Pécsi Tudományegyetem
Állam- és Jogtudományi Doktori Iskola

Kollár Gergő

Az európai adatjog jelene és lehetséges jövője

Doktori (PhD) értekezés

Témavezető:

Dr. Szőke Gergely László

Pécs

2025

Tartalomjegyzék

Ábrajegyzék

1. Bevezetés, kutatási célok és kérdések, kutatásmódszertan

1.1. Bevezetés

1.1.1. A változásról és az egyensúlyról

A világban a változás elkerülhetetlen, ez az univerzumunk talán egyetlen állandó jellemzője.[1] Ha a világ állandója pedig a változás, akkor az életé a folyamatos törekvés a fennmaradásra. Mondhatnánk, hogy ez is csak olyan, mint a biciklizés, csak akkor tudjuk az egyensúlyunkat megőrizni, ha mozgásban maradunk.[2]

Az egyensúly elérése és megtartása kiemelt kérdéskör számos filozófiai és bölcseleti iskola számára.[3] *Marcus Aurelius* az utolsó „jó" római császár és filozófus a Pax Romana végéhez közeledve *Elmélkedések* című írásában „lelke egyensúlyának"[4] mindenkori megtartásának fontosságáról írt az élet különböző viszontagságai között is. Gyakran idézett aforizma tőle „a világ változás, az élet felfogás dolga"[5] amelyet az egyensúlyra törekvő embernek szóló – a külső és a belső világ közti ellentétek kiegyenlítésére tett erőfeszítéseire vonatkozó – iránymutatásként is felfoghatunk. Bár egy jogtudományi tárgyú írást mindig jó megoldás egy római császár gondolataival indítani, meg kell jegyezni, hogy az egyensúly fontosságának hangsúlyozása ezen a célon túlmutat, hiszen az kiemelt jelentőségét megőrizve a világtörténelemben lépten nyomon felmerül. A szélsőséges érzelmektől mentes egyensúly gondolata – mint a boldogság kiemelt eleme – a sztoicizmus filozófiájából általában kiolvasható, azt mint *„apatheia"* jelölték.[6] Ezzel egyébként parallel gondolat az epikureizmusban is felfedezhető, amelyet *„ataraxiának"* neveztek és azt a kiegyensúlyozott nyugalmat jelentette, amiből semmilyen külső esemény sem képes a kizökkentésre.[7] Az arisztotelészi etikában szintúgy megtalálható mértékletesség és kiegyensúlyozottság eszméje, amelyet Horatius nyomán az arany középútnak *(„aurea mediocritas")* is nevezhetünk. A hellenizmustól eltávolodva a keresztény kultúrkörben is megtalálható az „*equanimity",* vagyis az egyenletesség és kiegyensúlyozottság erénye, amely egyes szerzők szerint olyan lényeges, hogy "szükség van rá a nap minden órájában, a világ minden helyén".[8]

A világunk változásai mára elvezettek az adatok fontosságának megnyilvánulásához és az életünkben betöltött valódi szerepüknek felismeréséhez. Jelen kutatás célja ezért az adatalapú működéssel járó élethelyzetek szabályozására tett európai uniós – és azon belül magyar – jogalkotási lépések vizsgálata. A terület vonatkozásában mind a szabályozással érintett viszonyok, mind a vonatkozó jog számottevő változáson ment keresztül az elmúlt évtizedben.

---

[1] Hérakleitosz görög filozófus frappáns megfogalmazásában: „Semmi sem marad változatlan, csak a változás maga."

[2] A gondolat talán Albert Einstein, 1930-ban fiának írt leveléből származik, amelyet Walter Isaacson 2007-ben publikált „Einstein: His Life and Universe" című művében. Elérhető: https://quoteinvestigator.com/2015/06/28/bicycle/

[3] Ryan Holiday: Az egyensúly a kulcs. Budapest, 21. Század Kiadó, 2020.16 o.

[4] Marcus Aurelius: Elmélkedések. Fordította: Huszti József. A fordítás alapjául szolgáló kiadás: I. H. Leopold: M. Antoninus imperator ad se ipsum. Oxonii, 1908. Elérhető: https://mek.oszk.hu/00600/00606/ 3 o. (továbbiakban: Elmélkedések)

[5] Marcus Aurelius: Elmélkedések 16 o.

[6] Massimo Pigliucci (City University of New York) „Stoicism", Internet Encyclopedia of Philosophy. Elérhető: https://iep.utm.edu/stoicism/#H4

[7] Tim O'Keefe (Georgia State University) „Epicuros", Internet Encyclopedia of Philosophy. Elérhető: https://iep.utm.edu/epicur/

[8] R.B. Seeley és W. Burnside: Twenty Essays on the Practical Improvement of God's Providential Dispensations, as Means of Moral Discipline to the Christian. Oxfordi Egyetem, 1838. 53-54 o. Elérhető: https://books.google.hu/books/about/Twenty_essays_on_the_practical_improveme.html?id=lFwEAAAAQAAJ&redir_esc=y

Mostanra azonban megvalósíthatónak mutatkozik az „adatjogi paradigma” egységes szerkezetű elemzése, az eddig kialakított álláspontok összehangolása és szükség esetén akár újragondolása, kiegészítése. Mindezt – bár némi filozófiai alátámasztással – de személyes meggyőződésem által vezérelve, az egyensúly, mint egyéni és társadalmi szinten is kívánatos cél elérésének szellemiségében teszem, hiszen a világ időnként szélsőséges változásai[9] közepette a fennmaradásunk egyik kulcsa az egyensúlyunk megőrzése lehet.

1.1.2. Az adatok általános jelentőségéről

A szerzői ars poetica körül járásakor a kutatás tárgyának, vagyis az adatoknak a fontosságát is érdemesnek tűnik bemutatni. Az adatok szerepének meghatározásával kapcsolatban széles spektrumon mozgó elképzelések között válogathatunk. Az egyik végponton egy talán köznapi elképzelésnek tekinthető „dataista” megközelítéssel,[10] amely az adatok fundamentális szerepét hangsúlyozza. E szerint „az univerzum adatfolyamokból áll és minden jelenség vagy entitás értékét az határozza meg, mennyiben járul hozzá az adatok feldolgozásához.”[11] Az elmélet alapján mind mikro, mind makro szinten, tehát az egyénitől a társadalmi működésig minden és mindenki (nem adatvédelmi jogi terminológia szerint) adatfeldolgozásként, illetve adatfeldolgozóként értelmezhető. A másik végponton egyes jogszabályi meghatározások[12] és a szikárabbnak mondható (jog)irodalom képviselőinek álláspontja szerepel, amely az adatok létezését csak, mint digitális állományok bináris kódja tudja elfogadni és kezelni, ezzel egy praktikusabb, de egyúttal szűkebb és merevebb értelmezést követve.

Azt gondolom, hogy az igazság valahol az arany középúton, a két véglet között lehet. Az adatok esszenciális tartalmának megragadása egy nagy és ráadásul igencsak interdiszciplináris kihívás, amihez bizonyosan át kell lépni néhány konvencionális határon. Azonban a gyakorlati alkalmazhatóság szempontját, legalábbis a jogtudomány, nem hagyhatja figyelmen kívül. Így a magam részéről az adatok értelmezésének a digitális megjelenésen túl, a pusztán elemzési képességeket lehetővé tevő funkción felül is látom a helyét,[13] sőt az ezzel kapcsolatos kiterjedtebb szabályozási szükséget is azonosíthatónak gondolom. Azonban mind a jogalkotást, mind a saját kutatásomat a realitás által diktált hatókörre tartom célszerűnek szabni, figyelembe véve, hogy a jelenlegi technológiai és társadalmi trendekben az adatok hegemónja a digitális adat, az azon való műveletek fősodorbéli típusa pedig többségében elemzési jellegű.

A bevezetőben az adatfogalom definíciós nehézségein egyelőre túlléphetünk, ennek vizsgálatára egyébként is külön fejezetet szentelek jelen dolgozatban. A jelentőséggel kapcsolatban annyit még azonban érdemes rögzíteni, hogy a digitális adatokon való műveletvégzés által elérhető értékteremtés – ami az adatok jelentőségének egyik kiemelt forrása – a közgondolkozásban viszonylag régóta megjelent, hiszen már 2006-ban rögzítésre

[9] 21. századi léptékkel extrém változások alatt gondolhatunk a COVID-19 járványtól kezdődően, az orosz-ukrán és izraeli háborúkra, vagy a különböző erőforrás alapú (pl. energia, félvezető) és pénzügyi válságokra.

[10] Nézőpont kérdése, hogy tudományos, tudománnyal határos vagy egyenesen tudományos fantasztikumnak tekintjük a szerző műveit, kétségtelen azonban, hogy a gondolatai nagy népszerűségnek örvendenek. A dataizmussal kapcsolatban részletesen ír: Yuval Noah Harari: Homo Deus: A holnap rövid története. Magyar kiadás, Animus Kiadó, 2016.

[11] U.o. 316-317 o.

[12] Az Európai Parlament és a Tanács 2022/868 rendelete az európai adatkormányzásról (továbbiakban adatkormányzási rendelet, vagy DGA) által alkotott általános jogi adatfogalom szerint az adatok az aktusok, tények vagy információk digitális megjelenítései

[13] Természetesen ezzel nem vagyok így egyedül, az Európai Parlament és a Tanácsnak a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló 2016/679 sz. rendelete (továbbiakban: általános adatvédelmi rendelet vagy GDPR) is az adatkezelés fogalma alatt értette mind az automatikus (pl. digitális) és a nem automatikus (pl. analóg) műveleteket, ezzel – még akkor is, ha feltételekhez kötötten – de elismerte a nem digitális adatok jelenlétét és azok jelentőségét.

került az azóta sokat ismételt frázis, miszerint „az adat az új olaj”.[14] A kijelentés lényegét tekintve az adatok erőforrás jellegére hívja fel a figyelmet akként, hogy az emberi civilizáció technológiai fejlődésére óriási hatást gyakorló fosszilis energiahordozókkal hozza párhuzamba.[15] A hasonlat tehát helyesen állapítja meg a gazdasági, politikai és társadalmi értékhordozó szerepet és egyébként azt is, hogy sem az adat, sem az olaj nem éri el a benne rejlő potenciált valamilyen feldolgozási/finomítási művelet nélkül.[16] Bár a felismerés lényegét nem csorbítja, a párhuzam pontossága gyorsan halványul, amint az adatok egyedi körülményeit is figyelembe vesszük (pl. rivalitás, megújulás kérdései). Az utóbbi évek európai fejleményei alapján azonban már azt is határozottan látjuk, hogy az adatokban rejlő értéket mind az uniós döntéshozók,[17] mind a szakirodalom[18] elismeri, sőt kifejezetten hangsúlyozza. Kétségtelennek tűnik tehát, hogy az adatok jelentőségét szakmai és tudományos érvek is alátámasztják.

1.1.3. A jog és a technológia kapcsolatáról

Az adatokat a digitalizációval jelenleg fennálló szoros kölcsönhatásuk miatt a technológiától elválasztva tárgyalni helytelennek tűnik. Azonban ahhoz, hogy e kettőt a jelen írásban összepárosíthassuk először a jog és a technológia kapcsolatát kell röviden megalapoznunk, lévén, hogy az adatokra vonatkozó, de jogi kutatás a jelen dolgozat tárgya.

Technológia alatt alapvetően az emberi képességeket javító megoldásokat értjük, ami így magába foglal a tűzgyújtástól kezdve a pattintott kőeszközökön és a gőzgépeken keresztül egészen az atombombáig vagy a nagy nyelvi modellekig mindent. A fejlődés az első írásos emlékünk megjelenése óta eltelt mintegy 5000 év nagy részében lassú, de biztos volt, azonban az elmúlt körülbelül másfél évszázadban meredek gyorsulás tapasztalható. Gondolhatunk a 3D nyomtatásra, virtuális valóságra, dolgok internetéhez tartozó okos eszközökre vagy különösen a mesterséges intelligenciára.[19] Előbbiek közül bármelyik olyannyira elrugaszkodottnak tűnhetne a 20. századi embernek, mint az első ezredforduló környékén iniciálét formázó ciszterci szerzetesnek a gutenbergi könyvnyomtatás. Nagy differenciát jelent azonban, hogy előbbi esetben az idő különbség évtizedekben, míg utóbbiban évszázadokban mérhető.

A jognak, mint a társadalmi normák egy formájának mindig is fontos szerepe volt a technológia alkalmazásának kérdéseiben, azonban annak a fejlődése (és jelenleg már sebessége is) az, ami az igazi kihívást jelenti. Bár számtalan kölcsönhatás azonosítható a technológia, a jog és a társadalom között, mégis azt mondhatjuk, hogy a jogszabályok a technológiai fejlődés által előidézett társadalmi változás utólagos leképződéseként jelennek meg. Így gyakorlatilag a

---

[14] Bart Custers, Helena U Vrabec and Michael Friedewald, „Assessing the Legal and Ethical Impact of Data Reuse: Developing a Tool for Data Reuse Impact Assessments (DRIA)”, European Data Protection Law Review (EDPL), 5(3), 2019. 317 o.

[15] Gondoljunk csak a Cambridge Analytica botrányra, aminek a napvilágra kerülése éppen elmúlt tíz éves. Ebben a targetált kampányoktól kezdődően, a Tech-óriások által üzemeltetett közösségi média platformok működési sajátosságain keresztül globális politikai (atomhatalmak nemzetszuverenitását érintő) kérdések is felmerülnek, miközben még mindig *csak* adatok elemzéséről van szó. Részletes beszámoló az ügyről elérhető: The New York Times, Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

[16] Eszteri Dániel, „Adatmonopólium és buboréklét”, Országút (Magyar Szemle Alapítvány). Elérhető: https://orszagut.com/tudomany/adatmonopolium-es-buboreklet-eszteri-daniel-4438

[17] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az Európa digitális jövőjének megtervezéséről (COM(2020) 67 final) megfogalmazás szerint az adatok által lehetővé tett átalakulás jelentősége „az ipari forradalomhoz mérhető.”

[18] Például lásd: Wolfgang Kerber, „A new (intellectual) property right for non-personal data? An economic analysis, MAGKS Joint Discussion Paper Series in Economics, No. 37-2016, Philipps-University Marburg, School of Business and Economics, Marburg. 2 o.

[19] Amelynek kapcsolata az adatokkal gyakorlatilag szimbiotikusnak mondható.

technológia az, ami sok esetben determinálja a jog alakulását és nem fordítva.[20] A kihívás pedig elsősorban abban áll, hogy a jogalkotás a társadalmi rendet és különböző jogokat, valamint szabadságokat fenntartsa, úgy, hogy a technológiai fejlődés elé ne állítson túlzott akadályokat. Másként megfogalmazva a jog egy stabil átjárást biztosító *(az egyensúlyi helyzetet fenntartó)* hidat kell képezzen a technológia és a társadalom között, ezáltal megfelelve mindkét rendszer értékeinek egyszerre.[21] Ezt az önmagában komoly feladatot tovább árnyalja egyfelől, hogy az egyre gyorsuló fejlődés kevéssé tűri a jogalkotás klasszikusan kimért tempóját. Másfelől fontos az is, hogy a technológiai jog, mint jogterület a technológia mindent átható/átjáró jellege miatt nehezen tudja a specialitás fogódzóit megtalálni és egységes, önálló identitást kreálni magának,[22] ezért sok esetben azonosítható az erre a területre irányuló joganyagnak az általános fragmentáltsága. Ez természetesen érthető, sőt, ha nemcsak a technológia és a jog, hanem a társadalom és a jog közrehatását is elkezdjük felfejteni, akkor olyan tényezők is láthatóvá válnak, mint a „szabályozói foglyulejtettség", vagyis az a helyzet, amikor a lobbierő a széleskörű jogvédelem helyett szűk érdekek szolgálatát kényszeríti ki a döntéshozóból.[23]

Végső soron tehát a jog és a technológia egyre szorosabb, de továbbra is rapszodikus kapcsolatát napról napra kell „megélnünk" és ahol lehet a helyes értelmezés megtalálásával az egyéni és a csoportos, valamint a köz- és magánérdekek kedvező egyensúlyát megtalálnunk.

1.1.4. A kutatott területről

A bevezető alapján tehát az adatok és az adatalapú életviszonyok kerülnek a kutatás fókuszába, abból a célból, hogy a jog által a szabályozásukra tett lépéseket áttekintsük, az elemeket és a közöttük lévő mintázatokat azonosítsuk. Mindezt azért, mert ebben a változásokkal teli világban a technológia és a társadalom közti egyensúlyt a jog eszközeivel helyreállíthatónak és tartósan megőrizhetőnek gondolom. Ehhez azonban mérleget kell vonnunk a múlt eredményei és a jövő lehetőségei között, tisztán és tárgyilagosan megítélve a jelent és a modern, adatalapú társadalmak állapotát. Ehhez számos alapvető és néhány speciális – mostanra konvencióvá alakult – határt kell megkörnyékezni (talán átlépni), amelyet a következőkben, mint kutatási célkitűzések és kutatási kérdések összegzek.

1.2. Kutatási célok és kutatási kérdések

1.2.1. A kutatás célkitűzéseiről

A munkám egyik egész dolgozaton átívelő céljaként *az adatalapú viszonyok egyensúlyát* szolgáló adatjogi megoldások azonosítását, illetve ilyenek hiányában meghatározását tűztem ki. Ennek két szintjét határoltam el.

A globális szint: Az Európai Unió technológia- és ezzel együtt adatszuverenitás elérését tűzte ki célul,[24] ami alatt olyan szabályokat értünk, amelyek egy (államhoz vagy szupranacionális szervezethez tartozó) adathalmaz feletti rendelkezés, az azon való műveletvégzés korlátozását érintik.[25] A célkitűzés mögötti motiváció az adatokban rejlő politikai és gazdasági erő

[20] Polyák Gábor, Szőke Gergely László, „Technológiai determinizmus és jogi szabályozás, különös tekintettel az adatvédelmi jog fejlődésére", In: E-közszolgálatfejlesztés. Nemzeti Közszolgálati Egyetem, Budapest (2014). 31 o.
[21] Tóth András, „A technológia szabályozásának jogi kihívásai", in: Tóth András (szerk.): Technológia jog – Új globális technológiák jogi kihívásai. Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2016. 27-29 o.
[22] Ződi Zsolt: Platformok, robotok és a jog. Budapest, Gondolat Kiadó, 2018. 67 o.
[23] Tóth, 2016. 31 o.
[24] COM(2020) 67 final
[25] Susan Ariel Aaronson, „What Do We Mean by Data Sovereignty and How Might It Impede Data Sharing?", Centre for International Governance Innovation (2023). 8 o.

megtartására és az európai érdekek és értékek védelmére irányul – indokoltan mondhatnánk – mivel az Unió sem az USA, sem Kína térnyerését nem tudta az elmúlt években sikerrel lekövetni. Jelenleg az európai adatalapú folyamatokat és az azokat körülvevő infrastruktúrát is Európán kívüli hatalmi koncentrációk irányítják,[26] a helyzet ellensúlyozását az EU saját adatgazdasági törekvéseit támogató, egyúttal az alapjogokat és európai értékeket figyelembe vevő megoldások szolgálhatják, amelyek kidolgozásához jelen dolgozat eredményei potenciálisan hozzájárulhatnak.

A közösségi szint: A világ adatállományának jelentős részét az államok mellett kevés piaci szereplő (egyes felmerések szerint körülbelül 70 multinacionális vállalat) tartja tényleges hatalmában.[27] Az adatok feletti kontroll pedig – mint értékteremtő és allokáló tényező – politikai és gazdasági erő összpontosítását teszi lehetővé. Ezt a folyamatot többféleképpen ismeri az irodalom. A *„második elkerítés”* (*second enclosure*, ami a 16-18. századi angol politikai-gazdasági folyamatokra utal vissza) jelenségeként[28] hivatkozzák, amikor mindenki számára hozzáférhető vagy egy gyengébb érdekérvényesítő képességgel rendelkező fél erőforrását (jelen esetben mondhatnánk az adatát) az erősebb elvonja. *„Megfigyelési kapitalizmus”* (*surveillance capitalism*) nevet kapta, mikor tömeges adatgyűjtésre és elemzésre alapuló üzleti/ügyviteli modelleken keresztül a gazdasági és társadalmi folyamatok predikciója és manipulációja történik.[29] E két elmélet gyakorlatilag fúziójaként jött létre a következő (vissza)fejlődési szakasz, a „techno- vagy adatfeudalizmus”, ami már a teljes dominanciára, úgynevezett digitális hűbéri rendszerre építkezik.[30] Végső soron mindben a már régóta ismert információs túlhatalom[31] *(vagy egyensúlytalanság)* rémképe, az, ami megjelenik. Ez előrehaladott stádiumaiban alapvető gazdasági, társadalmi és végső soron alkotmányos érdekeket veszélyeztethet. Az ilyen tendenciákkal szembeni fellépés földrajzi elhelyezkedéstől függetlenül, már közösségi szinten is értelmezhető, az enyhítésükre tett lépések pedig indokoltnak tűnnek. Ilyen lépések lehetnek az adatok akadálymentes áramlásának forgalmi és a kapcsolódó folyamatok kimeneteinek biztonsági előírásai, vagy az adatalapú gazdasági szegmensek nyitottsága felett őrködő rendelkezések. Ezeket jelen kutatás eredményei – az egyének és kiscsoportok érdekvédelmi esélyeinek javulását szem előtt tartva – potenciálisan szolgálhatják.

Összegezve az első célkitűzés az adatalapú viszonyok egyensúlyi helyzetére irányul, annak érdekében, hogy ahol egyensúlytalanság azonosítható, ott az helyreállítható legyen. Egyfelől globálisan, tehát Európa és a világ más hatalmai között, másfelől közösségi szinten az egyének és kiscsoportok között.

