányelvet, jogforrást alkottak: a *Directive 95/46/ of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data-t* és a *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector-t*. A XXI. században még két irányelv született, amelyek jelzik az adatvédelmi jog területeinek kiszélesedését és egyúttal alkalmazását: *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)*⁸ és *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC*.

A fentiekből mindazonáltal nem következik az, hogy az adatvédelemre vonatkozó jogalkotás, globális szinten vizsgálva a problémát, Európára korlátozódna. Az ázsiai térség is kitermelte a maga dokumentumait. Az *Asia-Pacific Economic Cooperation* miniszterei 2004-ben foglalkoztak egy Keretszabály (*APEC Privacy Framework*) kibocsátásának gondolatával. Az más kérdés, hogy az a terminus technicus, amit használnak a szövegben (*national exception*) a dokumentum kritikusai szerint túl tág teret enged a nemzeti jogalkotónak. Források tudósítanak arról, hogy Latin-Amerika is törekszik egy regionális egyezmény kidolgozására.⁹

Egy globális világban magától értetődő, bár csak utólag látható világosan, hogy az államhatárokon átmenő adatforgalom szabályozása megjelenik mint önálló törvényhozási tárgykör. Az alapvető kérdés természetesen először nem ez, hanem az, hogy valamely ország jogalkotása alapvető védelmet, *adequate protection*ot nyújt-e az információs önrendelkezési jog

(*informationelle Selbstbestimmung*) gyakorlásához. (Megjegyezzük: Magyarországon is komoly sajtóvitát váltott ki az, amikor magyar állampolgárok adatait, ugyan kutatási célú felhasználásra, de egy másik kontinensen lévő államba küldték.) Épp ezért olyan dokumentumoknak is jelentősége van, amelyekről még 2000. július 27-én tudósított a sajtó, hogy a Bizottság Svájc, Magyarország és az Egyesült Államok törvényhozását a magáéval egyenértékűnek ismerte el a személyes adatok védelmére vonatkozó törvényhozást illetően. Később, 2002-ben, ugyanebben az elismerésben részesítették a kanadai *Personal Information Protection and Electronic Documents Act*-et, majd 2004-ben Argentína, Új-Zéland, Ausztrália és Hongkong hasonló tárgyú jogszabályait. Az Egyesült Államok adatvédelmi rendszerének elfogadása egyáltalán nem ment könnyen: az ún. *Safe Harbor* egyezmény megkötéséről csak 1998-ban indultak a tárgyalások az Államok és az Európai Unió között.

A 2006-ban kirobbant SWIFT-botrány egy időre megakasztotta a tárgyalásokat. A SWIFT-ügy lényege: az európai és amerikai média felfedte az Egyesült Államok kormánya által létrehozott, a terrorizmus finanszírozását követő program létezését. A program lehetővé tette az Egyesült Államok hatóságai számára, hogy hozzáférjenek a 200 országban több mint 8000 üzleti bankot (köztük több központi bankot) tömörítő, Belgiumban működő, iparági együttműködésen alapuló SWIFT-rendszerben (Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság) tárolt összes pénzügyi adathoz.

A SWIFT-ben tárolt, az amerikai hatóságok által megszerzett információk több százezer európai polgárt érintenek, és ez egyebek mellett nagyszabású gazdasági és ipari kémkedést tesz lehetővé. Az Európai Parlament erre reagálva kiadott egy állásfoglalást, amely szerint veszélyeztetve érzi a magánélet és az adatok védelmét, és arra hívja fel a figyelmet, hogy „a személyes adatok harmadik országok részére történő átadására nemzeti és európai szintű adatvédelmi jogszabályok vonatkoznak, ennek értelmében az adatok átadását minden esetben igazságügyi hatóságnak kell engedélyeznie”.

A szöveg elfogadásával a Parlament azt követelte, hogy „az Európai Bizottság, a Tanács és az Európai Központi Bank szolgáljon alapos felvilágosítással arról, milyen mértékben volt tisztában a SWIFT és az USA kormánya közötti titkos megállapodással”. Végül is, hosszas vita után, amelybe a belga hatóságokat is bevonták, mivel a *Society for Worldwide Interbank Financial Telecommunication* székhelye Belgiumban van, 2007 júniusában a Tanács és az Egyesült Államok egyezséget kötött a személyes jellegű pénzügyi adatok SWIFT-ből az Államokba való jutásának módjáról (*Processing and protection of personal data subpoenaed by Treasury Department from the US based operation centre of the Society for Worldwide Interbank Financial Telecommunication*).

A SWIFT-ügy mutatja, hogy az információk áramlása, a rendelkezésre álló technikai feltételek miatt elengedhetetlenné vált a határokon átmenő adatokkal kapcsolatos adatvédelem jogi szabályozása. Ha történetileg nézzük a határokon átküldött adatáramlást, akkor a tudományos megfigyelések szerint az alábbi területeken voltak először regisztrálhatók: külföldön teljesített pénzügyi szolgáltatások, idegen ország oktatásában való részvétel, az elektronikus úton folytatott kereskedelem és orvostudományi kutatások. A szabályozás eredményessége elsősorban az adatvédelmi hatóságok közötti együttműködéstől függ, amiből következik, hogy maga a kooperáció önálló szabályozási tárgykör lett.

A külföldre menő adatokra vonatkozó szabályozási modellek kétfélek, nevezetesen vagy a fogyasztóvédelemen belül helyezik el a külföldre menő adatok normáit (Egyesült Államok, Japán) vagy a tárgykörre vonatkozó rendelkezések az általános adatvédelem és a magánélet védelmének részét képezik. Az Államokban nagy szerepet játszik a tárgyalat területen a *Federal Trade Commission* és a *Department of Justice for Criminal Proceedings*, miközben arra is utalást kell tenni, hogy a *common law* szabályai épp úgy érvényesek, mint az írott szövetségi

szintű normák. Japánban a magánélet általános védelméért a Miniszterelnöki Kabinet visel politikai felelősséget, míg a panaszokat a Fogyasztóvédelem Nemzeti Központjánál kell beadni.¹⁰

Európában, különösen az OECD-országok minisztereinek 1998-ban Ottawában tartott találkozója óta, a kártérítés mint szabályozási tárgykor a kodifikátori figyelem középpontjába került. Ez a törekvés vagy felismerés nyilvánvalóan az amerikai, a norvég és az ausztráliai szabályozás hatása, amelyben a szankcionálás célja a fogyasztó kártalanítása. Az OECD Munkacsoportja (73. láb.) 2005-ben, javasolja is ennek a szemléletnek a megvalósítását, de az OECD által 2003-ban kibocsátott dokumentum, (62, 39. láb.) az ajánlott politikáról és folytatandó gyakorlatról, a hangsúlyt még csak a multilaterális és bilaterális mechanizmusok javítására és fejlesztésére helyezi. A *spamekkel* kapcsolatos szabályozási problémák is érzékenyek.¹¹ Fejlesztendőnek találták a szakértők, továbbá a más országokban intézendő elektronikus formanyomtatványokat. Azok a jogsértések, amelyeket a brit, a kanadai vagy amerikai hatóságok észleltek a határokon átmenő adatfelhasználás területén, ugyan számosak, de eléggé ritkán jutnak bírói szakba. Következésképpen a témával foglalkozó elemzők – a számos létező nemzetközi megállapodás ellenére, mint amilyen *Safe Harbor*, a spanyol és amerikai hatóságok között létrejött megállapodás, az *Eurojust*, a Schengeni Megállapodás és a SID – további erőfeszítéseket kívánnak a különböző államoktól a bizalmas adatok kezelésének hatékony védelme érdekében. A határokon keresztül áramló adatok és információk szabályozásának aktualitását és bizonyos mértékig megoldatlanságát jelzi a 2003-ban kiadott *Lignes directrices régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses* és a 2006. áprilisi ajánlás: *Recommandation relative à la coopération transfrontière dans l'application des législations contre le spam*.¹² [A határokon átmenő információk nemzeti jogi szabályozásáról az OECD jelentést (*Rapport sur l'application transfrontière de la législation relative à la vie privée*) készítette.]

Szabályozási környezet: az információs társadalom

Nyilvánvaló tény, hogy adatvédelem korábban is volt, már csak nemzetbiztonsági megfontolásokból is, azonban az sem vitás, hogy a papíralapú adatrögzítést felváltó (vagy azzal párhuzamosan létesült) adatrögzítési és továbbítási módszerek teljesen új helyzet elé állították a különböző országoknak a törvényhozás előkészítéséért felelős apparátusait, illetve a nemzetközi kapcsolatok intézményeit. Ez az állítás akkor is igaz, ha a múlt század elejéről és közepéről ismertek olyan esetek, még irodalmi feldolgozásuk is van (Edgar Allen Poe, Forsythe stb.), amikor adatokat, igazolványokat, dokumentumokat megkettőztek, meghamisítottak vagy éppen elloptak. A jogalkotás és a jogalkalmazás szempontjából vizsgálva a problémát és a jelenséget, a különbség a tényállások tömegessé válása; az újabban ismertté vált esetek ezres és milliós nagyságrendű jogsértésekről szólnak.

Az információs társadalom egyik jellegzetessége, ami egyben meg is különbözteti a számítógépeket és elektronikus hálózatokat nem használó társadalomtól, az, hogy elődeink által nem ismert, korszerű kommunikációs technikákat használ a népesség egy része. Az viszont a modern ismeretek birtoklásának vagy nem tudásának ellenére szinte mindenkit érintő tény, hogy „... személyes adatokat akármelyikünkéről még soha ilyen egyszerűen és könnyen nem lehetett megszerezni, illetőleg továbbítani, továbbá: nyilvánosságra hozni és más adatokkal társítani, összekapcsolni” (Dieplinger, 2002). Nyilvánvaló tehát, hogy az adatvédelmi szabályozásnak ki kell terjeszkednie olyan kérdések megválaszolására, hogy ki, milyen adatainkat és milyen célra jogosult felhasználni és továbbadni. *Dieplinger* nézetei szerint alanyi jog az adatok törlésének kérelme, a téves adat kijavíttatása. Világos: az adatok gyűjtésével, felhasználásával stb.

kapcsolatos jogok és kötelezettségek terjedelme mutatja azt, hogy ún. *open society*-val vagy totalitáriánus állammal állunk szemben.

