SZABADSÁG VAGY INKÁBB KALITKA?

Nagy Valéria – Jánvári Tibor

Absztrakt: Az utóbbi években szinte nélkülözhetetlen az ún. IKT (**I**nfo**K**ommunikációs **T**echnológia) és a hozzá kapcsolódó informatikai (mobil) eszközök használata a mindennapjainkban, legyen szó akár tanulásról, akár munkavégzésről vagy éppen magánéleti/szabadidős tevékenységről. Az adattárolásra is alkalmas saját informatikai (mobil) eszközök – a továbbiakban „csak" eszközök – munkavégzési célú használatát sok esetben nem lehet megkerülni, sőt a munkáltatók talán magától értetődőnek tekintik, hogy a munkavállalóik a saját infrastruktúrájukat ellenszolgáltatás nélkül használják a munkájuk elvégzéséhez. E közlemény témája tehát közvetetten a munkavégzés keretfeltételeihez, szabályaihoz (is) kapcsolódik az általános adatvédelem okán. A téma rövid kifejtése előtt előre kell bocsátani, hogy a közlemény címében is sejtetett kockázat kapcsán megfogalmazódott gondolatfolyamnak természetszerűleg nem az a célja, hogy a szakmailag releváns lényeget teljes körűen feltárja és az esetleges problémákat megoldja, illetve a konfliktusokat feloldja, hanem sokkal inkább a témakör kontextuális értelmezésének tovább gondolására ad alkalmat. Nevezetesen, hogy milyen lehetőségekre és konfliktusokra adhatnak alkalmat az adattárolásra is alkalmas informatikai (mobil) eszközök használatának egyes aspektusai?

Abstract: In recent years, the use of ICT (**I**nfo**C**ommunication **T**echnology) and related IT (mobile) devices have become almost indispensable in our daily lives. This is a fact, whether it is about studying, working or even leisure activities. In many cases, the use of one's own IT (mobile) devices, which are also suitable for data storage – hereinafter "only" devices – for work purposes cannot be avoided, and employers may even consider it self-evident that their employees use their own infrastructure to perform their work without compensation. The topic of this paper is therefore indirectly related to the framework conditions and rules of employment due to general data protection. Before a brief explanation of the topic, it must be said that the flow of thought expressed in relation to the risk implied in the title of the paper is naturally not intended to fully explore the professionally relevant essence and to solve possible problems or to resolve conflicts. But rather to contextualize the topic provides an opportunity to further think about its interpretation. Namely, what kinds of opportunities and conflicts can be created by certain aspects of the use of IT (mobile) devices that are also suitable for data storage?

Kulcsszavak: általános adatvédelem, (jog)elvek, informatikai (mobil) eszközök, módszerek

Keywords: general data protection, (legal) principles, IT (mobile) devices, methods

1. Bevezetés

Minél inkább összeforr a munka és a magánélet, annál inkább abiotikus stresszorként vannak jelen az életünkben az adattárolásra is alkalmas informatikai (mobil) eszközök használatához kapcsolódó „szabályozott" és „szabályozatlan" jelenségek is. Másfelől pedig a modern kompakt eszközök adatokkal, információkkal olyan komplex műveletekre is képesek, amelyek azt vetítik előre, hogy a rendszereink folyamathangsúlyossá válnak, ezáltal a figyelemnek a folyamaton kell lennie: tanulmányozni kell a rendszerek időbeli és térbeli viselkedését. E közlemény keretei között rendszerek alatt a munkavégzéshez köthető és a magánéleti/szabadidős tevékenységek, továbbá azok elemei értendők. A cselekvési folyamatban érdekelt feleket tehát „érzékenyíteni" kell egymás irányába, hiszen az adattárolásra is alkalmas informatikai (mobil) eszközök használatának egyes aspektusai akár feloldhatatlan konfliktusokra is alkalmat adhatnak.