A második célkitűzés az elsőnél személyesebb indíttatású. A saját – adatokkal és azokon történő műveletvégzéssel kapcsolatos – tapasztalatom alapján egy nagyon fontos tulajdonság hiányát látom a jelenlegi, területre vonatkozó joganyagban. Ezt *adatjogi tisztánlátásnak* nevezném, ami szoros kapcsolatban áll a fenti helyzetekből adódó esetleges egyensúlyvesztett állapottal is. Azt mondhatjuk, hogy – számos érthető körülmény miatt, mint a fejlődés gyorsasága, a technológiai

[26] Tóth András, „Az Európai Unió (szabályozási) útja a szuverenitás felé az adatalapú gazdaságban”, Európai Tükör, Évf. 24 szám 2. (2021). 28 o.
[27] Susan Ariel Aaronson, „Private Firms Want to Control the Data They Collect and Prefer Not toShare It”, Centre for International Governance Innovation (2023). 5 o.
[28] James Boyle, „The Second Enclosure Movement and the Construction of the Public Domain” Duke Law School Public Law and Legal Theory Research Paper Series, Research Paper No. 53. 2003.
[29] Shoshana Zuboff, „Big other: surveillance capitalism and the prospects of an information civilization”, Journal of Information Technology (2015) 30, 2015. 75–89 o.
[30] Carlos Saura García, „Datafeudalism: The Domination of Modern Societies by Big Tech Companies”, Philosophy & Technology (2024) 37:90 https://doi.org/10.1007/s13347-024-00777-1
[31] Szabó Máté Dániel: Az információs hatalom alkotmányos korlátai. Miskolc, Miskolci Egyetem, 2012.

jog természetes töredezettsége – az adatokra vonatkozó jog egyfajta befejezetlenség érzetét kelti az alkalmazóban. Az látható, hogy némely alapvetőnek mondható kérdés kibontását mintha szándékosan kerülné az európai jogalkotó, amely miatt a jogszabályok körvonalai jól követhető egyenes vonalak helyett amőbához hasonló alaktalanságban szenvednek. A tisztánlátás hiányának eredményeként a jogalkalmazás során az a tapasztalás alakul ki, mintha egy sötét teremben néhol halvány, néhol élénk fényű zseblámpákkal próbálnánk egy bonyolult kirakós darabjait megtalálni és összeilleszteni. A probléma így az, hogy a zseblámpák adott pontokra irányuló fénye kétségtelenül hasznos, azonban a pontok közötti magasabb rendű összefüggések megvilágítása nélkül az előrehaladás bizonytalan, a kimenetele pedig kétséges. Ennek természetesen oka lehet a korábban említett foglyulejtettség, ami ellen jelen dolgozat megírásával semmit nem lehet tenni. Azonban van arra is lehetőség, hogy találhatunk egy hiányzó jogalkotási láncszemet, egy (vagy több) szabályozási hiányterületet, aminek a megléte esetén ez a diszfunkcionalitás orvoslásra kerülhet. Ez a hiányzó láncszem egyfajta adatjogi fundamentumként (vagyis a terembeli villanykapcsolóként) képzelhető el és a szerepe elsődlegesen az lenne, hogy alapot teremtsen az egyéb, speciálisabb jogi előírások hatékony működéséhez (vagyis a kirakós darabjainak összekapcsolódásához).

Összegezve a második célkitűzésem az adatjog jelenlegi állapotának feltárása és a diszfunkcionalitás kiváltó okának azonosítása és lehetőség szerinti megszüntetése, ezáltal az adatjogi tisztánlátás elérése.

1.2.2. A kutatási kérdésekről

A fenti két kutatási célkitűzés elérésére az alábbi kutatási kérdések megválaszolása szolgálhat.

1. Az adatok jog általi pontosabb megragadhatósága érdekében milyen lényeges szempontokat érdemes figyelembe venni?
2. Hogyan definiálhatjuk az európai adatjogot, milyen mozgatóelvek és elhatárolási pontok azonosíthatók az egyes elemei között az adatalapú életviszonyok vizsgálatának tükrében?
3. Milyen alterületekre bontható az adatjog és azoknak milyen főbb jellegzetességei vannak?
4. Az adatalapú működés szempontjából milyen általános hiányosságok azonosíthatók a vonatkozó joganyaggal kapcsolatban?
5. A feltárt hiányosságok alapján milyen javaslatok tehetők?

1.3. Kutatásmódszertan

A kutatás a gyakorlat nagyon is valós kérdéseire – jelen dolgozat keretei között – csak elméleti választ adhat. Ezért a Hans Kelsen féle *„sein”* vagyis a „mi van” kutatása mellett a *„sollen”*, tehát a „mi kell” területére szükséges kilépnünk. Azonban ezt sem tehetjük könnyelműen, hiszen a jog a megjelenésétől kénytelen saját létét igazolni, ehhez igazodva az én munkám sem lehet a légüres térnek címzett, önmagáért való iromány.

1.3.1. A módszertanról általában

A *sein* kutatásához a már létező és tervezett jogot, az arra vonatkozó szakirodalmat és döntéshozói kísérő dokumentációt, valamint a bírósági/hatósági gyakorlatot használtam fel. A módszereket tekintve a nyelvtani, a logikai, a rendszertani, a történeti és teleologikus megközelítést is alkalmaztam. A *sollen* esetében egyfelől a stabil elméleti alapozáshoz hasonló tárgyú és célzatú szakirodalmi és egyéb forrásokat vizsgáltam. Másfelől saját megoldásokat is kerestem a felmerülő kérdések megválaszolására, a következtetéseket az indukció, dedukció és szillogizmus eszköztárára alapozva igyekeztem létrehozni. A dolgozat hipotetikus elemeit *gondolatkísérletek* formájában alkottam meg, végig haladva a felmerülő szabályozási lehetőségeken és azok potenciális következményein. A kísérletek – természetükből adódó feltételezésekkel átszőtt – útvesztőjében nagy metodológiai kihívás a kell és a kell*het* vékony,

de annál fontosabb határának meghúzása, vagyis a szükségtelen *többlet* bevezetésének kerülése. Így az elméleti vizsgálódásom és következtetéseim tárgyának és hatókörének meghatározásakor is célzatosan (Ockham borotvájával a kezemben), a gyakorlati hasznosíthatóság eszméje által vezérelve igyekeztem eljárni. A módszertan gondolatkísérleti komponensét saját és szakmai környezetem tapasztalataival egészítettem ki. Az adatvédelem alkalmazásának területén közel egy évtizedes rutinnal rendelkezem, tanácsadóként számos piaci szegmens, illetve magán- és közszervezet működését ismertem meg, a benne dolgozók igényeivel és aggályaival együtt. Egyetemi kutatóként olyan kutatási és tudástranszfer projektekben vettem részt, amelyek által a tanácsadói látóteremet számottevően bővíteni tudtam. Az adathasznosítás tekintetében Magyarország első – Adatkormányzási rendelet[32] szerinti – semleges adatközvetítő szolgáltatójának társalapítójaként és ügyvezetőjeként az európai adatgazdaság jelen állapotáról egészen közeli és gyakorlati információkkal rendelkezem. Végezetül különösen hasznosnak találtam a *„Data Intermediaries Alliance”* tudományos bizottságában betöltött szerepemet, amin keresztül naprakész ismereteket tudtam szerezni a többi EU tagállam szereplőinek a területen szerzett tapasztalatairól.[33]

1.3.2. A kutatási módszerek megvalósításáról

1. Az adatok jog általi megragadhatóságához megfelelő távolságból kell indítani a kutatási folyamatot és olyan jogon kívüli (ismeretelméleti, filozófiai, technológiai) kitekintést kell eszközölni, ami a későbbi jogelméleti vizsgálódásokhoz megfelelő alapot tud biztosítani (2. fejezet). Ez alapvetően az adatfogalom-alkotás (szemiotikán alapuló) kísérleteiben nyilvánul meg, amelynél deduktív módszerrel az általánosan tudott vagy ismert törvényszerűségekből kiindulva törekszem az adatok egyedi ismérveinek feltárására, a jog számára értelmezhető alaptulajdonságainak rendszerbe szedett bemutatására. Az adatok ismérveinek és tulajdonságcsoportjainak összeállításával, valamint az elméleti létrejövetel folyamatának végig követésével létrejövő eredmények adhatják többek között a jogi minőség és a jogosulti kör kijelölésének elvi alapját. A 2. fejezetben az adatjog jelen állapotának értékeléséhez szükséges (technológiai és jogi) adatfogalmak összegzően, leíró-elemző módszerrel kerülnek áttekintésre az absztrakt adatfogalom szintaktikai és szemantikai rétegeinek vizsgálata keretében. Mivel az adatokhoz való értékrendelés számos kérdést vet fel a jelenlegi tudományos diskurzusban, az értékesség mibenlétének áttekintő vizsgálatára is sor kerül itt, ami kiindulópontként szolgál a monetizáció alkotmányos és magánjogi kérdéseinek, valamint az adatok polgári jogi megítélésének megválaszolásához.
2. Az európai adatjog létének kérdése alapvető fontosságú a terület vizsgálatához (3. fejezet). A vonatkozó hatályos joganyag kiterjedtsége és kora lehetővé teszi az érdemi vizsgálatot, így célszerűnek mutatkozik egy rövid történeti kitekintést tenni a terület vonatkozásában ahhoz, hogy a szabályozott életviszonyok (és alakulásuk) jól láthatók legyenek. Az adatjog létezésének lehetőségét és szükségességét, a joganyag csoportosítási lehetőségeit induktív módon, a létező és megfigyelhető jogi aktusok és kinyilvánított jogpolitikai célkitűzéseken keresztül vizsgálom. Ezzel a későbbi kutatási lépések kereteit és dogmatikai megalapozását kísérlem meg, egyúttal a fókuszpontként szolgáló hiányosságok (és az azokra tett javaslatok) vizsgálati spektrumát is ezzel tudom kijelölni. A 3. fejezetben a területen tapasztalható, az adatokkal kapcsolatos döntéssel és azok értékének (főként pénzben kifejezhető formában) kiosztásával kapcsolatos jogelméleti disszonanciát is vizsgálom, mivel annak megoldatlansága úgy gondolom a gyakorlat számára aránytalan zavart okoz. A szillogizmus módszerével megkísérlem a tényleges élethelyzetek alapján levonni a háttérben működő szabályszerű tendenciára (értékegyenlőségi elv) vonatkozó következtetést és annak

[32] DGA III. fejezet
[33] Lásd: https://www.dataintermediariesalliance.org/scientific-committee/

működési sajátosságait elméleti síkon feltárni. Ezzel az adatalapú életviszonyok – és így az adatjogi szabályozás – mögötti mozgató erőt igyekszem azonosítani azért, hogy a jelenlegi állapot helyesen értelmezhető, a jövőbeni események nagyobb valószínűséggel megbecsülhetők lehessenek. Az azonosított szabályszerűséget igyekszem alkotmányjogi és magánjogi kontextusba helyezni, annak érdekében, hogy annak elfogadhatósága (jog általi elismerése) egyáltalán lehetséges-e.

3. Az adatjog alterületeinek részletes, de lege lata vizsgálatára van szükség a jelenlegi állapot megítéléséhez és így a hiányterületek későbbi azonosításához (4. fejezet) A 3. fejezet klasszifikációs lehetőségeit (jogdogmatikai és pragmatikus) alapul véve az alterületeket általában és az oda vonható jogi aktusokat, jellegadó tulajdonságaik alapján leírom, elemzem és értékelem. Ennek az alapvető célja, hogy a közös vonásokat és az eltéréseket is ki tudjam emelni, ezzel egy általános körképet biztosítva a hatályos helyzetről. A jogszabályokat nyelvtani és rendszertani szempontból is vizsgálom annak érdekében, hogy egy közös következtetési alapot hozzak létre a teleologikus módszerrel történő kiegészítéshez. Fontos ugyanis annak legalább közelítő megítélése, hogy mi lehetett az elérni kívánt cél a jogi normák megalkotásakor, hiszen ennek tovább gondolása által lehetséges a hiányterületek orvoslására megfelelő javaslatokat tenni.
4. A jelent és a jövőt átkötő 5. fejezet kimondott célja a dolgozat addig a pontig elért eredményeinek szintetizációja, a „sein” tényleges és a „sollen” lehetséges irányainak felvázolása és értékelése. Ezt egy hipotetikus kontextus-elemzési technikán keresztül végzem el, aminek az eredményeként az adatjog hiányterületeinek azonosíthatósága fog reményeim szerint előállni.
5. A feltárt hiányosságok vonatkozásában, a felvetett problémákat esetlegesen orvosolni képes, javaslatokat fogalmazok meg (6. fejezet). Ezek tekinthetők de lege ferenda javaslatoknak, azonban azok egy része akár piaci önszabályozó eszközökön (pl. szabványokon) keresztül történő megvalósítással is elérhetik a vélelmezett jogpolitikai célokat. A javaslatok a kutatási célkitűzések által előrevetített helyzetekre kívánnak reagálni, vagyis fontos szempont, hogy azok az EU értékekkel és célokkal egy irányban, a gazdasági, jogi, technológiai és társadalmi érdekek egyensúlyának megőrzésére képes módon, az adatjogi tisztánlátást megvalósítva működjenek.

2. A szemiotikus adatfogalom

A jelen fejezetben az adatok absztrakt, általános és speciális ismérveit és tulajdonságait keressük azért, hogy a későbbi témáknak stabil alapot és összetartó kapcsot adhassunk. Ehhez a DIKW piramis újragondolásával megkísérelj̈ük az absztrakt adatfogalom megalkotását, megvizsgáljuk az adatok létrejöttének elméleti folyamatát, meghatározzuk az adatok öt általános ismérvét és tulajdonságaiknak öt csoportját. Megkülönböztetjük az adatfogalom szintaktikai és szemantikai rétegeit, ezzel körülhatároljuk a technológiai és jogi adatkategóriákat. Végül az adatok megnőtt értékességének hátterében álló folyamatokat is röviden áttekintjük.

Az adatalapú működés és az irányadó joganyag területeinek átlátható szeletekre bontásához és az azokon belül található fogalmi egységek értelmezéséhez fontos egy olyan közös nevező létrehozása, amelyre biztos alapok építhetők. Egy ilyen alapvető – jogászok számára kiemelten fontos – terület a definíciós kísérletek számbavétele és lehetőség szerinti egységesítése. Jelen fejezet célja az adat fogalmának és típusainak elemi vizsgálata, a későbbi komplexebb kérdések megválaszolásának terminológiai szempontú támogatása érdekében. A fejezet eredményeként egy olyan, a gyakorlati és elméleti szempontokat is figyelembe vevő, egységesen alkalmazható

adatfogalom-rendszer jöhet létre, amely jobban adaptálható a modern, sok esetben algoritmizált folyamatokhoz.

A jelelméleten alapuló (szemiotikus) fogalomalkotás a szakirodalom egy preferált megközelítése,[34] így ezt a módszertant követve először az absztrakt adatfogalomból építkezve határozom meg az adatok szintaktikai és szemantikai rétegeit.

2.1. Az adatok absztrakt fogalma

Az „adat" kifejezés rendkívüli népszerűségnek örvend a mai tudományos és köznapi diskurzusban egyaránt. Az adatfogalom azonban ritkán kerül kellő komplexitással kifejtésre, aminek következtében egy – a szükségesnél nagyobb – értelmezési nehézség alakul ki rögtön az adatalapú folyamat kezdő pontján. Ez egyébiránt visszatérő eleme azon jelenségeknek, amelyek első ránézésre túlzottan is egyszerűen definiálhatónak tűnnek, hiszen ki ne tudná mit jelent az, hogy adat? Azonban a határterületek és rokon fogalmak számbavétele során a pontos meghatározás nem is olyan egyszerű feladat. Márpedig abban az esetben, ha az e fogalom alá tartozó elemekkel valamit véghez szeretnénk vinni (pl. használni kívánjuk őket), tudnunk kell mire gondolunk pontosan.

Az adatok lényegének megragadása az adat legabsztraktabb[35] rendszertani elhelyezésén keresztül mutatkozik célszerűnek, amely során a különböző fő és alterületek is kifejtésre kerülhetnek, ezáltal az adatok esszenciális értelme jobban kiemelhető. Ehhez zsinórmértékül az un. DIKW piramis vagy hierarchia modell[36] szolgál, amelyet azonban olyan módon gondoltam újra, hogy az jobban illeszkedjen az adatok (kiemelten algoritmizált keretek közötti) használatának témaköréhez. Az új modell – az algoritmusokra jellemző működési mechanizmusokkal együttesen – segítheti a modern, adatalapú működési folyamat megértését.

A kognitív folyamat – hagyományos értelemben „gondolkodás" – jelentősége nehezen megkérdőjelezhető,[37] ennek azonban az adatok világában betöltött különösen fontos szerepét és az ezzel kapcsolatos összefüggését érdemes lehet további vizsgálatnak alávetni. Az említett piramis elemei az első említésük[38] óta eltelt időben számos alkalommal kerültek újra és újra értelmezésre, a modellt azonban történeti szempontból jellemzően az emberi elme folyamataként írták le.[39] A területre vonatkozó szakirodalmi[40] eredmények ismeretében azonban látható, hogy a technológiai fejlődés következtében a terület folyamatosan átalakulóban van, így a piramist is célszerűnek mutatkozik az új, algoritmizáció által megalkotott körülményekhez igazítani.

---

[34] Lásd például: Herbert Zech, „Information as property", 6 JIPITEC 192, para 1. (2015). 192-193 o.

[35] Ez a fogalomnak a valóságtól elvont, általános és eszmei szintű vizsgálatát jelenti elsősorban.

[36] A DIKW akroníma jelentése Data-Information-Knowledge-Wisdom, magyarul Adat-Információ-Tudás-Bölcsesség. A modell alapvetően az információelmélet és megismeréstudomány határán található, a népszerűségének egyik oka, hogy az informatika térnyerésével megerősödő adat- és információfeldolgozás elméleti megalapozását szolgálja.

[37] Pléh Csaba: A megismeréstudomány alapjai. Typotex Kiadó, 2012. 30 o.

[38] A piramis szintjeit először T.S. Elliot 1934-es „The Rock" című művében említi, azonban a mai értelemben vett térnyerése csak 1989-ben kezdődött. Lásd részletesen: David Weinberger, „The Problem with the Data-Information-Knowledge-Wisdom Hierarchy", Harvard Business Review. Elérhető: https://hbr.org/2010/02/data-is-to-info-as-info-is-not

[39] M.J. Adler: A Guidebook to Learning: For a Lifelong Pursuit of Wisdom. London, Macmillan, 1986. 113 o.

[40] Lásd például: Albert János, „Az iderendszer korai evolúciójának számítógépes modellezése", In: Pléh Csaba (Szerk.): A megismeréstudomány és a mesterséges intelligencia filozófiai problémái. Budapest, Akadémia Kiadó, 1998. 69-83 o.

- *A piramis első szintje*

A folyamat első lépéseként szükség van arra, hogy a körülöttünk lévő világban jelenségek létezzenek, illetve, hogy ezekkel kapcsolatban változások történhessenek, mehessenek végbe. A kiindulópont, tehát relatíve egyszerű, szükség van a potenciálisan megismerhető valóság létezésére, amely alatt érthetjük a fizikai világ tárgyi és az emberi lelkivilág eszmei jelenségeit egyaránt.[41] Ennek a szintnek a markáns[42] kiemelése az első eltérés az eredeti modellhez képest, ezt pedig összefoglalóan *tényszerűség*eknek[43] nevezhetjük. Fontos tulajdonságuk, hogy állandóan és a szemlélőtől függetlenül vagy legfeljebb azzal kölcsönhatásban (az un. megfigyelési effektus által [Observer Effect][44]) léteznek. Bár egy meglehetősen elvont kategóriának tűnhet, ennek a szintnek a vizsgálata a jogirodalom számára sem ismeretlen terület. Tárgyi jogi szempontból releváns tényszerűségeket jogi tényeknek nevezzük, amelyeket alapvetően három kategóriára szokás bontani. Ezek az emberi magatartások, a természetes és épített környezeti folyamatok és események, valamint az állami aktusok.[45] *Tényszerűségnek tűnik a fogalom alapján, hogy a bolygónkon a H_2O molekula szobahőmérsékleten folyékony halmazállapotú,* [46] *de tényszerűség az is, hogy én ebben a mondatban ezt állítom.*

- *A piramis második szintje*

A következő szint maga a kutatott fogalom, az *adat*, amely a tényszerűséget leíró alapvető paramétereket foglalja magába. Az minden esetben objektív, azonban önmagában csak egy nyers értéket hordoz.[47] A kognitív folyamat (függetlenül attól, hogy gépi vagy emberi gondolkozásról van szó) szempontjából azt is mondhatjuk, hogy az adatok a világot reprezentáló jelek (szimbólumok). A reprezentáció két szinten értelmezhető, az első, szintaktikai szinten a jel, a jelek közti összefüggés és a rögzülés módja (forma), a második, szemantikai szinten pedig a jelekben rejlő értelem (tartalom) azonosítható. Ezt a típusú rétegződést Zech munkássága alapján adatszemiotikának nevezhetjük.[48] *Adat lehet például minden, amit a vízzel kapcsolatban rögzíteni lehetséges, a fizikai tulajdonságai és kémiai összetétele, a feltételek, amiknek a fennállása esetén a halmazállapota megváltozik, hatásai a környezetére, az emberi szervezetre stb.*

A modellben a soron következő elem az *információ* (deklaratív, objektív és szemantikus formája) lenne, amit Floridi alapján az értelmezett, egyediesített értéket hordozó adatként foghatunk fel.[49] Balogh az információt, mint értelmes közlést definiálja, amelynek legalább egy része új ismeretet szolgáltat a fogadó félnek és az egyúttal valamilyen formában fontos

[41] Kengyel Miklós: Magyar Polgári Eljárásjog. Budapest, Osiris Kiadó, 2014. 287 o.
[42] Más szerzők is a piramis alapjaként jelölték meg a „világot", ezáltal, mint tényező elismerésre került, de a hierarchiában nem szerepelt. Lásd például: Rob Kitchin: The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences. SAGE Publications Ltd, 2014. 10 o.
[43] A magyar nyelv értelmező szótára (www.mek.oszk.hu): *„A valóság folyamatában lezárt szakaszt alkotó esemény, jelenség, mozzanat; olyan, ami a valóságban előfordulhat v. megtörtént."*
[44] Paul Adrien Maurice Dirac: The Principles of Quantum Mechanics. Clarendon Press, 1981. 314 o.
[45] Visegrády Antal: Jogi alaptan. Pécs, Janus Pannonius Tudományegyetem Állam- és Jogtudományi Kar, 1996. 44 o.
[46] Igaznak hat a kijelentés, de fontos, hogy a tényszerűséget nem feltétlenül tudjuk teljes valójában vizsgálni, csak a rendelkezésre álló adatokon keresztül. Még egy ilyen triviális esetben sem zárható ki, hogy a rögzített adatok hiányosak vagy pontatlanok és a kijelentés részben, vagy egészben valótlan.
[47] Todd Groff, Thomas Jones: Introduction to Knowledge Management. London, Routledge, 2003.
[48] Zech, 2015. 193-194 o. Zech a rétegződés egy harmadik szintjét is megkülönbözteti, a szintaktikai szinttől független strukturális szintet, amely az adatokat közvetítő csatornát, az adat hordozóját jelöli. Ezt a szintet jelen dolgozatban a szintaktikai szinten belül kezelem.
[49] Luciano Floridi, „Is Semantic Information Meaningful Data?" Philosophy and Phenomenological Research, 2005. 353 o.