Az információs társadalomban alkalmazott technológiák egy a polgári társadalom által támasztott igény kielégítését is lehetővé tették, nevezetesen azt, hogy a karkai kastély (az állam, vagy olyan államszerű konstrukció, mint az Európai Unió) átlátható és ellenőrizhető legyen. Ez az ún. hozzáférési jog, ami voltaképpen az állampolgárságból, az adófizetői státusból deriválható és derivált jog.

Az állam, vagyis pontosabban: az állami döntési folyamatok nyilvánossága, egy másik fájl, mármint az állampolgárok, a személyes adatok védelmének kimunkált jogához képest, de mivel az államigazgatás elektronizációja rohamléptékkal halad, az ún. e-kormányzás, az *e-governance*) visszahozza az általunk vizsgált képbe az adatvédelmet mint a jogi szabályozás egyik tárgyát.

Az e-kormányzat és az adatvédelem

Abban az elemzők egyetértenek, hogy a kormányok számára a politika iránti apátiából kitörési pontot jelent az elektronikus közigazgatás előnyeinek kihasználása.¹³ A sikeres angol példa mellett megemlíthetők a francia erőfeszítések is. A kormányprogram (*Programme d'administration électronique* [ADELE]) 2003. február 9-én indult, és természetesen számos az adatvédelemmel kapcsolatos kérdést vetett fel, többek között azt, hogy mely adatok legyenek rögzítve és mennyi időre. Szemmel láthatólag a program egészéhez a CNIL testülete és a jelentés készítője, Isabella Falque Pierrotin asszony, pozitívan viszonyult.¹⁴

A felmérések azt mutatják, hogy az elektronikus közigazgatás által nyújtott szolgáltatások (engedélyek, jogosítványok, regisztrációk, ún. ismétlődő szolgáltatások) felhasználói ma már nem csak a nagyvárosokban élő fiatalok, hanem, mert csatlakoztak hozzájuk, a kisebb településeken élő idősebbek is. Megállapítást nyert továbbá, hogy a világ pénzügyi kiadásainak 30 százaléka a kormányzati szférában történik, és amennyiben sikerül az adminisztratív kiadásokat csökkenteni, úgy annak haszonélvezői a kis- és középvállalkozások lesznek. Ennek politikai előnyeit választási szempontból nem lehet eléggé felülbecsülni. Az EU-27-ek szintjén több mint másfél százalékos GDP-növekedést prognosztizálnak (a skandináv államokat és Nagy-Britanniát illetően még ennél is többet) az e-közigazgatási és kutatási és fejlesztési programokból származóan. (Meg kell jegyezni: Európában az egyik legkorábban lépő ország épp Nagy-Britannia volt, ahol az 1999-ben kiadott „A kormányzat modernizálásának Fehér Könyve” fogalmazta meg az elektronikus kormányzással szemben támasztott követelményeket. A dokumentum szerint a kormányzati szolgáltatások 100 százalékos elektronikus feldolgozását és nyújtását 2005-re el kell érni – amit teljesítettek is.)¹⁵ Fontos azt is látni, hogy az e-kormányzat szolgáltatásainak fejlődését a *Capgemini* méri, immár 9 éve. Egyébként az Európai Unió a tagállamoknak 20 online közszolgáltatás megvalósítását ajánlja.

Az e-közigazgatás nem hordoz magában új veszélyeket, mármint ahhoz képest, amit az állam a történelem során produkált saját és területén tartózkodó külföldi állampolgárokkal szemben. Az esetleges szándékos jogsértéseket – bizonyos területeken – az ún. nyilvános kulcsú kódolással ki lehet védeni, mert a módszer két alapvető funkciót ellát, ti. a titkosítást és az elektronikus aláírás készítését. (E kódolás használatával kiszűrhető az illetéktelen hozzáférés, és nyomon követhető bármilyen módosítás.) Ez az állítás azt is jelenti, hogy az e-közigazgatás, de az adatvédelem joga és annak fejlesztése sem képzelhető el az elektronikus aláírásra vonatkozó joganyag (1999/93/EK irányelv) nélkül.

Anomáliák, jogsértések az adatvédelem fejlesztését megkövetelő jelenségek

A túlzott, a jogállami elveket meghaladó módszerekkel történő ellenőrzés ellen valószínűleg a legerősebb jogintézmény az adatok, az adatbázisok összekapcsolásának tilalma. A modern információs társadalom azonban számos olyan jelenséget (emberi magatartást) termelt ki, amely legalább olyan veszélyes, mint a *data base interconnection*. Ilyenek nyilvánvalóan az ún. adathalász-akciók, az álhonlapok létesítése, a spam (Goldwin, 2003: 75), a kémprogramok, a hackerek tevékenysége stb. A fentiekből már látszik: a terrorizmus nemcsak a személyiségi jogok hajóját lékelte meg, vagy legalábbis megkísérli azt, hanem a cyberbűnözés¹⁶ eszközei révén magát a nemzetbiztonságot támadja. Következésképpen, az adatvédelem szabályozási módszereit tárgyalva külön kell kezelni az utóbbi tényállásokat az előzőektől. Ugyanakkor nagyon nehéz egymást majdnem lefedő jelenségeket szabályozási szempontból elkülöníteni: ilyen például, amikor önkéntesen adott adatokat szerez meg bűncselekménnyel harmadik személy, amikor fölmerül a kötelező biztosítás bevezetésének gondolata vagy még inkább hiányának konstatálása az adatkezelő egyéni felelősségével együtt. Természetesen nem véletlen, hogy a biztosítás és az egyéni felelősség érvényesítésére a jogalkotó nem kerített sort, egészen speciális ez a problematika az elektronikus térben. (2007. augusztus közepén a világ egyik legnagyobb állasközvetítője ismerte be, hogy hackerek 1,6 millió felhasználó adataihoz jutottak hozzá.)

Adatvédelem, közérdekű adatok

A közérdekű adatokat nem illeti meg védelem, mert nyilvánvalóan az adatok minősítése megelőzi azt a folyamatot, aminek végén valamely adat közérdekűnek (és ezáltal nyilvánosnak) minősül. Aligha kétséges, más megközelítés is lehetséges. Ki lehet abból indulni, hogy minden adat nyilvános, majd ezt követi annak megállapítása, melyek minősülnek államtitoknak vagy szolgálati titoknak. A tárgykorre vonatkozóan voltaképpen két szabályozási modell különböztethető meg: az egyik a svéd, a másik német. Az elsőre egyfajta nyitottság jellemző, aminek eredete – a szakirodalom szerint – visszamegy az 1766. évi sajtószabadsági törvényre (hatályos az 1949. évi 105. törvény a sajtószabadságról), amelyen alapul a svéd állampolgárok állami aktákhoz való hozzáférése joga (1976. évi törvény). A német vagy svájci törvényhozás szelleme más: ezek a szabályozási módokra inkább azt lehet mondani: zárt. Ugyanis az állam, aktáit bizalmasan kezelteti köztisztviselőivel; egyfajta aktatitkosságról és bizalmas kezeléstről lehet beszélni, ha az adminisztrációt jellemezni akarjuk.

Az adatvédelem *soft law* forrásairól

Az adatvédelmi jognak nemcsak kapcsolt vagy kapcsolódó területei vannak, mint a *privacy* joga vagy az információszabadság joga vagy éppen az információkhoz való hozzáférés joga, hanem szemmel láthatóan létezik a pozitív jog mellett számos dokumentum, amelyek befolyásolják magáról az adatvédelmi jogról való gondolkodást, így többek között például a jogszabály-előkészítést. Ilyen a már említett „Munkacsoport 29”¹⁷ vagy a *Direction XV* által kibocsátott állásfoglalások, illetőleg az *European Committee of Standardization* által közzétett munkanyagok.

Nyilvánvalóan az adatvédelmi jog kemény magját képezik a nemzetközi megállapodások, a regionális jog (mint amilyen a közösségi jog) és a nemzeti jogok jogforrásai, illetve a bírói gyakorlat.

Az adatvédelmi jog kemény magjáról – a nemzeti jogok jogforrásairól

Előre kell bocsátani, hogy a joganyagot ebben a részben abban a felfogásban tárgyaljuk, hogy az adatvédelem nem azonos az információk önrendelkezési joggal és csak a szabályozást öleli fel, amely az egyén védelmére irányul, normákat alkotva az egyén személyes adatainak kezelésére. A joganyag centrumában az adatbiztonság és a technológiai eszközök állnak.

