

ÁTFOGÓ TÉMAKÖRÖK

Fejlesztés és működtetés

Ebbe a témakörbe tartoznak az alkalmazási rendszerek *létrehozásának és folyamatos működtetésének* teljes életciklusánál (igényfelmérés, tervezés, kivitelezés, bevezetés és üzemeltetés) használt módszerek és eszközök, beleértve a stratégiaalkotás, a fejlesztési munkafolyamatok és az állandó megújítás (innovációs) folyamatai technológiájának és szervezésének támogatását is.

Az informatikai rendszerek a technológia történelmében eddig nem tapasztalt mértékű *bonyolultságot* képesek elérni és *rugalmasságot* tudnak biztosítani az emberek számára. Bonyolultságuk és alakíthatóságuk kezdi közelíteni a biológiai rendszerekét.

A rendszerfejlesztés és -működtetés technológiai és munkaszervezési eszközeinek területén elért jelentős eredmények ellenére azonban az egyre összetettebb és kritikus feladatokat ellátó rendszerek a *határidőre* való elkészülés és *nagy megbízhatósággal* való működtetés terén továbbra sem felelnek meg a felhasználók – egyre növekvő – kívánalmainak.

A rendszerek bonyolult szoftverelemeit (például operációs rendszereket, adatbáziskezelőket) a kidolgozójuk gyakran termékként forgalmazza, azok működéséért, illetve továbbfejlesztéséért a felelősséget elvileg vállalja, ez azonban a gyakorlatban csak nehezen és töredékesen valósul meg.

Nagyon lényeges tendencia, hogy a bonyolultság növekedésével ez egyre inkább tarthatatlanná válik, és (többek között) ennek következtében jelennek meg a „nyílt forráskód” elvén alapuló megoldások, amikor a termékek karbantartását és követését a fejlesztők széles és jól együttműködő közössége végzi.

A szoftvertermékek felhasználásával kapcsolatos követelmények gyors és dinamikus változása párosulva a szoftver kézenfekvő és könnyen kivitelezhető módosításának igényével olyan új fejlesztési módszerek, valamint üzemeltetési és üzleti modellek kialakulásához vezet, amelyekben a termékek előállításával szemben a szolgáltatásszerű, azaz *szolgáltatásminőséget garantálni tudó* szempontok kerülnek előtérbe.

Ez egyrészt abban a *paradigmaváltásban* jelenik meg, hogy a hagyományos „programozás” helyébe a rendszerek meglévő – sok esetben webszolgáltatások formájában az interneten található és garantált – elemekből való összeépítése, integrálása lép. Másrészt a különböző alkalmazás- és infrastruktúra-üzemeltető cégek megjelenése, valamint a szoftver- és hardverelemek egységes IT-szolgáltatásokba történő beintegrálása mögött is ez áll.

1. Alkalmazásfejlesztés

Az alkalmazásfejlesztés fő célja, hogy egy adott felhasználói kör igényeit a lehetőségek szerinti legmagasabb szinten egy alkalmas szoftverrendszerrel kielégítse.

A szoftver különleges jellegzetessége, hogy technikai értelemben könnyű módosítani, ami nagyfokú rugalmasságot kölcsönöz az informatikai rendszereknek, ugyanakkor az ellenőrizetlen módosítások jelentős mértékben növelhetik a bonyolultságot, ami viszont alapvető problémát jelentettek az ilyen rendszerek létrehozásánál a kezdetektől fogva (ld. az először az 1960-as évek közepén jelentkező – majd utána többször „megújuló” – szoftverkrízis jelenségét).

Ma már jól látni, hogy a probléma az *egyszeri túl nagy változtatásban* és a *változtatások egyedi, nehezen ellenőrizhető jellegében* gyökeredzik. Az ilyen jellegű fejlesztés és működtetés merőben eltér a biológiai rendszerek kis változásokon és azonnali, egyértelmű teszten (ld. túlélés) alapuló fejlődési és működési modelljétől. Nem meglepő ezért, hogy a korszerű fejlesztési és működtetési módszerek igyekeznek ilyen biológiai indíttatású (gyorsfejlesztés, evolúciós fejlesztés, extrém programozás stb.) megközelítéseket alkalmazni.

1.1 Tervezési-elemzési nyelvek és támogató eszközeik

A tervezés-elemzés meghatározó szerepet játszik az alkalmazási környezetben és a technológiában bekövetkező változások megértésében és „átvezetésében” az alkalmazási rendszerekbe.

Ennek megfelelően egyre jobban integrálódnak az objektum-orientált elemzési-tervezési nyelvek, (melyek tényleges szabványa ma már egyértelműen a Unified Modeling Language, UML), másrészt az ún. üzletifolyamat-elemző (business process analysis, BPA) eszközök, valamint az adatbázistervezést támogató eszközök között. A következő öt évben várható, hogy az üzleti és technológiai modellek átláthatóvá és átjárhatóvá válnak az alkalmazásfejlesztés teljes életciklusában, és az üzletifolyamat-elemző (BPA), az UML-alapú modellező és az adatbázistervező eszközök – a versenyben megmaradó gyártóknál – egyetlen integrált eszközkészletté alakulnak át.

Az UML második verziója fogalmak szélesebb körét támogatja nagyobb következetességgel, és szűkíti a rést az üzleti és a műszaki követelmények között, azonban ezen új elemek szoftvertámogatásának elégtelenségei még késleltetik a terjedését.

1.2 Modellvezérelt és komponensalapú fejlesztés

Az alkalmazásfejlesztésben két tendencia érvényesül: az egyik az, hogy a teljes rendszer *modellekben*, azaz a további gépi feldolgozást lehetővé tevő, formális leírásokban fogalmazódik meg; a másik pedig, hogy a rendszer elemei egyre jobban – ha különböző mértékben is, de – szabványosakká válnak, azaz egyre inkább *standard komponensekből* épülnek fel.

A modellvezérelt alkalmazásfejlesztés a rendszer teljes, architekturális modelljéből indul ki, és két vagy több hierarchiaszinten keresztül finomítva és konkretizálva (például model driven architecture, MDA) jut el olyan modellekig, amelyekből már *programgenerálással* lehet az alkalmazási szoftver nagy részét automatikusan előállítani. Manapság az ún. „szolgáltatások” válnak a szoftverek komponensekre való felosztásának elsődleges egységeivé. Az – egymáshoz nyílt és szabványos felületen kapcsolódó – szolgáltatásokból a korábbinál jóval rugalmasabb architektúrával rendelkező szoftvereket lehet létrehozni (service oriented architecture, SOA).

Az architektúratervezésre, gyorsfejlesztésre, modellezésre és szolgáltatásszerű komponensekre alapuló megközelítéseknek a fejlesztés során való *együttes alkalmazásával* jelentős termelékenységjavulás érhető el. Ezt várhatóan olyan nyílt és széles körben használt keretrendszerek, illetve platformok teszik majd lehetővé, amelyeket mind az eszközyártók, mind a nyílt forráskódot támogatók, mind pedig a fejlesztők közösségei elfogadnak.

Azok az IT-szervezetek, amelyek modellvezérelt alkalmazásfejlesztést és szolgáltatásalapú keretrendszereket használnak a rendszerkomponensek létrehozására, kb. másfélszer *termelékenyebbek*, mint a hagyományos (3GL) integrált fejlesztési környezetek használói, és *reagáló képességük* is hasonlóan javul.

Nem véletlen ezért, hogy a nagy szoftverfejlesztő cégek ma már szolgáltatás-orientált architektúrára írják át alkalmazáscsomagjaikat, amely lazán integrált (és jellemzően már kész) ún. szolgáltatásokból építi fel. A SOA-ra való áttérés folyamán a legnagyobb kihívást az üzleti folyamatok és adatok *szemantikai egységesítése* jelenti, amelynek révén a gyakorlatban is ezen az új (szemantikai) szinten fog megvalósulni a folyamatok közötti együttműködésnek.