számára.[50] Az információ értelmezhetőséget, szubjektív értékhordozást és újszerűséget jelent az adatokhoz képest, amely ilyen kvalitásokkal (nyers érték lévén) nem feltétlenül rendelkezik. A hierarchiában történő önálló szerepeltetéssel kapcsolatban ezért az álláspontom az, hogy – kiemelten az algoritmizált folyamatok térnyerése által – a két fogalom egyre inkább összemosódik, kiüresítve az adat és az információ kategorikus elválasztásának megfelelőségét. Ennek elsődleges oka, hogy az „érték”[51] adathoz rendelése időben és térben is elválhat magától az alapfolyamattól, mivel annak résztvevői számára az érték nem mindig ítélhető meg az adott pillanatban.[52] Ezen nem változtat, hogy az értékteremtő kvalitások már az adatban is megtalálhatóak, mivel az információ értelmezés és értékelés kérdése (tehát gyakorlatilag minden adat információ *valakinek*). A másik kiemelt ok a külön szerepeltetéssel szemben, hogy információelméleti szempontból az adat és az információ a megismerési folyamatban olyan szoros kölcsönhatásban áll, hogy a szétválasztásuk szinte lehetetlen, ugyanis utóbbit a folyamat tartalmának, míg előbbit annak formájának tekinthetjük (ezt a megkülönböztetést jelelméleti megközelítéssel szintaktikai és szemantikai rétegeknek neveztük). Az kétségtelen, hogy hangsúlybeli eltolódás tapasztalható az adatnak a formai (szintaktikai) és az információnak az értelmi (szemantikai) szintek irányába,[53] aminek oka, hogy az információs egyediesített érték felismeréséhez óhatatlanul a tartalom ismeretére van szükség. Az álláspontom szerint azonban – ahogy az adat létrejöttének folyamatánál bemutatásra kerül – nem létezhet a két réteg egymás nélkül, így azokat csak jogi absztrakcióval választhatjuk el, ténylegesen nem. És ahogy a két réteget nem lehet ésszerű keretek között leválasztani egymásról, éppúgy nem lehet az adatot az információról. Ezért a jelen dolgozatban képviselt álláspont szerint az adatot akkor tekinthetjük információnak, ha annak értéke konkrét esetben realizálódott és a szemlélő rendelkezik a megértés, értelmezés képességével.[54] Ebből kifolyólag a továbbiakban az információt az adat egyedi esetben kikristályosított *bel*tartalmának tekintem, tehát az adat hordozza az információt, de azok nem kell elváljanak élesen egymástól.[55] *Jelen értelmezés szerint például az adat és az információ egyenértékű (gyakorlatilag szinonim) vagy esetleg következetlen használata nem jelent problémát, hiszen, ami valakinek adat, az másnak információ lehet, így a külső szemlélőnek valójában megállapíthatatlan, hogy éppen mi minősül információnak és mi adatnak.*

- *A piramis harmadik szintje*

Az adatok rögzülését és befogadását követően, azokon – a kognitív folyamat lépéseinek keretében – műveletek végezhetők. Logikailag az első lépések között kell szerepeljen az adatok eltárolása és valamilyen szempontok szerinti (pl. címkézés általi) rendezése. Mivel arra következtethetünk, hogy az adatok a megfigyelőtől függetlenül léteznek, el kell határolnunk azokat az adatokat, amelyek a világban potenciálisan léteznek, azoktól, amelyeket már megfigyeltünk és ezért megismertünk. Az adat ugyanis – Schrödinger macskájához[56] hasonlóan – folyamatosan egy átmeneti állapotban található. Ha a tényszerűség létezik, akkor az adat is létezik, de a szemlélő megfigyelő jelenléte által manifesztálódik, vagyis vált a nem megfigyelt állapotból a megfigyelt állapotba.

[50] Balogh Zsolt György: Jogi Informatika. Budapest-Pécs, Dialóg campus Kiadó, 1998. 17 o.
[51] Lásd: 2.1. fejezet
[52] Anya Bernstein, „What Counts as Data?”, Brooklyn Law Review, 86(2), 435-460 o.
[53] Václav Janeček, „Ownership of personal data in the Internet of Things”, Computer Law & Security Review Volume 34, Issue 5, 2018. 6 o.
[54] Balogh, 1998. 17 o.
[55] Nestor Duch-Brown, Bertin Martens, Frank Mueller-Langer, „The economics of ownership, access and trade in digital data”, JRC Digital Economy Working Paper 2017-01 (online) 7-8 o.
[56] John D. Trimmer, „The present situation in quantum mechanics: a translation of schrödinger's "cat paradox paper"”, Proceedings of the American Philosophical Society, 124, 323-338 o.

A feldolgozott, vagyis megismert adatokat tekinthetjük *ismeretek*nek, amik így valójában az adaton végzett művelet által létrejövő, tényszerűségre vonatkozó mentális reprezentációkat[57] jelentik. Ez alapján látható, hogy az adat ismeretté válásával képessé teszi a szemlélőt a tényszerűségről való gondolkozásra, ami által újabb tényszerűségek felfedezése történhet, amelyek egyébként további ismeretek létrejöttét tehetik lehetővé. Ezért az irodalom megkülönböztet a priori (közvetlen vagy érzékelés alapú) és a posteriori (közvetett vagy gondolati) ismereteket.[58] *Ismeret lehet, hogy a vizet meg lehet inni.*

- *A piramis negyedik szintje*

Az előző szintre alapozva valamilyen ismeret birtokát megszerezni, rendszerbe szedni, összekapcsolni más ismeretekkel és ezekből következtetéseket levonni magasabb szintű *tudást* fog eredményezni a tényszerűséggel kapcsolatban.[59] Fogalmazhatunk úgy, hogy az ismeretek építőelemei valami nagyobb, bonyolultabb rendszernek, amelynek a felismerése (felépítése) által a mentális reprezentáció pontosabbá, részletesebbé válik. Az ismeret és a tudás közti szoros kapcsolatot és e kettő jelentőségét Mayer-Schönberger és Cukier példáit felhasználva a következőképpen lehet a helyzetet érzékletesen szemléltetni: Lord Kelvin szerint a mérés tudás, Sir Francis Bacon óta pedig tudjuk, hogy a tudás hatalom.[60] *Tudást jelenthet, hogy egy anyag vagy felület egy szennyeződéstől vízzel megtisztítható, azonban forró víz használatával még bizonyos kórokozók is eltávolíthatóvá válnak.*

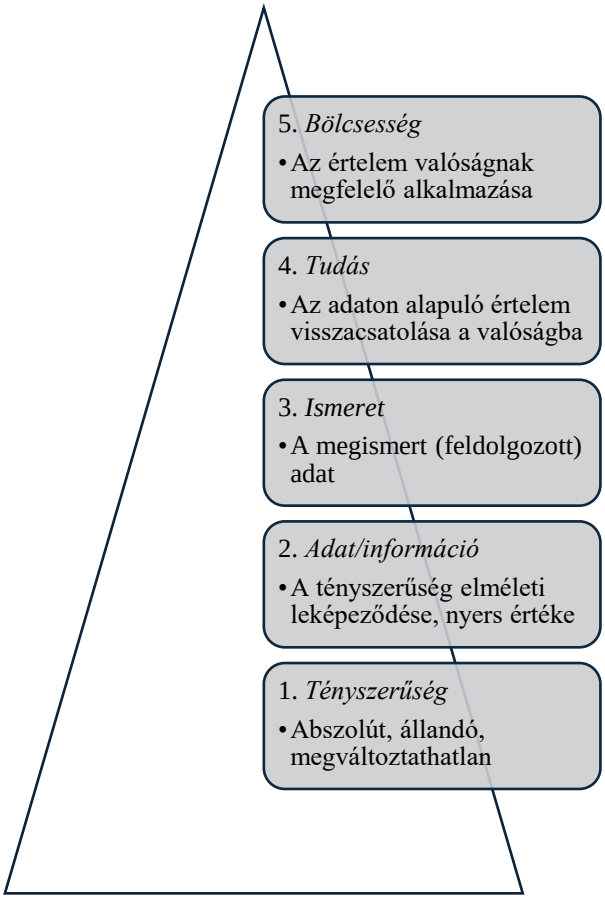
- *A piramis ötödik szintje*

Az utolsó szintje a piramisnak, az értelem valóságnak megfelelő alkalmazása, amit *bölcsességnek* nevezhetünk.[61] Ebben a lépésben a mentális reprezentáció a magas szintű absztrakció kissé légüres teréből visszacsatol a valóságba, vagyis a tudás a körülményeknek megfelelően alkalmazásra kerül. *Bölcsesség lehet, ha forró vízzel fertőtlenítjük a cumisüveget mielőtt egy újszülöttnek adnánk, mivel az immunrendszere fejletlensége miatt fokozott veszélynek van kitéve.*

Az újragondolt hierarchia[62] öt pontja alapján látható, hogy a legelemibb törvényszerűségektől, a magas szintű gondolkodásig, az értelem működéséig milyen út megtételére van szükség. Talán az adat megkülönböztett helye is kimutatható a folyamatban, hiszen a piramis második (a tényleges megismerési folyamatban első) szintjeként az adat az, ami összeköti a világ történéseit az elme folyamataival, ablakot nyitva a belső és külső világ megismerése, majd megértésére. Hogy ennek a kognitív folyamatnak mi célja a jelen átalakított modell szempontjából nincs jelentősége. Tehát ugyanúgy ide sorolhatók a tudományos kutatás céljából történő adatgyűjtések, mint a hírlevélküldéshez szükséges e-mail címek rögzítése, mivel mindkét esetben az adat ugyanazt a reprezentációs funkciót tölti be.

[57] Pléh, 2012. 34 o.
[58] Balogh 1998, 19 o. és Pléh 2012 34 o.
[59] David Boddy, Albert Boonstra, Graham Kennedy: Managing Information Systems: Strategy and Organisation. Pearson Education, 2008.
[60] Viktor Mayer-Schönberger, Kenneth Cukier: Big Data. Budapest, HVG Kiadó Zrt., 2014. 43 o.
[61] Leonard M Jessup, Joseph S Valacich: Information systems today: managing in the digital world. Upper Saddle River, N.J.: Pearson Prentice Hall, 2008.
[62] A modell általam alkalmazott, új felépítését (a korábbi verzióhoz hasonlóan az angol szavakat használva: Factualitiy-Data-Insight-Knowledge-Wisdom) a dolgozat további részében „FDIKW" rövidítéssel fogom azonosítani.

A piramisszerűen felépülő ábra mellett a folyamat-jelleg is hangsúlyozható, amihez az algoritmizált rendszerekből ismert tulajdonságok felhasználása által további pontosítás tehető a megismerési tevékenységgel összefüggésben. Egy algoritmus – amit egy zárt rendszeren belül lezajlódó, logikailag összekapcsolt lépések láncolataként foghatunk fel – működése alapvetően három fázisra osztható; egy bemenetre, egy számítási teljesítményre és egy kimenetre. Az algoritmizált folyamatnak tehát lényegi eleme, hogy a „bemenetből" létrejöjjön a „kimenet".[63] A fenti fogalmak által jellemzett kognitív folyamat meglátásom szerint megfelelően igazodik ebbe a konstrukcióba. E tekintetben a bemeneti oldalon a tényszerűségekből leképzett, azokat szimbolizáló adatok találhatók – amelyek a megfigyelő szubjektuma szerint információként is megjelenhetnek – míg a kimenetet első lépésként az ismeretek alkotják. Az algoritmusok törvényszerűségeinek megfelelően azonban az előző folyamat kimenete könnyen válhat a következő folyamat bemenetévé, így lehetséges, hogy az ismeretek (azok megismert adattartalmának) további feldolgozása által eljuthatunk a tudásig, majd később a bölcsességig. Ezek a ciklusok végtelenül kombinálhatók, a piramis egyes fokai között pedig a hierarchikus felépítettségre tekintet nélkül létezhet átjárhatóság. Így nem kizárt, hogy egy tudásalapú megismerési folyamat eredményeként eddig nem látott tényszerűségek válnak észlelhetővé, amelyekből leképzett adatok ismereteink bővítésére alkalmasak, azoknak azonban gyakorlati alkalmazhatósága egyéb tudás birtokának hiányában még nem lehetséges.



1. ábra: az FDIKW piramis

Az adatok absztrakt fogalma tehát így határozható meg: adat alatt a világ egy tényszerűségét tükröző, olyan jelet (szimbólumot) értünk, amely más ilyen jelekkel egy rendszert alkot, de a többi jeltől való elhatárolhatóságát megőrzi. Az adat így a kognitív folyamat hierarchikus struktúrájában a külvilág megismerési eszközének,[64] és közvetítő közegének[65] szerepét tölti be.

2.2. Az adatok általános dimenziói

Az adatok egyes kategóriáinak áttekintése előtt célszerű azokat általánosságban is megvizsgálni, hogyan jöhetnek létre, milyen általános vizsgálati szempontjaik lehetnek. Fontos, hogy az adatok rendszerén belül azok tipizálhatók, az adat-minőség pedig nem függ a megjelenésük formátumától (pl. tárolásra alkalmazott technológia, kifejezésre használt nyelv),

[63] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein: Introduction to Algorithms. Third Edition. Cambridge, Massachusetts, London, England, The MIT Press, 2009. 5 o.
[64] Mayer-Schönberger, Cukier, 2014. 28 o.
[65] Marc Amstutz álláspontját lásd részletesen: Parti Tamás: digitális adatok tulajdoni adaptációja a digitális javak vagyonjogi kölcsönhatásainak tükrében. Budapest, Wolters Kluwer Hungary Kft., 2024. 27 o.

ontológiai igazságtartamuktól vagy az ennek megfelelő értelmezhetőségüktől[66] (amit egyébiránt akkor kell vizsgálni, ha az adatra, mint információra szeretnénk hivatkozni).

2.2.1. Az adatok létrejöttének folyamatáról

Az adat létrejöttének folyamatát az absztrakt adatfogalom és az abból logikusan folyó következtetések alapján kísérelhetjük meg felépíteni.

Az adat létrejöttéhez minden esetben szükség van egy megfigyelhető tényszerűségre és egy megfigyelésre képes megfigyelőre, így kiindulópontként megállapíthatjuk, hogy adatok e két tényező egyidejű jelenléte hiányában nem jöhetnek létre.[67] A tényszerűségek, mint a valóságot alkotó elemek létét bizonyítani, illetve a valóság „nem létezésébe" belegondolni talán felesleges, azonban a megfigyelésre való képesség további vizsgálatot igényel. Az adat és az információ kapcsolatánál kifejtésre került, hogy e kettőt álláspontom szerint az különbözteti meg, hogy az információ az egyedileg (szubjektíve) értéket és újszerű ismeretet hordozó adatok egy szűkebb körét foglalja magába. Ezen a ponton fontos azt is kiemelni, hogy az értelmezhetőséget nem tartom azonos fogalomnak a megfigyelhetőséggel (és a megfigyelésre való képességgel).

Példaként vehetjük az erdőben kidőlt fa gondolatkísérletét. Az ebben szereplő kérdés, hogy ha az erdőben egy fa kidől, de nincs senki, aki hallaná, akkor adott-e valójában hangot? A régóta fennálló teoretikus vita megosztónak mondható, a válasz nagyban függ attól, hogy magát a hangot miként definiáljuk. Az adatok létrejöttének szemléltetésére a legkézenfekvőbb, George Berkeley által képviselt válasz szerint, ha a hangot, mint a levegőben terjedő mechanikai vibrációt fogjuk fel, akkor a válasz igen, a kidőlt fa akkor is ad hangot, ha nincs ott senki, aki hallaná.[68] Nézzük meg, hányféleképpen képzelhetjük el újra ezt a kísérletet úgy, hogy sikeres és sikertelen adat létrejövetelekre kapjunk példákat:

> A kiindulópontunk, hogy a fa kidőlése egy *megfigyelhető* tényszerűség, a levegőben terjedő vibráció (hang) az adat, aminek létrejöttét vizsgáljuk.
>
> Kezdjük az eredeti példával, ennek a lényegi eleme volt, hogy nem volt ott senki, aki hallotta volna a fa kidőlését. Ebben a helyzetben *hiányozott a megfigyelő* így a tényszerűségről *nem jött létre adat*.
>
> Első variációként képzeljünk el az erdőben egy siket embert. Ez az eset végeredményben megegyezik az előzővel, *most sem jön létre adat*, ezúttal a *megfigyelésre való képesség hiánya* miatt.
>
> A második esetben egy halló embert, de ezúttal egy *gyermeket* képzeljünk el az erdőben. A levegőben terjedő vibrációt a gyermek füle *képes észlelni*, de azt az elméje, a képzelőereje és tapasztalatlansága miatt nem, mint egy kidőlt fát, hanem, mint egy mitológiai farkas vonyítását értelmezi. Így most azt mondhatjuk, hogy *az adat létrejött*. A folyamat befejezettségének ugyanis az *értelmezhetőség (az értelmezésre való képesség*[69]*) nem feltétele*.

---

[66] Kitchin, 2014. 3-4 o.

[67] Ebben a folyamatban a létrejövetel pontosabban megfogalmazva azt jelenti, hogy az adatok a nem megfigyelt és megfigyelt létállapotuk között váltanak.

[68] StudyCorgi, „Locke and Berkeley: If a Tree Falls in a Forest." 2021. https://studycorgi.com/berkeley-and-locke-if-a-tree-falls-in-a-forest/

[69] Az értelmezhetőség hiányára gyakran említett példa egy nyelv speciális írásjeleinek nem ismerete. Attól, hogy az olvasó nem képes az értelmezésre, attól az írásjel írásjel, az adat pedig adat marad.

A harmadik példánkban nem változik semmi más, csak a gyermek helyére egy *felnőtt* kerül. Itt is *létrejön az adat*, a felnőtt pedig *értelmezve* megállapíthatja, hogy valahol kidőlt egy fa.

A negyedik és utolsó variációban helyezzük az erdőt egy *hegyvonulat havas tájába*. A kidőlő fa hangját most egy *szakavatott hegymászó* hallja meg. Ebben az elképzelt helyzetben az előzővel azonosan, *értelmezetten jön létre az adat*. Azonban tegyük fel, hogy az a hegymászó számára *egyedi értéket hordoz* és így egy potenciális *lavina érkezését előre jelző információvá válik*.

A fenti kísérletekből a következőket állapíthatjuk meg. A szimbólum leképezéséhez a tényszerűség sikeres megfigyelésére van szükség, ezáltal válhat lehetségessé az adat létrejötte. A példákban láthattuk, hogy az adatok létrehozásához minden esetben képességekre (hallás) és/vagy erőforrásokra (az emberi szervezet energiaellátottsága) van szükség, amelyeket a szintaktikai adatréteg milyenségétől függően organikus vagy technológiai megoldások is biztosíthatnak. A példáinkban ezek emberi (biológiai) funkciók voltak, tehát jellegüket tekintve organikusak. De az esetek ugyanígy megállnák a helyüket, ha az emberi fület egy technológiai megoldásra, például egy mikrofonra cserélnénk. Ezeket a képességeket és erőforrásokat egy kognitív és egy fizikai komponensre oszthatjuk, ez jelentheti a gépek szoftver és hardver vagy az élőlények elmebeli és testi kapacitásait. A jelenlegi tudásunk alapján e kettő egymás nélkül nem képzelhető el, így azt mondhatjuk, hogy együttes meglétükre az adatok létrejövetelekor is minden esetben szükség van.

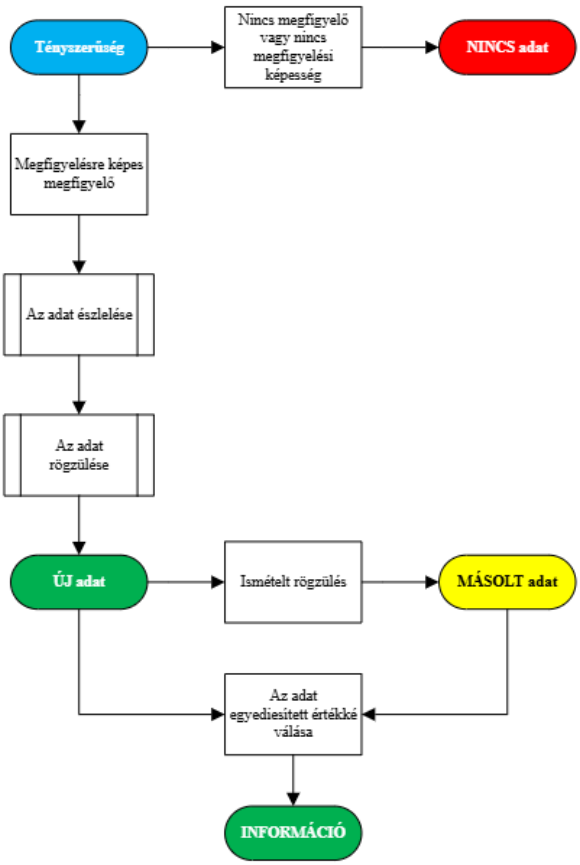
Az adat létrejöttének folyamata tehát nem egy, hanem legalább két lépésből áll. Az első az *észlelés*, a második pedig a *rögzítés*, amelyek megléte esetén azt mondhatjuk, hogy az adat *létrejött*.[70] Mivel az adat a tényszerűséget mindössze reprezentálja, de nem testesíti meg[71] annak feldolgozható formában történő létéhez egy (organikus vagy technológiai) adathordozóra van szükség.[72] A folyamat során minden esetben *egy egységnyi új adat* jön létre, amely a szimbolikus kapcsolatot a tényszerűséggel megőrzi, azonban a léte a tényszerűségtől elválva, önálló formában valósul meg.

Álláspontom szerint az észlelést és rögzülést – amelyek az adatok szintaktikai és szemantikai rétegeit fogják végső soron adni – egymástól elválasztani oly módon nem lehet, hogy *új* adat ténylegesen létrejöjjön. Ezt bizonyítandó vegyük a digitális fényképezőgép egyszerűsített példáját. Az eszköz egy vagy több tényszerűség fizikai megjelenését reprezentáló adatot képes létrehozni, amihez egyebek mellett egy lencserendszer és egy memória-kártya rendeltetésszerű működésére van szükség. Egy fenyőfa, mint tényszerűség a lefényképezésekor észlelhető, ha működik a lencserendszer, és rögzíthető, ha működik a memória-kártya. Ha utóbbi szenved valamilyen működési zavarban akkor a fényképezés során a fenyőfát reprezentáló adat nem érkezhet meg a létrejövetel befejezett szakaszába, hiszen az lehetetlenné vált a rögzítés képességének hiányában. Ha előbbi nem működik megfelelően akkor - ahogy a példabeli ember a siketsége miatt nem észlelhette a fa kidőlés hangját – a fényképező nem lehet képes a memória-kártyájára menteni a fenyőfa (vagy bármi egyéb) képét. Összegezve a két helyzetet: az észlelés képességének hiányában az adat szemantikai rétege (tartalma) nem tud megnyilvánulni, így az adat létrejöttének folyamata el sem kezdődhet. A rögzítési képesség

[70] Lásd részletesen: Zech, 2015. 194 o.
[71] Balogh, 1998, 90 o.
[72] Lásd részletesen lentebb.

nélkül pedig – bár a tényszerűség észlelhető – a szintaktikai réteg hiányában a „tartalom elszáll”, a létrejövetel nem tud befejezetté válni.