Az első törvényt az adatvédelemről 1978-ban alkották Ausztriában, 1986-ban módosították, majd 2000-ben harmonizálták. *Bundesdatenschutzgesetz*-et 1990. december 20-án hirdették ki (BGBl. I S 2954.). Németországban az első adatvédelmi törvény 1977. január 21-én született, amelyet 1990. december 20-án módosítottak, és 1999. augusztus 17-én született meg a *Datenschutzgesetz*, a BGBl. I Nr. 165/1999-ben jelent meg. A köz- és magánszektor viszonyait egyaránt érintő, a 95/46 irányelv megoldásait átvevő német szövetségi adatvédelmi törvényt 2001. május 18-án fogadta el a Bundestag; módosításai: BGBl.I. Nr. 136/2001 és BGBl. I Nr. 13/2005.¹⁸ Belgiumban 1992-ben fogadták el a homológ törvényt,¹⁹ majd 1998-ban, módosították azt. A Cseh Köztársaságban 2000. április 4-én szavazták meg a 104. számú törvényt a személyes adatok védelméről. A törvény több törvény módosítását is tartalmazza. Dániában két lépcsőben alkották meg a szóban forgó szabályozási tárgykört: 2000 májusában szavaztak a személyes adatok feldolgozásáról szóló törvényről és júliusban az adatvédelmiről. [A dánok már korábban is foglalkoztak a szabályozási tárgykörrel: 1978. június 8-án törvényt alkottak a magán- és köznyilvánosságok vezetéséről, amelyet 1988-ban és 1991-ben módosítottak.]²⁰ Az Egyesült Királyságban először 1988-ban hoztak törvényt az adatvédelemről, majd az 1998 júliusában hozott törvénnyel harmonizálták azt az irányelvvel. (*Data Protection Act 1998*).²¹ Finnországban 1999 áprilisában fogadták el a személyes adatok védelméről szóló törvényt, amelynek szövege összeegyeztethető volt a magánszféra védelmét a távközlési szektorra is kiterjesztő 97/66 számú irányelvvel. A holland adatvédelmi törvény 2001 júliusában került a szenátus elé és 2001. szeptember elsején lépett hatályba. A lengyel hatályos törvényt (*Ustawa o ochronie danych osobowych*) 1997. augusztus 29-én fogadták el, amely a személyhez fűződő adatok védelmével kapcsolatos normákat tartalmazza. Luxemburgban az új adatvédelmi törvény tervezetét, amelyet harmonizáltak a 95/46 irányelv rendelkezéseivel, 2000 októberében terjesztették a Parlament elé, de még 2002-ben is tárgyalták a Kormány 4735. számú törvénytervezetét (*Projet de loi no. 4735 relatif à la protection des personnes à l'égard du traitement des données à caractère personnel*). Olaszországban 2000. május 5-én lépett hatályba az adatvédelmi törvény. [Ezt megelőzően 1996-ban alkottak törvényt e tárgykörben (675. számú törvény, december 31.), és mindegyik évben módosították a törvény elfogadása után.]²² Franciaországban a hatályos joganyagot a 2004. augusztus 6-i törvénnyel (*Loi relative à la protection des personnes physique à l'égard des traitement de données à caractère personnel*) módosított 1978. január 6-i (*Loi relative à l'informatique, aux fichiers et aux libertés*) törvény tartalmazza. A svéd adatvédelem szabályairól az 1998. évi 204. törvény szól.²³ A svájci szövetségi törvényt (*Loi fédérale sur la protection des données*) 1992. június 19-én tárgyalta először a Konföderáció Nemzetgyűlése.²⁴ A törvény módosítása (2007. szeptember 28.) 2008. január elsején lépett hatályba.²⁵

Az adatvédelem kemény jogáról – részletesebben

A francia nemzeti jog releváns jogként, hivatalos szöveggként (*textes officiels*) kezeli, de természetesen nem nemzeti jogi forrásként tartja nyilván „Az alapvető emberi jogok európai kartája” címet viselő jogforrást (Hivatalos Közlöny, 2000. december 18.); A személyes adatok védelméről szóló Egyezményt (Európa Tanács); a 95/46/EK irányelvet; ugyanígy a 2002/58/EK

irányelvet és a Lisszaboni Egyezményt (Hivatalos Közlöny, 2007. december 17.). A kiegészítő források között említik az ENSZ Közgyűlése 1990. december 14.-én hozott 45/95 számú határozatát. A nemzeti jogi jogforrások között első helyen tartják nyilván a már említett 1978. január 6-i törvényt (*Loi 78–17 relative à l’informatique, aux fichiers et aux libertés*).²⁶ A törvényt 2004-ben módosították (*Loi 2004–801 du 6 août 2004, Loi relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel*). A 2005-ben kiadott rendelet (*Décret No. 2005-1309 du 20 octobre 2005 pris pour l’application de la loi No. 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés*)²⁷ a törvény végrehajtásáról rendelkezik. A rendeletet 2007-ben módosították (*Décret 2007-451 du 25 mars 2007*).²⁸ További nemzeti jogi rendelkezések között sorolják fel a postáról és az elektronikus kommunikációról szóló törvénykönyv (*Code*) 34. § (5) bekezdését (a piackutatás szabályai a természetes személyek körében); A Munka Törvénykönyvének 20. § (2) bekezdését (a szabadságjogok korlátozása arányosságának követelménye); a közbiztonság megőrzésének megvalósításáról szóló (*Loi no. 95–73 du 21 janvier 1995 d’orientation et de programmation relative à la sécurité*) 10. §-át és 17. § (1) bekezdését (kültéri videomegfigyelésre, illetve a kérelemre és hivatalból kezdődő közigazgatási eljárások során folytatható, a személyes adatokkal kapcsolatos vizsgálatokra vonatkozó magatartási szabályokról); a közigazgatás és az állampolgárok, illetve továbbá a jogi személyek közötti kapcsolatok javításáról szóló 78–753 számú törvény 3. § és 13. § szakaszait (a neveket tartalmazó információk (jegyzékek) kezeléséről, illetve a személyes adatok újrafelhasználásáról); a természetes személyek országos jegyzékéről szóló 82–103. (1982. január 22.) számú rendelet (*Répertoire national d’identification des personnes physiques, Décret 82–103*).

A törvény főbb tárgykörei a következők: elvek és fogalmi meghatározások; a személyes adatok kezelésének mint tevékenységnek a törvény által megkívánt előzetes feltételei; a Szabadságjogok és az Informatika Országos Bizottságára (*Commission Nationale Informatique et Liberté – CNIL*) vonatkozó rendelkezések; eljárásjogilag szabályozott feltételek az adatkezelésre; az adatok kezeléséért felelősek kötetmei és az érintett személy jogai; az adatkezelés ellenőrzése; a Szabadságjogok és az Informatika Országos Bizottsága által alkalmazható intézkedések; büntetőjogi rendelkezések; személyes adatok kezelése az orvostudományi kutatásban és az egészségügyben; személyes adatok kezelése a hírlapírás, irodalmi vagy más művészeti kifejezés céljából; az Európai Közösségen kívüli országba való adattovábbítás szabályai.

A jogszabály biztosítja (a 3. szakaszban) az állampolgárok számára azt a jogot, hogy tudja: vezetnek-e róla nyilvántartást, és ha igen, milyen; másképpen fogalmazva: szerepel-e valamilyen adata nyilvántartásban, és ha igen, akkor milyenben. [A Táblabíróóság (*Cour de Cassation*) 2004. szeptember 28-án hozott ítéletében kimondta, hogy minden személynek abszolút (sérthetetlen) joga az, hogy megtiltsa valamely szervezetnek (ebben a perben az *Association spirituelle de l’église de scientologie d’Ile France*-nak), hogy az adatait nyilvántartásában megőrizze.²⁹] A törvény intézményesíti a tiltakozáshoz való jogát, az adatkezelést illetően, különösen, hogy adatait kereskedelmi célból használják fel. Az adatkezelésről való informáltság jogát, a francia felfogás szerint, kiegészíti a személyi adatokhoz való hozzáférés joga. E jog gyakorlása elé akadályt lehet gördíteni nemzetbiztonsági, honvédelmi és közbiztonsági okból, továbbá az adatkezelő megtagadhatja a hozzáféréshez való jog gyakorlását akkor is, ha az adatok őrzése nem jelent kockázatot az adattulajdonos szempontjából. A törvény biztosítja az adattulajdonos számára, hogy éljen azokkal a jogokkal, amelyeket a jogszabály biztosít számára: így a téves adatok helyreigazításának jogát, az adatok kiegészítésének követelését vagy aktualizálását, vagy kitöröltetését (40. szakasz). Ehhez a joghoz kapcsolódnak a törvény korábbi rendelkezései (9. és 10. szakasz), amelyek megtiltják, a közigazgatási hatóságokon és igazságszolgáltatási szerveken kívül, olyan nyilvántartások vezetését, amelyek szabálysértésekre, bűncselekményekre

vagy biztonsági intézkedésekre vonatkoznak. Az adatok kezelése nem irányulhat személyes adatokra az állam szervezetén túl. A harmonizált szabályok, a 2004. évi törvénymódosítás nyomán a közszektor a továbbiakban nem kényszerül engedélyt kérni az adatkezeléshez az illetékes testülettől (ez lett az általános szabály); a törvényes adatkezelés feltétele egyszerű bejelentés. A törvénymódosítás voltaképpen a magánszektorra érvényes szabályt terjesztette ki a közszektorra. Az új jogszabály bevezette az egyszerűsített bejelentési rendszert is. Mindazonáltal a közszektorban, illetőleg a magánszektorban lévő ügyintézés közötti különbségtételt teljesen nem tüntette el az új törvény: egyes különleges adatok kezelése előtt az illetékes hatóságtól az adatkezelőnek véleményt kell kikérnie. Viszont, a magánszektor is, például a személyi azonosító szám használatára csak előzetesen megkért engedély birtokában jogosult. A német *Datenschutzbeauftragte* mintájára, a törvénymódosítás lehetőséget biztosít a közszektorban és a magánszektorban működő szervek számára, hogy a személyes adatok védelmével foglalkozó kapcsolattartót, levelezőt (*Correspondant Informatique et Liberté – CIL*) nevezzék ki. [Képviselők egy csoportja az Alkotmányjogi Tanácshoz fordult, mert álláspontjuk szerint a levelezők nem rendelkeznek azzal a mértékű függetlenséggel, amely szükséges a magánélet védelméhez. A Tanács (*Conseil Constitutionnel*) 2004-489 számú határozatában (2004. július 29.) úgy döntött, hogy a feladatukra vonatkozó szabályok egyetlen, az alkotmányból folyó követelményt sem sértenek.] Az adatvédelemért felelős levelezőt be kell jelenteni a hatósághoz, amelynek legújabb állásfoglalása szerint e személy lehet a szervezet alkalmazottja is. A hatóság egyébként nemcsak fogadja a bejelentéseket (amelyek között egyszerűsített és általánost különböztet meg a törvény), de a közszektor számára, és csak annak, kiad kötelező erejű véleményt (*avis*); engedélyt az adatkezelésre, illetve bizonyos esetekben felmentést (*dispense*) is kibocsát. A Testület társadalmi szerepét és tekintélyét jelzi az a döntés, amelyben 2007. március 8.-án nem engedélyezte a természetes személyek által felvett hitelek központi adatbázisának létesítését.