ISSN 1788-7593 (Nyomtatott) DOI: https://doi.org/10.14232/jtgf.2023.3-4.21-29
ISSN 2676-9867 (Online)

Egy előkelő műszaki kultúrával bíró, innovációra nyitott és hajlandó társadalom annál eredményesebb lehet minél inkább támogatott és segített perem- és keretfeltételekkel, keretszabályokkal, jogi aktusokkal. Célszerű jogelvekre támaszkodni, ugyanis a jogelvek elősegíthetik a jogszabályok alkalmazását (Szilágyi, 2006; URL1). Megjegyzendő azonban, hogy hazánkban hajlamosak vagyunk néhány „helytelen" magatartás kapcsán olyan szigorú és bonyolult rendelkezéseket megfogalmazni és kötelező érvényűnek elismer(tet)ni, amelyek a későbbiekben megnehezítik (vagy éppen ellehetetlenítik) a rendszerek eredeti elgondolás szerinti működését/működtetését.

Némiképp árnyalja a tanulmányozás lehetőségét, hogy az adatok, információk egy része pedig különös „bánásmóddal" felruházott. Általában véve az adat valaminek a megmagyarázására, megvilágítására, jellemzésére vagy kiegészítésére közölt tény, részlet, adalék. Tulajdonképpen valamely dologra vagy tárgykörre vonatkozó, ismert, nyilvántartott tény, illetve valakinek valamely szempontból tekintett körülményei, viszonyai, illetőleg az ezzel kapcsolatos tények (URL2). Az információ pedig valamely ügyre vagy személyre vonatkozó tájékoztatás, felvilágosítás, értesülés. Adat(ok)ból állítható elő feldolgozással, értelmezéssel. Egyfajta üzenet, amely új ismereteket hordoz (URL2). A célszerűség kedvéért itt most nem definiálandók a szemiotika, szintaktika, szemantika és pragmatika fogalmak.

A műszaki életben (is) két gyakran használt fogalom a vezérlés és a szabályozás. Míg előbbi tulajdonképpen a működés nyílt hatásláncú irányítása, addig az utóbbi olyan zárt hatásláncú irányítási folyamat, amely visszacsatolás révén éri el az adott jellemző kívánt értékét (Frigyes, 1965; Mizsey, 2012; Jancskárné, 2015).

Egy folyamat irányítási struktúrájának kialakítása annak megtervezését jelenti, hogy az adott célkitűzés elérése hogyan történik, mely paraméterét milyen módon kell vezérelni/szabályozni, hány jellemzőt kell irányítani.

2. (Jog)elvek, eszközök, lehetőségek, kötelmek, kérdések, bizonytalanságok

A különös „bánásmóddal" felruházott adatok és információk tekintetében fontos megemlíteni például a természetes személyeknek a személyes adatok kezelése során elvárt védelemről szóló Európai Parlament és Tanács 2016/679 rendeletét (GDPR), de az elektronikus információ biztonságáról szóló 2013. évi L. törvényt, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényt és az elektronikus hírközlésről szóló 2003. évi C. törvényt is stb.

A fenti jogi aktusok fogalomrendszerében személyes adatnak minősül az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés. Tehát ha egy munkáltató ilyen típusú adatokkal dolgozik, akkor adatkezelőként felel a hatáskörében folytatott adatkezelésekért (beleértve a felhasznált eszközt is).

Szintén a fentebbi jogi aktusok fogalomrendszere alapján definiált, hogy mi minősül adatkezelésnek – az alkalmazott eljárástól függetlenül: tulajdonképpen az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen azok

- gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint
- az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint
- a személy azonosítására alkalmas fizikai jellemzők rögzítése.

További előírás, hogy csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen (de a cél elérésére „éppen" alkalmas). A személyes adat ugyanis csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

A fentiekből kiolvasható, hogy az adatvédelem az eszközök fokozott térhódításának és komplexitásának köszönhetően irreális elvárásokat támaszthat nem csupán a munkáltatókkal szemben, hanem az eszközhasználat révén a munkavállalókkal szemben is. Továbbá többlet kötelezettségeket vonhat maga után. Ez utóbbira álljon itt a következő példa a munka törvénykönyvéről alkotott 2012. évi I. törvényből:

A 11/A. § (1) bekezdése szerint a munkavállaló a munkaviszonnyal összefüggő magatartása körében ellenőrizhető. A (2) bekezdés kimondja, hogy a munkavállaló a munkáltató által a munkavégzéshez biztosított információtechnológiai vagy számítástechnikai eszközt, rendszert – eltérő megállapodás hiányában – kizárólag a munkaviszony teljesítése érdekében használhatja. Amikor is érvényre jut a (3) bekezdés, vagyis hogy a munkáltató ellenőrzése során a munkaviszony teljesítéséhez használt számítástechnikai eszközön tárolt, a munkaviszonnyal összefüggő adatokba tekinthet be. Az (5) bekezdés szerint pedig a (3) bekezdést kell alkalmazni akkor is, ha a felek megállapodása alapján a munkavállaló a munkaviszony teljesítése érdekében saját számítástechnikai eszközt használ.