A helyzetet árnyalja az adatok másolhatósága. Az adat ez alapján – főszabály szerint – végtelenül sokszorozható, azonos időpillanatban korlátlan személy által funkcióvesztés nélkül használható.[73] Fontos azonban, hogy az adat észlelt, eszmei tartalma mindvégig változatlan marad (hiszen a reprezentált tényszerűség állandó), attól függetlenül, hogy az adat másolása technikailag megvalósítható. Ebben az esetben ugyanis a létrejövetel nem ismétlődik teljes egészében, az észlelési mozzanat nélkül csak az adatok rögzülése valósul meg többször. Másként megfogalmazva a másolás csak a szintaktikai szinten történő rögzítés megismétlését jelenti, nem érinti azonban a szemantikai szint értelmét, az változatlan formában létezik tovább (például egy digitális fotón ábrázolt havas táj a másolás következtében nem fog homokos tengerpartot mutatni). A gondolatmenet alapján kérdésessé válhat a másolt adatok megítélése, hiszen a létrejövetel folyamatának csak egyik lépését teljesítik. Az ellentmondás azonban látszólagos lehet. A másolat a rögzüléssel ugyanúgy a létrejövetel befejezett állapotába kerül, mint az eredeti, így az adatként való kezelése továbbra is indokolt, azonban nem, mint új adat, hanem mint másolat.



2. ábra: az adat létrejöttének folyamata

Az eredeti adat és a másolat megkülönböztetés jelentőségének megragadásához egy újabb klasszikus gondolatkísérletet adaptálhatunk az adatalapú működés sajátos világára. A kísérlet Thészeusz, Athén egyik nagy hősének hajójáról szól, amit az ókori görögök tiszteletük jeléül évszázadokon keresztül megőriztek. A kísérlet lényege, hogy e hosszú idő alatt a hajó egyes darabjai javításra szorultak, míg végül annyi darabját kellett kicserélni, hogy semmi nem maradt az eredetiből. A kísérlet első (kiindulóponti) fordulata, hogy vajon a hajó még mindig Thészeusz hajója-e vagy sem. A kísérlet második fordulata azonban még tovább megy. E szerint az eredeti hajó minden kivett darabját összegyűjtötték és végül újjáépítették az eredetivel teljes mértékben megegyező módon. Az új kérdés, hogy melyik valójában Thészeusz hajója, a renovált (a folyamatosan javított) vagy a rekonstruált (a kivett alkatrészekből épített) hajó. Szögezzük le az elején, hogy az alap, aggályosan áthidalható probléma a hajókkal kapcsolatban, hogy nehezen elgondolható, hogy egy fizikai tárgy egy időben a tér két különböző helyén legyen.[74] Ez azonban az adatoknál nem jelent problémát, így egészen egyértelmű válasz adható a kérdésekre. Mielőtt a válaszadásra rátérünk nézzük meg, hogy az adatok másolásához hogyan

[73] Lásd részletesen lentebb.

[74] Tőzsér János, „Metafizika. 4. fejezet: A fizikai tárgyak létezése az időben. 4.4 Thészeusz hajója”, ELTE Szabadbölcsészet. Elérhető: https://mmi.elte.hu/szabadbolcseszet/mmi.elte.hu/szabadbolcseszet/index7649.html?option=com_tanelem&id_tanelem=1069&tip=0

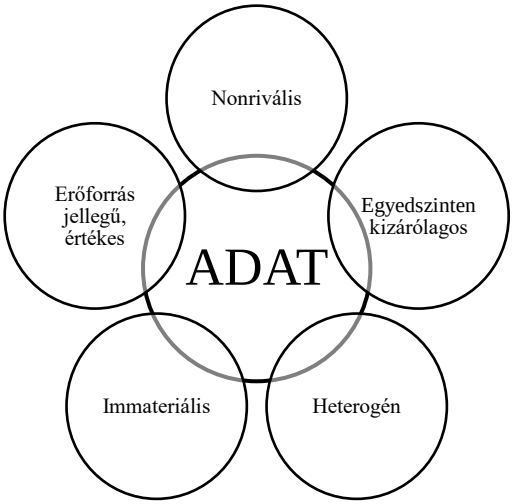
kapcsolódik Thészeusz hajójának példája. A kísérletünk célja a hajó átalakítása és az adatok másolása közötti párhuzam megtalálása. A kiindulópont, hogy az eredeti adat a Thészeusz által a görögökre hagyott hajó. Mint eredeti a tényszerűség szemantikai és szintaktikai rétegeit is elsődlegesen reprezentálja. Tételezzük fel azt is, hogy a hajón végrehajtott javítási folyamat nem évszázadok alatt végbemenő, fokozatos átalakulás, hanem – egy adatkezelési művelethez hasonlóan – szinte azonnali esemény.

> *A kísérlet első fordulata csak annyit kérdez, hogy a teljesen kicserélt darabokkal rendelkező hajó még mindig Thészeusz hajója-e vagy sem.* Az új hajó szemantikai tartalma változatlan (tehát, hogy ez Thészeusz hajója), azonban szintaktikai rétege kicserélődött (a hajó alkotóelemei), úgy, hogy az eredeti állomány nem került megőrzésre (ezúttal nem építettek új hajót a régi alkatrészeiből). Ha a hajó adat lenne, akkor ez gyakorlatilag egyet jelent az eredeti törlésével egybekötött másolásával.[75] A válasz a kérdésre tehát *nemleges*, az *új hajó* (adat) *nem azonos a régivel*, hanem annak a *másolata*.
>
> *A második fordulat bevezeti az eredeti hajó megőrzésének körülményét a kísérletbe*. A rekonstruált hajó esetében az megőrzi az eredeti darabokat, és tartalmi szempontból, mint Thészeusz hajója funkcionál. A renovált hajó esetében az alkotórészek teljesen kicserélésre kerülnek, azonban az eszmei tartalom, vagyis az, hogy ez Thészeusz hajója, nem változik. Ez alapján azt mondhatjuk, hogy a *rekonstruált hajó mind szemantikai, mint szintaktikai szinteken azonos Thészeusz hajójával*, így azt tekinthetjük az *eredetinek*. Ezzel szemben a *renovált hajó csak szemantikai rétegében azonos*, szintaktikai szempontból nem az, így ezt tekinthetjük a *másolatnak*.

A másolás tehát olyan folyamatként képzelhető el, amelynek eredményeként az eredeti adat megőrzi mindkét, létrejöveteléhez szükséges feltételét, míg a másolt adatnak az újdonsága csak szintaktikai rétegében fedezhető fel, eszmei tartalmában nem.

2.2.2. Az adatok öt ismérvéről[76]

Érdemes öt általános, az adatokat a világ más entitásaitól megkülönböztető ismertetőjegyet megvizsgálni. Ezek az adatokat minden esetben jellemzik, azok alap karakterisztikáját adják.



3. ábra: az adatok öt ismérve

[75] Az analógia kifejezetten jól működik digitális adatok esetén, ahol az adatok fájlokban kerülnek kezelésre. Az informatika működési törvényszerűsége szerint egy fájl áthelyezése pont így történik, tehát az eredeti fájl *törlésével* és új helyre *másolásával*.

[76] Ezekre tekinthetünk úgy, mint az adatok differentia specifica-jára.

- *Versengés*

Az adatokat az uralkodó álláspont, mint nonriválisan (nem-versengő) entitás jelöli[77] és ezért *(is)* sokszor hozza párhuzamba a szellemi alkotásokkal.[78] A gondolat egyfelől abban gyökerezik, hogy az adatok korlátlanul és kevés ráfordítás árán sokszorozhatók,[79] másfelől abban, hogy a használatuk által a rendelkezésre álló mennyiség nem – vagy nem számottevően[80] – csökken.[81] A sokszorozhatóság – és egyébként az ebből eredő egyidejű használhatóság – különösen fontos ismérve az adatoknak, azonban ez sokkal inkább a „másolhatóság" körülményéből adódik, mintsem a versengésből (bár azzal láthatóan szorosan összefügg). A nonrivalitás központi kérdése számomra sokkal inkább ugyanazon adat ismételt használhatóságában rejlik.

- *Kizárólagosság*

A versengés mellett a kizárólagosság az elsők között felmerülő kérdés, vagyis az, hogy egy adat esetén kizárhatóak e mások a használatból. A fizikai léttel bíró tárgyak esetén is felmerül ez, mivel vannak olyanok, amelyek esetében a kizárás nem lehetséges vagy a dolgok közvetve/közvetlenül társadalmi célokat szolgálnak (un. közdolgok).[82] Az adatokkal kapcsolatban azok non-exkluzív természetét szokás hangsúlyozni, az érvelés pedig a nonriválisjelleggel karöltve jelenik meg. A nonrivalitással ellentétben azonban ez egy kevésbé egyértelmű kérdéskör. Meg kell említeni ugyanis, hogy számos olyan megoldás létezik, amely egy konkrét adatállományt kizárólagossá tehet. Ezek akár szervezési-szabályozási, illetve jogi jellegűek[83] vagy akár tényleges erőhatalom[84] gyakorlásában megnyilvánulók is lehetnek. Így a kizárólagosság esetén tetten érhető egyfajta differenciálatlan megközelítés jelenléte. Az adatok nagyegésze esetén érthetően vonakodunk a kizárólagosság elfogadásától (főként, ha a közadatok kategóriájára gondolunk), azonban egy adott állomány vonatkozásában már annál inkább elképzelhetőnek tűnik, főként *egy egységnyi új adat* vonatkozásában vizsgálva. A létrejövetel folyamatában látható volt, hogy egy adat teljességében (eredeti szemantikai és szintaktikai rétegekkel) csak egyszer jöhet létre. Tehát egy tényszerűség egy aspektusa egy adott pillanatban csak egyféle adat leképezését teszi lehetővé, függetlenül attól, hogy az adatnak a befogadása lehet könnyebb vagy nehezebb feladat, a rögzítése pedig akár teljes és pontos vagy részleges és tökéletlen is.[85] Például egy fénykép egy fenyőfáról azonos pillanatban, azonos látószögben, azonos légköri viszonyok között stb. csak egyszer készülhet, a következő – akár

[77] Maryam Farboodi, Laura Veldkamp, „A Model of the Data Economy", NBER Working Paper No. 28427, 2021.
[78] Duch-Brown, Martens, Mueller-Langer, 2017. 6-12 o.
[79] Hal R. Varian, „Markets for Information Goods", Institute for Monetary and Economic Studies, Bank of Japan, 1999. Elérhető: https://people.ischool.berkeley.edu/%7Ehal/Papers/japan/
[80] Digitális adatállományokon (pontosabban: magukon a fájlokon) végzett műveletek (pl. írás, olvasás) esetén az állomány integritása sérülhet (un. data corruption). Ez azonban az informatikai rendszer tökéletlen működéséből ered, nem az adat általános természetéből.
[81] Josef Drexl, „Designing competitive markets for industrial data – between propertisation and access", Max Planck Institute for Innovation and Competition Research Paper No. 16-13, 2016. 28 o.
[82] Menyhárd Attila, „Köztulajdon - közdolgok – forgalomképesség", PJK, 2005/2.. 3-11. o.
[83] Susan Ariel Aaronson, „Why Are We Talking about Data as a Public Good?", Centre for International Governance Innovation (2023). 4 o.
[84] A tényleges erőhatalom vagy „factual controll" alatt olyan megoldásokat értünk, amelyek az adatokhoz hozzáférők körének meghatározásában, a másolás és továbbítás korlátozásában rejlenek és szervezési/szabályozási védelem helyett/mellett az adaton való műveletvégzés és az adat környezetének tényleges irányítása által megvalósuló védelmén keresztül érvényesülnek. Lásd részletesen: Herbert Zech, „Data as a Tradeable Commodity – Implications for Contract Law", Josef Drexl (ed.), Proceedings of the 18th EIPIN Congress: The New Data Economy between Data Ownership, Privacy and Safeguarding Competition, Edward Elgar Publishing, Forthcoming, 2017. 6 o.
[85] Kitchin, 2014. 3 o.

csak marginális metaadatok szintjén – de eltérő lesz.[86] Az adatok tekintetében – azok egyedisége miatt – a kizárólagosság akár lehetséges is lehet. Így tehát az adatokra, mint összességre non-exkluzivitás lehet jellemző (legtöbbször a kizárólagosság betartatásának lehetetlenülése miatt), azonban egyedenként vizsgálva (a metaadatszintű megkülönböztetés révén) lehetséges a kizárólagosság elérése.[87] Egy adattábla (a konkrét .csv fájl, vagyis a numerikus, digitális adatállomány), amely sosem volt felhőtárhelyre mentve, nem került sem nyomtatásra, sem elküldésre jó példa lehet. Ha az egy helyi meghajtón jött létre és kizárólag ott található meg, akkor a vélelmezett egyedisége és a hozzáférés korlátozottsága miatt azt mondhatjuk, hogy ennek a konkrét állománynak a használatából más személyek kizárhatók, tehát az, mint egyed kizárólagos.

- *Összetétel*

A versengés és kizárólagosság kutatása mögött gazdag szakirodalom található, de az adatfogalom összetételének kérdéséről, valamint a fogalmon belüli differenciálás fontosságáról viszonylag kevés. Például a jogi (pl. köz- és magánadatok) és technológiai (pl. digitális és analóg) kategorizálás[88] léte nem vitatott, de létjogosultságával kapcsolatban említhetők aggályok. Az európai adatvédelmi jog által a jogrend mélyébe kodifikált személyes és nem személyes adatkategóriák szeparációját számos kritika érte a 2010-es évek második felében a GDPR és az FFNPDR[89] hatályba lépésével. Ezek szerint az ilyen kettéválasztás életszerűtlen és a gyakorlatban követhetetlen helyzetekhez vezet, és ezért kimondottan egy általános szabályozási megközelítés mellett tették le a voksukat.[90] Fontos megjegyezni azonban, hogy ezzel – akarva vagy akaratlanul – egy homogén adatfogalom bevezetése mellett is érveltek. Az adatkategóriák egymástól való megkülönböztetésének akadályozása meglátásom szerint több aggályhoz vezet, mint amennyit megoldani képes. A homogén adatfogalomban ugyanis nehéz különbséget tenni adat és adat között, ezáltal nem csak a természetes személyek alapjogvédelme kivitelezhető bonyolultabban, az adatok életszerű szabályozása is megnehezedik. Az adatok heterogenitásának tudomásul vétele, az ebbéli tulajdonságukhoz igazodó[91] jogalkotás véleményem szerint célravezetőbb megoldás lehetne. Gondoljunk csak a folyami kavics és a gránit közti „szemantikai" értékek és „szintaktika" formák különbségére. Hiába számít mindkettő kőzetnek, a jog különbséget *tud* tenni pl. a folyóparti kavicsok gyűjtögetése és az ipari kőfejtés megítélése között.[92] Ekként nagy és valós különbség van a személyes és nem személyes, valamint köz- és magánadat kategóriája és a digitális, analóg vagy akár kvantum adatok törésvonalai mentén (akárcsak a gránit és a kavics között). De különbség van továbbá az egyes – főként újonnan létrejövő – állományok között is (vagyis kavics és kavics között),

[86] Hérakleitosz alapján úgy is fogalmazhatnánk, hogy: „egyetlen ember sem léphet kétszer ugyanabba a folyóba, mert az már nem ugyanaz a folyó, és ő már nem ugyanaz az ember."

[87] A kizárólagossá tételre alkalmas lehet például valamilyen blokklánc-alapú technológia alkalmazása. Lásd: Kinza Yasar, What is blockchain? Definition, examples and how it works, TechTarget. Elérhető: https://www.techtarget.com/searchcio/definition/blockchain

[88] Lásd lentebb, mint szintaktikai és szemantikai rétegek bemutatása.

[89] Az Európai Parlament és a Tanács (EU) 2018/1807 rendelete a nem személyes adatok Európai Unióban való szabad áramlásának keretéről (továbbiakban: FFNPDR)

[90] Lásd például: Inge Graef, Raphaël Gellert, Martin Husovec, „Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation", TILEC Discussion Paper, Tilburg University, 2018. Megjegyzendő, hogy egy kevert adatállomány vonatkozásában a GDPR és az FFNPDR személyes és nem személyes adatok elválaszthatatlan összekapcsolódásakor párhuzamosan alkalmazandók, tehát bizonyos tekintetben a jelenlegi szabályozás is holisztikus szemléletre épül. Lásd: FFNPDR 2. cikk (2) bekezdés

[91] Például az adatbázisoknál ismert, egyed-tulajdonság-kapcsolat, illetve generikus/specifikus dimenziók szerint, lásd részletesen: Balogh, 1998, 92-93 o.

[92] Hasonló párhuzammal érvel Parti, lásd részletesen: Parti, 2024. 39 o.

amiket a tényleges tartalmon felül a hozzá kapcsolt metaadatok mutathatnak meg (pl. rögzítés dátuma, sorozatszáma, operációs rendszer vagy alkalmazás típusa stb.).

- *Testiség*

Az adatok fizikai létével összefüggésben azok testi vagy testetlen (eszmei/anyagtalan) mivoltára keressük a választ. Ezt a létrejövetelnél vázolt folyamat értelmezésével úgy gondolom eldönthetővé tehetjük. Itt az észlelés és a rögzülés két mozzanatát különböztettük meg, ami alapján akár arra is következtethetnénk, hogy az adat *a rögzülést* követően *materiálissá* válik,[93] azonban ez nincs feltétlenül így. Az adat hordozótól való fogalmi elválaszthatóságát Zech absztrakció általi szeparációként írja le.[94] Ebből arra következtethetünk, hogy az adat az adathordozón való rögzülése által nem válik maga adathordozóvá, illetve fordítva sem igaz, az adathordozó sem válik adattá. A papírlap, papírlap marad akkor is, ha egy pénzügyi kimutatást nyomtatunk rá. Tehát a „matériát" az adathordozó adja, nem az adat. Ha az adat és az adathordozó mind jogi, mind technikai értelemben megőrzi önállóságát, akkor a köznapi értelemben vett testi tárgy az adathordozó, ezzel szemben az adat csak immateriális, azaz „testetlen tárgy" lehet.

- *Értékesség*

Az adatok értékességével számos kutatás[95] foglalkozott, a jelenlegi konszenzus pedig, hogy mind a személyes, mind a nem személyes adatok vonatkozásában ez azonosítható.[96] E tekintetben meg kell említeni az adatok egyre erősödő *erőforrás,*[97] vagyis gazdasági tényező jellegét.[98] Az adat ebben a szerepben monetizálódik, tehát pénzben kifejezhető értéket vesz fel. Ezt összegszerűen, az Unió adatpiacának értékében tudjuk kifejezni. Ebben folyamatos növekedés tapasztalható, a 2013-ban mért 47 milliárd €-ról 2022-re 73 milliárd €-ra emelkedett.[99] Az értékesség természetének vizsgálatával külön alpontban foglalkozunk, az adatok erőforrás jellegével kapcsolatban azonban még annyit célszerű rögzíteni, hogy az egyedülállóan egy (előre látható felső határ nélkül skálázhatóan) *bővülő* erőforrás. A Big Data jelenségnél kifejtetettekre előre utalva, a rendelkezésre álló globális adatmennyiség évről évre növekszik, tehát a növekvő használat mellett láthatóan nemhogy fogyatkozik, még csak nem is megújul, hanem exponenciálisan bővül.

---

[93] Hasonló szóhasználat létezik a szellemi alkotások és hordozóik egyesülésére, láthatóan azonban ott sem válik ettől a szellemi alkotás testi tárggyá, polgári jogi értelemben dologgá. Lásd részletesen: Lontai Endre, Faludi Gábor, Gyertyánfy Péter, Vékás Gusztáv: Magyar polgári jog, szerői jog és iparjogvédelmi jog. Budapest, Eötvös József Könyv- és Lapkiadó Bt., 2015. 21 o.

[94] Zech, 2017. 12 o.

[95] Lásd például: Bart Custers és Gianclaudio Malgieri írásait a témában, főként személyes adatokat érintően vagy Andreas Wiebe kutatását, nem személyes magán adatok vonatkozásában: Custers, Malgieri, „Priceless data: why the EU Fundamental Right to Data Protection is at Odds with Trade in Personal Data", Computer Law & Security Review 45., 2022.; és Malgieri, Custers „Pricing Privacy the Right to Know the Value of Your Personal Data" Computer Law & Security Review Volume 34, Issue 2., 2018.; és Andreas Wiebe, „Protection of industrial data – a new property right for the digital economy?" Journal of Intellectual Property Law & Practice, 2017, Vol. 12, No. 1.

[96] Szőke Gergely László, „A közadatok újrahasznosítása – a szabályozás alapjai", In: Czékmann Zsolt (Szerk.): Infokommunikációs Jog. Budapest, Dialóg Campus, 2019. 227-228 o.

[97] Bart Custers, Daniel Bachlechner, „Advancing the EU Data Economy - Conditions for Realizing the Full of Potential of Data Reuse", Information Polity, 22(4). 2017. 2 o.

[98] Thomas Streinz, „The Evolution of European Data Law" In: Paul Craig, Gráinne de Búrca (Szerk.): *The Evolution of EU Law,* 3rd edn. Oxford, 2021. 46 o.

[99] The Lisbon Council, „European DATA Market Study 2021–2023", D2.5 Second Report On Policy Conclusions. 15 o.