A belga adatvédelmi jog első helyre sorolható jogforrása a magánélet védelme a személyes jellegű adatok kezelése területén (*Loi r la protection de la vie privée r l'égard des traitement de données r caractre personnel*) 1992. december 8-án került kihirdetésre, majd az irányelvvel való összeegyeztethetőség miatt 1998. december 8-án módosították. 2003. február 26-án is módosították a törvényt, de ez már belga törvényhozók kezdeményezésére történt. A Parlament elfogadta azt a végrehajtó hatalom által favorizált modellt, amelyben ágazati adatvédelmi bizottságok működnek. A javaslat természetesen szükségessé tette az addig egyedüli *Commission de la protection de la vie privée* hatáskörének megváltoztatását. A módosított törvény szükségessé tette rendelet (*Arrêté royal du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative r la protection de la vie privée a l'égard des traitements de données r caractre personnel*) kiadását. A rendelet meghatározza azokat a feltételeket, amelyek mellett valamely korábbi személyes jellegű adat felhasználható statisztikai célra, vagy a történettudományban, illetőleg más tudományokban. Szabályokat tartalmaz az érzékeny adatok kezelésére. Kitér azokra a módokra (betekintési jog, helyesbítéskérés vagy adatok töröltetésének joga), amelyekkel valamely személy élhet az őt megillető jogok érvényre juttatása érdekében. A rendelet meghatározza, továbbá, a személyes adatok kezelésére vonatkozó ún. adatkezelési bejelentés formáját. A 2003. februári törvény is megkívánta végrehajtási rendelet (*Arrêté royal du 17 décembre 2003 fixant les modalités relatives r la composition et au fonctionnement de certains comités sectoriels institués au sein de la Commission de la protection de la vie privée*) kiadását. A jogszabály az ágazati bizottságok működéséről rendelkezik, és a törvényhez képest részletesebb szabályokat alkot a bizottságba felkért szakértőkről és azok munkájáról. Az adatvédelem területén a második legfontosabb törvény (*La loi 8 aout 1983 organisant un Registre national*

des personnes physiques) tárgyköre: a természetes személyekről vezetett országos nyilvántartás. A jogforrás meghatározza azoknak az információknak körét, amelyek az Országos nyilvántartásban szerepelnek, továbbá rendelkezik megőrzésük és frissítésük módjáról. Megállapítja a nyilvántartás mint rendszer igazgatásának szabályait és a személyi szám (pontosan: „az Országos nyilvántartásban szereplő szám” – „*numéro de Registre national*”) használatára vonatkozó normákat, továbbá egyedülként e hatósághoz telepíti azt a hatáskört, hogy a hozzá forduló személyek és szervezetek számára engedélyezze a nyilvántartásban szereplő információkhoz való hozzáférést. A törvény meghatározza azon intézmények körét, amelyek használhatják a személyi számot. A jogszabály rendelkezik arról, hogy adott esetben ki igényelheti, hogy hozzájuthasson a nyilvántartásban lévő információkhoz. Végül rendelkezéseket tartalmaz a norma az Országos Nyilvántartás Ágazati Bizottsága összetételéről, feladatairól és hatásköreiről. A harmadik jogszabály, amely a belga adatvédelem jogforrásai között szerepel, elrendeli elektronikus hálózat létesítését az Országos Nyilvántartás és a Társadalombiztosítás között (*Loi du 15 janvier 1990 relative à l'institution et l'organisation d'une Banque – Carrefour de la Sécurité Sociale*). Az intézmény nem adatbank, hanem a társadalombiztosítás által működtetett hálózat, amely például az állampolgárok részére lehetővé teszi, hogy az adatokat ne kelljen összegyűjteniük vagy többször elküldeniük. Adatvédelmi okokból az információk közvetlenül az internetről nem érhetők el, sőt, ha intézmények közötti információáramlásról van szó, a Társadalombiztosítás Ágazati Adatvédelmi Bizottságához kell először fordulni, amely – miután jogi vélemény kiadását kéri a „*Banque*”-tól – az után engedélyezi a törvényben megnevezett hálózaton („*Banque-Carrefour*”) keresztülfutó információátadást. A tárgykört érintő legújabb, 2007. március elsején hatályba lépett törvény alapvetően módosította az egészségügyi adatokkal kapcsolatos információáramlás és adatkezelés szabályait. Megváltoztatták az ágazati bizottságra vonatkozó szabályozást is; az egységes ágazati bizottságban két testületet létesítettek: egyet a társadalombiztosítással összefüggő ügyek, egyet az egészségügy területére. 2003-ban a törvény (*Loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses dispositions*) egy másik háló, amit éppen nyilvántartásnak is lehet nevezni, ugyanis ez a „*Banque*” nyilvántartja a vállalati adatbázisok adatait és azokat az adatokat, amelyeket más nyilvántartások (a kereskedelmi, az általános forgalmi adóé és mások) tartalmaznak. A hálózattal kapcsolatban vannak: az Adóhivatal, a Társadalombiztosítás Országos Hivatala, a kereskedelmi bíróságok törvényszéki irodái és a vállalati kifizetőhelyek pénztárai. A két évvel később, 2005-ben elfogadott törvény (*Loi du 10 août 2005 instituant le système d'information Phenix*) rendelkezései, több más célkitűzés mellett, egy, a joggyakorlatot is elérhetővé tevő adatbázis létrehozását célozták meg, ahogy az igazságügyi statisztika fejlesztését is megcélozták. Nyilvánvaló, miután a „*Phenix*” ágazati információs rendszer, a jogalkotónak szektorális Bizottság létesítését is kellett rendelnie. A hivatalos statisztikára vonatkozó törvény (*Loi du 4 juillet 1962 relative à la statistique publique*) 2006. március 22-i módosítása, a magánélet változatlan védelmének fenntartása céljából, elrendelte ágazati (a statisztikai) felügyelő bizottság létesítését. 2007. júniusában pedig kiadták e bizottság működésére és összetételére vonatkozó rendeletet (*Arrêté royal du 7 juin 2007 fixant les modalités relatives à la composition et fonctionnement du Comité de surveillance statistique institué au sein de la Commission de la protection de la vie privée*). A belga rendszer tehát egy „Főbizottságot” (*Commission de la protection de la vie privée*) és hat ágazati bizottságot működtet; ezek közül egy a szövetségi szintű hatóságok „szabályozó hatósága”, mert ez is véleményezi a személyes adatok védelme szempontjából a jogszabálytervezeteket; a *Comité sectoriel pour l'Autorité Fédérale* is ajánlásokat tesz az adatkezeléssel kapcsolatosan. Ez a szervezet is, ahogy a többi ágazati bizottság, engedélyezi a személyes adatok kezelését, ha annak törvényi feltételei fennállnak.

A belga adatvédelmi jog anyagát, a szabályozás módját egy másféle módszerrel is át lehet világítani, nevezetesen azzal, hogy megvizsgáljuk az adatvédelem szempontjából érzékeny területeken van-e, és ha van, milyen a szabályozás. A belga jogalkotó igen messzire ment, amikor a 2001. augusztus 10-i törvénnyel megalkotta „A Magánszemélyek Hiteleit Nyilvántartó Központot (*La Centrale des Crédits aux Particuliers*), bár igaz, hogy az információs rendszer a Belga Központi Bank részét képezi. Az is a minőségi adatvédelmet jelenti, hogy 1992-től a politikai pártok, a képviselőjelöltek és a megválasztott képviselők kötelesek azt a szabályt tiszteletben tartani, hogy a személyes adatok kezelés csak célhoz kötött lehet, és a választási kampány idejére szorítkozik, a törvény ereje folytán. Azok irányába, akik támogatói vagy egyéb listára felkerülnek, Nyilatkozatot kell kiadni, amely tartalmazza az érintettek jogait. Törvényt (*Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance*) alkottak Belgiumban a biztonsági kamerák felszereléséről és használatáról is. A személyes adatok kezelésére bejelentési kötelezettséget jogszabály írja elő (*Arreté royal 13 février 2001*, megjelent a *Moniteur Belge* 2001.03.13. számában), a bejelentés illetve elektronikus út után 25 euró, papíralapú adatkezelés esetén 125 euró.

Másfajta metszetben is bemutatható a belga adatvédelmi jog szabályozása. A jog prezentációjának technikája az, hogy veszünk néhány nagyon fontos szabályozási tárgykört, úgymint: a) a személyes jellegű adatok kezelése; b) a személyes jellegű adatok gyűjtése; c) a célhoz kötöttség; d) fogalom meghatározás: az érzékeny adatok; e) az adatok minőségére vonatkozó előírások; f) az érintett jogai az adatkezelő irányába; g) személyes adat külföldre továbbításának szabályai.