A SOA elterjedése a szoftvercsomagok licencvásárlása helyett a szolgáltatások *előfizetése* felé fogja eltolni a szoftverbevételeket, valamint a monolitikus szoftvercsomagoktól az *összetett alkalmazások* – azaz több, különböző szolgáltatásból összeépített alkalmazások – irányába való elmozdulást eredményez. Az elkövetkező években már az új alkalmazási szoftverekből származó bevételek nagy része SOA-t használó szoftvertermékekből realizálódik, akár hagyományos licenc-, akár előfizetési díjak formájában. Emellett a szoftverintegrátorok és a szoftvergyártók közötti megkülönböztetés egyre inkább elmosódik, ahogy az alkalmazási csomagokat részekre bontják, és azokat szolgáltatás-orientált alkalmazásként szállítják.

1.3 Nyílt forráskódú szoftverek

A nyílt forráskódú (open source software, OSS), licencköteles termékek piaci részesedése növekszik, és ez több szoftverpiacon is nyomást gyakorol a hagyományos, vásárolt szoftvermegoldásokra. Emellett a nyílt forráskód fejlesztésének bevált gyakorlata alapvető változásokat kényszerít ki az informatikai ipar szoftverfejlesztéshez, -elosztáshoz és -támogatáshoz való hozzáállásában. Ezek a hatások globális méretekben játszódnak le, és hamarosan megváltoztathatják a szoftverpiaci erőviszonyokat.

Az OSS-modell hatással van a szoftvert kifejlesztésének módjára, ugyanis a hangsúlyt a felülről jövő, szigorú ellenőrzéssel szemben az együttes és együttműködő erőfeszítésekre helyezi, valamint a szoftver támogatására is hatással van, mert a hangsúlyt a minőség biztosítása és a szoftver evolúciója terén közvetlenül a felhasználói közösségre helyezi. Mindez befolyásolja a szoftverek használati módját, előtérbe helyezve a szolgáltatásalapú kereskedelmi modelleket a szoftverlicenccel szemben: azaz a felhasználó nem magáért a szoftvertermékért fizet, hanem az annak hosszabb távú felhasználásához szükséges oktatási, testre szabási, karbantartási, üzemeltetési stb. szolgáltatásokért. A nyílt forráskódú szoftverek terjedése jól mutatja, hogy nem önmagában a szoftver kód az érték, hanem az a fejlesztői-üzemeltetői kapacitás, amely mögötte áll.

Mindazonáltal látni kell azt is, hogy a „nyílt forráskód” elsősorban a fejlesztő számára igazi érték: ő ért hozzá, tud tanulni belőle, tud átvenni megoldásokat, és cserében a saját maga által fejlesztett kódot – hasonló feltételekkel – fel tudja ajánlani a tágabb fejlesztői közösség számára. A végfelhasználó (azaz az emberiség túlnyomó többsége) számára azonban továbbra is csak a szoftver által nyújtott és kezelt információ az érték.

1.4 Alkalmazásintegráció

Ellentétben a hagyományos szoftverfejlesztés „először programozni” (és csak azután összeépíteni) megközelítésével, mind a vállalatokon belül, mind a szélesebb (web, illetve

web 2.0) felhasználói körben egyre inkább terjed az *integrációs megközelítés*: azaz, hogy elsődlegesen meglévő szoftverelemek (például webszolgáltatások) összetételével állítani elő alkalmazásokat, és csak ezután foglalkozni azzal, hogy kell-e valamit az így összeállt alkalmazáson esetleg programozással módosítani. Az alkalmazásintegráció a szoftveripar területén az innováció fő hajtóereje volt az elmúlt évtizedben, amely a vállalati informatikán belül alakult ki, de hamar átvette a webközösség is, és az ún. *montázsstecnika* (mashup) néven a web 2.0 szerves részévé tette.

A jövőbeni alkalmazásintegrációs környezeteknél stabil elemként várható valamilyen központi, *integrált metaadattár* használata, amely az integrációval kapcsolatos összes metaadat egységes kezelését biztosítja. A nem alkalomszerűen végzett integrációnál, például a vállalati IT-infrastruktúrában *szolgáltatásbuszok* (Enterprise Service Bus, ESB) megjelenése várható, mint a köztesszoftverek új típusa, amelyek ötvözik a korábbi köztesszoftverekben található tulajdonságokat. Az ESB-ek szolgáltatásregisztrációt és -felkutatást tesznek lehetővé, a kommunikációban rugalmasságot, és általában a szolgáltatásminőség magasabb szintjét biztosítják. Az ESB-eket ki lehet majd terjeszteni teljes integrációs keretrendszerre is, üzletifolyamat-kezeléssel, B2B-képességekkel és alkalmazási adapterekkel bővítve.

Az alkalmazásintegráció egyéb, jelen pillanatban periférikusnak számító technológiai és platformjai például az ágensalapú integrációs eszközök, a szótár- (pontosabban: ontológia-) alapú transzformációs eszközök és az ún. vállalati információintegráció (Enterprise Information Integration, EII) is hatalmas lehetőségeket rejtenek magukban, és a szoftverinfrastruktúrák területén belül várhatóan itt történik majd a legtöbb innováció.

2. Szoftverminőség-menedzsment

A szoftverminőség nem azonos a műszaki kiválósággal (technical excellence), mert magában foglalja a gazdasági szempontokat is. Alapvetően négy dimenzió mentén célszerű vizsgálni:

- 1) *használati* (funkcionális) *tulajdonságok*, azaz milyen mértékben alkalmas a tervezett használatra;
- 2) *működési* (nem-funkcionális) *tulajdonságok*, azaz milyen mértékben áll megbízhatóan rendelkezésre a használathoz;
- 3) *szállítási idő*, azaz mennyi idő szükséges a szoftver létrehozásához vagy megváltoztatásához;
- 4) *ráfordítás*, azaz mennyi munka szükséges a szoftver létrehozásához vagy megváltoztatásához

Ennek értelmében a jó minőségű szoftver olyan optimális állapotnak felel meg, ahol a lehetséges mértékű *ráfordítás* a szükséges információkezelési *tulajdonságok* elegendően rövid *szállítási idő* alatti előállítását teszi lehetővé. A szoftverminőség-menedzsment lényegében e négy dimenzió folyamatos kiegyensúlyozását, és a szoftver (ilyen értelemben vett) optimálishoz közeli állapotban való tartását jelenti, amely a szoftverminőség folyamatos monitorozását is igényli. Ehhez nyújtanak támogatást a szoftvermetrikák, illetve az ezeken alapuló hibahajlandósági, karbantarthatósági, változtathatósági, megérthetőségi modellek, valamint a problémás programrészek azonosítása és ezek (fél)automatikus transzformációja (refactoring).

2.1 Teszt- és vizsgálati módszerek

Tipikus, hogy a teljes szoftverfejlesztési ráfordítás közel felét a tesztelési, karbantartási költségek jelentik. Ezért várható olyan szoftvertechnológiai módszerek széles körű elterjedése, amelyekkel ezek a költségek jelentősen csökkenthetők. Azok a szervezetek, amelyek ilyen módszereket nem használnak már a közeljövőben ki fognak szorulni a szoftverfejlesztési piacról.

A gyakran több millió soros rendszerek változtatását és – ehhez kapcsolódóan – folyamatos tesztelését segítik az ún. *regressziós tesztelési eljárások*, amelyek segítségével lehetőség nyílik arra, hogy csak a változások miatt módosult részeket és azok hatásait kelljen újra tesztelni. Ez a technológia a forrásprogramok nagyon pontos függőségi analízisén (szeletelés) alapul, amihez sok technikailag nehéz problémát kell megoldani, például statikus hivatkozások hatékonyság analízise.

A szoftverminőség fontos dimenzióját alkotó, nem-funkcionális tulajdonságokat (teljesítmény, rendelkezésre állás, folytonosság és biztonság) különböző – összefoglaló néven – *teljesítménytesztelési eszközökkel* lehet ellenőrizni és mérni. A távolabbi jövőben pedig a nagy szoftverrendszerek új (például webes) környezetbe való *bevezetésénél* (migration) segíthetnek sokat az olyan módszerek, amelyek segítségével automatikusan megállapíthatók e rendszerek bizonyos funkcionális tulajdonságai (aspect mining), illetve tervezési struktúrája (design pattern recognition).