2.2.3. Az adatok öt tulajdonságcsoportjáról

Az ismérvek mellett – Kitchin munkásságára építkezve[100] – meghatározhatunk olyan tulajdonság-csoportokat,[101] amelyek az adott terület specifikumától mentesen, minden adatot jellemezni képesek:

<table>
<tr><td>Forma (Form)</td><td colspan="5">Az adatok formájuk szerint lehetnek kvantitatívak és kvalitatívak. Előbbi a numerikus (számokkal kifejezhető) adatokat jelenti, míg utóbbi az ettől eltérőket (pl. szöveg, álló- vagy mozgókép, hang stb.)</td></tr>
<tr><td>Struktúra (Structure)</td><td colspan="5">E szerint az adatok lehetnek strukturáltak, részben strukturáltak, és strukturálatlanok. A strukturált adatok konzisztens rendszert alkotnak, ezért könnyen átláthatóak. Ezt egyfelől úgy is megragadhatjuk, hogy az állomány oszlopokra/sorokra bontható táblázatos formában vagy egy relációs adatbázis részeként létezik, de azt is mondhatjuk, hogy a strukturáltsághoz metaadatokra van mindössze szükség, nem feltétel a táblázatos forma. Ehhez képest a strukturálatlan adatok ezen tulajdonságokat nélkülözik (nincs könnyen azonosítható szervezőelv az adatok között, nincsenek metaadatok), míg a részben strukturáltak e kettő elemeit vegyítik.</td></tr>
<tr><td>Forrás (Source)</td><td>Rögzített adat (Captured data): az adatszerzés eredeti formája, a tényszerűség direkt megfigyelésének eredményeként jön létre</td><td>Lehulló[102] adat (Exhaust data): a főfolyamat során, melléktermékként létrejövő adat</td><td>Származtatott adat (Derived data): a már létező adatok újbóli feldolgozása által létrejövő, a bemeneti adattól eltérő, új (kimeneti) adat</td><td>Múló adat (Transient data): ide sorolhatók a nagymennyiségben létrejövő, majd használat nélkül törölt/ hátrahagyott adatok</td><td>Salak adat (Pollution data[103]): ide az adatalapú működésből visszamaradó, értéktelen vagy normasértő adatok tartoznak[104]</td></tr>
<tr><td>Előállítás (Producer)</td><td colspan="5">Ez a kategória az adat előállítása és feldolgozottsága szerint tesz különbséget primer, szekunder és tercier adatok között. Így primer adat az eredeti cél érdekében rögzített és használt adat, a szekunder adat ugyanezen adatállomány más célra történő használatát jelöli, míg a tercier adat egy új adatállomány, amely a primer vagy szekunder állományon alapul.</td></tr>
</table>

[100] Kitchin, 2014. 4-9 o.

[101] Ezeket az adatok genus proximuma-ként is elképzelhetjük, mint minden adatra valamilyen formában jellemző adottságok csoportjai.

[102] A „lehullott” adat a járulékosságot jelenti, nem azt, hogy az adat használhatatlan vagy alacsony értékű.

[103] Omri Ben-Shahar, Data Pollution, 11 J. Legal Analysis 104 (2019)

[104] Az adatszennyezésnek is nevezett folyamat eredményeként létrejövő, olyan nem kívánt adatokra lehet gondolni, mint például a mesterséges intelligencia rendszerek által kéretlenül, tömegesen gyártott sematikus tartalmak, vagy a deep weben található „adatszivárgási” oldalak tartalmai

Típus (Type)	*Indexáló adatok* azok, amelyek valamilyen tényszerűség egyedi azonosítását teszik lehetővé. Ezen belül is elkülöníthetünk direkt azonosítókat és kvázi-azonosítókat. Előbbi önmagában képes a tényszerűség azonosítására, míg utóbbi csak más hasonló adatokkal együttesen. *Az attribútum adatok* a tényszerűséget leíró (arról paramétereket tartalmazó) adatok, amelyek jellemzően nem alkalmasak egyedi azonosításra. A harmadik típuscsoport a *metaadatok,*[105] amelyek az adatokra vonatkozó adatokat jelentik (másként megfogalmazva a metaadatok a tényszerűség reprezentációjára vonatkozó adatok).

A fenti tulajdonságok bármely adat definiálását lehetővé teszik. Azt, hogy a különböző területeken előforduló adatok mégis különböznek egymástól az öt tulajdonság-csoport valamilyen egyedi konstellációja fogja eredményezni. Így egy cetlire feljegyzett bevásárló lista is és egy önkormányzati lakcímnyilvántartás is adatnak minősül, azonban érezhetően lesznek eltérések az egyes kategóriák jelenlétének súlyában.

Az adatok gyűjtésének és rögzítésének módjai, valamint a felhasználás céljai nagyban meghatározzák annak jellemzőit, amelyeket az adat két rétegének és az adatok értékességének vizsgálatával fogunk az alábbiakban közelebbről megismerni.

2.3. A szemiotikus adatfogalom két rétege

2.3.1. A szintaktikai rétegről

A szintaktikai réteg alatt az adat jel és jelkapcsolati (kódolási és fizikai megnyilvánulása[106]) szintjét értjük. Az adatok szintaktikai szintjének egyik legjellegadóbb területe az azokon végzett műveletekhez használt technológia, így jelen dolgozatban alább kifejtett organikus-technológiai adatfogalom különbségtétel alapvetően ezt a szintaktikai adatszintet írja le (megjegyzendő, hogy ezen az alkalmazott nyelv is értelmezhető lehet, de ennek vizsgálatától jelen dolgozatban eltekintünk).

Az adat szó használata és annak térnyerése egyébként is mindig szorosan együtt mozgott a tudomány és a technológia fejlődésével. Mint főnév – bár latin eredetű, a *dare* (adni) igéből származik[107] – az 1640-es évektől tényszerűségek azonosítására szolgált, később az 1890-es évektől már kifejezetten a számszerűsített tényeket nevezték adatoknak. A mai értelmét az informatika megjelenésével szerezte meg. 1946-ban „továbbítható és tárolható információként" jelölték az adatot, amellyel „számítógépes műveleteket végezhetők", ezt követően 1954-ben jelentek meg az adatfeldolgozás és 1962-ben az adatbázis szóösszetételek.[108] Az adatok használatának majdnem összes aspektusára jelentős hatást gyakorolnak a technológiai fejlődés által indukált folyamatok. Fontos azonban, hogy amennyire az FDIKW piramist ki kellett terjesztenünk az elme kognitív folyamatain túl, a technológia világára, most legalább ennyire fontos látnunk, hogy az adatok nem kizárólag a technológia határain belül léteznek. Így az alkalmazott technológia, mint vizsgálati fókuszpont esetén, legmagasabb szinten kettő nagy kategóriára oszthatók az adatok, technológiai és nem technológiai jellegű (organikus) adatokra. Mindkettő az FDIKW modell absztrakt megközelítésének megfelelően valamilyen

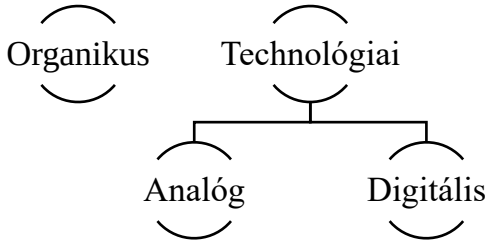
[105] DA 2. cikk 2. pontja szerinti megfogalmazásban a metaadat az adat tartalmának vagy felhasználásának strukturált leírása, amely egyszerűsíti az említett adat kereshetőségét és felhasználását

[106] Zech, 2015, 194 o.

[107] Kitchin a szó etimológiai tisztázása során kitér az adat (datum) kifejezés helytelenségére is. Szerinte az adni ige helyett az elvenni találóbb lenne, hiszen a mérés és rögzítés mozzanatán keresztül a környezettől elvesszük az adatokat, nem pedig megkapjuk. Így a megfelelő kifejezés latinul a „captum" angolul pedig „capta" lenne. Lásd részletesen: Kitchin 2014 2 o.

[108] Etymonline, „Online Etymology Dictionary" Harper Family LLC. Elérhető: https://www.etymonline.com/word/data, Letöltve: 2024.01.14.

tényszerűséget reprezentáló szimbólumot jelent, de előbbi kifejezetten a technológiához köthető, míg utóbbi azt nélkülözi.



4. ábra: a technológiai adatkategóriák

A technológiai adatok alapvető tulajdonsága, hogy azok a technológia valamely eszköze által jönnek létre, tárolódnak, illetve hasznosulnak, míg ezzel szemben az organikus adatok azok, amelyek nem kapcsolódnak a technológia semmilyen formájához. Organikus adatok kezelésére kognitív képességek birtokában lévő lények lehetnek képesek. Ezen lények – különösen az ember – elméje és teste (előbbi, mint szoftver, utóbbi mint hardver) is végső soron algoritmusok lefuttatásának sokaságát hajtja végre, így nem tűnik elrugaszkodottnak ezeket a biológiai rendszereket úgy elképzelni, mint amelyek adatokat rögzítenek és azokon műveleteket hajtanak végre.[109] Organikus adat lehet például az emlék, amely elektroenkefalográfiai (EEG) vagy funkcionális mágneses rezonanciavizsgálattal (fMRI) detektálható az emberi vagy állati agyban.[110] Az agy organikus műveletvégzésének megfigyelésére a fenti két technológia mellett számos másik is említhető (MRI, MEG, (f)NIR/DOT, CT, PET/SPECT, EROS), amelyek az egészségügyi adatkezelés területén, mint „neuroadatokként"[111] ismert adattípust rögzítenek,[112] de az adatvédelmi szakirodalom szerint ezeket, mint biometrikus és/vagy egészségügyi adatokként is értelmezhetjük.[113] Ide vonhatók továbbá a biológiai minták,[114] ám ezeket azzal a kitétellel kezelnünk, hogy az organikus adatokra a GDPR definíciója nem kifejezetten alkalmazható, mivel a jogszabály hatókörének racionalizálása érdekében azt szándékosan az azokból kinyerhető technológiai adatokra szűkítette. Tehát a GDPR által definiált genetikai adatok[115] és biometrikus adatok[116] a szerv vagy biológiai minta elemzéseként létrejövő technológiai adatok. Ezeknek organikus megfelelője lehet ezen adatok forrása (pl. a vérminta maga) vagy például maga a bőrfelszínen képzett ujjnyom. A két adattípus közti átjárhatóságot látszik erősíteni az un. exocortex technológia,[117] amely az organikus és mesterséges elemek

[109] Pléh, 2012. 65 o.

[110] Emily R. D. Murphy, Jesse Rissman, 'Evidence of Memory from Brain Data' (2020) 7(1) Journal of Law and the Biosciences 1. 11 o.

[111] Fontosnak tartom az egyértelműség kedvéért rögzíteni, hogy az idézett berendezések által rögzített „neuroadatok" technológiai adatoknak minősülnek, de azok valójában az agy „adatalapú" műveleteire vonatkoznak. Így gyakorlatilag az agyi organikus adatokat konvertálják technológiai formátumra.

[112] Paul de Hert, Michael Friedewald, Dara Hallinan, Philip Schütz, „Neurodata and Neuroprivacy: Data Protection Outdated?", *Surveillance & Society* 12(1), 2014. 58 o.

[113] Eszteri Dániel, „Az új technológiák megjelenésének hatása a személyes adatok védelmére: gépi tanulás, blokklánc, internet-of-things, agyhullám-olvasás.", Szemelvények az információs jogokról - a rendszerváltástól napjainkig. Budapest, Patrocinium Kiadó, 2021. 164-193 o.

[114] A GDPR (35) preambulumbekezdésével összefüggésben, de azt a jelen kontextushoz igazítva a biológiai minta valamely testet alkotó anyagot jelenti.

[115] A GDPR 4. cikk 13. pontja alapján nem csak természetes személyekre szűkítve a következő módon határozhatjuk meg a genetikai adatokat: egy *élőlény* örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan adat, amely az adott élőlény fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett élőlényből vett biológiai minta elemzéséből ered.

[116] A GDPR 4. cikkének 14. pontja alapján, nem csak természetes személyekre szűkítve a következő módon határozhatjuk meg a biometrikus adatokat: egy *élőlény* testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert adat, amely lehetővé teszi vagy megerősíti az *élőlény* egyedi azonosítását.

[117] Az exocortex egy olyan beültett vagy hordható eszköz, amely az agy magas szintű biológiai kognitív funkcióit támogatja, illetve közvetlenül neurális jelekkel való kommunikációt tesz lehetővé az agy és az ilyen jelek fogadására képes környezet között. Lásd részletesen: T. Bonaci, J. Herron, C. Matlack and H. J. Chizeck, "Securing

szoros integrációját teszi lehetővé, ezzel az organikus adatokat technológiaivá alakítva és fordítva.

A technológiai jellegű adatokat szintén tovább bonthatjuk analóg és digitális adatokra, amely megkülönböztetés alapja a rögzítéshez felhasznált technológia, valamint az adathordozó típusa. Megjegyzendő, hogy a jelenleg elterjedt két alkategória mellett a kvantumszámítógépek megjelenésével együtt a kvantum adatok is megjelenhetnek és elterjedhetnek.[118] Tekintve, hogy az algoritmizált adathasználat tárgyköre kifejezetten a technológiai adatokkal mutat szoros kapcsolatot, ezekkel foglalkozok részletesebben.

2.3.1.1. Az analóg adatokról

Analóg adatnak tekinthetünk egyfelől minden formák megjelenítésére alkalmas mesterséges vagy természetes felületen, illetve anyagon, leképzett adatot. Ezen kategória elsődleges képviselői a papír alapú iratanyagok, de ide tartoznak például a műanyagokra nyomott különféle kártyák, a vászonra – vagy akár barlangfalra – felvitt festmények, illetve a polaroid fotók is. Másfelől léteznek modern analóg eszközök, amelyeknek közös jellemzője, hogy bennük az adatáramlás és tárolás folytonos analóg jelekkel (pl. elektronikus, mechanikus, pneumatikus, hidraulikus) történik ellentétben a digitálissal, ahol ez (bináris) számokból álló formában zajlik.[119] Az ilyen analóg eszközök tovább bonthatók nem-elektromos és elektromos eszközökre. Előbbiekre példaként említhetők a napórák, a higanyos hőmérők vagy a mérlegek. Utóbbiak között szerepel a legtöbb ma használt digitális technológiai eszköz előképe, mint az analóg televízió és rádió, vagy a teleautográf,[120] továbbá az analóg adathordozók között említhetjük a kazettákat vagy mágnesszalagokat.

2.3.1.2. A digitális adatokról

A digitális adatok – digitális számítógépek számára feldolgozható adatok[121] – így a számítástechnika működési elveinek megfelelően döntően numerikus értékekkel (bináris rendszerben) kerülnek létrehozásra, tárolásra és továbbításra.[122] Az ilyen informatikai eszközök szinte teljes működési ciklusuk alatt valamilyen adatkezelési műveletet végeznek. Meglévő adatot gyűjtenek, illetve rögzítenek, új adatot hoznak létre, mindezeket tárolják, összekapcsolják, valamilyen cél érdekében használják vagy továbbítják. Minden rendszer kezdő pontján (input), a működése során és a folyamat zárásakor (output) adatokon végzett műveletek zajlanak. Egy operációs rendszer napló fájljainak generálásától, az okostelefonok térkép applikációjának útvonalterv készítésén keresztül az olyan bonyolult folyamatokig, mint egy fejlett nyelvi modell kommunikációja mind ezen az elven működik. A digitális adatkategóriához tartozik a digitális formában létező szöveg, kép (álló vagy mozgó), hang, szám és bármilyen automatikusan rögzített technikai leírás (log) is, továbbá ide tartoznak a

---

the exocortex: A twenty-first century cybernetics challenge," *2014 IEEE Conference on Norbert Wiener in the 21st Century (21CW)*, Boston, MA, USA, 2014, 1-8 o.

[118] A kvantumszámítógép a kvantummechanika alapján végzi a műveleteket, így ellentétben a digitális rendszerekkel ezeknél nem bitekről, hanem qubitekről beszélünk, amelyek már nem csak 1-ek és 0-ák lehetnek. Lásd részletesen: M.A. Nielsen, I.L. Chuang: Quantum Computation and Quantum Information, 2000, Cambridge University Press; első kiadás.

[119] W.K. Jenkins: Signal Processing, Analog. Encyclopedia of Physical Science and Technology (Third Edition) 2003. 711-735 o.

[120] "The Writing Telegraph", Scientific American. 40 (13): 196. March 1879. Elérhető: https://sciam-cms.s3.amazonaws.com/sciam/cache/file/9AFDF555-B4F7-4FEB-8867941F917A1005.pdf Letöltve: 2024.05.19.

[121] Juan Ortiz Freuler, "Datafication, Identity, and the Reorganization of the Category Individual", Temple Law Review, vol. 95, no. 4. 2023. 378 o.

[122] Britannica.com, Encyclopædia Britannica, https://www.britannica.com/technology/digital-computer Letöltve: 2024.01.14.

rögzített tartalmakat leíró egyéb digitális adatok (metaadatok) is. Ezek az informatika állása és az alkalmazott keretrendszer szerint sokféle – egyre bővülő számú – fájlformátumban létezhetnek. Így szöveg lehet a TXT vagy DOCX, kép a JPG, míg audió a FLAC, a videó pedig az AVI.

2.3.1.3. A Big Data jelenségről

A Big Data mára már kevéssé számít nóvumnak, hiszen egyes felfogások szerint legalább 2012-óta a Big Data korában élünk,[123] ettől függetlenül az ezzel kapcsolatos tanulságok a téma szempontjából továbbra is relevánsak, főként mivel a digitális adatokkal kapcsolatban sokszor kerül említésre. A jelenség a világon adott pillanatban, potenciálisan rendelkezésre álló, (hatalmas és gyorsan növekvő mennyiségű, változatos tartalmú) összes adatot jelöli. [124] A Big Data tehát nem jelent egy önálló adatkategóriát, azonban a téma szempontjából kiemelt jelentőséggel bíró digitális adatok mai leglényegesebb megjelenési formája.[125] A mai nagy adathalmazok jelentős része nyers adatként létezik, így azok további feldolgozása szükséges, ahhoz, hogy ténylegesen használhatóvá váljanak. A Big Data mögött található adatok ugyanis kiemelt forrásai a használható – ezáltal technológiailag és jogi szabályozás szempontjából kezelendő – adatoknak. A nagy adathalmazokat több szempont szerint lehet leírni, annak jobb megértése érdekében. Ezt a felosztást (angol nyelven) összefoglalóan az 5V attribútumoknak szokás nevezni:[126]

- mennyiség (volume), ami rendkívül nagy, 2028-ra a becsült Big Data állomány elérheti a 394 zetabyte[127] mennyiséget, [128]
- sebesség (velocity), ami a gyűjtés sebességét jelenti és szintén értékelendő, hogy sok esetben valós időben történik (nem véletlen tehát, hogy az előbbi mennyiségi tényező exponenciális bővülését tapasztaljuk),
- változatosság (variety), a változatosság jelen esetben a formátumok változatosságára utal, ez digitális adattípusok esetén megegyezik a korábban taglaltakkal (így pl. TXT, FLAC, AVI, XML stb.),
- hitelesség (veracity) alatt az adatforrás megbízhatóságát (egyúttal bizonytalanságát) értjük. A megbízhatóság (pontosság) jellemzően az állomány méretének növekedésével csökken.[129]
- értékesség (value), ami az adatból kinyerhető hasznot (tehát az adott cél elérésére való alkalmasságot) takarja.

A nagy adathalmazok térnyerésének és a mindennapi életünkhöz szervesen kapcsolódó pontjainak megértéséhez további három, a jelenség alapvetően input oldaláról, tehát a bemenő adatokat befolyásoló tényezőkről szükséges röviden szót ejteni. Ezek a Dolgok Internete

[123] Steve Lohr, The Age of Big Data, N.Y. TIMES (2012) Elérhető: https://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html, Letöltve: 2024.01.16.
[124] Alexandra Anghel, Elena Novacescu, Madalina Cuc, „Big Data and Its Secrets: Types of Big Data" Romanian Intelligence Studies Review 27. 2022. 54-73 o.
[125] Fontos, hogy a Big Data önmagában nem csak a digitális adatokra vonatkozik, abba bele tartozik minden adatkategória. Lásd részletesen: Mayer-Schönberger, Cukier, 2014. 91 o.
[126] Amy Affelt, "Big Data, Big Opportunity" Australian Law Librarian, vol. 21, no. 2, 2013. 78-89 o.
[127] A mérték érzékeltetése érdekében megjegyzendő, hogy 1 zettabyte egyenlő 1 000 000 000 terabyte-al.
[128] Petroc Taylor, „Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2023, with forecasts from 2024 to 2028" STATISTA, 2024. Elérhető: https://www.statista.com/statistics/871513/worldwide-data-created/#:~:text=Over%20the%20next%20five%20years%20up%20to%202028%2C,data%20created%20and%20replicated%20reached%20a%20new%20high. Letöltve: 2025.01.31.
[129] Mayer-Schönberger, Cukier, 2014. 44-45 o.

eszközök, az adatosítás társadalmi trendje és a web 2-es alkalmazások használatának elterjedése.

- A Dolgok Internete (Internet of Things, IoT) hálózatra kötött, egymással jellemzően IP[130] alapon kommunikáló és szenzorosan adatokat gyűjtő, valamint továbbító eszközöket jelenti.[131] Az IoT egyre elterjedtebbé válik számos iparágban, többek között a közlekedésben, a mezőgazdaságban és az egészségügyben is. Az ilyen eszközök olyan előnyökkel járnak, mint valós idejű adatgyűjtés és feldolgozás, pontos és naprakész visszacsatolási hurkok létrejötte, valamint a távoli felügyelet és irányítás képessége, amelyek a köz- és a magánszféra szervezetei számára egyaránt nagyobb működési hatékonyság elérését teszik lehetővé.[132] Az IoT eszközök árnyoldalához tartoznak különösen adatbiztonsági és adatvédelmi aggályok, úgy, mint a folyamatos bekapcsoltságból eredő túlzó adatgyűjtési tendenciák vagy adatbázisok jogellenes összekapcsolása.[133]
- Az internet, fennállása alatt több átalakuláson is keresztülment, az adatok szempontjából legnagyobb horderejű a második korszaka (web 2.0). Az előző állapotában az adatáramlás leginkább vertikálisan épült fel és egy egyirányú útként képzelhető el az adatot létrehozó és az adatot fogyasztó felhasználó között. A web 2.0 adatáramlása ehhez képest horizontális kiterjedésű, az adatot létrehozó és a felhasználó mellérendeltek, sőt a két pozíció jellemzően egymásba is csúszik, tehát az adatot létrehozó egyszerre felhasználó is és fordítva, a felhasználó maga is létrehoz adatot.[134] A web 2.0 állapot lehetőséget biztosított mindenki számára (cégek, államok és magánszemélyek) az adathoz való hozzáférésre és az adat megosztására egyaránt, ami nagyban járult hozzá a nagy adathalmazok mennyiségi duzzasztásához.[135]
- Az adatosítás („datafication") egy olyan modern jelenség, amely a világ eseményeinek adattá (ma döntően digitális adattá) történő átalakításának folyamatát, egyre növekvő trendjét jelenti.[136] Mérhető a hatása ebben a folyamatban is az IoT eszközök térnyerésének, de az adatosítás a társadalmi együttélés digitalizációjának egy aspektusaként[137] is azonosítható.[138] Az online terek (és az azokat működtető szolgáltatók) egyértelmű törekvése, hogy a felhasználók minél több mindennapi emberi magatartásukat és életük átlagos eseményeit digitális adatként is leképezzék. Az adatosítás kiemelt jelentősége kifejezetten az új, korábban adatként nem létező adattípusok összegyűjtésében, illetve generálásában rejlik. A különböző, web 2.0-es

[130] Az internetprotokoll, az interneten keresztüli kommunikáció egyik alapvető szabványa.
[131] Techopedia: What Does internet of Thnigs (IoT) Mean? https://www.techopedia.com/definition/28247/internet-of-things-iot (2022.08.02.)
[132] Larisa-Antonia Capisizu, "Legal Perspectives on the Internet of Things," Conferinta Internationala de Drept, Studii Europene si Relatii Internationale 2018. 523 o.
[133] Eszteri Dániel, „Elosztott adatbázisok, okoseszközök, automatikus döntések és a GDPR: adatvédelmi kapcsolódási pontok néhány új technológia vizsgálata kapcsán", MJ, 2022/9., 505-515. o.
[134] Darin K. Fox, "What Is Web 2.0", AALL Spectrum, vol. 13, no. 9. 2009.
[135] Az internet következő web 3.0 szakasza a Big Data szempontjából kevésbé, adatjogi szempontból annál inkább fontos, minthogy az internet (eredeti elképzelés szerinti) „közösségesítését" tűzte ki célul. Ez elméletileg egy blokklánc alapú, decentralizált szisztémát jelent, ami internetes közösségek által működtett és felügyelt. Ennek többek között például a magánszféra védelemre lehetne pozitív hatása. Lásd részletesen: What is Web3?, McKinsey & Company. Elérhető: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-web3#/
[136] Ulises A. Mejias, Nick Couldry, „Datafication", Internet Policy Review Journal On Internet Regulation Volume 8 | Issue 4. 2019. DOI: 10.14763/2019.4.1428
[137] Clare Southerton: Datafication. Laurie Schintler, Connie McNeely, (Szerk.): Encyclopedia of Big Data. (Springer, 2020) 1-4 o.
[138] Fontos kiemelni, hogy itt sem szükségszerű az, hogy az adatok digitális formában keletkezzenek. Lásd részletesen: Mayer-Schönberger, Cukier, 2014. 44-45 o.