Az első feladat nyilvánvalóan az, hogy ismertessük: milyen adatokat minősít a belga jog³⁰ személyes jellegűnek. A törvényhozás ilyenként definiálja egy személy nevét; a róla készült fotót; telefonszámát (hivatalit is); kódjait, bármire is legyenek azok felhasználhatók; bankszámlaszámát; e-mail címét, újjelnyomatát. Még az előzőeknél is tágabban határozza meg a törvényhozó a személyes adat fogalmát, ugyanis a jogalkotó felfogása szerint egy adat attól lesz személyes, hogy az adat által, annak nyomán, az érintett személy azonosíthatóvá válik. A jogalkotó értelmezése szerint nemcsak a magánélettel, hanem a közélettel és a hivatással kapcsolatos, a személyre vonatkozó, az azonosítási művelet elvégzésére alkalmas adatok is személyes jelleggel bírnak. Az adatok kezelése alatt ért a belga jog minden olyan műveletet, ami magában foglalja az adatok gyűjtését, felhasználását, rendezését vagy közlését. Az adatok gyűjtését a jog bejelentéshez köti, továbbá megkívánja, hogy ez a részművelet is követhető, azaz átlátható legyen. A jog meghatározza az adatkezelő kötelezettségeit és tartalmazza a tiltott magatartásokat. Az adatvédelmi jog nagyon pontosan meghatározza azon adatok körét, amelyek ún. érzékeny adatok. Ezek a következők: az érintett személy egészségi állapota, politikai nézetei, hívő vagy ateista volta, szexuális irányultsága, büntetőjogi szempontjából releváns múltja. Kivételesen az alábbi esetekben a törvény mégis lehetőséget ad az érzékeny adatok kezelésére, nevezetesen, ha az adatkezelő erre írásbeli felhatalmazással bír; ha ez nélkülözhetetlen az ápoláshoz, gondozáshoz, orvosi ellátáshoz; és végül, ha a munkajogi szabályok ilyen adatok rögzítését előírják. A belga jog inkorporálta az „adat minősége” fogalmát, és ez alatt azt érti, hogy az adatoknak maguknak is bizonyos feltételeknek meg kell felelniük, így mindenképp annak, hogy pontosnak kell lenniük. A jog továbbá megköveteli, hogy az adatokat bizalmasan kezeljék, szigorúan őrizzék, tehát azok ellopására ne adjanak alkalmat, és elvesztésükre ne kerüljön sor. A belga jog is több jogosultságot biztosít az érintett személynek az adatkezelő irányába, így mindenképp azt, hogy a róla vezetett adatokról joga van informálódni, továbbá kérdéseket feltennie az adatkezelőnek. Jogként biztosított az is, hogy az érintett tájékoztatást kapjon a róla vezetett adatok fajtáiról, ilyen értelemben azt mondhatjuk, hogy a belga jog ismeri az érintett hozzáférési jogát saját adataihoz. A hozzáférési jogot a személyazonosságot igazoló dokumentum másolatának megküldésével vagy e-mail és utána elektronikus aláírás megküldése után

lehet gyakorolni. Valamely adat hozzáférésehez közvetett úton is hozzá lehet jutni a belga jog szerint. A közvetett úton való hozzáférést biztosító joggal, a magánélet védelmét szolgáló Bizottsághoz intézett levéllel lehet élni. A szövetségi jog biztosítja az adatok helyesbítésének jogát. Amennyiben az adatkezelő egy hónapon belül nem teljesíti a kérelmet, úgy a Bizottsághoz lehet fordulni panasszal. Az érintettet a nemzeti jog szerint megilleti a tiltakozás joga is, például a direkt marketing eseteiben. Az adatvezetés ellen nem lehet élni a tiltakozás eszközeivel, ha az adatkezelés szerződésen alapul vagy jogszabály rendelte el. Az érintettet megilleti továbbá a panasz előterjesztésének joga a magánéletet védő Bizottsághoz, illetve, hogy a királyi ügyészhez vagy a bírósághoz forduljon. Az adatok külföldre továbbíthatóságának kérdésében a belga jog két esetet különböztet meg. Az egyik esetben az adat az Európai Unión belül marad, a másik esetben áthalad annak határán. Ez utóbbi esetben az adatok továbbíthatóságához az a feltétel szükséges, hogy az Unió Bizottsága úgy ítélje meg: az illető ország biztosítja az adatok védelméhez szükséges elegendő védelmet.

Az adatok védelméről szóló 1992. júniusi törvény nyolc fejezetből áll. Az első meghatározza a törvény célját, hatályát és közli a fogalommeghatározásokat. A második rész az általános rendelkezéseket tartalmazza. A harmadik az adatkezelés szabályaival foglalkozik. A negyedik fejezet a személyes adatok szövetségi szervek általi kezelése közbeni szabályokat írja elő. Az ötödik a szövetségi szintű szervek vezetőinek kinevezéséről, jogállásukról, hatáskörükről rendelkezik. A hatodik rész (amely csak egy szakaszból áll) a jogorvoslati lehetőségeket tartalmazza, megállapítja a Szövetségi Közigazgatási Bíróság elnökének hatáskörét előzetes intézkedés meghozatalára, és alkalmazni rendeli a Polgári Perrendtartásról szóló 1947. december 4-i törvény 79–84. szakaszait. A hetedik részbe a büntetőjogi normákat foglalták bele. A nyolcadik rész az átmeneti rendelkezéseket tartalmazza.

A *Bundesdatenschutzgesetz*-et (BDSG) 1990. december 20-án hirdették ki, utolsó módosítása 2006. augusztus 22. A törvény tárgyi hatálya kiterjed a hagyományos és a gépi adatkezelésre, de a jogalkotó kiveszi a törvény tárgyi hatálya alól a személyes vagy családi eseményeket rögzítő adatfelvételt. A törvény különbséget tesz a közhatalom és a nem az állami szférában történő adatkezelés között és megengedi az ágazati sajátosságok figyelembe vételét. Az adatkezelésről nyilvántartás vezetését írja elő, az ellenőrzés kiterjed a tartalomra is. Az adatkezeléshez jogalap szükséges, amely alapulhat törvényi felhatalmazáson, vagy az érintett hozzájárulásán, illetőleg szerződés is megteremtheti azt. Az ún. érzékeny adatoknál jogalapot teremt az adatkezelésre az érintett írásbeli hozzájárulása, vagy az a körülmény, hogy az adatkezelés létfontosságú érdeke az adatalanynak, de beleegyezése a rendelkezésre álló időben nem szerezhető meg. A jogorvoslati lehetőségek, ahogy nemzeti jogokban, itt is számosak: panaszt lehet benyújtani az adatvédelmi biztoshoz az adatkezelés tárgyában, aki határozatot hoz a beadványról. Az adatvédelmi biztos elrendeli az adatok kijavítását, adott esetben azok kiegészítését; megtiltja az adattovábbítást vagy törölteti az adatokat. Döntése ellen bírósághoz lehet fordulni.

A német törvény 3. szakasza határozza meg az anonimizáló és pseudoanonimizáló tevékenységet, ami voltaképpen nem más, mint a személyes adatok megváltoztatása. A törvény 3. § (9) bekezdés szerint a faji vagy etnikai hovatartozásra, a politikai véleményre, a vallási vagy világnézeti meggyőződésre, a szakszervezeti tagságra, az egészségi állapotra vagy a szexuális életre vonatkozó adatok különleges adatnak minősülnek. Az adatvédelmi törvény nagyon részletesen szabályozza az érintett jogait. Jogorvoslatért az adatvédelmi biztoshoz kell fordulni. Az adatalany joga van, hogy a jogsértőkkel szemben polgári jogi, illetőleg büntetőjogi és szabálysértési szankciók érvényesítését kérje. Kára megtérítésére is lehetősége van az adatalanynak. Objektív alapú a kártérítési felelősség az állami szervek esetében, a kártérítés összege 130 000 euróig terjedhet. A nem állami szerveknél a törvény vétkesség alapú felelősségi rendszert alkotott.

Az Egyesült Királyság adatvédelmi törvénye, a *Data Protection Act 1998* [1998 Chapter 29], ahogy a Parlament más aktusainál is megfigyelhető, a fogalommeghatározásokkal indít (adat, személyes adat (*personal data*), különleges adat (*sensitive personal data*)). [Itt a szöveg utal a szakszervezeti és munkakapcsolatok törvényére (*Trade Union and Labour Relations (Consolidation Act 1992)*) és a szakszervezeti tagságot ilyennek minősíti.] Az 1998. évi törvény az 1984-ben született *Data Protection Act 1994*-et váltotta fel, hogy a szöveg összeegyeztethető legyen a 95/46/EC irányelvvel. A jogszabály nagy törvényhozási tárgykörei: a személyes adatok, az érintett jogai, az adatvédelmi elvek, a kivételek és a büntetendő cselekmények. A törvény külön területként, célként jelöli meg az újságírást, általában a művészetet és nevesítve a szépirodalmi tevékenységet. [Part 1.,3.] A II. rész 7. pontja részletezi az adóalany jogait: a tájékozódáshoz (az adataihoz való hozzáféréshez), a kijavításhoz, a tiltakozáshoz, a törléshez való jog. Az előbb említett területek (újságírást, szépirodalom) az adatkezelés szempontjából különlegesek; alapesetben az adatkezelés jogalapját az érintett hozzájárulása vagy jogszabály teremti meg. Az általánostól eltérő szabályok vannak még az adatkezelést illetően, a törvényhozó által értékelt cél miatt részletesen meghatározott szabályozási hatáskörök esetén, az egészségügy, a munkaügy és a versenyjog területén. A különleges adatok kezelésének jogalapja az angol jogban is szigorúbb: írásbeli hozzájárulás szükséges az érintettől vagy az érintett létfontosságú érdeke teremtheti azt meg, illetve fakadhat valamely foglalkoztatási jogviszonyból, illetőleg visszavezethetőség megkívánt valamely egészségügyi tevékenységre. Megalapozza továbbá állami kötelezettség is a különleges adat kezelésének jogalapját; és végül történhet kutatási célból. A törvény negyedik része (Part IV) számos kivételt felsorol, ezek közül megemlítendő a nemzetbiztonság (*national security*). A törvényi szabályozás értelmében (Section 28) a kivételezés kiterjed a törvény második részére (Part II), tehát az adatokhoz való hozzáférés jogának érvényesítésére; a harmadik részre (Part III), azaz: az adatkezelés kötelező bejelentésére; az ötödik részre (Part V): a kötelező szankciók alkalmazására és az adatok törvénytelen módon való megszerzésének tilalmára (Section 55). A törvény értelmében még a különleges adatok kezelése is megengedett, ha bűncselekmény megelőzése vagy felderítése érdekében történik, ide értve az adózással kapcsolatos bűncselekményeket (*crime and taxation*). Végül az összes adatvédelmi elv, ti. a második és harmadik részben szabályozottak, vagyis az adatokhoz való hozzáférés joga vagy az adatkezelés bejelentésének kötelezettsége felfüggesztett, ha az adatgyűjtés célja otthoni dolgokra, vagy a háztartással összefüggő, illetőleg családi ügyekre vonatkozik (*domestic purposes*). A jogterülethez kapcsolódó nemzeti joganyag a *Freedom of Information Act 2000* és a *Computer Misuse Act 1990*, közösségi jog a *Privacy and Electronic Communication (EC Directive) Regulations 2003*.