Növekvő szerepet kapnak a jövőben a különböző tesztelési és egyéb vizsgálati módszerek menedzsmentjét (például ütemezését, automatikus végrehajtását) biztosító ún. *tesztmenedzsment-eszközök*.

2.2 Érettségi modellek

A szoftverminőség *szervezeti szintű* garantálásának több mint két évtizede megalkotott ún. képességérettségi modellje (Capability Maturity Model, CMM) egyre szélesebb körben terjed, mivel megújított, integrált változata (Capability Maturity Model Integrated, CMMI) még jobban megfelel a mai korszerű szoftverfejlesztési szemléletnek. A CMMI több szintű folyamat- és szervezetcélmérési megközelítése lényegesen alaposabb és finomabb értékelésre és javaslatételre ad lehetőséget, mint például az ISO 9001 szerinti felülvizsgálat.

A CMMI kiegészítve a fejlesztő csapatokra (Team Software Process, TSP) és a fejlesztőkre, mint egyénekre (Personel Software Process, PSP) szabott fejlesztési folyamattal igen hatásos eszköz lesz a következő évtizedben is a szoftvergyártással foglalkozó szervezetek számára a szoftverminőség garantált és gazdaságos biztosítására. Nem véletlen, hogy a nagy európai IT-tanácsadó és rendszerintegrátor cégek stratégiai célul tűzték ki a CM-modell 3-5. szintjének elérését.

2.3 Szoftverprojekt-menedzsment

A szoftverminőség-menedzsment talán legfontosabb területe a fejlesztési projektek menedzsmentje: ennek keretében lehet csak a szoftverminőség mind a négy dimenzióját, azaz a használati és a gazdasági szempontokat egyaránt kiegyensúlyozni.

A projektmenedzsment területén ma két módszert lehet elterjedtnek tekinteni: a PMBOK-ot (Project Management Body Of Knowledge) a PMI-től (Project Management Institute), illetve a PRINCE-t (PRojects IN Controlled Environment) az APM Group-tól (Association of Project Managers). Mind a két módszer igen kiértékelt megközelítés, amelyeket számos projekten sikeresen alkalmaztak. A különbségek nem lényegesek,

inkább szemléletbeliek. Várható, hogy e két módszer (illetőleg újabb változatai) a következő évtizedben is meghatározó szerepet töltenek be azoknál a szervezeteknél, amelyek a projektjeik irányítására megbízható és intézményesíthető megoldásokat keresnek.

A projektmenedzsment általános módszereinek és eszközeinek fejlődése mellett tovább terjednek a fejlesztést, mint *csoporthatást támogató eszközök* (groupware), amelyek figyelembe veszik a fejlesztő csapatok gyors átalakításának (rekonfigurálásának) igényeit is.

A szoftverfejlesztés menedzsmentjében ma már jelentős szerepet játszanak a különböző gyorsfejlesztési módszerek (Rapid application Development) is, amelyek gyakran műszakiterv-vezéreltek (design-driven) és felhasználó-orientáltak a fejlesztés gyors és iteratív megvalósítása érdekében. A gyorsfejlesztési módszereken belül az alábbiak segítségével a fejlesztés kockázatának radikális csökkentése érhető el:

- a követelmények fokozatos (iteratív) feltárása a felhasználók intenzív bevonásával,
- az architektúra folyamatos hozzáigazítása a követelményekhez,
- a programozás jelentős részének kódgenerálással való kiváltása és
- a projektadminisztráció minimálisra csökkentése.

Az ilyen fejlesztési megközelítéseket gyakran ún. *agilis módszereknek* is nevezik, amelyek közé tartozik például a DSDM (Dynamic System Development Method), a SCRUM és az XP (eXtreme Programming).

A szoftverfejlesztési projektek javításának új irányát képviselik az *empirikus, kísérleti megközelítések* (experimental software engineering), amelyek alapelve, hogy csak olyan változtatásokat szabad végrehajtania folyamatokban, amelyek kimutathatóan és bizonyíthatóan eredményeket hoznak a szoftverminőségben: ne elfogultan az eszközökön vagy a módszereken legyen a hangsúly, hanem mindig az eredményt, illetve a legjobb eredményt hozó megoldásokat valósítsák meg.

3. IT-szolgáltatásmenedzsment

Az IT-szolgáltatásmenedzsment szűkebb és eredeti értelmezésben az informatikai rendszerek üzemeltetésével és ezen belül is elsősorban az IT-infrastruktúra fenntartásával foglalkozó tevékenységkör volt. Ma már azonban a szolgáltatásmenedzsment fogalmát kiterjesztik az *IT-rendszerek teljes életciklusára*, azaz az előkészítés (stratégia), a fejlesztés, a bevezetés és az üzemeltetés szakaszaira, valamint ezek folyamatos továbbfejlesztésének tevékenységkörére.

A vállalati informatika korszerűsítése során egyre nagyobb mértékben tölt be *integráló szerepet* ez a 2000 óta egyébként is erősödő IT-szolgáltatásmenedzsment tevékenységi kör, amellyel *egyensúlyt lehet teremteni* a tárgyi jellegű IT-erőforrások (például hardver, szoftver) és a nem-tárgyi, szellemi jellegű IT-képességek (például folyamat, kultúra, tudás) között. És bár kétségtelen, hogy az IT-szolgáltatásoknál egyre meghatározóbb az automatizálás szerepe, az automatizálásban fennálló esetleges hiányosságokat és elégtelenségeket ilyen módon az IT-szolgáltatásmenedzsmenttel mindig át lehet hidalni. Ez a hangsúlyeltolódás a következő évtized első felében már megmutatkozik abban is, hogy a hardverköltések és a karbantartási munkaköltségek helyett a szolgáltatásmenedzsment működtetésének és menedzsmentszoftverek költségei lesznek a meghatározóak. Az IT-szolgáltatásmenedzsment folyamatos fejlesztésének képessége

egyre fontosabbá válik mind a belső, mind a külső IT-szolgáltatóknál olyannyira, hogy a piacszerzés eszköze és a versenyben maradás feltétele lesz.

3.1 ITIL

Az ITIL (IT Infrastructure Library) a legismertebb és legjobban elterjedt megközelítés az IT-szolgáltatásmenedzsment területén. Az 1980-as évek végén eredetileg az IT-infrastruktúra menedzselésére létrehozott ajánlásgyűjtemény, 2000-tól kezdve nötte ki magát a *szolgáltatásmenedzsment nemzetközi szinten is meghatározó keretrendszerévé*, amely alapján hozták létre az IT-szolgáltatásmenedzsment ISO/IEC 20000-es nemzetközi szabványát is. A felgyülemlett tapasztalatok alapján az ITIL-t 2007-ben ismét megújították, és az ekkor kiadott harmadik verziója szerinti szolgáltatásmenedzsment ma már *szolgáltatási életciklusra* épül, amely öt tevékenységekörből áll.

A *szolgáltatásstratégia* tevékenységei határozzák meg, hogy milyen célokat követve, milyen irányelveket betartva, milyen szolgáltatásokat kell nyújtani rövid, illetve hosszabb távon. A *szolgáltatástervezés*, *-bevezetés* és *-üzemeltetés*, az életciklus egymásra épülő szakaszai ezt a stratégiát valósítják meg, és ezek során jönnek létre, változnak és alakulnak át a szolgáltatások. Végül az *állandó szolgáltatásfejlesztés* keretében valósul meg a szervezeti szintű tanulás, és hajtódik végre a szolgáltatások továbbfejlesztése megfelelő intézkedések, projektek és programok segítségével.

Az ITIL v3 felfogásában az IT-szolgáltatás, azaz az informatika szolgáltatásszerű nyújtása, a szervezetek *információval való ellátásának*, és ezen keresztül a számukra történő *értékteremtésnek* olyan módja, amely a szervezet számára szükséges információkat, és az ezáltal elérni kívánt eredményeket anélkül biztosítja, hogy bizonyos (például tulajdonlásból származó) költségeket és kockázatokat az adott szervezetnek vállalnia kellene.

