

Károli Gáspár Református Egyetem
Állam- és Jogtudományi Doktori Iskola

**Az Európai Unió Általános Adatvédelmi Rendeletében biztosított védelem szintjének
elemzése**

Tézisek

dr. Szabó Endre Győző

Témavezető:

Dr. Tóth András tanszékvezető

egyetemi docens

Budapest

2020

1. A kontextus, a kitűzött kutatás felvázolása

A személyes adatok kezelése egyre nagyobb mértékben befolyásolja az egyének életét. Ez számos jogviszonyban nyilvánvalóvá vált az elmúlt évtizedekben, ahogyan a való élet jelenségei egyre inkább digitálisan is megjeleníthetővé válnak, és az interneten keresztül befolyásolhatók valós körülmények, amelyekre hatásunk korábban csak az offline világban lehetett. Mindemellett az is megfigyelhető, hogy az internetes közeg már nem csupán a való élet leképeződése, kiegészítése, hanem egyre nagyobb szerepet játszanak az online közegben végbemenő események az emberek életében. Az online világ történései már önmagukban is fontos társadalmi események. Mindezeknek a fényében szükséges értékelnie a jogi gondolkodásnak, hogy milyen eszközei vannak a védelem megtartására és erősítésére azon adatok tekintetében, amelyek mindezeket a lehetőségeket megteremtik, és amelyek kezelése életet, élethelyzeteket, emberi kapcsolatokat képes befolyásolni. A kockázatokkal és a rosszhiszemű magatartásokkal folyamatosan számolni kell, a védelem végső soron ezekkel szemben fogalmazódik meg.

Mire irányult a kutatásomk? Az EU jogalkotója a magas védelmi szintet tűzi ki célul, de nem ad eszközrendszert arra, hogy a saját maga által nyújtott védelmet szintekre tudja tagolni. A kutatás előtt azt feltételeztem, hogy speciálisan erre irányuló jogi szabályok nélkül is van lehetőség ezt a védelmi szintet meghatározni.

2. Az elvégzett kutatás, vizsgálat, elemzés leírása, a módszer rögzítése, a források számbavétele

Az elvégzett kutatás leírása

A kutatás tárgya maga a Rendelet, és annak európai uniós, valamint esetenként magyar jogi kapcsolódásai. Ilyen értelemben a kutatás tárgya nem csupán a Rendelet, hanem szükségszerűen mindazok a jogi normák, amelyek a Rendelet értelmezése körében figyelembe veendők.

Kutatásom során arra a kérdésre kerestem a választ, hogy a személyes adatok védelmének szintje jogi eszközökkel meghatározható-e, illetve a védelem egyes szintjei definiálhatók-e.

Amennyiben erre a kérdésre igenlő válasz adható, úgy mik azok a kritériumok, amelyek alapján az egyes szintek között minőségi különbség tehető? Mi az egyes szintek közötti összehasonlítás alapja? Mindezek fényében milyen lehetőségek adódnak a védelem szintjének alakítására, milyen jogi eszközökkel javítható a védelem minősége?

Értekezésem célja az, hogy a tömegével előforduló és a nehéz ügyekben egyaránt hasznosítható elemzés álljon rendelkezésre a védelem szintje tekintetében. A disszertációban elvégzett elemzés nem csupán tudományos megfontolásokat kíván szolgálni, hanem az egyes ügyek megértését és értelmezését is elősegíteni hivatott, ilyen értelemben a gyakorlatra tekintettel is született. Gyakorlati beállítottságú a szerző, de a napi hatósági munka során is fel kell ismerni, hogy az elméleti kérdések elmélyült vitatása mindig hozzájárul a gyakorlati munka hatékonyságához.

Alkalmazott módszerek

A kutatás során a kritikai, forráselemző módszert követtem a vonatkozó hazai és külföldi források feldolgozása terén. A védelmi lépcső elméletének kidolgozása és megalapozása során alkalmaztam az összehasonlító és a történeti módszert is.