> olvasztótégelyben megalakult, közösségi média platformok élen járnak az adatosítás társadalmi jelenlétének proliferációjában. A felületeik és funkcióik kiosztásával, valamint fejlett algoritmizált eszközeik és hatalmas mennyiségű felhasználói személyes adat használatával képessé váltak alapvető hormonális impulzusok és tevékenységi hurkok létrehozására, amelyekkel maximalizálni képesek az adatmegosztási késztetést.[139]

Fontos megemlíteni az MI rendszerek által történő adatok (jellemzően szöveges vagy képi tartalmak) generálásának szintén gyorsan terjedő jelenségét.[140] A kapcsolat az MI és a BigData között nyilvánvaló, ennek adatjogi jelentőségét azonban egy ide vonatkozó egyedi fogalom tudja leginkább megvilágítani. Ez a fogalom az un. „deepfake", amely az MI által generált vagy manipulált olyan kép, audio- vagy videótartalmat jelenti, amely hasonlít létező személyekre, tárgyakra, helyekre, entitásokra vagy eseményekre, és amely egy személy számára megtévesztő módon autentikusnak vagy valóságosnak tűnhet.[141] Tehát a deepfake olyan MI által generált vagy módosított tartalom, amelyet jellemzően abból a célból alkot(tat)nak meg, hogy úgy tűnjön egy adott esemény megtörtént, vagy hogy valaki másképp viselkedett vagy nézett ki, mint valójában. Az ilyen deepfake-elt adatok létrehozása a személyiségi jogok megsértéséhez, személyiséglopáshoz, dezinformációhoz, egyúttal a közbizalom sérüléséhez, a társadalmi és interperszonális kapcsolatok átláthatóságának csökkenéséhez vezethet.[142] Az MI rendszerek szabályozása az adatok védelménél egy speciálisabb, a területre szabott norma hatókörébe tartozó kérdésnek tűnik, amely szerepet jelenleg Európában az MI rendelet tölt be. Ettől függetlenül megjegyzendő, hogy személyes adatok kezelése esetén az azokra vonatkozó védelmi előírások mind a modell létrehozásakor (mint tanító adatok), mind annak alkalmazásakor (mint bemeneti vagy akár kimeneti adat) betartandók.[143]

Összegezve az adatok szintaktikai rétege az alkalmazott technológiától függően differenciálódik. Az adathasználat tekintetében a klasszikusnak tekinthető analóg eljárások mellett az utóbbi évtizedben a digitalizáció által előtérbe helyezett digitális adatok vezető szerepe figyelhető meg.

2.3.2. A szemantikai rétegről

Az adatok absztrakt fogalmának kutatása során rögzítettük, hogy az adatszemiotikának megfelelően azok szintaktikai és szemantikai szintekre oszthatók. Az előbbiekben az adatok szintaktikai, tehát a jelszintje, mely jelen dolgozatban a rögzítéshez és feldolgozáshoz alkalmazott technológia szintjeként került kifejtésre. Az adatok szemantikai szintje, vagyis a jelentésbeli minőségük több oldalról is vizsgálható, de jelen dolgozat – témájából fakadóan – alábbi fejezetében a jogi jelentéssel, ezáltal a jogi adatfogalommal fog foglalkozni.

---

[139] Trevor Haynes, „Dopamine, Smartphones & You: A battle for your time" Harvard University, Science in the News. Elérhető: https://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time/ Letöltve: 2024.01.16.

[140] Proofed, „What Is AI-Generated Content?". Elérhető: https://proofed.com/knowledge-hub/what-is-ai-generated-content/

[141] MI rendelet 3. cikk 60. pont

[142] Keleti Arthur, „Nem minden az, aminek látszódni akar - a deepfake és a hitelesség jelene és jövője" In: Aczél Petra, Veszelszki Ágnes (szerk.): Deepfake: a valótlan valóság. Budapest, Médiatudományi Könyvek, 2023. 70-73 o.

[143] Eszteri Dániel, „A deepfake-technológia adatvédelmi értékelése a GDPR tükrében" In: Aczél Petra, Veszelszki Ágnes (szerk.): Deepfake: a valótlan valóság. Budapest, Médiatudományi Könyvek, 2023. 146-150 o.

Az adatfogalom normatív meghatározottságát a vizsgált jogszabályokban a jogág vagy jogterület szektorális jellege és a joganyag megalkotásának ideje nagyban befolyásolja. A számítástechnika kellő fejlettségi foka és az adatok jelentőségének felismerése a 2010-es években érte el az európai jogalkotást, ezért a korábbi aktusok az adatokat kevésbé tematizáltan kezelték. Időbeli meghatározottságtól függetlenül a döntéshozók jogot a jogpolitikai célkitűzéseik mentén alkotnak, ott, úgy és akkor, amikor az életviszonyok (megítélésük szerint) szabályozásra szorulnak. E két tényező együttesen sporadikus, sokszor csak egy jogszabályi kontextusban, izoláltan létező adatfogalom meghatározást eredményezett (ez alól az uniós jogalkotás 2010-es évek második felétől egyértelmű kivételt jelent). Szintén az ágazati jogalkotásból következik, hogy bár az adatfogalmak jogterületekhez igazodnak, de azok között létezik valamelyest átjárás, azáltal, hogy egyes fogalmakat kereszthivatkozzák, a helyett, hogy újból definiálnák azokat (tipikus példa erre a személyes adat fogalma). A vizsgálatom az uniós és hazai jogszabályok áttekintésére irányult, ezek közül is elsődlegesen azokra, amelyek leginkább kötődnek a későbbiekben vizsgálat adatjog területéhez.

2.3.2.1. A releváns jogforrásokban található adatfogalomról

Az adat általános érvényű definiálására uniós szinten (és a témával legszorosabb kapcsolatban) viszonylag későn, 2022-ben került sor, az Adatkormányzási rendelet[144] által. Ez a fogalom megjelenik több másik, az Unió „digitális jogalkotási hullámához" tartozó joganyagban, így a Digitális Piacokról szóló rendeletben[145] és az Adatrendeletben.[146] A definíció szerint az adat: *„aktusok, tények vagy információk bármilyen digitális megjelenítése, vagy az említett aktusok, tények és információk összeállításai, többek között hang-, kép- vagy audiovizuális felvétel formájában is"*.[147] A fogalom aktusok, tények és információk megjelenítésére utal, ahol az aktus (tett, cselekedet[148]) és a tények nagyban megegyeznek az FDIKW-piramis alapján meghatározott absztrakt adatfogalommal. Az aktusok, tények és információk összeállításainak említése az adatok eredeti és származékos jellegére utal helyesen. Az információ fogalomba építése sem okoz alapvetően értelmezési nehézséget, ha azt, mint az adat egy másik állapotát fogjuk fel. A fogalom elméletben és gyakorlatban is alkalmazhatónak mutatkozik, kiemelendő továbbá, hogy formátumra kifejezett utalást tartalmaz, így az csak a digitális adatokra vonatkozik.

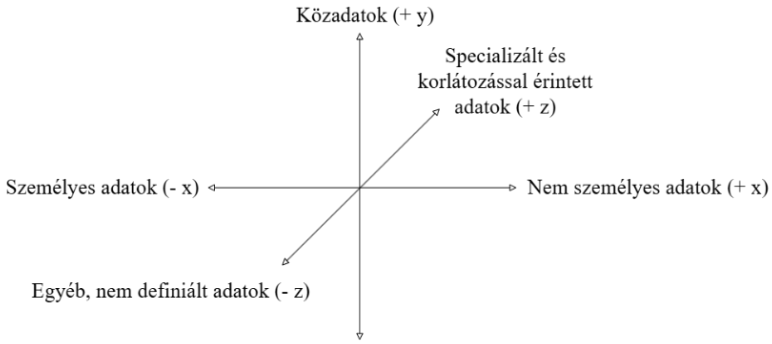
Elhagyva az uniós jogot, hazai jogunk eredményeként is találunk adatfogalom meghatározásokat. Elsőként kiemelendő, hogy a nemzeti adatvagyon hasznosítására irányadó legújabb joganyag átvette a DGA által bevezetett adatfogalom meghatározást.[149] Egy korábbi saját adat fogalom is említhető, amely 2025. január 1-ig az Ibtv-ben[150] volt megtalálható. Hatályon kívül helyezése miatt jelenleg utódjában[151] olvasható. Ez alapján adat: „az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas."[152] Ez a

[144] Adatkormányzási rendelet 2. cikk 1. pont
[145] Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (továbbiakban: Digitális Piacokról szóló rendelet vagy DMA) 2. cikk 24. pont
[146] Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete a méltányos adathozzáférésre és -felhasználásra vonatkozó harmonizált szabályokról (adatrendelet, DA) 2. cikk (1) bekezdés
[147] DGA 2. cikk 1. pont; DA 2. cikk (1) bekezdés; DMA 2. cikk 24. pont
[148] *Aktus*. Idegen Szavak Gyűjteménye. https://idegen-szavak.hu/aktus (2024.04.30.)
[149] A nemzeti adatvagyon hasznosításának rendszeréről és az egyes szolgáltatásokról szóló 2023. évi CI. törvény (továbbiakban: Nah.tv.) 2. § 1. pont
[150] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.) 1. § (1) bekezdés 1. pont
[151] Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (továbbiakban: Kib.tv.) 4. § 1. pont
[152] Ibtv. 1. § (1) bekezdés 1. pont

fogalom az eredeti törvény (Ibtv.) megalkotásának idejére tekintettel valamivel absztraktabb, ettől függetlenül (sőt talán pont ezért) mind szóhasználatában, mind logikájában fedi az eddigiekben felépített adatfogalmunkat. Az Ibtv.-hez kapcsolódott egy információ fogalom is, amelyet az utódja nem vett át, azonban az információ lényegének megragadásához továbbra is jól alkalmazható. Az Ibtv. szerint információ: „bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti."[153] Elmondható, hogy hasonlóan az adatfogalomhoz az Ibtv. információ meghatározása is megfelel jelen dolgozat által képviselt felfogásnak, abban megjelenik az egyediesített érték hordozása és az újszerűség fontossága.

2.3.2.2. A jogi adatkategóriák csoportosításáról

Az egyes, jogrendszerben előforduló adattípusok igen színes képet mutatnak, így a csoportosításuk során egy egyszerű, az adathasználat jogi szabályozása szempontjából azonban fontos kiindulópontként szolgáló felosztást ismertetek,[154] amely az adatokat egyrészt személyes adatra és nem személyes adatra, másrészt, e kategóriákat vertikálisan érintve közadatokra és magánadatokra bontja. A koordináta-rendszer elemei a jelenlegi társadalmi és gazdasági körülmények között nagyjából állandónak tekinthetők és kellő rugalmasság mellett akár múltbeli vagy jövőbeli adatok definiálására alkalmas. A négy nagy jogi adatkategória azonos tengely mentén haladva egymást kölcsönösen kizárja, egyúttal az ellenkező tengely mindkét elemét szükségszerűen metszi. A kategóriák közti könnyebb megkülönböztetés érdekében általánosságban elmondható, hogy az y tengelyen található közadatok és magánadatok lényegi eleme, hogy a jog miképpen definiálja a közadatokat, ugyanis ehhez képest – negatíve – értelmezhetőek a magánadatok (vagyis minden magánadat, ami nem közadat). Az x tengely személyes és nem személyes adatainak elhatárolási pontja, hogy kire vagy mire vonatkoznak.[155] Egy egyszerű és sematikus példával érzékeltetve: egy természetes személy neve mindig személyes adat lesz, de attól függően, hogy mint egy cég munkavállalója vagy mint egy önkormányzat polgármestere tevékenykedik lehet személyes közadat vagy magánadat.



5. ábra: a jogi adatkategóriák

Az ábra térbeli kiterjedését jelentő z tengely az adatjog „keresztülfekvő" jellegét modellezi és így egy tágabb értelmezést mutat be. A z tengely egyik oldala az adatok speciális adatkategóriáit jelöli, amelyeknek nem feltétlenül, de sok esetben közös jellemzője, hogy a kezelésükkel kapcsolatban valamilyen korlátozó rendelkezés van érvényben. Ezek főszabály szerint továbbra is megfelelnek a jelen dolgozatban kidolgozott absztrakt adatfogalomnak, a koordináta rendszerben a példának megfelelően elhelyezhetők, azonban egy további megkülönböztető paraméterrel is rendelkeznek. A példát folytatva a személyes adat egy cég esetében könnyen

[153] Ibtv. 1. § (1) bekezdés 25. pont
[154] A felosztás alapjai Szőke Gergely Lászlótól származnak. Szőke Gergely László: Mikor tűnik el az ember a személyes adatok mögül? - Avagy az anonimizálás kihívásai. Konferencia-előadás „Az ember a legújabb technológiák között" c. konferencián, Budapest, Nemzeti Közszolgálati Egyetem, 2023.05.31.
[155] Ibid.

lehet, hogy egyúttal üzleti titoknak is minősül, míg egy állami szerv vonatkozásában felmerülhet a minősített adat jelleg. A z tengely másik végpontja a jelenlegi adatfogalmakon kívül létező, eddig nem definiált adatokat takarja. A nem definiált adatok kategóriája biztosítja a modell rugalmasságát, a potenciálisan ide vonható adatok az aktuális technológiai és társadalmi trendekkel jelenhetnek meg vagy tűnhetnek el, azonban közös bennük, hogy a jog által bármikor nevesíthetők, tipizálhatók lehetnek.

2.3.2.3. A személyes adatokról

A jelenleg hatályos jog szerint személyes adat az „azonosított vagy azonosítható természetes személyre vonatkozó bármely információ."[156] Az azonosíthatósággal kapcsolatban ugyanitt további útmutatás található, e szerint „azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosítója (…) alapján azonosítható". A fogalom láthatóan meglehetősen tág, az azonosíthatóság első ránézésre úgy tűnik, hogy a direkt azonosító adatok[157] alapján való azonosíthatóságot preferálja, ez azonban az újfent tágan meghúzott „közvetett" azonosíthatóság lehetőségével felülírásra került. Ezért a személyes adatokat a szakirodalom jellemzően két típusra osztja. Az első az un. azonosító (indexáló) adat, amely az adatkezeléssel érintett személy egyediesítését, másoktól való megkülönböztetését szolgálja. A második az un. leíró (attribútum) adat, amely az adatkezelés célja szerint releváns személyes adatot takarja.[158]Az azonosíthatóság kapcsán a GDPR preambuluma szerint „minden olyan módszert figyelembe kell venni […], amelyről észszerűen feltételezhető, hogy az adatkezelő vagy más személy a természetes személy közvetlen vagy közvetett azonosítására felhasználhatja."[159] Ez a mérce tehát sok esetben csak a körülmények pontos ismeretében teszi eldönthetővé, hogy valamely adat személyes adatnak vagy nem személyes adatnak minősül, továbbá az adatkategóriák közötti dinamikus átjárást is lehetővé teszi.[160] A fogalmi meghatározás jelentősége az adathasznosítás iránti igény növekedésével együtt az elmúlt években számottevően megnőtt, és döntő szerepe van abban, hogy mely jogszabályi előírás alkalmazandó.[161] A 2018-óta kialakult gyakorlat ismeretében elmondható, hogy a jelenlegi személyes adat fogalom tartalmi szempontból meglehetősen inkluzív, olyannyira, hogy egy frappáns közmondás szerint „ha valamivel kapcsolatban felmerül, hogy személyes adat, akkor valószínűleg az is". Ez természetesen nem jelenti a parttalan értelmezés helyeslését, nem véletlen, hogy a személyes adatok mellett a nem személyes adatok kategóriájának létrehozására is sor került. Rendszertani megítélésük szempontjából hangsúlyozandó, hogy a személyes adatok fogalmilag csak természetes személyekre vonatkozhatnak, és mint ilyenek a védelmüket az Uniós és hazai jog alapvető jogként nevesíti. A személyes adatok terminológiai meghatározottsága kevésbé fragmentált, elsődlegesen – uniós rendelet jellegéből adódó alkalmazási elsőbbsége révén – a GDPR határozza meg, míg az Info.tv. ezt kiegészítheti, pontosíthatja. Az egyéb (frissebben megalkotott) jogszabályok a fogalmat konzekvensen

---

[156] GDPR 4. cikk 1. pont; Tartalmilag nagyon hasonló az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Info.tv.) 3. § 2. pontjában meghatározott személyes adat fogalom, amely szerint ez az érintettre (értsd: természetes személyre) vonatkozó bármely információ

[157] Például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó, egy vagy több tényező

[158] Balogh, 1998. 170-171. o.

[159] GDPR (26) preambulumbek.

[160] Nadezhda Purtova, „Do property rights in personal data make sense after the Big Data turn? Individual control and transparency", 10(2) Journal of Law and Economic Regulation, 2017. 1-2 o.

[161] Czapári Dóra, Szőke Gergely László, „Az adatvédelem és az adathasznosítás egyik kulcskérdése: a személyes adatok anonimizálása", JURA, 2022/4. 26. o. Az anonimizálás komplex értelmezését ld. ugyanitt.

átveszik vagy hivatkozzák, így a hazai és az uniós jogrendszerben nem tapasztalható zavar a személyes adatok fogalmát illetően.

A személyes adatok belső halmazát alkotja a különleges adatok kategóriája, amelyek érzékenységük miatt megkülönböztetett védelemben részesülnek. Különleges adatnak minősülnek a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.[162] Fontos továbbá, hogy szintén speciális megítélésűek a bűnügyi személyes adatok, amelyek a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adatok.[163] A különleges adatok felsorolt elemei közül a genetikai,[164] a biometrikus[165] és az egészségügyi adatok[166] külön definiálásra kerültek.

A személyes adatok fogalmával kapcsolatban az látható, hogy a jogalkotó az általános meghatározásokon túl az egyedi, a kor kihívásaira reagáló speciális fogalmakat is törekszik megalkotni.

2.3.2.4. A nem személyes adatokról

Jogi szempontból láthatóan különös jelentősége van annak, hogy egy adat egy természetes személyre vonatkozik-e vagy sem. Amennyiben igen, úgy a kezelésre vonatkozó előírások a fentieknek megfelelően rendkívül kiterjedtek és részletesek, az alapvető szabályozási hozzáállás elsődleges az adatok védelmét és csak másodsorban az adatok szabad áramlását célozza. Ezzel szemben a nem-személyes adatokra vonatkozó rendelkezések lényegesen heterogénebbek, ritkán az adatok védelmét írják elő, míg sok esetben azok kifejezett nyilvánosságra hozatalát (pl. az FFNPDR kifejezett célja annak biztosítása, hogy a személyes adatoktól eltérő adatok az Unión belüli szabad áramolhassanak[167]). Fogalmi szempontól a nem személyes adatok (a magánadatokhoz hasonlóan) negatív megfogalmazással kerültek meghatározásra, így a DGA alapján azt mondhatjuk, hogy nem személyes adat minden, ami a személyes adattól eltérő.[168] A személyes adat fogalmát átalakítva úgy is fogalmazhatunk, hogy nem személyes az adat, ha az alapján természetes személy nem azonosított és nem is azonosítható.

A két eltérő szabályozói hozzáállás miatt fontos kérdés, hogy a két kategória egyidejű jelenléte esetén mi a helyes eljárás, vagyis, hogy milyen megítélés alá esik egy „kevert" adatállomány. Először is lényeges tisztázni, hogy a jog nem írja elő „a különböző típusú adatok elkülönített tárolásának kötelezettségét",[169] tehát személyes és nem személyes adatok kerülhetnek egy adatbázisba. Másodszor az FFNPDR 2. cikk (2) bekezdését kell ilyen esetben alapul venni, ami szerint a GDPR és az FFNPDR által létrehozott szabályrendszerek párhuzamosan alkalmazandóak, attól függően, hogy a kevert adatállomány mely eleme, milyen megítélés alá esik (tehát személyes adatra a GDPR-t, nem személyes adatra az FFNPDR-t kell alkalmazni).

[162] GDPR 9. cikk (1) bekezdés; Info.tv. 3. § 3. pont
[163] Info.tv. 3. § 4. pont
[164] GDPR 4. cikk 13. pont
[165] GDPR 4. cikk 14. pont
[166] GDPR 4. cikk 15. pont
[167] FFNPDR 1. cikk
[168] DGA 2. cikk 4. pont
[169] FFNPDR (10) preambulumbekezdés

Abban az esetben, „ha egy adatkészletben a személyes és a nem személyes adatok elválaszthatatlanul összekapcsolódnak” akkor a párhuzamos helyett a két rendelet egyidejű alkalmazása az elvárt.[170]

2.3.2.5. A közadatokról

Az adatok vizsgálata függőleges spektrumon azt jelenti, hogy azok valahol metszik a vízszintes tengelyen található személyes és nem-személyes adatok kategóriáit. Így az alábbi adatkategóriák között egyedileg eltérő valószínűséggel, de potenciálisan bárhol találhatunk személyes és nem személyes adatokat is.