Tulajdonképpen ez utóbbi testesíti meg a munkavállalói többlet kötelezettséget, ha és amennyiben a munkavállaló a saját eszközét használja. És itt történik meg a fentebb említett adat- és információvédelmi rendelkezéseknek való megfelelés érdekében a felelősség tovább hárítása, hiszen, ha a munkavállaló a saját eszközét (és esetenként saját tárhelyét) „kénytelen" használni, akkor

- egyúttal vállalja a felelősséget az adatok és információk védelméért,
- továbbá betekintést biztosító kötelezettség is terheli.

Az eszközhasználat vonatkozásában pedig többféle mód (Jamaluddin et al., 2014; KÖFOP, 2016) is elterjedt napjainkra, ilyenek lehetnek a

BYOD (Bring Your Own Device = Hozd a saját eszközöd), vagyis a munkavállaló a saját eszközét használja munkavégzésre, amely kétféleképpen valósulhat meg:

- az eszköz részben be van kapcsolva a munkáltató informatikai rendszerébe (Itt megjegyzendő, hogy az eszközön végzett tevékenység ezáltal lekövethető is.)
  vagy
- az eszköz nincsen bekapcsolva a munkáltató informatikai rendszerébe.

CYOD (Choose Your Own Device = Válaszd ki a saját eszközöd), vagyis a munkáltató meghatározza, hogy milyen eszközök használatát preferálja és engedélyezi, és a munkavállaló csak ezek közül választhat. Ez a fajta eszközhasználat szintén kétféleképpen valósulhat meg:

- az adott eszköz lehet a munkavállaló saját eszköze (bekapcsolva vagy nem bekapcsolva a munkáltató informatikai rendszerébe)
  vagy
- a munkáltató eszköze, amely be van kapcsolva a munkáltató informatikai rendszerébe.

COPE (Corporate Owned, Personally Enabled = Munkáltatói tulajdonú eszköz és megengedett a magánhasználat), vagyis az eszköz a munkáltató tulajdona, a munkavállaló csupán a munkavégzéséhez veszi birtokba azt, de a munkavégzési célú használat mellett a magánhasználat is megengedett. Ez esetben az eszköz természetesen be van kapcsolva a munkáltató informatikai rendszerébe.

COBO (Corporate Owned, Business Only = Munkáltatói tulajdonú eszköz és csak munkavégzési céllal használható), vagyis az eszköz a munkáltató tulajdona, a munkavállaló a munkája elvégzéséhez veszi birtokba azt, és kizárólag munkavégzés céljára használhatja, a magánhasználat nem megengedett. Az eszköz természetesen ebben az esetben is be van kapcsolva a munkáltató informatikai rendszerébe.

És máris felmerül a kérdés, hogy az YOD (Your Own Device) típusú használati lehetőség, nevezetesen az adattárolásra is alkalmas saját informatikai (mobil) eszközök hivatali célú használata tulajdonképpen egy jogi értelemben vett munkavégzési „szabadság”-nak tekintendő vagy inkább egy jogi „kalitka” lesz a munkavégzés folyománya?

A fentiek alapján körvonalazódik, hogy van olyan típusú tevékenység – példának okáért a kötetlen munkarendben ellátott egyetemi oktatói munkakörhöz rendelt feladatok –, ahol munkavégzési és magánéleti szempontból egymástól nehezen elhatárolható tevékenységek összességét látja el az oktató. De ha még tovább megyünk, akkor nem csupán a feladatok elhatárolása, hanem azok időbelisége is és térbelisége is korlátozó tényező lehet e tekintetben. Szintén bonyolítja a helyzetet, hogy saját és munkáltatói eszközökön egyaránt végez munkát. Tehát ilyen módon a(z együttes) rendelkezés sérülékenyen megoldható a már említett 2012. évi I. törvény 11/A. § (1)–(5) bekezdéseiben foglaltak okán (is).