Az ITIL szolgáltatási életciklusa *ismétlődő jellegű és többdimenziós*, amely biztosítja, hogy a szervezet eszközei és képességei egymással kiegyensúlyozottak legyenek, és minden körülmények között alkalmasak a mindenkorai szolgáltatási célok elérésére. Olyan PDCA-modellre épülő, zártkörű szabályozó rendszert alkalmaz, amely mindenfajta változtatást be tud fogadni és meg tud valósítani – legyen az stratégiai, taktikai vagy akár operatív szinten megfogalmazva.

3.2 Közműszerű IT-szolgáltatás

Az üzleti és egyedi felhasználók IT-alkalmazásokra és -infrastruktúrára vonatkozó igényeit egyre inkább „erőforrásraktárak”-ból elégítik ki és nem egyedi, specializált erőforrásokkal. Az ilyen ún. informatikai közmű típusú szolgáltatás magában foglalja mind az infrastruktúra-, mind az alkalmazásszolgáltatásokat.

A közműszerű IT-szolgáltatás úgy határozható meg, mint egy olyan stabil, megbízható, gyakran a szolgáltatás minőségére vonatkozó megállapodásokkal külön is garantált, *tömegigényeket* kielégítő szolgáltatása informatikai kapacitásoknak és funkcióknak, amely mögött korszerű, hatékonyan működtetett IT-infrastruktúrák állnak.

A közműszerű IT-szolgáltatás legkorábbi formája a *grid*, amelyet eredetileg kutató intézetekben, egyetemi kutatóhelyeken használtak és fejlesztettek ki azon célból, hogy a nagy számú, kihasználatlan számítógépes (többnyire PC-s) erőforrást nagy számítási igényű feladatok megoldására egységes infrastruktúrába lehessen szervezni. Jellegetessége ennek a megközelítésnek, hogy nem épít ki külön hardver- és hálózati

infrastruktúrát (különösen nem speciális számítóközpontokat), hanem a meglévő, szigetszerűen működő kapacitásokat valamilyen köztesszoftver segítségével szuperszámítógép-teljesítményű *virtuális infrastruktúrává* egyesíti. Legújabb és legperspektivikusabb formája viszont az az ún. *hiperszámítástechnikai* (cloud computing) megközelítés, amikor igen nagy mértékben és mindkét irányban (lefelé és felfelé is, azaz *elasztikusan*) skálázható eszközeiket, valamint IT által támogatott képességeiket a szervezetek „szolgáltatásként” nyújtják nagy számú, külső ügyfelük számára internet-technológiák felhasználásával. Jellegzetessége ennek a megközelítésnek, hogy korszerű, szerverek ezreit alkalmazó, specializált (hiper)számítóközpontokat épít ki, és alkalmaz a közműszerű szolgáltatásnyújtásra. Ez a 2007-ben megjelent hiperszámítástechnikai megközelítés biztosítja leginkább a nyílt, egységes hozzáférést, de – eltérően a gridtől – alapvetően piaci orientáltságú. A mai elnevezési szokás szerint lehet akár *IT Utility 2.0*-nak is nevezni, azaz a web 2.0 korszakában használatos informatikai közműnek.

Biztonság

Az elmúlt évtizedekben bekövetkezett egyik legszokatlanabb gazdasági-társadalmi változás az, hogy egyrészt a legkülönbözőbb szervezetek működésében – mind üzleti, mind közszolgálati területen –, másrészt az egyének szintjén is eddig nem látott mértékben megnövekedett a *függés az információtól* és különösen az azt kezelő informatikai rendszerektől. Nem meglepő ezért, hogy előtérbe került az információ-biztonság, amelynek célja – a szervezetek információellátásában zavarokra vezető *gyenge pontok és veszélyek* meghatározása mellett – olyan *védintézkedések* meghozatala és megvalósítása, amelyek a fellépő kockázatok kezelésével és egyéb követelmények teljesítésével az *információellátás folyamatos működését* biztosítják összhangban a szervezet általános biztonsági és működési céljaival. De nem lehet meglepő az sem, hogy az egyéneknél a *magánélet* (privacy) védelme fokozott jelentőséget kap a megnövekedett veszélyek miatt.

A biztonság témakör két, az IKT-k iránti bizalom megeremtését szolgáló területet fog össze. Az egyik az *információbiztonság*, a másik pedig a *magánélet-védelem*. Ez utóbbi terület európai viszonyok között leginkább a személyes adatok védelmének kérdéseként értelmezhető a gyakorlatban. Az információbiztonság a szervezeti értelemben vett biztonság megeremtésének eszköze, míg a *személyesadat-védelem* a felhasználóknak és az ügyfeleknek az egyre növekvő kiszolgáltatottsággal szembeni biztonságérzetének megőrzését elősegítő eszköz.

Az információbiztonság egyik meghatározó pillére az *informatikabiztonság*, amely alatt az informatikai rendszerek és eszközök (szoftver, hardver vagy ezek együttese) elvárt működését (biztonságos működését) akadályozó vagy veszélyeztető kockázatok (cselekmények, külső hatások vagy ezek következményeként előálló állapotok) elleni *védetség* értendő. Az informatikabiztonság (biztonságos működés) – definíció szerint – csak a konkrét használati cél alapján *egyedileg meghatározható minőség*, ami ugyanakkor azonban nem zárja ki a tipizálás lehetőségét. Az „informatikai rendszer és termék” kifejezés az üzemeltetést és használatot is átfogó széles értelemben használatos, ahol az informatikai rendszerekbe az internetes alkalmazások és szolgáltatások növekvő szerepére való tekintettel beleértendők az adatátviteli-távközlési hálózatok is. Nem tekintendő ugyanakkor – szűkebb értelemben – az informatikabiztonsági kérdések közé tartozónak azon fejlesztéshez és üzemeltetéshez kapcsolódó minőségbiztosítási kérdések, amelyek ugyan hatással vannak az informatikai termékek és rendszerek biztonságára, de biztonsági kockázatok hiányában nem okoznak problémát.

Az információbiztonság és a személyes adatok védelme az IKT világában szorosan összekapcsolódik. A két terület egyszerre van *egymást kiegészítő és egymásnak ellentmondó* viszonyban. A kiegészítő viszony annak köszönhető, hogy a személyes adatok kezelése során az adatok védelme információbiztonsági megoldások nélkül elképzelhetetlen. A kezelt személyes adatok védelmének nézőpontjából az információbiztonság egyike azon kérdéseknek, amelyek megfelelő kezelése *elengedhetetlen tényező* a személyes adatok védelmében.

A magánélet védelmének azon aspektusa azonban, amely a személyes adatok kezeléséhez való jogosultság megszerzéséhez kapcsolódik már ellentmondásokhoz vezet a két terület között. Az információbiztonság megeremtésében ugyanis rendkívül fontos szerepet

játszik a felhasználók megfelelő azonosítása, valamint a felhasználókról történő kiterjedt adatgyűjtés az egyes biztonsági eseményekért való felelősségnek a későbbi megállapíthatósága érdekében. Az információbiztonság megteremtésének nézőpontjából ezért a személyes adatok védelme az információbiztonság megteremtését *akadályozó tényező*ként is jelentkezik a gyakorlatban.

1. A biztonság területének főbb változásai

A biztonság területén várható átfogó, legfontosabb tendenciák a következők:

- a kockázatok növekedése,
- a proaktív kockázatkezelés előtérbe kerülése,
- a polgári célú kriptográfia szerepének erősödése,
- az információbiztonság és az adatvédelem között feszülő ellentmondás csökkenése.

Az IKT használati körének kiterjedésével egyidejűleg folyamatosan nőttek a *biztonsági kockázatok* az információbiztonság és magánélet-védelem területén is. Ez az elkövetkező évtizednek is általános trendjeként fog megmaradni.