A kívánatos védelmi szint meghatározása során értelemszerűen a jogfejlesztésre irányuló javaslatokat fogalmazok meg, ennek kapcsán pedig a *de lege ferenda* megközelítést alkalmazom. A jelenlegi védelmi szint meghatározása során a deskriptív, illetve ehhez szorosan kapcsolódva a kritikai-elemző módszert használtam.

Tekintettel arra, hogy az értekezés jelentős mértékben jogértelmezési kérdésekre fókuszált, szükséges megemlíteni az alkalmazott értelmezési módszereket. Ezek körében a nyelvtani értelmezés, a normacél szerinti (teleologikus) értelmezés módszerét alkalmaztam. Egyes jogértelmezési kérdésekben az Európa konform jogértelmezés eszközeit is használtam. Tekintettel a feldolgozott joganyag kiterjedt voltára, a rendszertani megközelítés az értekezésben gyakorlatilag mindenhol tetten érhető. A jogesetek feldolgozása során az induktív módszert is igénybe vettem. A különböző védelmi szintek meghatározása, a védelmi lépcső egyes fokozatainak definiálása során a komparatív módszert is alkalmaztam.

Források

A kutatás során hazai és a külföldi szakirodalmat egyaránt kutattam. Felhasználtam számos intézmény forrásait, így a külföldi adatvédelmi felügyeleti hatóságok dokumentumait, a 29. cikk szerinti Adatvédelmi Munkacsoport, az Európai Adatvédelmi Testület, az európai

adatvédelmi biztos, az ENSZ dokumentumait. Ahol releváns volt, hazai intézményi dokumentumokat is kutattam, így a Gazdasági Versenyhivatal, illetve a magyar adatvédelmi hatóság dokumentumait. Az Európai Bizottság közleményei, véleményei kitüntetett szerepet töltek be a kutatásban, ahogyan a bírósági ítéletek is. A magyar ítéletek mellett az Emberi Jogok Európai Bíróságának, valamint az Európai Unió Bíróságának számos ítéletét dolgoztam fel.

Mindezek mellett természetesen a vonatkozó magyar és külföldi, uniós jogszabályok, nemzetközi egyezmények elemzése is a kutatás tárgyát képezte. Külön meg kell említeni az uniós normákat bevezető preambulum bekezdéseket, amelyek a normacél szerinti módszer kapcsán fontos tájékoztató pontként szolgáltak.

Figyelembe véve, hogy a privacy jogát érintően nem csupán a szakirodalmi, hanem egyes ipari szereplők megnyilvánulásai is megemlítendőek egy adatvédelmi tárgyú írásban, szűkebb körben internetes, illetve sajtóban elérhető forrásokat is felhasználtam.

3. Az új tudományos eredmények tézisszerű összefoglalása

Az Európai Unió Általános Adatvédelmi Rendelete által nyújtott védelem szintjének elemzése az Európai Emberi Jogi Bíróság esetjoga alapján

Az értekezésben számos döntésen keresztül vizsgáltam az Európai Emberi Jogi Bíróság esetjogát. Témánk szempontjából ez azért releváns, mert az EU Alapjogi Chartája szerint a Chartában biztosított jogok tartalmát és terjedelmét azonosnak kell tekinteni azokéval, amelyek az Egyezményben szerepelnek. Ilyen értelemben a strasbourgi esetjog minimum védelemként értelmezhető. Ennek elemeit vettem számba, és a sporadikus képet mutató esetjog alapján elemeztem a strasbourgi bíraskodás által meghatározott védelem aspektusait. Ez az elemző munka során fontos eredménynek tekinthető.