Tekintve, hogy a mai technicizált világban a munkavállaló és az eszköz „egybeforrt”, és sok esetben ezt kiegészíti a mesterséges intelligencia, ezért az adatok, információk biztonságossága terén óhatatlanul csapdahelyzetek alakulnak ki: akár egy ártatlannak tűnő alkalmazás jóhiszemű letöltése is nemkívánatos adat- és információbiztonsági eseményt vonhat maga után.

Az eszközök és a különféle informatikai termékek hamar társadalmi elfogadottságra találnak, viszont alkalmazásuk majd csak később vet fel számos olyan aggályt, amely már az elfogadásuk pillanatában is jelen volt, de akkor nem az volt az elsődleges szempont.

A kérdések ezért örökérvényűek:

- Megvalósult-e korábban, megvalósul-e jelenleg, meg fog-e valósulni valaha a teljes körű adat- és információbiztonság?
- Megoldást jelent-e a különféle határozatok, kódexek, irányelvek, stratégiák, cselekvési tervek, törvények és egyéb más jogalapú szabályozások szigorítása, számának növelése, az újabb és újabb kiskapuk bezárásával egy még újabb nyitása vagy éppen a polgári peres eljárások és büntető eljárások lefolytatása?
- Vagy egyáltalán kell-e mindent jogi aktusokkal normalizálni és ezzel keretek közé szorítani?

Sok a nyitott kérdés. Talán nem is mindegyikre kell konkrét választ adni, de azokra mindenképpen válaszolni kell, amelyek konfliktusokra, kockázatokra adhatnak alkalmat az adattárolásra is alkalmas informatikai (mobil) eszközök használatának egyes aspektusain keresztül. Válaszok folyamatirányítással nyerhetők. Az irányítási művelet (Mizsey, 2012) pedig a dinamika elveivel és törvényeivel azonosulva az alábbi részműveletekből áll:

- észlelés/érzékelés: információszerzés az irányítandó folyamatról és/vagy a zavaró körülményről
- mérlegelés/ítéletalkotás: határozás a kapott információ alapján a rendelkezés szükségességéről és annak mértékéről
- döntés/rendelkezés: utasítás beavatkozásra
- cselekvés/beavatkozás: a rendelkezés alapján az irányított folyamat működésének befolyásolása valamely paraméterének/jellemzőjének módosításán keresztül

Tehát e részműveletekből álló irányítás két, lényegében eltérő módon valósítható meg: vezérléssel, szabályozással.

3. Anyag és módszer

Az előző fejezetben leírtak azt vetítették előre, hogy az infokommunikációs technológia és az adattárolásra is alkalmas informatikai (mobil) eszközök munkavégzési célú használata által életre hívott – a közlemény címében is sejtetett – kérdés megválaszolása folyamathangsúlyos. Egyfelől azért, mert a horizontális hierarchián alapuló (az adott feladatokhoz hangolt) eszközhasználat más és más helyzetet teremt, ami időben változó. Ez azt jelenti, hogy nem csupán az elvégzendő feladatok sokfélék, hanem a folyamatos innovációnak köszönhetően maguk az eszközök és technológiák is változatosak és folyamatosan változnak is. Míg a feladatok viszonylag jól körül határolhatók, addig az eszközök és/vagy infokommunikációs technológiák változása nem határozható meg előre.

Módszertanilag a *„Szabadság vagy inkább kalitka?”* kérdés megválaszolása tehát a rendszerek dinamikus viselkedésének tanulmányozásával, illetve leírásával,

modellezéssel kezdődik (feltárandó, hogy milyen konfliktus(ok)ra, kockázatokra adhatnak alkalmat az adattárolásra is alkalmas informatikai (mobil) eszközök használatának egyes aspektusai), különös tekintettel az idő értelmezésére és figyelembe vételére, majd folyamatos szimulációval „szuboptimalizáció" következik. Ilyen módon lehetővé válik az elvégzendő feladatok sokfélesége és különösen az eszközök és/vagy technológiák változása által okozott változások elemzése és kiértékelése.

4. Eredmények és értékelésük

Az eszközhasználatban és a használatukhoz kapcsolódó jogi aktusokban rejlő konfliktusok, illetve kockázatok – mint bizonytalanságok hatásai – lehetnek fenyegetettségek, de lehetőségek is.