Az IKT használatát érintő biztonsági kockázatok kezelése az elmúlt időszakban elsősorban *reaktív* volt. Az ok, hogy a biztonsági szempontokat – a legtöbb esetben – a *fejlesztés fázisában* nem érvényesítik. Az információbiztonsági és adatvédelmi kockázatok ezért növekednek automatikusan az IKT-eszközök intenzívebb használata következtében. A biztonsági szempontok érvényesítésének elmaradása a fejlesztés fázisában azt eredményezi, hogy a biztonsági kockázatok csak utólagos, reaktív eszközökkel kezelhetők. Ennek a helyzetnek elsődlegesen az az oka, hogy a biztonságos IKT előállítására hosszabb időt igényel és többletköltségekkel jár, amit a piac rövidtávon nem nagyon honorál. Emellett azonban fontos szerepet játszik az a tény is, hogy kellő biztonsági szintet garantálni tudó *termék- és rendszerfejlesztési módszertanok* nem voltak eddig használatban.

A következő évtizedben nagy előrelépés várható ezen a területen. A biztonsági kockázatok csökkentését és kezelését szolgáló technológiák, értékelő és auditmódszertanok, gyakorlatok, valamint szabályozási eljárások gyakorlati alkalmazásának általánossá válása a következő évtizedben elkerülhetetlenül be fog következni. Ennek eredményeként a biztonsági kockázatok kezelésében a hangsúly a reaktív megoldásokról a *proaktív megoldások irányába* tolódik el.

Ezt erősíti az is, hogy – ha egy évtizednyi vajúdas után is, de – 2005 végén megegyezés született az az információbiztonság-menedzsment (Information Security Management, ISM) nemzetközi szabványában (ISO/IEC 27001). Nemzetközi szinten is egyértelművé vált, hogy az információbiztonság legmagasabb, menedzsment szintjén milyen követelményekkel kell szembe nézniük azon szervezeteknek, amelyek ISM-rendszereik kiválóságára törekednek, és ezen belül a proaktivitást helyezik előtérbe. Jól alátámasztja ezt a várakozást az is, hogy ennek a proaktivitásnak és a fejlesztésre – sőt a termékek, rendszerek és szolgáltatások *teljes életciklusára* – kiterjedő *biztonságtudatosságnak* a jegyében született meg az IT-szolgáltatásmenedzsment nemzetközi szabványának (ISO/IEC 20000) követelményrendszere, majd 2007-ben az ITIL v3 ajánlásgyűjteménye is.

A *kriptográfiai technológiák* a bizalmasság, az azonosítás és hitelesítés megvalósításának legfontosabb eszközei, és ebből adódóan kiemelt szerepet játszanak az

információbiztonság és a magánélet-védelem területén is. Az információbiztonság és az adatvédelem számára is nélkülözhetetlenek ezért a polgári célú kriptográfiai technológiák, amelyeknek a folyamatos felértékelődése várható. Emellett a hitelesítés céljára használt kriptográfiai megoldásoknak a bővülő számítási kapacitások és a javuló teljesítmény miatti avulása azt eredményezi, hogy a kizárólag kriptográfiaiak mellett előtérbe kerülnek a *hitelességmegőrzési eljárások és szolgáltatások*.

A jelenleg használt kriptográfiai megoldások avulásának ütemében nem várható nagy változás, bár matematikai felfedezések bármikor eredményezhetik az éppen használt kriptográfiai eszközpark lecserélését. Ha azonban a technológiai fejlődés oldaláról nézzük a kérdést, akkor nem várható az avulás ütemének felgyorsulása. Például a *kvantumszámítástechnika* megjelenése a *nyilvános kulcsú kriptográfián* alapuló biztonsági és hitelesítési megoldásokat elavulttá teheti, ugyanakkor gyakorlatban használható kvantumszámítógépek megjelenése a következő évtizedben még nem várható.

Az IKT világában az elmúlt húsz évben az információbiztonság és az adatvédelem ellentmondásos viszonya jellemezte a biztonság átfogó területét. A jelenlegi ellentmondásos helyzet várhatóan a következő évtizedben is fennmarad, azonban az ellentmondások kiélezettsége csökkenni fog. Ennek a háttérben az áll, hogy a biztonsági kockázatok kezelésében a reaktív megoldások szerepe háttérbe szorul, ezáltal pedig csökken az információbiztonság területén a *személyes adatok gyűjtése és hosszú idejű tárolása* iránti igény.

Várható továbbá, hogy a következő évtizedben az informatika szolgáltatása és védelme *még szorosabban egymásba fonódik*, és szabványos, ugyanakkor (a biztonságra is) különböző garanciaszinteket biztosítani tudó *információszoftvertársaság* alakul át.

2. Információbiztonság

2.1 Kockázatok

Az információbiztonsági kockázatok könnyen számszerűsíthetők, mivel az információ, egy-egy dokumentum illetéktelenek kezébe vagy nyilvánosságra kerüléséből, továbbá informatikai rendszerek rosszindulatú támadások eredményeként előálló időleges vagy végleges *működésképtelenségéből* potenciálisan származó kár mértéke elég jól meghatározható.

Az információbiztonsági kockázatok változása ezért szorosan összefügg az informatikai eszközök és rendszerek *üzleti értékével*, sőt megállapítható, hogy az IKT üzleti folyamatokban betöltött szerepének növekedésével együtt nőnek az információbiztonsági kockázatok. Tekintettel arra, hogy az üzleti folyamatok IKT-függősége folyamatosan nőni fog a következő évtizedben, az információbiztonsági kockázatok tartós növekedésére lehet számítani.

Az információbiztonsági kockázatok jövőbeli alakulása azonban a technológiai változások mellett a *potenciális támadók* körének jövőbeli alakulásától is függ. Az informatika korai időszakát jellemző individuális elkövetők helyébe az elmúlt időszakban egyre inkább a professzionális, jól szervezett, elkövetői csoportok léptek. Ez a folyamat várhatóan tovább fog erősödni.

2.2 Információbiztonsági technológiák

Az információbiztonsági technológiák köre igen széles. Ide sorolhatók mindazok a hardver- és szoftvereszközök, amelyek az információbiztonsági kockázatok csökkentését segítik. Egyes *reaktív információbiztonsági eszközök* (például vírusirtó, tűzfal) használata mára már általánossá vált. Az azonosítási megoldások is sokat fejlődtek az elmúlt évtizedben. Ennek a területnek a következő évtizedben tapasztalható nagy változása lesz, hogy az egyfázisú azonosítást fokozatosan és általánosan kiváltják a *kétfázisú azonosítási megoldások*.

A biztonsági kockázatok elleni proaktív védekezés előtérbe kerülése a technológiák szintjén elsősorban a szoftverfejlesztés átalakulásában ragadható meg. Ennek a változásnak egyik legfontosabb eredménye az lesz, hogy a következő évtized második felére általánossá válik az információbiztonsági szempontok figyelembe vétele a *termékek és rendszerek tervezése* során is. Néhány jellemző példája ennek a folyamatnak a Microsoft Trustable Computing Platform-jának megjelenése, valamint az olyan tervezési módszerek, specifikációk kialakulása és használatának általánossá válása, mint a USA CERT Survivable Systems Engineering kutatásainak eredményeként előálló módszertanok, a Trustable Computing Group biztonsági specifikációi, valamint az internetprotokolljainak biztonsági igényeket is figyelembe vevő változatának gyakorlati elterjedése (IPv6-ra történő átállás).

Az egysíkú, csupán néhány fenyegetettségre koncentráló megelőző típusú védekezést felváltja a többszintű, *átfogó behatolást megelőző* rendszerek használata.

2.3 Üzemeltetés

Az információbiztonság fenntartásában kiemelkedő és meghatározó szerepe van az IT-üzemeltetés során végzendő *megfigyelési és mérési tevékenységnek*. A paradox helyzetet az adja, hogy ezek megfelelő szinten történő végrehajtására csak akkor van esély, ha az IT-rendszerekbe eleve bele lettek tervezve az ehhez szükséges megfigyelési és mérőpontok a fejlesztés során, valamint ki lettek alakítva, és be lettek vezetve a szükséges eszközök. Erre épülhet rá aztán egy olyan *eseménymenedzsment* tevékenység, amely a megfigyelési információkat összevetve és értékelve – a lehetőség szerinti legnagyobb mértékben automatizálva – kellő időben való reagálást tesz lehetővé a várhatóan bekövetkező, kisebb-nagyobb üzemzavarok különböző szintű kezeléséhez (*incidens-, probléma és folytonosságmenedzsment*).