A védelmi lépcső elmélete

Az adatvédelem szintjének eróziója vagy fejlődése nem feltétlenül nagy és látványos intézkedésekből adódik össze. Éppen ez a jogi elemzésem célja, hogy azonosítsa azokat a pontokat, ahol a védelem indikátorai megtalálhatók. A védelem egyes komponensei inkább statikusak, mint például az adatvédelmi szabályozás a következő módosításig, vagy a hatóságok léte, illetve az adatvédelmi tisztviselői intézmény. Ezek megalkotása szükségszerűen része a

védelem struktúrájának, a védelem minőségéről önmagukban is sokat mondanak. A védelem nem a statikus elemek ideális struktúrát követő összeillesztéséből, hanem sokkal inkább a privacy-t érintő kockázatokhoz dinamikusan alkalmazkodni képes rendszer létrehozatalából áll. A védelmi lépcső ebben a megközelítésben már sokkal komplexebb elemzést kínál: ahhoz ad támpontot, hogy a nagyobb kép egyes részleteiben is megtalálja azokat az összetevőket, amelyek látszólag talán nem jelentősek, módosításuk, vagy éppen elavulásuk mégis kihat a védelem szintjére.

A lépcső gondolata annak lehetőségét kínálja, hogy azon felfelé és lefelé is vezet az út. Az új jogalkotás nem feltétlenül jelent minden esetben előrelépést a lépcsőn, hanem könnyen elképzelhető, hogy egyes elemeiben visszalépésként értékelendő.

A védelmi lépcsőn álláspontom szerint nem szükséges sok fokozat azonosítása. A lépcső elméletében természetesen egy felfelé végtelenbe mutató, lineáris lépcsőt képzelhetünk el, amely a védelem javulásának és alkalmazkodásának kifogyhatatlan lehetőségét jeleníti meg a jövőben. Egzakt módon sem a lefelé, sem a felfelé vezető fokok nem határozhatók meg nagy számban. Nincs is erre szükség, az elemzés szempontjából három szint meghatározása azonban elengedhetetlen. Az egyik az a fokozat, amelyen a védelem szintje jelenleg megragadható. A másik az, amelyikről a jelenlegi szintre felfelé, vagy éppen lefelé lépett a védelem. A harmadik szint pedig a kívánatos, előre lépésnek tekinthető védelem szintje. Nem lényeges, hogy a szintek között mekkora a különbség, akár egy kisebb minőségi javulás is új szintként azonosítható. Az szükséges, hogy a kettő között a különbséget egyértelműen meg tudjuk határozni. Emellett az is másodlagos, hogy a védelmi szintek közötti előrelépés egy szerves fejlődés eredménye, vagy például egy teljesen új intézmény meghonosításában áll.

Miben áll a minőségi különbség két fokozat között? E tekintetben számos tényező jöhet szóba. A minőségi javulás indikátora lehet, ha az érintett jogai bővülnek, vagy a jogok változatlan katalógusa mellett is javul a jogérvényesítés lehetősége. Amikor az érintett számára elérhető információk köre bővül, vagy a szabályozás e tekintetben világosabb követelményeket határoz meg, szintén minőségi javulást eredményez.

Az előrelépés jellemzője, hogy az adatkezelőket az adatkezelés kapcsán terhelő kötelezettségek az alkalmazott technológia és az üzleti modellek fényében fejlődnek. Az adatkezelő szervezetén belül a dedikált adatvédelmi szakértelem megjelenése, a kontroll mechanizmusok erősödése szintén minőségi változás.

Az adatvédelmi hatóságok mozgástere, feladat- és hatásköre szintén minőségi jellemzője a védelem szintjének. A minőségi előrelépés megmutatkozhat a jog hatékonyságában is. Amint értekeztem róla, az adatvédelmi jog hatékonyságának jogi fokmérője, hogy a magánszféra védelme erősödik, fejlődik. Amennyiben ez megvalósul, úgy a védelmi lépcsőn előrelépés történik.

A minőségi fejlődés fontos fokmérője, hogy az adott változás képes-e hozzájárulni az adatvédelmi kultúra kialakulásához, illetve fejlődéséhez. Az adatvédelmi kultúrát olyan „táptalajnak” tekintjük, amelyben az adatvédelmi előírások természetesen vezetnek magasabb magánszféra-védelemhez egy alacsonyabb adatvédelmi kultúrát megjelenítő közeggel összehasonlítva.