Az *Anyag és módszer* fejezetben említett szuboptimalizáció megvalósulása lehetséges (csupán) az adatvédelem területén, ugyanis az eszközök és technológiák változása mindig lépéselőnyben van. Ezért konkrét rendelkezések helyett tehát sokkal inkább iránymutatásokra van szükség, ezeknek a lehetőségét kell megteremteni. Ezáltal pedig olyan jogalapú folyamatirányítás, környezet és munkafeltételek alakíthatók ki, ahol a biztonságos információáramlás támogatása is megvalósítható.

Az előbbiekben leírtak alapján az elégtelen folyamatirányítás, pl. az alulszabályozás mellett kerülendő lenne a túlszabályozás is, mert az inkább turbulenciát okoz, ami a hatékonyság/innováció gátja lesz és az eredményességben is törés lesz. Ugyanakkor kerülendők a nem kiforrott intézkedési gyakorlatok is, azonban tény az is, hogy nem szükséges mindent szabályozni, sok esetben elegendő a vezérlés is, hiszen legtöbbször az idő szűk keresztmetszetnek bizonyul. Mindig az irányítandó folyamat jellege dönti el, hogy milyen folyamatirányítást szükséges alkalmazni.

A folyamat(szakasz) megismerésének és az ehhez célszerűen megválasztott folyamatirányítási struktúrának a felépítéséhez az alábbi feladatok elvégzése indokolt:

- Cél (adat- és eszközbiztonság és/vagy hatékonyság és/vagy hasznosság) meghatározása a hozzá tartozó jellemzőkkel/paraméterekkel.
- Lehetséges zavarások számbavétele (technikai és technológiai fejlődés által életre hívott „újdonságok" stb.). A szabályozással mindenféle zavarás kiküszöbölhető, míg vezérléssel csak az előre számításba vett zavarások hatása. Viszont lehetőség (mindig) a bizonytalanságban rejlik (egy kisebb zavar felfogható inspirációnak is, mozgásteret engedve ezzel a szabályozásnak).
- Módosított/módosítható jellemzők kiválasztása.

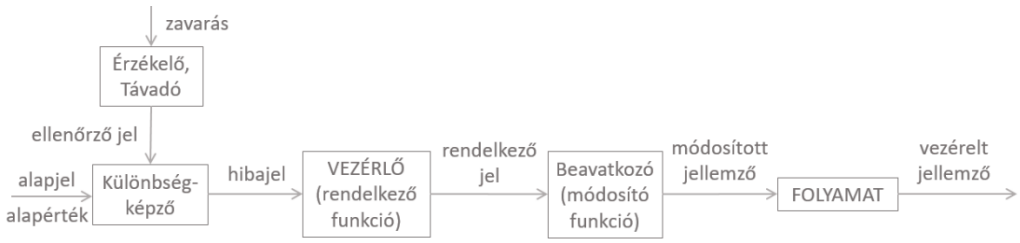
Egy többváltozós folyamat irányítása azonban összetett folyamat. Ezért különösen lassú folyamatok irányításánál előnyös a zavarkompenzáció, ugyanis a folyamat(szakasz)ok rejthetnek kereszthatásokat, illetve ellentmondásokat, amelyeket gyakran csak a kiteljesedésük után lehet feloldani. És az is alapkövetelmény, hogy a zavarások kiküszöbölése csak végső esetben járhat a

feladatvégzés korlátozásával, tehát nem a korlátozás révén kell például az adatvédelemnek megvalósulnia. A zavarkompenzáció tulajdonképpen a két irányítási folyamat: a vezérlés és a szabályozás kombinálását jelenti.

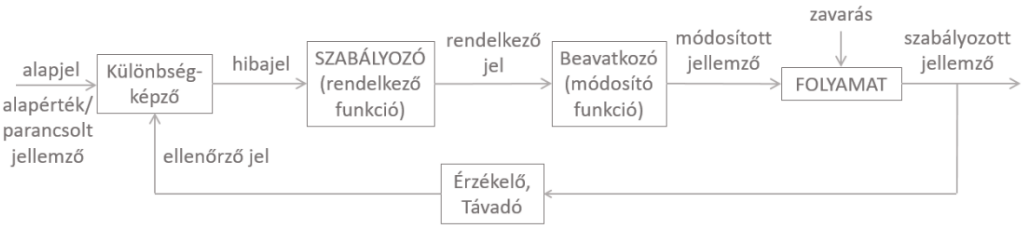
Az *1. ábra* mutatja a lehetséges folyamatirányítás elvi vázlatát *a)* vezérlés és *b)* szabályozás vonatkozásában.