Az üzemeltetés során biztonsági szempontból kiemelt szerepet kap a *hozzáférésellenőrzés* a személyazonosság ellenőrzésében és a jogosultságok kiosztásában. Komplexitása miatt (sok rendszer, sok felhasználó, összetett jogosultsági viszonyok, áttekinthetőség igénye) ma már jellemzően specifikus szoftvereszközöket használnak erre a célra. Végül az információbiztonsággal kapcsolatos fenti tevékenységek alapját szerteágazó, *napi szintű feladatok végrehajtása* képezi az *adatmentésektől* a különböző *rendszer- és adatbázisadminisztrációs* munkákig.

Az ezen tevékenységekhez és eszközökhöz szükséges, egyre specifikusabb IKT-szaktudás és -kapacitás miatt a kis- és közepes méretű vállalkozások körében fokozatosan általánossá válik a *biztonságrendszer-felügyelet* külső szolgáltatáson keresztül történő biztosítása. A nagyobb vállalatoknál a belső IT-szervezetnek kell végeznie vagy legalábbis koordinálnia az üzemeltetést, amelynek megvalósításánál a következő évtizedben még feltétlenül meghatározó szerepe lesz az ITIL vonatkozó ajánlásainak. Emellett azonban itt is egyre növekvő mértékben vannak be külső szolgáltatókat, ami az

évtized második felében már jellemzően *közműszerű IT-szolgáltatás formájában* valósul meg.

2.4 Információbiztonsági értékelés és tanúsítás

A különböző értékelési és tanúsítási megközelítések egyre fontosabb szerepet játszanak az IKT biztonsága és megbízhatósága tekintetében, amelyeket részben *állami szabályozás* ír elő, részben bizonyos gazdasági szektorok, területek *ön szabályozása* révén válik kötelező előírássá. Ilyen a NATO-beszállítók előzetes értékelése és tanúsítása, a pénzügyi szektort érintő követelmények megjelenése (Basel II), vagy a New York-i tőzsde cégeire vonatkozó Sarbanes-Oxley törvény (2002).

További konszolidáció várható a jelenleg versengő biztonsági szabványok és tanúsítási rendszerek között (ISO/IEC 27001, a COBIT és az ISO/IEC 15408 – Common Criteria), és egyre inkább a piacon maradás feltétele lesz a megfelelő tanúsítvány megléte. E megközelítések közös jellemzője, hogy *komplex átfogó megoldásokat* kínálnak az információbiztonsági problémák kezelésére. Fontos azonban azt is látni, hogy az egyes megközelítések esetében a hangsúlyok eltérnek. Így például a Common Criteria az IKT-rendszerek és -eszközök *biztonsági értékelésére* használatos, az ISO/IEC 27001 elsősorban az *információbiztonság menedzsmentfolyamatainak* megítélésére, a COBIT-ot pedig a felelős, számonkérhető és *átlátható IT-irányítás* vizsgálatánál alkalmazzák. Várható, hogy ez a *munkamegosztás tovább erősödik*, ugyanakkor az egyes elemek jobban fognak egymáshoz illeszkedni. A jelenleginél is határozottabban elválnak a menedzsmentjellegű, a rendszer- és eszközszintű biztonsági szabványok, és az ezekre épülő értékelési és tanúsítási rendszerek, valamint az egyes szinteken történő értékelést és tanúsítást támogató technológiák. Ezzel párhuzamosan általánossá válik a biztonsági követelményeknek való megfelelést vizsgáló és ellenőrző, a biztonsági előírások kikényszerítését támogató *IT-alkalmazások használata*.

3. Magánélet, személyes adatok védelme

3.1 Adatvédelmi kockázatok

A személyes adatok kiterjedt használatában rejlő kockázatok – az információbiztonsági kockázatokkal ellentétben – nehezen fejezhető ki pénzügyi vagy más könnyen mérhető mutatókkal. Az adatvédelmi kockázat ugyanis az *egyének kiszolgáltatottságának mértékében* ragadható meg. A kiszolgáltatottság azonban nagyon relatív érték: kultúránként, életkorunként, de akár élethelyzetünként is eltérő lehet, hogy mikor érzi valaki magát kiszolgáltatottnak. Ettől a szubjektív megítélésből adódó bizonytalanságtól eltekintve kijelenthető, hogy: *minél több egyénre vonatkozó adat* érhető el mások számára, annál inkább növekszik a kiszolgáltatottság kockázata, és ez független attól, hogy hol található az a pont, amit valaki esetleg konkrétan problémásnak talál.

A számítási, adattárolási és adatátviteli kapacitások bővülését eredményező új technológiák megjelenése általánosságban növeli az adatvédelmi kockázatok szintjét. Az IKT-eszközök és -szolgáltatások használatának növekedésével egyidejűleg nő az ezen eszközök által gyűjtött és kezelt adatok mennyisége. Különösen a *személyazonosítást* is lehetővé tevő technológiák (például RFID, mobiltelefon-, internethasználat) megjelenése, elterjedése és általánossá válása járult hozzá eddig a kezelt *személyes adatok mennyiségének* – és ezáltal az adatvédelmi kockázatoknak – a növekedéséhez. Az elmúlt évtizedben az adatvédelmi kockázatok növekedéséhez leginkább a *federált (azaz*

kombinált) személyazonosság-kezelési rendszerek megjelenése és elterjedése, valamint a közösségi oldalak használatának növekedése járult hozzá.

A következő évtizedben az adatvédelmi kockázatok növekedésének – a kezelt adatok mennyiségnek növekedése mellett – egy másik fontos oka lesz a *fejlett adatbányászati eszközök* megjelenése és használatuk elterjedése. Ezen belül különösen a *kép- és mozgókép-elemzési technológiák* megjelenése és elterjedése hoz be új dimenziókat, és növeli látványosan e kockázatokat.

3.2 Adatvédelmi technológiák

Adatvédelmi technológiák közé azok a technológiák sorolhatók, amelyek lehetővé teszik vagy elősegítik az adatvédelmi kockázatok csökkentését. Ezeket a technológiákat szokás *magánszféra-erősítő technológiáknak* (Privacy Enhancing Technologies, PET) nevezni. A PET-ek jelentősége növekvőben van. A következő évtizedben elsősorban nem újabb megoldások kifejlesztése várható, hanem a PET-ek *integrálása a személyazonosság-kezelésbe*, továbbá komoly törekvések várhatók, e technológiák *szabványos réteggént* való beépítésére az informatikai alkalmazásokba, például a federált személyazonosság-kezelésbe.

A szűk értelemben vett technológiai oldal mellett az adatvédelem megteremtésében fontos szerepe lehet az adatvédelmi kockázatok csökkentésében az adatvédelmi szempontokat figyelembe vevő *adatgyűjtési és -kezelési üzletviteli gyakorlat* megjelenésének és elterjedésének. Ezt a folyamatot jelentősen segítheti az adatvédelmi előírások megfelelő *szankciórendszerének* kialakulása.

3.3 Adatvédelmi átvilágítás és audit

Az adatvédelmi elvárásoknak való megfelelés előzetes vizsgálatának és utólagos ellenőrzésének eredményességét növeli az adatvédelmi átvilágítás és az adatvédelmi audit. Hasonlóan az információbiztonsági értékeléshez és tanúsításhoz, az adatvédelmi auditot megkövetelő előírások megjelenése, *adatvédelmi auditszabványok* és *szabványos gyakorlatok* alkalmazásának elterjedése prognosztizálható.

Szabályozás

Az IKT szektorhoz kötődő tevékenységeket érintő állami szabályozás ma már kiterjedt és sokrétű. A szabályozásnak négy megjelenési formájával találkozhatunk: a) *jogi szabályozás*, b) *államilag támogatott piaci önszabályozás*, c) *támogatási politika* és d) *szabványosítás*.