A védelmi lépcső elméletének hasznosítása

Az értekezés talán legfontosabb eredménye, hogy lehetővé teszi a GDPR mögött álló védelem szintjének meghatározását egy összehasonlítást kínáló elmélet alkalmazásával. Bízhatunk abban, hogy a szakirodalomban több reflexió jelenik majd meg ezzel kapcsolatban, és ilyen módon egy vitát indít el a védelmi szintek mérhetősége kapcsán.

De lege ferenda javaslatok

Értekezésemben arra is kerestem a választ, hogy a Rendelet által megteremtett védelem milyen módon tehető hatékonyabbá a jövőben, az általunk jelenleg ismert feltételek ismeretében. Ezzel azt is állítom természetesen, hogy a Rendelet nem az elérhető legmagasabb szintű védelmet biztosítja. A magánszféra védelmét hatékonyabban szolgáló norma- és intézményrendszer is létrehozható. Éppen ebben áll a védelmi lépcső elméletének gyakorlati jelentősége, hogy ezekben a kérdésekben válaszokat lehessen megfogalmazni a segítségével.

Az adatvédelem szintje nem csupán a szabályozáson múlik, hanem döntések sorozatán, az adatkezelő szervezetén belül az adatkezeléseket érintően, vagy éppen hatósági és bírósági döntéseken áll. Ezért is van különleges jelentősége, hogy a jövőbe tekintve felvázoljunk egy olyan állapotot, ahol a védelem erősebb, mint a jelenleg tapasztalt. Ez minden esetben az a harmadik fok, ahova érdemes továbblépni, ahol a jog hatékonyabban szolgálja a jogalkotói célt, témánk körében a magánszféra védelmét.

Az adatvédelmi tisztviselői szerepre vonatkozó következtetések és javaslatok

Ami az adatvédelmi tisztviselői intézményt illeti, javaslatom szerint tovább kell erősíteni, professzionalizálni szükséges, és egy sokkal kötöttebb rendben kell helyüket elfoglalni az adatkezelő szervezeten belül.

Az Európai Adatvédelmi Testülethez telepítendő kvázi végrehajtási rendeleti szabályozás révén bővíthető a kinevezési kötelezettség alá eső adatkezelők köre. A védelem erősítése akkor várható, ha annak személyi, intézményi, eljárási feltételei adottak.

Ami a személyi feltételeket illeti, a tisztviselő végzettségét előzetesen nem tartom vizsgálandónak, azonban egy uniós akkreditációjú vizsga előírása fontos garanciaként szolgálhatna. A vizsgán túl valamilyen kamarai tagságot is előírhatónak tartok. A személyes rendelkezésre állás az előírt vizsga és a kamarai tagság révén erősíthető. Ezt szükségesnek tartom annak érdekében, hogy a tisztviselői munkáért vállalt felelősség ne váljon szétporlaszthatóvá.

Követendő az Európai Unióban működő adatvédelmi tisztviselők munkajogi védelmére vonatkozó rezsím, nevezetesen, hogy a tisztviselő csupán akkor bocsátható el állásából idő előtt, amennyiben azt az adatvédelmi felügyeleti hatóság is jóváhagyja.

Javaslatom szerint, amennyiben a tisztviselőt foglalkoztató adatkezelő szervezet új adatkezelést kíván bevezetni, és ezt a tisztviselő ellenzi, úgy azt be kell jelenteni az adatvédelmi hatóságnak. Olyan mélységű ellenőrzést jelentene ez, amelyre az adatvédelmi hatóságok a jelenlegi modell szerint képtelenek lennének.

Szükséges az új tisztviselői szerep a leírt védelmi deficit ellensúlyozására. Az adatkezelők oldalán fennálló transzparencia hiányt fel kell számolni, és ennek hathatós eszköze lenne a konfliktus-bejelentési kötelezettség.

Ez az új rezsím jelentős változást eredményezne az adatkezelő és a tisztviselő együttműködésében. A tisztviselő a védelmi deficit ellensúlyozására hivatott, ennek megfelelően pozíciója erőteljes reformra szorul a közeli jövőben. Ennek lehetséges modelljét vázolja fel az értekezés.