A közadatok fogalmát expressis verbis a magyar jog adja meg, de a DGA (24) preambulumbekezdése is rögzíti a „nem személyes közadatok” létezését. Hazai jogunk szerint[171] a közadatokhoz tartoznak a digitális formában létező közérdekű adatok és közérdekből nyilvános adatok, valamint a kulturális közadat és a kutatási adatok. A közadatokhoz tartozó egyes típusok – a kulturális közadat[172] és a kutatási adat[173] – fogalmai a főfogalmat megalkotó idézett törvényben olvashatók,[174] míg a közadatok másik altípusai – a közérdekű adat[175] és a közérdekből nyilvános adat[176] – az információszabadság[177] jegyében az Info.tv-ben találhatóak.

A közadatok léte az államszervezet működéséhez nélkülözhetetlen. Ezentúl azonban – az információszabadság érvényesülésének biztosítása mellett – kiemelt jelentőségük az adathasznosítás lehetőségében rejlő potenciál – ahogy az Európai Unió a közszféra információinak további felhasználásáról szóló 2003/98/EK irányelvének megalkotási ideje is mutatja[178] – korai felismerésében és jogalkotói deklarációjában áll. A két idézett jogszabály a közadatokhoz való hozzáállás két állapotát is megjelöli, míg az Info.tv. klasszikusan az információszabadság általi megismerhetőséget és közéleti átláthatóságot várja el,[179] addig a Nah.tv. az ilyen adatok[180] további hasznosításának és újrahasznosításának a lehetőségét teremti meg.[181] A két szabályanyag együttesen a teljes nemzeti adatvagyon hasznosítását teszi lehetővé. A folyamat támogatására Magyarországon a Nemzeti Adatvagyon Ügynökség (NAVÜ) hivatott, amely a Kormány által rendeletben kijelölt, a nemzeti adatvagyon hasznosításával kapcsolatos állami feladatokat közfeladatként ellátó szervezet.

---

[170] A FFNPDR 2. cikk (2) bekezdés második fordulata szerint „elválaszthatatlanul összekapcsolódás” esetén az FFNPDR a GDPR sérelme nélkül alkalmazandó.
[171] Nah.tv. 2. § 15. pont
[172] Nah.tv. 2. § 19. pont
[173] Nah.tv. 2. § 20. pont
[174] A Nah.tv. szabályozási rezsimje és fogalomhasználata továbbra is a nyílt hozzáférésű adatokról és a közszféra információinak további felhasználásáról szóló 2019/1024/EU irányelv (továbbiakban: PSI irányelv) előírásaira épít
[175] Info.tv. 3. § 5. pont
[176] Info.tv. 3. § 6. pont
[177] A közügyek átláthatóságához, a közérdekű és a közérdekből nyilvános adatok megismeréséhez és terjesztéséhez fűződő kommunikációs alapjog
[178] Szőke Gergely László, „A közadat-újrahasznosítás új európai szabályozása - egy újabb lépés előre” MJSZ, 2021/1., 1. Különszám, 2021. 327-337. o.
[179] Lásd még: Hohmann Balázs, „Interpretation the Concept of Transparency in the Strategic and Legislative Documents of Major Intergovernmental Organizations”, Közigazgatási és Infokommunikációs Jogi PhD Tanulmányok 2(1), 2021, 48-56. o.
[180] Például meteorológiai adatok, különböző állami nyilvántartások adatai
[181] 2023. évi CI. törvény végső előterjesztői indokolása a nemzeti adatvagyon hasznosításának rendszeréről és az egyes szolgáltatásokról

2.3.2.6. A magánadatokról

A közadatoktól eltérő – tehát az előző pontban ismertetett adatoktól különböző – adatok csakúgy, mint a nem személyes adatok egy igen heterogén kört ölelnek fel, amelyet összefoglalóan magánadatnak hívhatunk,[182] de például az Európai Unió adatstratégiája „magánkézben lévő adatoknak" nevezi őket[183]. Ezek egy része természetesen személyes adat, és ennek megfelelő kezelése indokolt, egy másik része azonban nem személyes adat, akár azért, mert anonimizált adat, akár azért, mert eleve nem személyes adatként jött létre. Ezek hasznosításában igen jelentős potenciált lát az Európai Unió,[184] még akkor is, ha ezen adatok egy része üzleti titokként[185] védett.

2.3.2.7. Egyéb, speciális és korlátozással érintett adatokról

A jogi adatfogalommal kapcsolatban szükséges megemlíteni, hogy a jog az eddig említetteken felül számos individualizált adat- és titoktípust nevesít, amelyek potenciálisan szinte bármelyik fenti kategóriát érinthetik,[186] és létezhetnek olyan adatok is, amelyek a jog által egyáltalán nem szabályozottak. Ebbéli tulajdonságuk miatt az adatjog legtágabb értelmezését jelentik a négy nagy jogi adatkategóriához képest. Az ide tartozó adatok köre attól függ, hogy az éppen hatályos szabályozási rezsim mit tekint valamilyen szegmensben adatnak, illetve attól, hogy miket tekint védettnek. Specializált adatnak tekinthetjük például az MI rendelet[187] által bevezetett tanítóadatokat[188] vagy a DA által megalkotott kapcsolódószolgáltatás-adatokat,[189] a Nah.tv. felsorolása alapján[190] védett adatokat, továbbá a Mavtv. által nevesített minősített adatot.[191]

2.4. Az adat értékessége

Az adat értékességét önmagában nehéz meghatározni. Főként, ha a piacgazdaság azon alapvető tulajdonságát is figyelembe vesszük, hogy valaminek a hiánya az – a kereslet magas, a kínálat alacsony szintje miatt – ami az érték növekedéséhez vezet. Egy adat értékessége alapvetően valamilyen szükséglet vagy igény kielégítési képességében rejlik.[192] Ezt a szükségletet kielégítheti elsődleges vagy másodlagos formában is, Mayer-Schönberger és Cukier megfogalmazásával az adatok értékessége (elsődleges) felhasználásukkal nem szűnik meg,

---

[182] Fehér Könyv a nemzeti adatpolitikáról, Fehér Könyv a nemzeti adatpolitikáról, Budapest, Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete, Budapest, 2016, https://www.magyary.hu/wp-content/uploads/2019/09/Adatpolitikai_feher_konyv_201608.pdf (2024.04.30), 12. o.

[183] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Európai adatstratégia (COM/2020/66 final), 8. o.

[184] Az Európai Unió adatstratégiájának egyik pillére ezen adatkör megosztását igyekszik bátorítani, és ennek jegyében indult el a ma adatrendelet néven ismert jogszabály [Az Európai Parlament és a Tanács (EU) 2023/2854 Rendelete]. Ld. Európai adatstratégia, 15-16. o.

[185] Az üzleti titok védelméről szóló 2018. évi LIV. törvény 1. § (1) bekezdés

[186] A titoktípusok kategorizálásáról ld. Szőke Gergely László: Gondolatok a hazai titokvédelmi szabályozás rendszeréről, JURA, 2018/2., 241-257. o.

[187] Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról (továbbiakban: MI rendelet)

[188] MI rendelet 3. cikk 29. pont szerint a tanítóadatok olyan adatok, amelyeket egy MI-rendszernek a megtanulható paramétereinek illesztése révén történő tanítására használnak

[189] DA 2. cikk 16. pont szerint ezek az összekapcsolt termékhez kapcsolódó felhasználói műveletek vagy események digitalizálását képviselő, valamely kapcsolódó szolgáltatás szolgáltató általi nyújtása során a felhasználó által szándékosan rögzített vagy a felhasználói művelet melléktermékeként generált adatok.

[190] A Nah.tv. 2. § 36. pont terminológiája szerint védett adatok a személyes adat kivételével a törvény által védett, így különösen szakmai, üzleti, vám-, banktitoknak minősülő, valamint az egyedi statisztikai adat és a szerzői joggal védett adat.

[191] A minősített adat védelméről szóló 2009. évi CLV. törvény (továbbiakban: Mavtv.) 3. § 1. pont szerint nemzeti minősített adat vagy külföldi minősített adat

[192] Corwin D. Edward, „The Meaning Of Quality", Quality Progress, Volume 1 Issue 10. 1968. 36-39 o.

csak mindaddig szunnyad, amíg sor nem kerül (másodlagos) hasznosításukra.[193] A tény, hogy az adatok mennyisége a használattal nem csökken, hanem inkább növekszik arra utalhatna, hogy az értékessége nem lehet számottevő, hiszen elvileg bárki számára szinte korlátlanul hozzáférhetők.[194] Fontosnak tartom azonban azt hangsúlyozni, hogy az adatoknak a megismerési folyamatban betöltött pozíciójuk miatt nem közvetlenül, hanem közvetetten jelentkezik az értékessége az ismeretanyag és a tudás bővítésén keresztül. Az adatok bővülése ellenére történő értéknövekmény magyarázatául a Dunning-Kruger hatás[195] is említhető, ami szerint minél többet látunk egy adott területből, annál biztosabbak lehetünk abban, hogy mire nem terjed ki az ismeretanyagunk és a tudásunk azzal kapcsolatban. Ezt az adatokra lefordítva egy megismerési felhajtóerőként azonosíthatjuk, hiszen minél több adatunk van annál több potenciális ismeret és tudás birtokába kerülhetünk. Azonban több ismerettel és tudással egyre nő az igényünk az újonnan megjelenő kérdések megválaszolására, ezáltal még több adat használatára. Az adatok értékességével kapcsolatban az álláspontom tehát, hogy az adatok növekvő mennyisége nem csökkenti azok értékességét, hanem növeli.

A már nem hatályos Közadattv.[196] 4. § 14. pontjának fogalommeghatározása – bár kifejezetten a közadatok újra-hasznosítására vonatkozik – továbbra is segítségül hívható az adat értékesség mibenlétének megragadásához. E szerint nagy értékű az az adat, amely újra-hasznosítása fontos előnyökkel jár a társadalomra, a környezetre és a gazdaságra nézve, különös figyelemmel arra, hogy lehetővé teszi hozzáadott értéket képviselő szolgáltatások, alkalmazások, továbbá új, magasabb hozzáadott értéket képviselő munkahelyek létrehozását, valamint figyelemmel az adaton alapuló, hozzáadott értéket képviselő szolgáltatások és alkalmazások lehetséges felhasználóinak számára.[197] A fogalom tehát egy kollektív jellegű értékességet, kvázi társadalmi hasznosságot definiál, azonban látható, hogy mik azok az elemek, amiktől az adat maga értékessé válik: az adaton végzett műveletek által ezeken alapuló új szolgáltatások, alkalmazások és tevékenységek hozhatók létre, amelyek hozzáadott értéket képviselnek valamely szereplő vagy szereplők csoportja számára.

Az adatok értékességének változására kézzel fogható példa lehet egy elkészült termelési statisztika egy takarmánykeverő üzem havi teljesítményéről. Ez értékes biztosan a szervezet számára az erőforrásai helyes allokációjának megvalósításához, azonban általánosságban kijelenthető, hogy az értékesség fokozatosan csökken ahogy távolodunk az agrárágazattól, így még hasznos lehet a kereskedelmi szektor számára, de egy kórháznak nagy valószínűséggel, ebben a formában nem. Az adat értékessége tehát nagy mértékben szubjektív alapokon nyugszik, azt ezért mindig az egyedi eset körülményeire tekintettel kell megvizsgálni. Ráadásul – ahogy fentebb említettem – az értékítélet meghozatala elválhat az adat gazdájától, illetve az adatot előállító, azon elsődleges műveleteket végzőktől. Az előbbi kijelentést árnyalja az adat mennyiségének és korának hatása a teljes adatállomány értékére. Ha nem egy takarmánykeverő üzem, hanem Európa összes üzemének kimutatásai kerülnek összesítésre és rendelkezünk a feldolgozáshoz szükséges informatikai kapacitással, akkor az adat értéke mennyiségével és kiterjedtségével potenciális növekszik.[198] Ez igaz lehet függetlenül attól, hogy a benne levő „zaj" is egyre nagyobb. Így bár a szószerinti értelemben vett adatminőség romlik, magának az

[193] Mayer-Schönberger, Cukier, 2014. 118 o.
[194] Ezért létezhet az un. „közdolog" vagy „public good" megközelítés a jogirodalomban az adatokkal kapcsolatban.
[195] Robert D. McIntosh, Elizabeth A. Fowler, Tianjiao Lyu, Sergio Della Sala, „Wise up: Clarifying the role of metacognition in the Dunning-Kruger effect", Journal of Experimental Psychology: General, vol. 148, no. 11., 2019. 2 o.
[196] A közadatok újrahasznosításáról szóló 2012. évi LXIII. törvény
[197] A fogalom PSI irányelv 2. cikk 10. pontján alapult
[198] Polyák Gábor, Pataki Gábor, „A személyes adatok értéke a Facebook–WhatsApp összefonódás versenyjogi értékelésében", In: Polyák Gábor (Szerk.): Algoritmusok, keresők, közösségi oldalak és a jog – a forgalomirányító szolgáltatások szabályozása. Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2020. 268 o.

adatállománynak az értéke nő, mivel potenciálisan több szükséglet kielégítésére lehet így alkalmas.[199] Szintén értéknövelő potenciál rejlik a különböző időszakokban mért adatverziók összehasonlításának képességében, amely által változási tendenciák, mintázatok lehetnek azonosíthatók. Ebben az esetben akár egy takarmánykeverő üzem termelési statisztikájának az értéke is megnőhet, ha nem egy, hanem több hónap statisztikája fellelhető benne, vagy ha az adatokat nem időszakosan (mintavétel-szerűen), hanem folyamatosan (pl. szenzoros adatokkal) rögzítették.[200] Mayer-Schönberger és Cukier szerzőpáros nyomán azt is mondhatjuk, hogy az adat mennyiségi növekedésével a pontosság jelentősége csökken.[201]

2.4.1. Az értékesség megjelenési lehetőségeiről

Az adatok értékük szerinti tipizálása szinte lehetetlen, hiszen ahány szereplő annyi kielégíthető igény. Mégis egy rövid, példálózó felsorolással járulnék hozzá a terület kontextusba helyezésének megkönnyítéséhez. Fontos megjegyezni, hogy az adat értékét erkölcsi szempontok figyelembe vétele nélkül, objektív alapokon célszerű vizsgálni. Tehát attól például, hogy nagy mennyiségű adat használatával országos választások kimenetelének mesterséges megváltoztatására is lehetőség van, nem csökkenti az adat értékességét.[202]

Adat által képviselt érték	*Az érték mérésének lehetősége*
Politika: az államirányítást ellátó politikai vezetés számára egyértelműen hasznos a választópolgárok jobb ismerete, döntéseik előrejelzése, befolyásolásának lehetősége[203]	Az érték a támogatottságot vizsgáló közvéleménykutatások, állami statisztikák, illetve egy-egy választás eredményének vizsgálatával mérhető.
Egészségügy: betegadatok hasznosításával a gyógykezelési képességek gyorsabb tempóban fejlődhetnek, új eszközök, módszerek és eljárások alakíthatók ki, új típusú gyógyszerek hozhatók létre.[204]	A korábban nehezen vagy egyáltalán nem gyógyítható betegség túlélési esélyeinek javításával, akut vagy krónikus betegségeknek a betegre gyakorolt negatív hatásainak csökkentésével egyértelműen kimutatható a hasznosított adatok értéke.
Üzemi/vállalati/szolgáltatási hatékonyság és produktivitás: Mind a termelő, mind a szolgáltató szektorban alapvető fontosságú, hogy egységnyi idő alatt a lehető legnagyobb eredményt lehessen elérni. Ez a kijelentés a 2020 óta eltelt években különösen igaznak bizonyul, a sorozatos válsághelyzetek miatt.[205] A saját és más szervezetek	A racionalizált folyamat-megoldások – megfelelően hasznosítva – csökkenthetik a környezetterhelést, magasabb gazdasági hozzáadott-értéket érhetnek el, miközben a munkameneteket biztonságosabbá és költséghatékonyabbá tehetik. A magasabb szintű, ügyfélbarát szemlélet a hazai és a világ közigazgatási rendszereit is igyekszik

[199] Jingran Wang, Yi Liu, Peigong Li, Zhenxing Lin, Stavros Sindakis, Sakshi Aggarwal, „Examining the Dimensions, Antecedents, and Impacts of Data Quality", J Knowl Econ, 2023.
[200] Mayer-Schönberger, Cukier, 2014. 50-51 o.
[201] U.o. 54 o.
[202] Julia Carrie Wong, „The Cambridge Analytica scandal changed the world – but it didn't change Facebook", The Guardian, 2019. Elérhető: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook Letöltve: 2024.01.18.
[203] A nudging és manipuláció témaköréről lásd részletesen: Ződi, 2018. 76 o
[204] Sastry Chilukuri, „The role of big data in medicine", McKinsey & Company, 2015. Elérhető: https://www.mckinsey.com/industries/life-sciences/our-insights/the-role-of-big-data-in-medicine#/ Letöltve: 2024.01.18.
[205] SARTORIUS, „How Manufacturers Are Using Big Data Analytics to Improve Processes", 2019. Elérhető: https://www.sartorius.com/en/knowledge/science-snippets/how-manufacturers-are-using-big-data-analytics-to-improve-processes-507146 Letöltve: 2024.01.18.

működési adatainak, valamint a fogyasztók vagy ügyfelek elégedettségének, szokásainak elemzése segítheti a köz- és a magánszféra szervezeteinek hatékony működését.	áthatni, így a közpénzek átgondolt költése mellett magasabb közszolgáltatási színvonal is elérhető lehet. Ezek az eredmények igazolnák az ilyen típusú adatok értékét.
Piaci pozíció: a piac megszerzése és megtartása folyamatos és komoly kihívás a gazdasági szereplőknek a szabadversenyre épülő rendszerekben. A marketing és PR törekvések fogyasztói és felhasználói adatokra épülő megtervezése stabilabb és kiszámíthatóbb működést tehet lehetővé.[206]	Mind a marketing, mind a PR terület már jelenleg is kimagasló haszonélvezője az adatalapú működésnek, a megbízható analitikai adatok értéke e tekintetben igazoltnak tekinthető.
Mesterséges intelligencia fejlesztése: a magasan fejlett, neurális hálózatra épülő algoritmizált folyamatok fejlesztésének elengedhetetlen eleme megfelelő mennyiségű és minőségű adat rendelkezésre állása.	Az egyre kockázatosabbnak tartott,[207] de mégis vágyott általános mesterséges intelligenciának[208] a létrehozása hatalmas előrelépést jelentene az augmentációs és automatizációs folyamatokban,[209] ami a civilizált élet minden területére hatással lenne. Az MI kutatás jelenleg látható végpontja – a még kissé sci-fi hangzatú – un. MI szingularitás elérése, vagyis az emberi mentális képességeket meghaladó mesterséges szuperintelligencia kifejlesztése szintén elképzelhetetlen nagy mennyiségű adat használata nélkül.[210]
Adatok monetizációja: az adatok gazdasági értékkel rendelkeznek, így jogügyeletek tárgyai is lehetnek. Ilyenkor az adat tényleges, piaci értéke kerül beárazásra, nem feltétlenül a hasznosítása által keletkező közvetett értékteremtő hatás.	Az érték egyszerűen, pénzben kifejezhető.

[206] Chase Bibby, Jonathan Gordon, Gustavo Schuler, Eli Stein, „The big reset: Data-driven marketing in the next normal", McKinsey & Company, 2021. Elérhető. https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-big-reset-data-driven-marketing-in-the-next-normal Letöltve: 2024.01.18.

[207] Jyoti Narayan, Krystal Hu, Martin Coulter, Supantha Mukherjee, „Elon Musk and others urge AI pause, citing 'risks to society'", Reuters, 2023. Elérhető. https://www.reuters.com/technology/musk-experts-urge-pause-training-ai-systems-that-can-outperform-gpt-4-2023-03-29/ Letöltve: 2024.01.18.

[208] IBM, „What is strong AI?". Elérhető: https://www.ibm.com/topics/strong-ai, Letöltve: 2024.01.18.

[209] Az emberi munka támogatására vagy kiváltására irányuló folyamatok

[210] Rahul Rao, „What happens if AI grows smarter than humans? The answer worries scientists.", Popular Science, Elérhető: https://www.popsci.com/science/ai-singularity/ Letöltve: 2024.01.18.

2.5. A jelen fejezet főbb kutatási eredményei

Az FDIKW modell létrehozása

- A kognitív folyamat hierarchiája e szerint: Tényszerűség → Adat/Információ → Ismeret → Tudás → Bölcsesség

Az absztrakt adatfogalom

- E szerint az adat legáltalánosabb megfogalmazásban: a világ egy tényszerűségét tükröző, olyan jel (szimbólum), amely más ilyen jelekkel egy rendszert alkot, de az elhatárolhatóságát megőrzi. Az, a kognitív folyamat hierarchikus struktúrájában a külvilág megismerési eszközének, és közvetítő közegének szerepét tölti be.

Az adatok létrejöttének elméleti folyamata

- Megfigyelhető tényszerűség létezése
- Megfigyelésre képes megfigyelő jelenléte
- Az adat észlelése
- Az adat rögzülése
- Az új adat létrejötte
- Az adat rögzülésének ismétlésével másolt adat jön létre
- Az adathoz szubjektív érték társításával, azt információnak tekinthetjük

Az adatok öt ismérve

- Nonriválisés másolható,
- Egyedszinten kizárólagos,
- Heterogén fogalmi összetételű,
- Immateriális
- Erőforrás-jellegű értéket képviselő

Az adatok öt tulajdonságcsoportja

- Forma (kvantitaív, kvalittatív)
- Struktúra (strukturált, strukturálatlan, részben strukturált)
- Forrás (rögzített, lehulló, származtatott, múló, salak)
- Előállítás (primer, szekunder, tercier)
- Típus (indexált, attribútum, meta)

A szintaktikai adatréteg

- A szintaktikai adatréteg alatt az adatok jelszintjét, jelen dolgozatban pontosan az alkalmazott technológia szempontját értjük. Megkülönböztettünk organikus és technológiai adatkategóriákat. A technológiai kategórián belül az analóg és digitális adatokat.

A szemantikai adatréteg

- A szemantikai adatréteg alatt az adatok eszmei/jelentésbeli tartalmát, jelen dolgozatban pontosan a jog általi meghatározottságot értjük. Megkülönböztettünk két (két dimenziós [vízszintes] síkban) adatkategória párt, a személyes/nem személyes és a köz-magánadatokat. Ezen felül (három dimenziós [függőleges] térben) a négy jogi adatkategóriát metsző, speciális és korlátozással érintett adatok, valamint a nem definiált adatok kategóriáit is megjelöltük.