A személyhez fűződő adatok védelméről szóló osztrák törvény szerkezete, szabályozási módja és struktúrája, természetszerűleg, inkább a kontinensen született törvényekhez hasonlít, mint az Egyesült Királyságban elfogadotthoz; például az osztrák törvény nem a jogszabályszöveg elején adja a fogalommeghatározásokat, hanem később, a 4. §-ban. Az osztrák jogszabály is különbséget tesz a közügyek és a magánvállalkozás területe között. Az államhatalom területére esik minden olyan adatkezelési tevékenység, amely annak megbízásából történik, akkor is, ha magát az adatkezelést már nem közjogi szervek végzik. A jogalkotó miután megkülönböztette az egyes szabályozási területeket, rendelkezik a tárgyi és személyi hatályról, majd ezt követik a törvényben használt fogalmak. A következő szabályozási tárgykör: az adatkezelés elvei, illetve annak felsorolása, hogy mi teremti meg az adatkezelés jogcímét általában, illetve érzékeny adatoknál. Végül: a jogszabály rendelkezik az ellenőrzési eljárásokról (16–25. §§), majd az adóalany jogairól (26–29. §§). Ami az ellenőrzéssel kapcsolatos rendelkezéseket illeti, az eljárás az, hogy a bejelentési kötelezettséget előzetes ellenőrzés, majd regisztráció követi, ha az adatkezelés különleges adattal történik, vagy büntetőjogi szempontból értékelhető adatokról

van szó; illetőleg, ha az adatkezelés az érintett hitelképességének megállapítását célozza, és akkor, ha az adatkezelés közös informatikai rendszerben folyik. A bejelentési kötelezettség alá eső adatkezelést nyilvántartásba veszik. A nyilvántartást külön e célra létrehozott adatvédelmi Bizottság vezeti. Az adatkezelés, a megjelölt kivételeket nem számítva, a bejelentés után megkezdhető. Az adóalany jogait több helyen szabályozza a törvényben a jogalkotó: 1. § (4); 8. § (1);, illetve 9. § (6) és a 26.-tól 29. szakaszokban. Az adatalany a vállalkozási szektor jogsértései ellen, kivéve a tájékoztatáshoz való jog megsértését, polgári peres úton tud fellépni, egyébként a Bizottság a jogorvoslati fórum. [(1. § (4) bekezdés] Az adatalany hozzájárulását írja elő a törvény az adatkezeléshez, és megadja az adatalany számára az adatkezelésre vonatkozó hozzájárulás visszavonásának jogát. [9. § (6)] Az adatalanyt megilleti a tájékozódáshoz való jog, ami kiterjed az adatforrásra, az adatkezelőre, az adatai továbbítására. Maga a tájékoztatás megtagadható, ha az közérdekbe ütközne, és ha ellentétes lenne a büntetőeljárás céljaival, vagy sértené az alkotmányos rendet, illetőleg a nemzetbiztonság érdekeit. Ha az adatkezelésnek nincs törvényes jogalapja, úgy az adatalany élhet tiltakozási jogával, amely alapján jogosult az adatokat töröltetni, kijavíttatni az adatot, ha az az információt összességében meghamisítja. [27. § (1) bekezdés] Az adatvédelemhez való jog egyébként mindenkit megillet. Olyan adatok tekintetében viszont nem érvényesíthető, amelyek bárki számára hozzáférhetők. Az osztrák adatvédelmi törvény szerint az érintett nem csak természetes személy lehet, hanem jogi személy is. A törvény 4. § 1. pontja szerint az osztrák jog ismeri a közvetetten személyhez fűződő adat fogalmát. A nyilvános és közvetetten személyhez fűződő adatokra nem terjednek ki az adatkezelési szabályok. A közvetetten személyes adat, ha különleges adat, akkor a különleges adatok kezelésére vonatkozó szabályt kell alkalmazni. Különleges adatok kezelésének jogalapját megteremti a katasztrófaelhárítás. Az adatkezeléshez való hozzájárulás nem visszaható hatályú. Az adatvédelmi Bizottság eljárása bejelentés alapján indul. Döntései és intézkedései ellen a közigazgatási bírósághoz lehet fordulni. A Bíróság megállapítja az érintett jogainak érvényesíthetőségét, és kártérítést ítél meg (Jahnel – Siegwart – Fercher, 2007: 258).

A luxemburgi jog vagy inkább a luxemburgi jog harmonizálásának esete a 95/46/EC irányelvvel különösen érdekes. Az elkészült törvénytervezet, az érintett személyek védelme személyes adataik kezelése tekintetében (*Projet de loi 4735 relatif à la protection des personnes à l'égard du traitement des données à caractère personnel*) több szervezet véleményezte, így többek között a Köztisztviselők és Közalkalmazottak Kamarája (*Chambre des fonctionnaire et employés publics*), a Magánalkalmazottak Kamarája (*Chambre des Employés privés*) és az Emberi Jogok Tanácsadó Testülete (*Commission consultative des droits de l'homme [CCDH]*). Különösen figyelemre méltóak ez utóbbi szervezet megjegyzései. A CCDH véleménye szerint a tervezet 9. szakasz (2) bekezdése, amely az újságírási, művészeti és szépirodalmi célú tevékenység kapcsán elkezdődő adatgyűjtést (adatkezelést) bejelentéskötelezetté teszi az Adatvédelem Országos Bizottságához.

A Testület álláspontja szerint a véleményszabadság jogának gyakorlásával összeegyeztethetetlen az újságírói munka során, illetőleg a művészeti és szépirodalmi tevékenység esetében végzett adatgyűjtésre vonatkozó a Tervezetben lévő szabályok. A szöveg készítői annak a véleményüknek adtak kifejezést, hogy a fenti tárgyköröket célszerűbb lenne külön törvényben szabályozni, amelyben az Emberi Jogok Európai Egyezménye elveinek alkalmazásával kapcsolatosan felvetődő kérdések rendezhetők lennének. A tanácsadó testület úgy találta, hogy azok a feltételek [16.§ (2) bekezdés], amelyek mellett a banki adatbázisokban meglévő személyes adatok összekapcsolhatók lennének nem eléggé világosak, kimunkáltak, és azzal a szabállyal, amit az 5. szakasz (1) bekezdés f) pontja tartalmaz, ti., hogy az adatkezeléshez az érintett személy kifejezett beleegyezésének megadása szükséges, nincs összhangban. [Voltaképpen tehát arról van szó: úgy is történhet az adatok összekapcsolása, hogy az érintett személy kifejezett bele-

egyezésével az adatkezelő nem rendelkezik.] A Bizottság úgy vélekedett továbbá, hogy a jogszabálytervezet előkészítőinek újból át kellene gondolniuk az adatvédelemért felelős jóváhagyására vonatkozó rendelkezéseket az érintettel kialakuló későbbi konfliktusok megelőzése érdekében. A CCDH úgy foglalt állást véleményében, hogy a 41.-ban lévő rendelkezések jobb, ha három különböző szakaszba kerülnek (megkönnyítve ezzel a jogszabályszöveg érthetőségét), ugyanis így azok a jogosítványok, illetve lehetőségek, amelyek egyrészt megilletik az államügyészt, másrészt a vizsgálóbírókat és harmadjára „minden személyt”, kívánatos, ha egymástól elkülönítetten szerepelnek a majdani törvényben. A Bizottság javasolta azt is, hogy a parlamenti frakció kommunikációjának ellenőrzésére vonatkozó szabály kerüljön ki a tervezetből, mert így a büntetőeljárásról szóló törvény 81-től 88. §§-ig terjedő szakaszaira nem kell a szövegben utalni.