Az adatvédelmi felügyeleti hatóság feladatellátása tekintetében levont következtetések

A hatékony feladatellátás kapcsán javasolom a panaszokat megelőző stratégiát. Ha a hatóság nem a panaszokat követő, hanem a panaszokat megelőző stratégiát követ, sokkal nagyobb hangsúly jut az utóbbi feladatoknak.

A koncentrált adatkezeléssel és sok konfliktushelyzetet magában hordozó jogviszonyokra összpontosítva a hatóságoknak javasolt lenne olyan programokat indítani, amelynek célja az adatkezelő kezébe megfelelést könnyítő eszközöket adni. Az adatkezelők, illetve adatkezelők szövetségei, érdekképviselői szervei ilyen módon a hatósággal partnerségben alakíthatnák adatkezeléseiket, szabályzataikat, belső eljárásrendjüket. A magánszférát érintő megfontolásokon túlmutató érvek is felhozhatók e modell mellett, hiszen társadalmi szinten sokkal gazdaságosabb egy ilyen rendszer fenntartása. A jelenleginél hatékonyabb modell lenne ez, amely a védelmi lépcsőn is mérhető előnyökkel járna.

Az adatalanyok oldalán ez a modell azt ígéri, hogy az adatkezelők nagyobb eséllyel fognak nem csak jogkövető, hanem jogi kérdésekben tájékozott módon eljárni. Professzionálisabb adatkezelői eljárás és az érintetti jogok érvényesítése nem választható el egymástól. Az adatkezelő oldalán a jogbiztonság erősödik, és a modell a hatóságok számára azért jelentene könnyebbséget, mert jól kalkulálhatóan csökkenne a panaszok száma. Egyszerűen azért, mert a tipikus konfliktusos helyzetekben az adatkezelők megnyugtató válaszokat tudnának adni mind a munkavállalóknak, mind a többi érintettnek.

Az új modell kedvező hatása a költségek csökkenésében is mérhető, továbbá a magánszféra körében megvalósuló jogsértések számának csökkenésében is megragadható. Ez a javaslat a jog hatékonyabb érvényesülése révén jelent kimutatható előnyt a védelmi lépcsőn.

Az adatvédelmi felügyeleti hatóságok hatásköreivel összefüggő következtetések és javaslatok

A védelmi lépcső alapul vételével az értekezésben arra jutottam, hogy önmagában az, hogy az adatvédelmi hatóságok hatásköre szélesedik, olyan mozgástér-többletet hoz, amelyet a védelem szempontjából minőségi előre lépésként értékelünk. Az irányelvi szabályozással összevetve a minőségi előrelépés abban ragadható meg, hogy a Rendelet az új hatáskörök révén gyakorlatilag minden olyan életviszonyba beavatkozási lehetőséget biztosít a hatóságok számára, amely a magánszféra védelmét érintheti.

A védelmi lépcső elmélet fényében minőségi javulásként tarthatjuk számon, hogy a hatóságok bővülő hatásköre révén javul a jogérvényesítés lehetősége. Szintén minőségi előrelépést jelent

a hatáskörök tekintetében az, hogy a hatósági mozgástér bővülése világosabb szabályozási környezetet eredményez, ennek révén az adatkezelők oldalán is egyértelmű, hogy milyen esetekben kerülhet sor hatósági beavatkozásra. A Rendelet új hatásköri szabályai a védelmi lépcsőn minőségi előre lépésként értékelendők, az irányelvvel való összehasonlítás, valamint a védelmi lépcső által elvárt minőségi jellemzőkkel való összevetés is ezt mutatja.

Álláspontom szerint a hatáskörök rendszeres felülvizsgálata és karbantartása szükségszerűen fogja a jelenlegi védelmi szintet legalábbis fenntartani, vagy újabb szintváltást nem eredményező módon megőrizni.