1. ábra: **Jogalapú folyamatirányítás elvi vázlata**

a) vezérlés



b) szabályozás



Forrás: a szerző saját szerkesztése.

A kockázatalapú szemlélet (MSZ ISO/IEC 27001; Nagy, 2013) alapján az adatvédelemre irányuló folyamatirányítás szempontjából biztonsági eseménynek tekintendő minden olyan esemény (bizonyos meghatározott körülményekben történő bekövetkezett változás), amelynek kedvezőtlen következménye lehet az adatok védelmét illetően. Az adatok védelme, az informatikai biztonság akkor teljes körű és zárt, ha a védelem a rendszer, a folyamatok összes elemére, szakaszára kiterjed és az összes releváns veszély (fenyegetettség) figyelembe lett véve a védelmi intézkedések megtervezésénél és megvalósításánál. Kockázatokkal arányosnak és folyamatosnak pedig akkor minősül, ha a védelem költségei arányosak a potenciális védelmi és elhárító intézkedésekkel, amelyekkel a kockázatok elviselhető mértékűre mérsékelhetők, illetve az időben változó körülmények ellenére is megszakítás nélkül valósul meg a védelem.

A védelem mellett azonban biztosítani kell a feladatvégzéshez szükséges információáramlást, de az YOD típusú eszközök (ahol egyébként az adatvédelem felhasználói felelősség) használatának bizonyos módja zavarás lehet e folyamatban a szabályozott jellemző (az adatvédelem) vonatkozásában. Előfordulhat zavarásként nem aktív és nem rendszeresen frissített vírusvédelem, az érzékeny adatok nem

titkosítva történő tárolása, az eszköz felügyelet nélkül hagyása, stb. Az eszközökhöz társítható zavarás lehet még a felhasználói tulajdonú adathordozó használatával okozott kár (pl. vírusos adathordozó használata), e-mail használata adattömegek mozgatására, más felhasználók zavarása (indokolatlan hálózati futtatás), stb. E zavarok kétségkívül veszélyeztetik az adatvédelmet, ezért ezekre szükségképpen reagálni kell rendelkezés/szabályozás és módosítás/beavatkozás formájában (hozzáférés menedzselése, jogosultságok személyi használata átadás nélkül, titoktartási nyilatkozat, végső soron az információbiztonság kultúrájának kialakítása és fenntartása), különösen a kritikus és kiemelt rendszereket illetően. A figyelmen kívül hagyott és nem értékelt zavarások akár katasztrófákhoz is vezethetnek.

Az adattárolásra is alkalmas informatikai (mobil) eszközök használata témakörben tehát célravezető a (preventív és) direktív jogalapú szabályozás és kockázatkezelő kontroll. Továbbá a folyamatban az esetleges zavarok jelzése automatikus monitorozó komponensekkel történjen és ne (csupán) a felhasználók észrevételei szolgáljanak az információbázis alapjául. Azonban a feladatok elvégzésénél, a problémák megoldásánál, valamint a kihívások leküzdésénél kétségkívül szükséges az emberi önkorlátozás képessége is, aminek eszköze az érdekeltek bevonása és a változások meggyőző és érthető kommunikálásának támogatása. Ez pedig a környezeti, a gazdasági, a műszaki és a társadalmi fenntarthatóság folyamatjellemzőinek szuboptimalitását is szolgálja. (Itt megjegyzendő, hogy a felsorolás nem prioritási sorrend.)

A munkavégzés során a munkáltató és munkavállaló közötti folyamatok irányítása (akár vezérlés, akár szabályozás) tehát többnyire adat- és információbiztonsági tárgyúak, ahol egyáltalán nem kerül a felszínre például a saját informatikai (mobil) eszközök hivatali célú használatának erkölcsi kérdése, az avulás. Míg a saját tulajdonban lévő személygépkocsi hivatali, üzleti célú használata során a szabályozások az üzemanyag költség mellett némi normaköltséget is definiálnak – figyelemmel arra, hogy a gépjárművek értékcsökkenése ötéves periódussal számítható –, addig a saját informatikai (mobil) eszközök hivatali célú használatának vonatkozásában ilyen fel sem merül.