Az IKT szektort érintő szabályozásról beszélhetünk szűkebb és tágabb értelemben is. Tágabb értelemben ehhez a területhez sorolhatók mindazok a szabályozások, amelyek közvetett módon vonatkoznak az IKT szektorhoz kapcsolódó tevékenységekre. Ebbe a tágabb körbe tartoznak például azok az előírások, amelyek az orvosi eszközök megbízhatóságára vonatkoznak, ha az adott berendezés információs és kommunikációs technológiákat is használ.

Szűkebb értelemben azok az állami előírások tekinthetők az IKT szektort érintő szabályozásnak, amelyek kifejezetten egyes IKT eszközök és termékek használatára, vagy döntően IKT eszközök és termékek használatán alapuló szolgáltatásokra vonatkozó specifikus, továbbá az IKT eszközök használatát közvetve érintő szabályozások (IKT szolgáltatások – például hírközlési vagy elektronikus kereskedelmi szolgáltatások). A szűkebb értelemben vett IKT szabályozás jelentősebb szabályozási tárgykörei:

- szoftvereket érintő szerzői jogi előírások,
- internetes felhasználásokra vonatkozó szerzői jogi előírások,
- hírközlési szabályozás,
- elektronikus kereskedelemre vonatkozó fogyasztóvédelmi szabályok,
- elektronikus aláírás használatának szabályai,
- tág értelemben vett elektronikus ügyintézésre (elektronikus közigazgatási szolgáltatások igénybevételére és a közigazgatási ügyvitel elektronikus formáira) vonatkozó előírások,
- elektronikus aláíráshoz kapcsolódó szolgáltatásokra és hiteles elektronikus dokumentum használatára vonatkozó szabályok,
- IKT eszközök és szolgáltatások biztonságosságával kapcsolatos jogszabályi előírások,
- IKT eszközök és szolgáltatások használatához kapcsolódó specifikus büntetőjogi szankciók,
- specifikusan az elektronikus médiaszolgáltatások nyújtására vonatkozó előírások.

A nem IKT-specifikus, azaz a tágabb értelemben vett IKT szabályozás kiemelkedő jelentőségű területei:

- a) iparjogvédelmi szabályok – elsősorban szabadalmi oltalom, valamint a mikrochip topográfia oltalom,
- b) személyes adatok kezelésére vonatkozó szabályok,
- c) titokvédelemre vonatkozó szabályok.

1. Szabályozási tendenciák

A szűkebb értelemben vett IKT szabályozás kialakulásának kezdetei az 1970-es évekre tehetők. Ekkor jelentek meg a szoftverekkel kapcsolatos szerzői jogi szabályok.

(Természetesen ebben az időszakban is létezett már hírközlési – akkori nevén távközlési – szabályozás, tartalmát tekintve azonban nagyon kevés közös elem található a mai hírközlési és a távközlési liberalizációt megelőzően létezett szabályozás között.)

Az elmúlt ötven év IKT szabályozásának fejlődésében az alábbi fontosabb tendenciák érvényesültek:

1. szabályozási tárgykörök bővülése,
2. szabályozás részletesebbé válása és egy-egy szabályozási tárgykörön belüli szabályozási anyag mennyiségi növekedése,
3. államilag támogatott önszabályozás megjelenése,
4. kötelezően alkalmazandó szabványok számának csökkenése,
5. a szabványnak nem tekinthető műszaki specifikációk (de facto szabványok) szabályozási szerepének növekedése,
6. eltolódás a nemzetállami jogi szabályozás felől a nemzetközi (Magyarország esetében elsősorban európai uniós) eredetű jogi szabályozás irányába.

Az elkövetkező tíz évben e tendenciák közül az első kettő továbbra is érvényes marad. Az új IKT-specifikus szabályozási tárgykörök megjelenése mellett, fel fog gyorsulni a szabályozás részletesebbé válása és mennyiségi növekedése.

Az államilag támogatott önszabályozás, az *internetes tevékenységek állami szabályozásával szembeni ellenállás* eredményeként jelent meg az IKT szabályozás eszköztárában. Ennek a szabályozási módnak a hatékonysága azonban meglehetősen alacsonynak bizonyult, ezért az államilag támogatott önszabályozási kezdeményezések visszaszorulása várható.

Hasonlóképpen a kötelezően alkalmazandó szabványok tekintetében is a korábbi trend *megfordulása* várható. Valószínűbb, hogy a kötelezően alkalmazandó szabványok köre bővülni fog az elkövetkező tíz évben. Ennek a változásnak az okai között elsősorban az IKT termékekkel szemben támasztott minőségi, biztonsági és interoperabilitási elvárások erősödése, valamint egyes IKT szolgáltatások közműszerűsödése, továbbá az állami beszerzések révén érvényesülő közvetett szabályozási hatás (például nyílt szabványoknak megfelelő termékek használatának megkövetelése) említendő.

A szabályozási eszköztár tekintetében a nemzeti jogi szabályozás felől a nemzetközi (Magyarország esetében elsősorban európai uniós) eredetű jogi szabályozás irányába történő várható eltolódás korántsem tekinthető IKT-specifikus tendenciának, csupán azért érdemes kiemelni, mert az IKT-k jellegéből adódóan – a legtöbb IKT-specifikus szabályozási tárgykör esetében – a globális vagy regionális szinten egységes, vagy harmonizált szabályozási megoldások jelentik az egyetlen hatékony megoldást.

Az elkövetkező évtized további új jelensége lesz, hogy az IKT szabályozáson belüli mennyiségét és jelentőségét tekintve *megerősödik az informatika- és hálózatbiztonsággal kapcsolatos szabályozás*.

2. Fontosabb jelenlegi IKT szabályozási területek változásai

2.1 Elektronikus üzletvitel

Az elektronikus üzletvitelt érintő szabályozás finomhangolása és bővülése várható az olyan jelenleg is szabályozott területeken, mint az elektronikus kereskedelmi szolgáltatásokat érintő *fogyasztóvédelem*, az *elektronikus aláírás* használata, *elektronikus ügyintézés*, *elektronikus archiválás*, valamint az *elektronikus fizetési rendszerek* használata.

A közmű jellegű informatikai szolgáltatások elterjedésével az IKT szabályozás kiemelt területévé válik az ezen szolgáltatások nyújtását érintő fogyasztóvédelmi jellegű szabályozás (biztonsági követelmények, rendelkezésre állási követelmények, hatósági felügyelet).

2.2 Szellemi alkotások védelme

Megkerülhetetlen szabályozási kérdéssé válik a *digitális jogkezelési rendszerek* (digital rights management, DRM) használatával kapcsolatos kérdések rendezése, valamint a meglévő szabályozásnak az olyan új jelenségekhez igazítása, mint a szerzői műveknek a *Creative Commons* alapú és *open source* felhasználási szerződések alkalmazásával történő jogosítása.

Az open source megközelítés megjelenése az iparjogvédelem körébe eső szellemi alkotások vonatkozásában az iparjogvédelmi szabályozásmódosítását is szükségessé teheti.

A 3D-s nyomtatási és szkennelési technológiák megjelenése a szerzői jog által védett szöveges, képi és hangalapú alkotásoknál tapasztalt illegális felhasználáshoz hasonló problémát eredményez a szerzői jog által védett ipar- és képzőművészeti tárgyi alkotások, valamint az ipari mintaoltalom és formatervezési mintaoltalomban részesülő szellemi alkotások vonatkozásában is, és szükségessé teszi a szerzői jogi és iparjogvédelmi szabályozás módosítását.

2.3 Cyberbűnözés és -bűnüldözés

Az információs és kommunikációs hálózatok büntetőjogi védelme a hálózatok működését veszélyeztető magatartásokkal szemben elkerülhetetlen szabályozási feladat. A 2010-es évek kiemelkedő szabályozási feladata lesz a közcélú helyi, regionális és *globális szenzor- és aktuátorrendszerek* büntetőjogi védelmének megteremtése.