A meglévő különbségek a tagállami közigazgatási eljárási szabályok között több kérdést is felvet. A Rendelet hiányosságának tartom, hogy az anyagi jogi szabályok mellett nagyon kevés a harmonizált eljárásjogi követelmény. A Rendelet hatékony érvényesítését rábízta a tagállami jogszabályokra akkor, amikor minimális eljárási szabályokat sem épít bele a kikényszerítés szabályrendszerébe.

A védelmi lépcsőn az jelent majd előrelépést, ha a hatáskörgyakorlás is a tagállamok által meghatározott közös szabályrendszer szerint fog megvalósulni. A Rendeletet közigazgatási kódexszel, vagy legalább minimális eljárási garanciarendszerrel kell kiegészíteni. E nélkül egy olyan hatékonysági deficittel kell számolnunk, amely a védelmi lépcső elért fokát rendkívül törékennyé teszi, folyamatos visszacsúszás fenyegeti. Azzal is számolni kell, hogy az uniós jogalkotás a tagállami jogalkotásnál lényegesen lomhább, ezért a védelmi lépcsőn érvényesülő, felfelé mutató „gravitáció” sem képes ezt a hiányosságot olyan időn belül ellensúlyozni, hogy az ne járhatna valós védelmi veszteséggel.

Ennek kapcsán fogalmaztam meg azt a javaslatot, hogy az egyablakos ügyintézésnél szorosabb, közös mechanizmusban döntsenek a hatóságok a határon átnyúló ügyekben. Egy elképzelt európai uniós adatvédelmi hatóság eljárhatna minden olyan ügyben, amelyben határon átnyúló adatkezelésekről van szó. A döntéshozatalt a Testület mellett működő jogi szolgálat készíthetné elő, természetesen mindazon tagállami hatóságok számára követhető és transzparens módon, amely véleményét már ebben a fázisban is hangoztatni szeretné. A döntéshozatal pedig a Testület előtt, a vitarendezésre egyébként irányadó szabályok szerint folyhatna. Ez a javaslat az eljárási szabályok hiányosságait is pótolhatná bizonyos mértékben.

Az adatvédelmi bírság kapcsán levont következtetések és javaslatok

Annak érdekében, hogy a személyek magas szintű védelme szavatolható legyen, többek között a bírságolás terén is egységesítette a szabályozást és a tagállami hatóságok hatáskörét. A Rendelet ezen újítását a védelmi lépcső fényében előre lépésként értékelhetjük, mert a kötelezettségek az alkalmazott technológia és az üzleti modellek fényében fejlődnek. A hatóságok a bírság révén értékelni tudják az új üzleti megoldásokat, azok hatását a magánszférára. A pénzügyi szankció a védelmi lépcső több minőségi indikátora tekintetében is kedvező eredményt mutat. A jogérvényesítés esélye javul, a pénzügyi kockázat egyértelmű ösztönző a jognak való megfelelés terén. A Rendelet által is bevezetett magas összegű bírság tekinthető hatékonyságot növelő ösztönzőnek.

A védelmi lépcső alapján *de lege ferenda* javaslatokat is megfogalmaztam, így előrelépést jelentene álláspontom szerint, ha nem csupán egy elméleti plafonig, hanem a kár mértékéig terjedhetne a kiszabható bírság. Nem fogadható el ugyanis, hogy az adatok jogellenes kezelése révén az adatkezelő gazdagodhasson. Ennek lehetőségét a jelenlegi szabályozás nem zárja ki. Emellett pedig a kár enyhítése terén tett intézkedéseket is megfelelő súllyal kell figyelembe venni.

Szintén javasoltam, hogy ne csupán a ténylegesen érintett személyeket vegyék számba a bírság megállapítása során, hanem mindazokat, akikre a jogellenes cselekmény irányult. Ehhez részben kapcsolódik az a javaslat, hogy a hatósággal szembeni transzparencia szabályait fordítsuk meg. Ne az számítson enyhítő körülménynek, ha a hatóságot egy jogsértőnek tűnő gyakorlatról tájékoztatja, hanem az számítson súlyosító körülménynek, ha ezt elmulasztja megtenni. Ebben az adatvédelmi tisztviselőnek is van szerepe, ahogyan erről szintén értekeztem.