5. Összegzés, záró gondolatok

Általánosságban elmondható, hogy komoly kihívást jelent az adatvédelem kimenetű vezérlés és szabályozás egy olyan környezetben, mint amilyet az infokommunikációs technológia és az adattárolásra is alkalmas informatikai (mobil) eszközök munkavégzési célú használatának a folyamatos változása teremt. Az adatvédelem, mint a folyamat vezérelt/szabályozott jellemzője, vagyis az eredmény szuboptimális lesz a feladatokhoz hangolt eszközhasználat, és a már említett időtényező (pl. reagálási idő, felkészülési idő) okán is.

Kétségkívül tetten érhető az a törekvés is, hogy minél inkább érvényesüljenek a biztonsági szempontok (többnyire a munkahelyi biztonság megőrzése ember/eszköz vonatkozásában, valamint az információbiztonság kontextusában) a teljes jogszabályi hierarchiában, azonban ennek ellenére sem jelenthető ki, hogy a jogalapú szabályozó rendszer összehangolt és egységes.

A munka és a magánélet ugyan összeforr(t), de alapvetés, hogy az adatvédelem nem korlátozhatja sem a feladatvégzést, sem pedig az eszközhasználatot, de a tételmondat megfordítása is igaz, hiszen a feladatvégzés és eszközhasználat sem csorbíthatja az adatvédelmet.

Zárásként pedig Móricz Zsigmond (1879–1942) örökérvényű gondolata öleli fel mindazt, amit e rövid közlemény felvetett a *„Szabadság vagy inkább kalitka?”* kérdés megválaszolásához: *„Idő kell, míg új gondolat, új eszme elterjed, míg mindenütt megértik s megismerik, kivált ha nem olyan formában jelenik meg, hogy bárki rögtön magáévá tehesse; ha meg ellentétben is áll a régiekkel, egyenesen harcot kell állania.”*

Irodalomjegyzék

Frigyes A. (1965): *Bevezetés a technológiai folyamatok automatizálásába.* Tankönyvkiadó Vállalat, Budapest. 153 p.

Jamaluddin, H., Ahmad, Z., Alias, M., Simun, M. (2014): Personal Internet Use: The use of personal mobile devices at the workplace. *Global Conference on Business and Social Sciences, Kuala Lumpur*. < https://www.researchgate.net/publication/270742194_Personal_Internet_Use_The_use_of_personal_mobile_devices_at_the_workplace> (2023.07.07.)

Jancskárné A. I. (2015): *Szabályozástechnika I.* Pécsi Tudományegyetem Műszaki és Informatikai Kar, Pécs. 63 p. <https://docplayer.hu/18704065-Szabalyozastechnika-i.html> (2023.07.07.)

Mizsey P. (2012): *Folyamatirányítási rendszerek.* BME Vegyészmérnöki Kar, Budapest. 275 p.

Nagy V. (2013): *Kockázatmenedzsment az iparban.* SZTE Mérnöki Kar, Szeged. 104 p.

Szilágyi P. (2006): *Jogi alaptan.* Osiris Kiadó, Budapest. 338 p.

KÖFOP-2.2.2-VEKOP-16-2016-00001 tanulmány (2016)_Mobil eszközök hivatali használata.

MSZ ISO/IEC 27001:2014 *Információbiztonsági irányítási rendszer*

2003. évi C. törvény az elektronikus hírközlésről. <https://net.jogtar.hu/jogszabaly?docid=a0300100.tv> (2023.07.07.)

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. <https://net.jogtar.hu/jogszabaly?docid=a1100112.tv> (2023.07.07.)

2012. évi I. törvény a munka törvénykönyvéről. <https://net.jogtar.hu/jogszabaly?docid=a1200001.tv> (2023.07.07.)

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról <https://net.jogtar.hu/jogszabaly?docid=a1300050.tv> (2023.07.07.)

2016/679 GDPR Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról <https://net.jogtar.hu/jogszabaly?docid=a1600679.eup> (2023.07.07.)

URL1: http://acta.bibl.u-szeged.hu/6902/1/juridpol_049_599-605.pdf (2023.07.07.)

URL2: https://mek.oszk.hu/adatbazis/magyar-nyelv-ertelmezo-szotara/szotar.php (2023.07.07.)