Az információs és kommunikációs hálózatok felhasználásával elkövetett bűncselekmények fizikai tértől való függetlensége elengedhetlenné teszi a büntetőjogi szabályozásnak e területet érintő nemzetközi egységesítését, valamint a globális információs és kommunikációs hálózatok sajátosságait figyelembe vevő, a nemzetközi bűnüldözési együttműködés új és hatékonyabb formáit lehetővé tevő szabályozás kialakítását.

2.4 Hírközlési szabályozás

2.4.1 Diszruptív hírközlési technológiák és piacsabályozás

A diszruptív technológiák alapvető jellemzője, hogy megjelenésükkel a piaci verseny (a technológiák közötti innováció formájában) erősödik. A hírközlés területén számos potenciálisan diszruptív technológia fog megjelenni vagy megerősödni az elkövetkező évtizedben. Ahhoz azonban, hogy ezek (és általában a technológiai innováció) piaci versenyt erősítő hatása érvényesülhessen, *technológiasemleges szabályozás* és piacsabályozási beavatkozások válhatnak szükségessé.

Három potenciálisan diszruptív – egymással egyébként szorosan összefüggő – technológiai jelenséget érdemes kiemelni:

1. IP-alapú adatátviteli technológia általánossá válása,
2. újgenerációs hálózatok megjelenése,

3. fix és vezeték nélküli adatátviteli szolgáltatások konvergenciája.

A három technológiai jelenség együttesen olyan, jellegében új szolgáltatási infrastruktúra létrejöttét eredményezi, amely a korábban liberalizált hírközlési piacokon ismételt monopóliumok létrejöttét is lehetővé teszi. A szabályozási következmény az lesz, hogy a következő évtizedben mindenképpen *megmarad a hírközlési piacsabályozás*.

2.4.2 Hírközlési és média szolgáltatások konvergenciája

A távközlési, a tartalomipari és az informatikai szolgáltatások piacának (műszaki és üzleti) konvergenciája szükségessé teszi a média- és a távközlési szabályozás egymáshoz való viszonyának tisztázását, továbbá ezeknek a változó műszaki és piaci körülményekhez való igazítását. Az egyes, ma még relatíve önálló területeken jelentkező problémákat együttesen és átfogóan kezelni képes piacsabályozásra, és a piacfelügyeletet lehetővé tevő szabályozási környezet kialakítására lesz szükség.

2.4.3 Frekvenciahasználat szabályozása

A vezeték nélküli adatátviteli technológiák fejlődése és népszerűsége egyre több frekvenciatartomány használatát igényli. Az ebből eredő *frekvenciatartomány-szűkösségi problémák kezelése* csak a jelenleginél rugalmasabb frekvenciagazdálkodást lehetővé tevő szabályozási keretek mellett lehetséges. A rugalmas és hatékony szabályozási keretek megteremtése az elkövetkező évtized egyik központi kérdése lesz.

A frekvencia szűkösséget ugyanakkor enyhítheti az új *software radio*-s (software defined radio, SDR) technológiák használata, amelyek a frekvenciatartományokat a jelenlegi rádiós technológiáktól eltérően, rugalmas és adaptív módon használják ki. Ez a hatékony technológia a frekvenciakiosztás és frekvenciagazdálkodás jelenlegi szabályozási keretektől *alapjaiban eltérő szabályozási megközelítését* (például az ún. szabad frekvenciasávok kijelölését) teszi szükségessé. Az adaptív frekvenciahasználatra épülő rádiós berendezések megjelenése szükségessé teszi továbbá a rádió-berendezések megfelelőségvizsgálati szempontrendszerének átalakítását is. A jelenlegi berendezés- (hardver)orientált megfelelőség-értékelés helyett a rádió-berendezésen futó (a berendezések rádiókommunikációs tulajdonságait befolyásoló) szoftverösszetevők értékelésére helyeződik át a hangsúly.

3. Új szabályozási tárgykörök

Az alábbiakban részletesen áttekintjük az elkövetkező tíz év legjelentősebbnek ítélt új szabályozási tárgyköreit. Ezek jelentőségük szerinti sorrendben az alábbiak:

1. IKT implantátumok használati feltételeinek meghatározása
2. Virtuális szervezetek
3. Elektronikus ágensek működésével kapcsolatos szabályozás (elektronikus képviselők)
4. Virtuális jelenléthez (elsősorban a virtuális világokhoz) kapcsolódó szabályozási kérdések

3.1 IKT implantátumok

Az *emberi testbe épített, az emberi képességeket pótló és növelő* eszközök használata megkerülhetetlen etikai és szabályozási kérdéseket vet fel. A képességnövelő, valamint

az emberi viselkedést módosító vagy az embert (testi működést, gondolkodást, érzelmi állapotot) monitorozó implantátumok beültetésének és használatának szabályozása a 2010-es évek kiemelkedő fontosságú szabályozási feladata lesz. Fontosabb szabályozandó kérdések: a) beültetés feltételei, b) implantátumok biztonsága, c) harmadik felek tájékoztatása, d) monitorozhatóság feltételei, e) implantátumok által okozott károsodásokért való felelősség, f) implantátumokkal történő visszaélésekért való büntetőjogi felelősség szabályozása.

3.2 Virtuális szervezetek

Az infokommunikációs technológiáknak köszönhetően egyre nagyobb szerephez jutnak a *dinamikus, hálózatos, rugalmas, távollévők közötti együttműködésen alapuló munkaszervezési megoldások* a tradicionális, hierarchikus, bürokratikus és közös fizikai teret igénylő vállalat szervezési modellekkel szemben. Ezeket az új munkaszervezési módokat a virtuális szervezet elnevezéssel szokás leírni.

A virtuális szervezetekben történő munkavégzés megjelenése és elterjedése a munka- és a társasági jogi szabályozás módosítását vagy kiegészítését teszi szükségessé. Az átalakulási folyamat első jelei között említendő a *táv munkával kapcsolatos specifikus szabályok* megjelenése a munkajogban.

A virtuális szervezetek megjelenése elsősorban a tudásintenzív ágazatokban (például a szoftveriparban) várható, ami előrevetíti az ezen szervezetekben történő munkavégzés eredményeként létrejövő szellemi alkotások felhasználásával kapcsolatos specifikus szabályozási igények megjelenését is.

3.3 Elektronikus képviselők, gépi jogok

Egyre több olyan alkalmazás jelenik meg, amelyek üzemeltetőjük által programozott módon képesek szerződéses tárgyalások lebonyolítására, a tárgyalások során a felmerülő szempontok mérlegelésére és a szerződési feltételek értékelésére, valamint a kialakított megállapodás értékelésére és jóváhagyására vagy elutasítására. Ezen alkalmazások következő generációja képes lesz előre nem programozottan, *autonóm módon* reagálni szerződéses tárgyalások során. Az ilyen „intelligens” elektronikus ágensek alkalmazásának megjelenése és elterjedése szükségessé teszi ügyletkötési képességük szabályozását, valamint az ágensek működtetéséért való felelősségi viszonyok szabályozását.

Az elkövetkezendő tíz évben valószínűtlen – de nem kizárt – a szuperautonóm, „öntudattal” rendelkező ágensek megjelenése. Amennyiben ez realitássá válik, számos, az ágensek „életben maradásához” és felelősségéhez kapcsolódó új szabályozási kérdés merül fel.

3.4 Virtuális jelenlét és a virtuális világok jogi kérdései

A virtuális jelenlétet lehetővé tevő technológiák megjelenése és elterjedése szintén számos új szabályozási kérdést vet fel, amelyek közül a következők fontosabbak: virtuális környezetben folytatott tevékenységek (például munkavégzés, oktatás) szabályozása, virtuális környezetben elkövetett bűncselekmények, virtuális környezetben való bűnüldözés és bűnmegelőzés szabályai, valamint a virtuális környezet és a virtuális környezetekben található virtuális tárgyak feletti rendelkezési jogosultságok (módosítás, átruházás, megszüntetés, virtuális tárgyak eltulajdonításáért való büntetőjogi felelősség) rendezése.