A védelmi lépcső fényében javasoltam, hogy a bírsággal sújtható személyi kört bővítse a jogalkotó, így az adatvédelmi tisztviselő új szerepében a transzparenciához kötődő kötelezettségeinek elmulasztása esetén bírsággal is büntethető legyen. A közhatalmi szervek bírságolása terén pedig azt javasoltam, hogy a szerv vezetője is szankcionálható legyen olyan esetekben, amikor a szervezetet ért kárért való helytállása elvárható. A cél ebben az esetben is a személyes felelősség erősítése, annak ellensúlyozásaként, hogy a felelősség sok esetben elmosódik a jogsértések kapcsán.

A bírságolás terén a *forum shopping* jelenségének elkerülése érdekében azt is nélkülözhetetlennek tartom, hogy a tagállami hatóságok hasonló ügyekben hasonló bírságokat

állapítsanak meg. E feltétel nélkül nem valósul meg a védelmi szintek egyenlősége a tagállamok között, és a védelem eróziója indul meg, amely szükségszerűen vezet a Rendelet által megalkotott rendszer széttöredezéséhez.

Az adatvédelmi bírság terén is kirajzolódik tehát az általam azonosítani javasolt három szint, nevezetesen az irányelvi szabályozást jellemző széttöredezettség és alacsonyabb szintű védelem, a Rendelet által megállapított védelem, amely egységes és szigorú szabályai révén magasabb védelmet kínál, végül pedig az általam javasolt módosítások figyelembe vételével a következő, magasabb védelmi szint. Az értekezés következtetése az, hogy hiába áll kézzelfogható közelségben hozzánk a magasabb védelmi szint, amikor a *forum shopping* révén a széttöredezettség és az alacsonyabb védelmi szint felé a visszacsúszás lehetősége is elképzelhető.

Zárszó

Minél erősebb és összetettebb kihívások érik az elért védelmet, annál fontosabb a saját rendszerünk erősségeinek, valamint gyengéinek ismerete, annak érdekében, hogy közös vívmányainkat megőrizhessük, és a védelem szintjét a jövőben ne csak megőrizni, hanem emelni is tudjuk. Ennek a szintnek a kritikus elemzéséhez és a gyakorlati alkalmazás elősegítéséhez nyújt támpontokat a védelmi lépcső elmélete.

4. A doktorjelölt teljes publikációs jegyzéke

A szerző témához fűződő publikációi– időrendi sorrendben	
1.	Szabó, Endre Győző Az adatvédelmi biztos első féléves tevékenysége INFOKOMMUNIKÁCIÓ ÉS JOG 2. pp. 66-69., 4 p. (2004) Közlemény:3401166 Jóváhagyott Forrás Folyóiratcikk (Szakcikk)
2.	Szabó, Endre Győző Az Európai Adatvédelmi Biztosról INFOKOMMUNIKÁCIÓ ÉS JOG 15 pp. 153-157., 5 p. (2006) Közlemény:3401168 Jóváhagyott Forrás Folyóiratcikk (Szakcikk)
3.	Szabó, Endre Győző A személyes adatok védelmének kérdései a virtuális világban. In: Talyigás, Judit (szerk.) Az internet a kockázatok és mellékhatások tekintetében Budapest, Magyarország: Scolar Kiadó, (2010) pp. 43-65., 23 p. Közlemény:3401029 Jóváhagyott Forrás Könyvrészlet (Könyvfejezet)
4.	Szabó, Endre Győző (szerk.) International Data Protection Conference 2011 Budapest, Magyarország: (2011) ISBN: 9789639722965 Közlemény:3401191 Jóváhagyott Forrás Könyv (Konferenciakötet) Hiányos
5.	Baka, Péter; Dudás, Gábor; Filipovits, Viktória; Freidler, Gábor; Keszely, Gábor; Kuthiné, Nagy Andrea; Révész, Balázs; Somogyvári, Katalin; Szabó, Endre Győző; Sziklay, Júlia; et al. Adatvédelem és információszabadság a mindennapokban Budapest, Magyarország: HVG-ORAC (2012), 480 p. ISBN: 9789632581637 OSZK Közlemény:2159442 Admin láttamozott Forrás Könyv (Szakkönyv)
6.	Balogh, Zsolt; Balogh-Békési, Nóra; Bándi, Gyula; Csink, Lóránt; Hajas, Barnabás; Koltay, András; Marosi, Ildikó; Schanda, Balázs; Szabó, Endre Győző; Zakariás, Kinga; et al. Alkotmányjog-Alapjogok Budapest, Magyarország: Pázmány Press, PPKE JÁK (2014) ISBN: 9789633081891 Közlemény:3401188 Jóváhagyott Forrás Idéző befoglalója Könyv (Felsőoktatási tankönyv) Oktatási
7.	Szabó, Endre Győző; Révész, Balázs Adatvédelmi jogi ismeretek In: Christián, László (szerk.) Az információs társadalom jogi vetületei: Alkalmazott jogi informatika Budapest, Magyarország: Pázmány Press, (2014) pp. 141-180., 40 p. Közlemény:3401183 Jóváhagyott Forrás Könyvrészlet (Könyvfejezet)