Hosszas vita után aztán 2002. augusztus 2-án fogadták el a személyes adatok kezeléséről szóló törvényt (*Loi du 2 août 2002 relative à la protection des personnes et à l'égard du traitement des données à caractère personnel*), ami aztán ugyanazon év december 2-án lépett hatályba, és szövegét összeegyeztethetőnek ítélték a Parlament és a Tanács által kibocsátott 95/46/EK irányelv szövegével. Másképpen fogalmazva: a törvény szövegét harmonizálták az irányelvvvel. A törvény tárgyköre a természetes személyek szabadságjogainak és alapvető jogainak védelme, közelebbről a magánélet védelme az adatkezelési tevékenység kapcsán vagy területén, és olyan szabályok megalkotása, amelyek jogkövető magatartást tanúsítását kényszerítik ki a jogi személyektől. A törvényt egyformán alkalmazni kell az állam általi adatkezeléskor éppúgy, mint amikor arra a vállalatok tevékenysége folytán vagy az egyesülési jog gyakorlása közben kerül sor. A törvény célja, hogy megtalálja az egyensúlyt az információs társadalom igényei és a magánélet védelmének követelménye között. A jogalkotó célkitűzése volt az is, hogy kiegyensúlyozott legyen az adatkezelőt terhelő kötelezettségek és az érintett személy alapvető jogai közötti viszony. A törvény a fenti célok megvalósulása érdekében meghatározza a személyes adatok kezelésének feltételeit, kereteit. E törvény értelmezésében ez azt jelenti, hogy minden természetes személynek joga van arra, hogy tudomása legyen a róla vezetett adatokról és azokat folyamatosan ellenőrizhesse. A törvény tehát az érintettet védi az államtól, a fogyasztót a termelőtől vagy kereskedőtől, a javak előállításával és forgalmazásával hivatásszerűen foglalkozóval szemben, ugyanígy az alkalmazottat a munkaadó irányában. A törvény személyes adatnak minősít minden olyan információt – ide értve a hangmást és a képet –, amely alapján a személy azonosítható válik. A törvény kiterjeszti a védelmet a jogi személyekre is, tehát azok az adatok is védettek, amelyek alkalmasak a közvetett azonosításra. Ezek közül információk közül kiemeli a személyi azonosítót, vagy az olyan ismérveket, amelyek egyediek, legyenek azok testiek vagy pszichológiai vonatkozásúak, illetőleg, amelyekkel az érintett genetikailag, kulturálisan, leírható, illetőleg társadalmilag vagy gazdaságilag jellemezhető. A törvény meghatározza az adatkezelést; minden olyan műveletet ebbe a körbe tartozónak ítélt, amely során adatgyűjtést végeznek, adatot rögzítenek, adatmegőrzést folytatnak, az adatot használják vagy módosítják vagy előállítják, átadják, illetve bármilyen formában másnak rendelkezésére bocsátják; továbbá, ha adatokat összekapcsolnak vagy ellenkezőleg, elzárnak, kitörölnek valamilyen nyilván tartásból vagy megsemmisítenek. A törvény rendelkezik az adatbankfelelősök feladatairól, így az adatkezelő kötelességévé teszi a jogalkotó, hogy az adatkezelést bejelentse, vagy rendelkezzen olyan előzetesen beszerzett engedéllyel, ami az adatkezelést lehetővé teszi. Az adatkezelő feladata ugyanez, ha személyes adatok gyűjtése, nyilvántartásba vétele vagy felhasználása tevékenysége tárgya. A törvény három eljárást különböztet meg. Az első az általános, amely előzetes bejelentéshez kötött. A másodikban előzetes hozzájárulás kérése szükséges, például, különleges adatok kezeléséhez. A harmadik, az előzőektől eltérő eljárás, az állami szervekre vonatkozik, és jogszabály írja elő. Az Adatvédelmi Országos Bizottság (*Commission nationale*

pour la protection des données) az adatkezelési bejelentés, bejegyzés menetére nézve ábrát tett közzé³¹ (Communiqué, 2003). A Bizottság több ajánlást is közzétett néhány adatkezelés bejelentésének egyszerűsített eljárására ezek, többek között, egyesületek, alapítványok tagjai, támogatói, önkéntesei nyilvántartásáról szóló bejelentésekre vonatkoznak. Magát a formanyomtatványt, amely tevékenységi fajták szerint készült, az internetről letölthetővé tették. Az érintettek joga van az adatgyűjtés megkezdésekor tudomást szerezni az adatkezelés tényéről, és a tájékoztatáshoz való joggal később is élhet, tehát az adatkezelés folyamán bármikor. A pontatlan és az adatgyűjtés céljához viszonyítva mellékes (nem odatartozó információk) törlését kérheti. Tiltakozhat az érintett az adatgyűjtés ellen, amennyiben érvei törvényes alapon állnak, és ha az adatgyűjtés piackutatási (kereskedelmi) célú.

Az állampolgároknak joguk van ahhoz, hogy az országos szintű nyilvántartások vezetése átlátható legyen. Ugyanígy joguk van ahhoz, hogy panasszal forduljanak a Bizottsághoz, illetve kérjék a testületet: vizsgálja meg valamely adatkezelés törvényi feltételei fennállnak-e. Végül: joguk van ahhoz, hogy adatokat olyan országba, külföldre küldjenek, ahol az adatvédelem a közösségi vívmányoknak megfelelő, azzal azonos szintű.

Luxemburgban 2007. szeptember elsején lépett hatályba az ugyanezen év július 27-én elfogadott törvény, amely módosította a már említett 2002. augusztus 2-i törvényt, továbbá az elektronikus kommunikációs ágazatban a magánélet védelméről szóló törvényt (*Loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques*) és a médiumokban gyakorolható véleményszabadságról szóló törvényt (*Loi du 8 juin 2004 sur la liberté d'expression dans les médias*) is. A jogszabály néhány egyszerűsítést léptetett életbe a bejelentési kötelezettséggel kapcsolatban, illetve néhány rendelkezés fogalomhasználatát pontosította, összhangba hozva a törvényt 95/46/EK irányelvvel. A módosított törvény mentesíti az értesítési előírás alól az újságírókat, az írókat, a művészeket, az ügyvédeket, a jegyzőket és a bírósági végrehajtókat. Tekintettel arra, hogy bizonyos esetekben nem sérülnek az alapvető szabadságjogok, a törvény bővíti továbbá azokat a kivételeket az adatkezelésre vonatkozólag, amikor a vállalatokra, a közigazgatásra, az egyesületekre és a szabadfoglalkozást gyakorlóakra nem hárul az értesítési kötelezettség. [Az értesítési kötelezettség alóli általános kivételeket a törvény 12. § (2) bekezdése tartalmazza.] A törvény egyszerűsíti az adatvédelmi felelőshöz való fordulást, aki a törvény hatályba lépése után alkalmazott is lehet. Megkönnyíti továbbá a törvény az egészségügyi szakszolgálati dolgozók számára az egészségügyi és szexuális életre vonatkozó adatok kezelését, kivéve a genetikai állományra vonatkozókat. Ugyanígy rendelkezéseket tartalmaz a törvény a kutatásokat illetően. Enyhíti a törvény a korábbi szigorú előírásokat a pénzügyi szektorban is a saját ügyfelek tekintetében a hitelezés és a fizetőképesség megállapítását illető adatkezelés tekintetében. A biztonsági kamerákkal kapcsolatban hatályon kívül helyezték az előzetes engedélyezési kötelezettséget, előíró rendelkezést. A rendelkezés helyébe lépett a kamerák üzembe helyezéséről való értesítési előírás. A közösségi joggal történő harmonizáció érdekében az adatok megőrzésére való kötelezettség időtartamát az elektronikus távközlés területén (mobiltelefon és vezetékes telefon, internet, fax és SMS), a forgalmazás tényére és helyére vonatkozólag, 12 hónapról 6 hónapra csökkentették. A rendőrség és az igazságszolgáltatás irányába meglévő adatmegőrzési kötelezettség ideje továbbra is 12 hónap, ha az ügy a büntetőjogi szakban van. Szintén az európai joggal való összeegyeztethetőség miatt rendelkezik a 2007. július 27-i törvény úgy, hogy a biometrikus adatok kezelésére ezentúl a testület előzetes engedélyére van szükség. A biztonsági célú, genetikai állományra vonatkozó adatgyűjtés továbbra is az engedélyhez kötött rendszerében marad.

Összefoglalás: a szabályozási módszerek általános vonásai

A vizsgálat alapján úgy tűnik, hogy ha az adatvédelmet szabályozó joganyagban különbségeket keresünk, és ez alapján akarjuk modellezni az általunk tanulmányozott nemzeti jogokat, akkor bizonyos formai és tartalmi jegyek alapján ez a művelet elvégezhető.

Formai jegyként megjelölhető az, hogy az adatvédelem megjelenik-e a vizsgált nemzeti jog alkotmányában. Olyan országok közül, amelyeknek Alkotmányában megemlíti az adatvédelmet, felsorolhatjuk a Cseh Köztársaságot [10. § (3)]; Észtországot [42–45. §]; Magyarországot [59. §]; Litvániát [22. §]; Lengyelországot [47. és 51. §§-ok].

Ez alapján képezhető két nagy csoport, de abból következően, hogy az írott alkotmány hiánya (Egyesült Királyság, Svédország) és az alkotmányosság színvonala között nincs egyenes arányosság, látható, hogy e formai jegy alapján túl messzire menő következtetést nem lehet levonni. Amennyiben azonban mégis használható szempontot ad a formai jellegű vizsgálódás, hoztunk rá példát, hogy a jogszabályok, jogszabálytervezetek alkotmányosságát vizsgáló testületek (Németországban, illetve Franciaországban) közbe tudnak avatkozni, ha az Alkotmányt sértő normákat észlelnek.

Azt is láttuk vizsgálódásaink során – ez is lehet egy modellképzési ismérv – hogy a civiljogban illetékes bíróságok is képezhetnek védvonalat nagy hatású döntéseket hozva az adatvédelem területén, idéztünk is eseteket, (Franciaország, Luxemburg). A „jogalkalmazás hatásának intenzitása az adatvédelem területén” természetesen már olyan indikátor, ami a hagyományosan értelmezett „szabályozási modell”-en kívül esik, nem a normák tartományát vizsgálja.

Mégis úgy gondoljuk, ha szabályozási módszerekről, szabályozási modellekről beszélünk, ma már igen helytelen lenne mind a jogpolitika tervezésénél, mind valamely ország szabályozása értékelésnél ezt az aspektust figyelmen kívül hagyni, ti., hogy milyen szerepet játszanak a jogalkalmazók a személyes adatok védelme területén. És itt nemcsak a bíróságokról van szó, hanem az adatvédelmi tevékenység felügyeletét ellátó nemzeti hatóságról, ami egyúttal a jogkövetés ellenőrzését ellátja.