8.	Szabó, Endre Győző A személyes adatok védelméhez és a közérdekű adatok megismeréséhez fűződő jog In: Balogh, Zsolt; Balogh-Békési, Nóra; Bándi, Gyula; Csink, Lóránt; Hajas, Barnabás; Koltay, András; Marosi, Ildikó; Schanda, Balázs; Szabó, Endre Győző; Zakariás, Kinga - Schanda, Balázs; Balogh, Zsolt (szerk.) Alkotmányjog-Alapjogok Budapest, Magyarország: Pázmány Press, PPKE JÁK, (2014) pp. 245-266., 22 p. Közlemény:3401189 Jóváhagyott Forrás Könyvrészlet (Könyvfejezet)
9.	Szabó, Endre Győző; Bojnár, Katinka; Buzás, Péter Új globális technológiák kihívásai a magyar jogban In: Tóth, András (szerk.) Technológia jog: Új globális technológiák jogi kihívásai Budapest, Magyarország: Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, (2016) pp. 51-97., 47 p. Közlemény:3193720 Admin láttamozott Forrás Könyvrészlet (Szaktanulmány)
10.	Dr. Szabó, Endre Győző; Dr. Révész, Balázs: Adataink biztonságban - adatainkban a biztonság? INFORMÁCIÓS TÁRSADALOM: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT XVII. évfolyam: I. szám pp. 45-54., 10 p. (2017) Közlemény:30707366 Jóváhagyott Forrás Folyóiratcikk (Szakcikk)
11.	Dr. Szabó, Endre Győző Új technológiák adatvédelmi jogi elemzése In: Klein, Tamás; Tóth, András (szerk.) Technológia jog - Robotjog - Cyberjog Budapest, Magyarország: Wolters Kluwer (Budapest), (2018) pp. 26-67., 42 p. Közlemény:30344277 Jóváhagyott Forrás Könyvrészlet (Könyvfejezet)
12.	Szabó, Endre Győző A GDPR alkalmazásának kihívásai a magyar adatvédelmi hatóság szempontjából Szeged, Magyarország: Innovariant Nyomdaipari Kft. (2019) Közlemény:30681222 Jóváhagyott Forrás Könyv (Konferenciakötet)
A szerző egyéb publikációi	
13.	Gerhard, Robbers (szerk.); Szabó, Endre Győző (fordító) Állam és Egyház az Európai Unióban Budapest, Magyarország: Pápai Református Teológiai Akadémia (PRTA) (2004) ISBN: 9638645849 Közlemény:3401198 Jóváhagyott Forrás Könyv (Kézikönyv) Oktatási