Felfogásunk szerint, aminek alapjait tanulmányunkban kifejtettük, a francia CNIL, a belga *Commission de la protection de la vie privée*; a luxemburgi CCPD, stb. parakodifikációs szervek, érteve ez alatt azt, hogyha maguk szigorú értelemben nem is alkotnak általános szabályt, az általuk kibocsátott dokumentumok mégis egy kisebb személyi és nemzeti körre nézve magatartási normákat fogalmaznak meg. Például hoztuk a CNIL-nek azt a döntését, amely nem engedélyezte, hogy a hitelintézetek központi adatbankot létesítsenek a természetes személyek hitelállományáról.³²

De ide tartozónak tartjuk az összes olyan állásfoglalást, amelyeket a köz- és magánszférában működő adatvédelmi felelősök szerepének alkalmazási feltételeivel, függetlenségük biztosítékaival kapcsolatban adtak ki.

Szabályozási modellre jellemző ismérv az is, hogy az adatvédelem területének állami felügyeletét ellátó hatóság személyi állományát mennyire tekintélyesre tervezték, ki jelöli a személyeket, választottak-e vagy kinevezettek stb. Nyilvánvaló, hogy a jogalkotó választásából lehet bizonyos következtetéseket levonni a szervezet és az adatvédelem társadalmi beágyazottságáról, fontosságának elismertségéről. Csak zárójelben jegyezzük meg, hogy egy felmérés szerint a franciák 61%-a igen fontosnak tartja azt tudni, hogy vezethetnek-e róla nyilvántartást.³³

Ezzel a „fontossággal”, azaz a tárgykör társadalmi elismertségével függ össze, és ez egyben a szabályozási modelleket tekintve ismérvképző, hogy az adatvédelem mint törvényhozási tárgykör hol helyezkedik el a jogszabályok láthatatlan hierarchiájában. Szerencsésebben fogalmazva: mennyire jegyzett ez a törvény vagy jegyzettek azok a normák, amelyek a személyi adatok

védelmével függnek össze. Magunk részéről jellemzőnek tartjuk, hogy a *Dalloz Code Civil*-je több más norma mellett, ami a napóleoni *Code Civil* után született, de jelentős a civil élet szempontjából, tartalmaz olyat, ami a különleges (érzékeny) adatok védelmével függ össze.

A személyes adatok védelme társadalmi fontosságának, látszólag jogon kívüli problémája átvezet minket a szabályozási modellek vizsgálatának egy másik kérdéséhez, a szabályozás struktúrájához. Vizsgálódásaink végén úgy látjuk, hogy a szabályozási módszerek két, egymástól eléggé távol lévő, mondhatnánk ellentétes pont között szóródnak. Az egyik módszer egy jogszabályba több tárgykört (magánélet védelme, adatvédelem, közérdekű adatokhoz való hozzáférés) sűrít bele, viszont a végrehajtást, lényegileg a jogalkalmazó szervekre bízta. A másik szabályozási módszer több törvénnyel és több ágazatspecifikus jogszabállyal operál. (A távközlési törvényekben, például a német *Telekommunikationsgesetz*ben [2004] lévő adatvédelmi, adatkezelési szabályok tipikus példák erre.) E modellbe sorolhatónak tartjuk a magyar szabályozást. A magyar elektronikus információszabadság szabályozásáról több kritikus megjegyzést tesz Tényi Géza és Térey Vilmos (Tényi – Térey, é.n.).

Félreértés lenne azt hinni, hogy az első modellbe tartozó országok szabályozása nem használja a törvénynél alacsonyabb szintű szabályozás módszerét. A különbség csak az ágazatspecifikus jogszabályok számában van. Ez a megállapítás azonban nem hordoz magában értékítéletet: az elektronikus adatfeldolgozás annyi közigazgatási, de a gazdasági civiljog által szabályozott területe került alkalmazásra, hogy a túlszabályozottság vádjá nem lenne alapos első megközelítésben.³⁴

A szabályozási modell ismérvképző szempontja lehet az is, hogy mely ország joga jobban vagy kevésbé harmonizált a közösségi joghoz jelentést.³⁵ A luxemburgi adatvédelmi törvény tervezetéhez felkérésre készített szakvélemények tanulmányozása során láttuk, hogy itt nagyon kis véleménykülönbség már nagyon távoli álláspontok kialakulásához vezet. Magunk részéről úgy véljük, hogy az igazi modellkülönbségek akkor állapíthatók majd meg, ha az amerikai vízummentesség megadásával kapcsolatos tárgyalások befejeződnek az érintett országokkal, és akkor láthatjuk, hogy más országok átértelmezik-e a személyes adatok védelmét, illetve az Unió kívülre transzportálható adatok körét.

Felhasznált irodalom

David Calcutt's *Report of the Committee on Privacy and Related Matters* (1990) QC, Cmnd 1102, London, HMSO.

Goldwin, Mike (2003): *Cyber rights*. Massachusetts, The MIT.

Jahnel, Dietmar – Siegwart, Stefan – Fercher, Natalie (2007): *Aktuelle Fragen des Datenschutzrechts*. Wien, Facultas Verlags- und Buchhandels AG.

Roberts, Alasdair (2004): *Szervezeti pluralizmus a közigazgatásban és az információhoz való jog*. Fundamentum, 4. szám.

Tényi Géza – Térey Vilmos (é. n.): *Az adatvédelem és az információszabadság szabályozási kérdései a magyar és a közösségi jog fényében*. (Absztrakt)

Warren, Samuel – Brandeis, Louis (1890): *The Right to Privacy*. Harvard Law Review, 4. szám, 193–220.

Jegyzetek

¹ Ez a megállapítás az ún. *Calcutt Committee* jelentésében szerepel. A Bizottság készített egy definíciót: „The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information.”

² „The Australian Privacy Charter”. University of New South Wales, Sydney (1964).

³ Bundesverfassungsgericht definiert neues Grundrecht. ww.eulenspiegel.org/2008/02/07/page/3/

⁴ La justice allemande ouvert la voie à la surveillance des ordinateurs dans les affaires antiterroristes. *Le Monde*, 2008. 02. 27.

⁵ A szakirodalom megkülönbözteti a magánélet védelmében alkalmazott jogi módszerek között a „*comprehensive laws*”-t; a „*sectoral laws*”-t, a „*self-regulation*”-t és a „*technologies privacy*”-t. Privacy International (Overview of Privacy), 2007.12.17. www.privacyinternational.org/article

⁶ *The Times*, 2008. 02. 11.

⁷ A svédek 1973. május 11-én fogadták el adatvédelmi törvényüket, és az 1998. október 24-i törvénymódosítással harmonizálták azt a közösségi joggal.

⁸ Az Európai Parlament és a Tanács 2002/58/EC irányelve a személyes adatoknak az elektronikus ágazatban történő feldolgozásáról és magánjellegetek védelméről.

⁹ *Data Protection Review*, 2007. 06. 25.

¹⁰ Privacy International, i. m. 7. old.

¹¹ www.oecd-antispam.org. Lásd még: *Recommandation relative à la coopération transfrontière dans l'application des législations contre le spam*. [C(2006)57]

¹² www.oecd.org/dataoecd/12/48/38876531.pdf

¹³ A sikeres angol példa mellett megemlíthetők a francia erőfeszítések is. A kormányprogram (*Programme d'administration électronique* [ADELE] 2003. február 9-én indult, és természetesen számos, az adatvédelemmel kapcsolatos kérdést vetett fel, többek között azt, hogy mely adatok legyenek rögzítve és mennyi időre.

¹⁴ [www.Cnil.fr/index.php?id=1527&news\[uid\]=113&Hash=32fe...](http://www.Cnil.fr/index.php?id=1527&news[uid]=113&Hash=32fe...)

¹⁵ A világ előrehaladása az információs társadalom terén 1998–2008. [39. old.] www.ittk.hu/web/docs/ITTK_WPR_1998-2008.pdf

¹⁶ A számítástechnikai bűnözésről egyezmény (*Convention on Cybercrime*) született (ETS no.185, Council of Europe).

¹⁷ Art 29 Datenschutzgruppe: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_de.htm

¹⁸ www.datenschutz.de

¹⁹ www.privacycommission.be/fr/legislation/national

²⁰ www.datatilsynet.dk

²¹ www.dataprotection.gov.uk

²² www.garanteprivacy.it

²³ www.datainspektionen.se

²⁴ www.admin.ch/ch/f/rs/235_1/index.html

²⁵ www.svv.ch/index.ctm?id=852

²⁶ www.cnil.fr/index.php?id=301

²⁷ sos-net.eu.org/conso/tig/tigdata9.htm

²⁸ www.legifrance.gouv.fr/VVAspad/UnTexteDeJorf?numjo=JUSCO720211D-56k-

²⁹ *La Cour de cassation confirme le droit absolu de toute personne à ne pas figurer dans un fichier d'une organisation politique, philosophique ou religieuse.* 2004. 12. 17. www.cnil.fr/index.php?=48

³⁰ *La protection des données à caractère personnel en Belgique.* www.privacycommission.be/fr/static/pdf. [3. old.]

³¹ *Communiqué: Schéma de notification établi par la Commission nationale pour la protection des données.* 2003. 04. 09.

³² *La CNIL refuse la création d'un fichier central de crédit.* 2007. 04. 13. www.cnil.fr/index.php?id=1002

³³ CNIL. Communiqués. www.cnil.fr

³⁴ Ezt az állításunkat akkor is fenntartjuk, ha látjuk: az információs társadalommal kapcsolatos magyar jogszabályok száma – negyvenegy. Forrás: Információs Társadalom Koordinációs Tárcaközi Bizottság közreadott Jogtár. www.ikt.hu/engine.aspx?page=jogtar. Az más kérdés, hogy a bizottság által tervbe vett ajánlás az adatvédelmi előírásokról elkészült-e. www.ikt.hu/engine.aspx?page=showcontent=webtev. [Újraszabályozták a kormányzati webtevékenységet.]

³⁵ A Bizottság készítette e témáról jelentést [*Premier rapport sur la mise en oeuvre de la directive relative à la protection des données (95/46/CE)*]. Premier rapport, 2003. 05. 15., COM (2003) 265 final.