Az adatok értékessége

- Az adatok értékességét valamilyen eredmény elérési vagy szükséglet kielégítési képességében találtuk meg.

3. Az európai adatjog áttekintése

A jelen fejezetben az európai, adatalapú folyamatokra irányuló jogalkotás és a joggyakorlat elméleti, valamint gyakorlati aspektusainak vizsgálatára kerül sor, annak érdekében, hogy az adatjog jelenlegi állapota feltárható legyen. Ennek a keretében az adatjogi szabályok kategorizálási lehetőségeit és az egyes kategóriákhoz tartozó jogi eszközöket vesszük számításba. Ezek alapján az adatalapú folyamatok – és szabályaik – hátterében álló, azokat mozgató törvényszerűségek azonosítását is megkíséreljük.

3.1. Az adatjog története

3.1.1. Az adatokról és az adatalapúságról

Az absztrakt adatfogalom szerinti adat gyakorlatilag egyidős magával az élettel. Az első (organikus) adatot az első megfigyelésre képes lény rögzíthette, mikor kapcsolatba került a környezetével. A korai emberek számára ezen organikus adatoknak a közvetítő közege a szóbeliség volt, amelyen keresztül a gondolatok megoszthatóvá (másolhatóvá) váltak. A technológiai adatok analóg változatának léte is több tízezer évre nyúlik vissza. Legkorábbi formáiban azt a barlangrajzok testesítették meg, amelyek emberek és állatok képmásait rögzítették festéssel vagy véséssel a kőzetek felszínére. Előre haladva az időben az írásbeliség megjelenésével a maihoz jobban hasonlító analóg (numerikus) adatok kerültek rögzítésre, például az államok által lefolytatott népszámlások alkalmával.[211] Az analóg adatokról a digitálisra való átállás, vagyis a digitalizáció folyamata jelenkorunk egyik nagy célitűzése és kihívása is egyben.[212] Ezt a négy állomást (beszéd, írás, nyomtatás, digitalizáció) információs forradalmakként ismerik és a civilizációs fejlődés négy fontos mérföldkövét is jelképezik.[213] A következő forradalmat a digitális technológiák meghaladásával a kvantum adatok hozhatják el.[214]

A technológiai adatok értelemszerűen szoros kapcsolatban állnak magának a technológiának a fejlődésével. A barlangrajzok nem jöhettek volna létre kőeszközök vagy szén, illetve más pigmentáló anyagok használata nélkül. Később hasonlóan szükség volt a pergamen- és festékkészítés technikájára, ahhoz, hogy az ókor írásos emlékei fennmaradhassanak. Az írni és olvasni tudás terjedésével és a 15. századtól a könyvnyomtatás megjelenésével a technológiai adatok száma és jelentősége növekedni kezdett. Az adatalapú működés globális térnyeréséhez az informatika 20. századi megjelenésére volt azonban szükség, aminek a folyamatát három szakaszra oszthatjuk. Az 1950-es évektől kezdődő első időszakot a „nagy-számítógépek" korának nevezhetjük, ekkor vált az informatikai kapacitás az államok (többsége) és néhány nagy magánszervezet számára elérhetővé. A második korszak az 1980-as évektől a 2000-es évek elejéig tartott és a személyi számítógépek (PC) elterjedésével, majd az internethálózat megjelenésével a számítási kapacitás elérhetővé válása és az online „hiperkapcsoltság"[215] megjelenése határozta meg. A harmadik, máig tartó korszakot a lezáratlansága miatt még nehéz

[211] Mayer-Schönberger, Cukier, 2014, 23-30 o.

[212] A digitális technológiák két arcúságát Stiegler a „pharmakon" görög kifejezéssel jellemzi, amely egyszerre jelent gyógyszert és mérget. Lásd részletesen: Bernard Stiegler: The age of Disruption: Technology and Madness in Computational capitalism. Campbridge, Polity, 2019. Idézi: Tóth András: a digitális átalakulás szabályozása az Európai Unióban. Budapest, ORAC Kiadó Kft., 2024. 19 o.

[213] Balogh, 1998. 145-146 o.

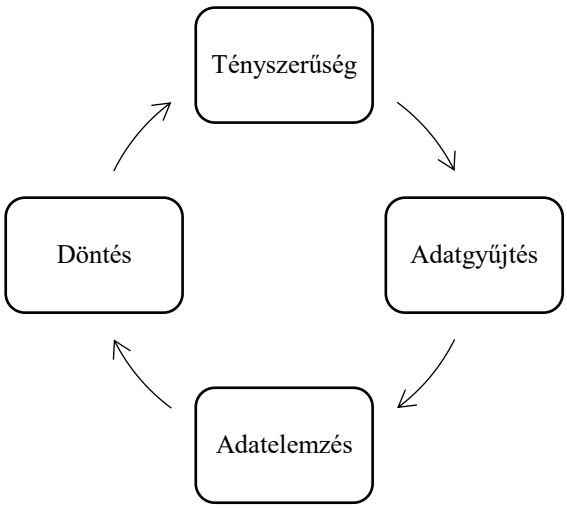
[214] Az ilyen „nagy teljesítményű számítástechnikai" rendszereknek (HPC) a fejlesztését az EU szintén, mint célt rögzítette, lásd részletesen: Tóth András: A digitális állam információbiztonsági kihívásai. Budapest, Nemzeti Közszolgálati Egyetem Ludovika Egyetemi Kiadó, 2022. 20 o.; EU Quantum Technology Strategy, „Supporting Quantum Technologies beyond H2020" Elérhető: https://qt.eu/app/uploads/2020/04/Strategic_Research-_Agenda_d_FINAL.pdf

[215] Tóth, 2024. 21 o.

megítélni, azonban a jelentőségét vélhetően az IoT eszközök, a felhőszolgáltatások és a web2 alkalmazások elterjedése, valamint az algoritmizáció fogja megadni.[216]

3.1.1.1. Az adatalapú működés fogalmáról

Az informatika fent leírt fejlődése magával vonta a digitalizáció jelenségét és vele az *adatalapú működés modernizálásának* lehetőségét. Az eddigiek alapján látható, hogy – absztrakt értelemben legalábbis biztosan – minden kognitív folyamat adatalapúan működik. Az itt említett, modernizált megközelítést kifejezetten az új technológiák eredményeként előálló, egyre növekvő mennyiségben generált digitális adathalmazzal összefüggésben szokás használni. Ez a modern adatalapúság ugyanis az eddigiekhez képest minőségi változást hozott az *észlelés* és a *rögzítés* módszertanában. A fejlett mérési (pl. szenzoros) képességekkel új tényszerűségeket fedezünk fel, illetve már ismert tényszerűségekről új adatokat *észlelünk*. A digitális jellegből adódó könnyű tárolhatóság miatt ezek az új adatok pontosan, biztonságosan és tartósan képesek *rögzülni*. Szintén fontos, hogy a mesterséges számítási képességek megjelenésével és gyors fejlődésével a már létező adatok elemzéseként ugyancsak új adatok jönnek létre. Ezért ezt az új típusú adatalapúságot – amelynek fontos, mondhatni jellegadó eleme az innováció[217] – a különböző adatkategóriák kiterjedt gyűjtésével, kifinomult elemzésével és az elemzés eredményét figyelembe vevő döntéshozatallal tudjuk jellemezni.[218] A modern adatalapú működés így egy zárthatásláncú körfolyamatként képzelhető el, amiben az adatgyűjtés-elemzés-döntés majd az ennek következtében előálló új körülményekre vonatkozó adatgyűjtés-elemzés-döntés (stb.) ciklikussága valósul meg. Az adatokra irányadó jog szempontjából különösen fontos az adatalapú működés, mivel valójában a szabályozott/szabályozni szándékozott *életviszonyt* jelenti.



6. ábra: az adatalapúság körfolyamata

3.1.1.2. Az adatalapúságra adott társadalmi és a gazdasági reakciókról

A digitalizált adatalapúság megjelenésére a társadalom, a gazdaság és a jog is megadta a maga válaszát. Elsőként az információs társadalom kifejezés merül fel, amely William J. Martin szerint „egy olyan társadalom, amelyben az élet minősége éppúgy, mint a társadalmi változások és a gazdasági fejlődés egyre nagyobb mértékben az információtól és annak felhasználásától függ”.[219] Az elképzelés tehát az adatok (információk) termelő és szervező erejére[220] és az azokra épülő rendszerek használatára, vagyis a társadalmi folyamatok adatvezéreltségére épül. A fogalom megalkotása óta eltelt idő tanulságai alapján azt mondhatjuk, hogy Martin nem járt messze az igazságtól. Az adatalapú működés egyik fő motívuma lett a jól szervezett és hatékony

[216] Bankó Zoltán, Szőke Gergely László: Az információtechnológia hatása a munkavégzésre. Pécs, Utilitates Bt., 2015. 19 o.
[217] OECD, „Data-Driven Innovation: Big Data for Growth and Well-Being”, Paris, OECD Publishing, 2015
[218] Michelle Knight, „What Is Data-Driven?”, Dataversity, 2021. Elérhető: https://www.dataversity.net/what-is-data-driven/
[219] Maria Nikolova, „The Approach of the European Union to the Information Society” Working Paper, European Parliamen, INDU 101 EN, 2003. 5 o.
[220] Balogh, 1998, 151 o.

működés mind a magán- mind a közszférában. Ezzel párhuzamosan azonban régi félelmek is felélénkültek és sok esetben szintén igazolódni látszanak. Az információs társadalom árnyoldalaként felfogható *megfigyelési társadalom* („surveillance society") megjelenésével Lyon az egyéni kiszolgáltatottság és megfigyeltség növekedését, a gyűjtött adatokkal összefüggésben pedig nem csak a múlt, hanem a jövő előrejelzés alapú rögzítését is vizionálta.[221] A két megközelítés közti vita, vagyis a technológia általi felszabadulás (technofil) vagy alávetés (technofób) kérdése azóta sem került egyértelmű eldöntésre,[222] sőt úgy vélem jelen dolgozatnak is valahol feladata e kettő szélsőség közötti helyes navigáció (többek között az egyensúlyra való törekvés jegyében).

A társadalmi adaptáció mellett a gazdaság is reagált a digitális technológiák adta új lehetőségekre. A gazdaság digitalizációja alatt egyfelől a szűken értelmezett infokommunikációs szektort értjük, másfelől azonban ide tartoznak ezen szektor által biztosított elektronikus szolgáltatásokat igénybe vevő vállalkozások külső és belső informatikai fejlesztései, illetve az ilyen eszközök fejlesztésére irányuló kutatási és innovációs folyamatok.[223] A digitális gazdaság legnagyobb metszete, az egyúttal az adatok vonatkozásában is kiemelt szerepet betöltő un. platformgazdaság. A hatályos jog szerint a platform „egy olyan tárhelyszolgáltató, amely a szolgáltatást igénybe vevői által rendelkezésre bocsátott információkat a szolgáltatást igénybe vevői kérésére nemcsak tárolják, hanem nyilvánosan terjesztik."[224] Ez az üzleti modell teljes egészében adatok gyűjtésére és elemzésére épül, ráadásul a vonatkozó szakirodalom szerint ezen túlmenően az adatok *előállítása* is zajlik.[225] Az online platformoknak a globális gazdaságban betöltött szerepe megkérdőjelezhetetlen. A világmárkák értékbecslésének vizsgálatával Mezei és Harkai arra jutottak, hogy a világgazdaság domináns szereplőinek nagy része erről a területről kerül ki (2023-as mérés alapján az első négy helyezett az Amazon, az Apple, a Google és a Microsoft, mind a platformgazdaság tagjaként működő technológiai nagyvállalatok).[226] A digitális adatalapú gazdaság rendkívüli pénzügyi potenciállal rendelkezik, a legnagyobb képviselői dollármilliárdban mérhető piaci tőkeértékkel rendelkeznek. Ezen (döntően USA-beli és kínai) vállalkozások súlya mára már egyértelműen egyes államokéval vetekszik. A régi mondás, miszerint az állami „nagy testvérek" mellett a vállalatok a „kistestvérek" már jó eséllyel nem állja meg a helyét, ezért az adatjognak a szabályozási törekvéseit csupa nagy – és egyre mostohább – testvér figyelő tekintete mellett kell valahogyan megvalósítania.

3.1.2. Az adatok szabályozásának történetéről

Az adatokra vonatkozó rendelkezések az idők folyamán hasonló rendszerben épültek fel. Az adatok lényege mindig is létrejövetelükkel kapcsolatban volt igazán megragadható, ezért a szabályok vagy az észlelés vagy a rögzülés mozzanatai köré csoportosíthatók. Előbbi esetén a megfigyelhető tényszerűségre, míg utóbbi esetén magára az adatra fókuszálva. Funkciójukat tekintve pedig vagy védelmi célzatúak voltak vagy a használatra tartalmaztak előírásokat.

[221] David Lyon: Surveillance Society: Monitoring Everyday Life. McGraw-Hill Education (UK), 2001. 89 o.
[222] Pintér Róbert, „Úton az információs társadalom megismerése felé", In: Pintér Róbert (Szerk.): Az információs társadalom - Az elmélettől a politikai gyakorlatig. Budapest, Gondolat Kiadó, Új Mandátum, 2007. 15 o.
[223] Nemzeti infokommunikációs stratégia 2014-2020, 5 o.
[224] Az Európai Parlament és a Tanács 2022/2065 rendelete a digitális szolgáltatások egységes piacáról (továbbiakban: DSA) (13) preambulumbekezdés
[225] Mezei Péter, Harkai István: A platformgazdaság szerzői jogi kihívásai. Budapest, ORAC Kiadó Kft, 2024. 18 o.
[226] U.o. 15 o.

A történelem során számos megközelítés alakult ki. Az állami működés mindig is nagyarányú adat kezelésére irányult, amelynek két szélső pólusa a titkosság és a nyilvánosság.[227] Ennek észlelésre vonatkozó szabályaiként az állami információvédelem területét említhetjük, amely egyszerre irányulhatott a saját lakosságra és más államokkal kapcsolatos viszonyokra.[228] Az információvédelem a már rögzített adat kezelési korlátainak felállítására szolgált, a ma ismert célokkal, vagyis a sértetlenség, rendelkezésre állás és hitelesség megőrzésével közel azonos megfontolások által vezérelve. Ide olyan megoldásokat sorolhatunk, mint az uralkodói pecsét használatát, a rejtjeles írást (szteganográfia, ami a kriptográfia elődje volt),[229] vagy a postagalambok megfelelő idomítástechnikáját.[230] Az információvédelem egy egyedileg intézményesült és a szélesebb társadalomban is elterjedt formája a titokvédelem. A titok egy kifejezetten *emberi* jelenség, mint a kommunikáció negatív formája már a kezdeti társadalmakban is jelen volt (pl. kultikus, diplomáciai, katonai).[231] A szabályozási megközelítések általában az egyes titokfajtákat a köztitokhoz és magántitokhoz közelítő kategóriákra osztották. Előbbi az állam titkait, utóbbi a társadalomét jelentette (ide tartoztak például a levéltitkok vagy a különböző hivatási titkok).[232] Érdekes területe az adatokra vonatkozó szabályanyagnak a cenzúra intézménye, vagy másként megfogalmazva a különböző típusú tartalomkorlátozások. Ezek úgyszintén egyidősek lehetnek az emberi kommunikációval[233] és a rögzült adattal kapcsolatos utólagos kontrollfunkciót valósították meg.

Szintén ősi időkre vezethető vissza a magánszféra védelme, ami ebben az értelemben a magánéleti tényszerűségek megfigyelésével kapcsolatos észlelést és rögzítést szabályozta. Westin kutatásai szerint a magánszféravédelem alapvető megnyilvánulási formái az állatvilágban is jelen vannak, ezt a territoriális viselkedés fogalmával hozta összefüggésbe. Úgy látta, hogy számos szervezett organizmus formál igényt a föld, a víz vagy a levegő valamely területére, és ennek a területnek a védelmét hajlandó saját fajtársaival szemben is megvalósítani. Itt megfigyelhetők a magánszféra fizikai határait kijelölő általános mechanizmusok, a személyes távolság („personal distance") és az elkülönülő csoportok közt fellépő távolság („social distance") megtartására.[234] Elhagyva az állatvilágot, a múlt és a jelen primitív emberi társadalmairól is elmondható, hogy mindben léteznek és érvényesülnek a magánszféra mindhárom szintjére (egyén, család/háztartás, nagyobb közösség) vonatkozó normák, de ezek hatalmas eltéréseket mutatnak a mai társadalmakhoz képest. A kezdetleges territoriális magatartás ösztönösen kielégítette az egyének védelmi igényeit, azáltal, hogy „többfunkciós" megoldásai egyéb szükségleteknek is eleget tettek. Így nem elrugaszkodott gondolat, hogy a meleget benntartó és az időjárási viszontagságokat, illetve egyéb fenyegetéseket kinn tartó barlangfal vagy kunyhó egyúttal a benntartózkodók magánéletét is megóvta, bármilyen külön intézkedés nélkül is. A technológiai és társadalmi együttélés fejlődése, valamint a lakosságszám, illetve népsűrűség párhuzamos növekedése együttesen idézett elő olyan

[227] Sziklay Júlia: Az információs jogok kialakulása, fejlődése és társadalmi hatása. Doktori értekezés, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskolája, 2011. 6-7 o.
[228] Adrienne Wilmoth Lerner, „Espionage and Intelligence, Early Historical Foundations" Encyclopedia of Espionage, Intelligence, and Security. Elérhető: https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/espionage-and-intelligence-early-historical-foundations
[229] Győrffyné Holló Krisztina, „Az információbiztonság jelentősége és története", Gradus Vol 8, No 2 (2021) 102-112. 108 o.
[230] Z. Karvalics László: Információ, társadalom, történelem. Válogatott írások. Budapest, Typotex Kiadó, 2003. 135 o.
[231] Gál István László. „The Protection of the State Secret in the Legal History of Europe", Zbornik Radova: Pravni Fakultet u Novom Sadu Vol. 56, no. 2, 2022. 584-585 o.
[232] Szőke, 2018. 241-242 o.
[233] Gosztonyi Gergely: Cenzúra - Arisztotelésztől a Facebookig. Budapest, Gondolat Kiadó, 2022. 25-31 o.
[234] Jóri András: Adatvédelmi Kézikönyv, Elmélet, Történet, Kommentár. Budapest, Osiris Kiadó, 2005. 12 o.

változásokat, amelyek lényegesen nagyobb behatolást tettek lehetővé a magánszférába, és ezzel szemben a korábbi magánéletet védő megoldások már nem tudták ellátni a feladatukat.

3.1.2.1. A magánszféra védelem szabályozásáról

A magánszféra védelem modern aspektusai az angolszász területekre jellemző *right to privacy* és az inkább kontinentális *adatvédelem* szabályozási megközelítéseiben öltöttek testet. Előbbinek első – 19. századi – említését is már a technológiai fejlődés (fényképezés) és a magánéletbe behatóló adatrögzítés (bulvársajtó megjelenése) idézte elő.[235] A privacy szemlélet lényege, hogy meg kell húzni azt a magánélet és a közösségi élet közötti határt, amin keresztül az ember magát a külvilágtól képes lehet elhatárolni. A szemlélet alapján ezen határon belül lehet az ember önmaga, így végeredményben a privacy lényege, hogy jogot biztosítson arra, hogy az ember egyedül, önmaga legyen.[236] Az adatvédelmi jog kialakulását és a személyes adatok védelembevételét az 1960-as évektől induló technológiai fejlődési ugrás (informatika és digitalizáció) következtében előálló társadalmi és technológiai változások idézték elő. Akadtak olyanok, akik képesek voltak előre látni az eljövendő eseményeket. Gondolhatunk József Attilára, mikor 1935-ben „Levegőt" című versében híváslistájának lekérdezéséről, profil alkotásról, valamint mindezekkel történő visszaélésről vízionált. Szintén jó példa lehet George Orwell 1949-ben kiadott 1984. című regénye, amelyben a totális állam általi megfigyelés veszélyeire hívta fel a figyelmet. Az európai adatvédelmi szabályozás történeti alakulása szoros összefüggésben mozgott az informatika fejlődésével, így Szőke álláspontját követve ezt is három generációra oszthatjuk.[237]

- Az 1960-as évekre tehető első generáció kezdő időszakától az adatok koncentrációja kevés adatkezelőnél (főként állami szerveknél) valósult meg. A későbbi visszaélések megakadályozása érdekében az első adatvédelmi előírások az új technológiák alkalmazóinak transzparenciáját és ellenőrizhetőségét célozták, a hatalmi eltolódás megelőzése érdekében. Megjegyzendő, hogy rendelkezési jogot nem biztosítottak az érintett számára. Az első törvények között meg kell említeni a német Hessen tartomány által elfogadott adatvédelmi törvényt (1970), illetve Svédország (1973), a Német Köztársaság szövetségi szintű (1976), valamint Franciaország (1977) és az Egyesült Királyság adatvédelmi törvényeit.
- A második generáció a német alkotmánybíróság 1983-as nagy horderejű népszámlálálás-ítéletével kezdődött, amely évekre meghatározta az adatvédelmi jog fejlődését, mikor kimondta, hogy az egyénnek joga van ahhoz, hogy maga döntsön személyes adatainak kiszolgáltatásáról és felhasználásáról. Ebben az időszakban csökkent az adatvédelmi jogban a technológia-specifikus szabályok alkalmazása, valamint megjelentek az érintetti jogok, így például a tiltakozáshoz való jog (marketing célú adatkezeléssel szemben) és a törléshez való jog (elavult adatok esetén).
- A harmadik generációt az egyre növekvő kihívásokra reagálni kívánó szabályozási kísérletek sorozataként lehet legjobban leírni. A szabályozás az érintetti jogok szélesítése mellet az adatkezelők kötelezettségeit is jobban részletezi. Németország jogfejlesztő tevékenysége révén bekerült az adatvédelmi jogba az adattakarékosság elve, és a környezetvédelmi audit mintájára az adatvédelmi audit is. Az adatvédelmi

[235] Szőke Gergely László, „Az adatvédelem szabályozásának történeti áttekintése", Infokommunikáció és Jog, 2013/3. (56.), 107-112. o.
[236] Samuel D. Warren, Louis D. Brandeis, „The Right to Privacy", Harvard Law Review, Vol. 4, No. 5. 1890. 195 o.
[237] Szőke, 2013. 107-112. o.

irányelv[238] számos olyan rendelkezést tartalmazott, amelyek megalapozták a mai adatvédelem alapvető előírásait (mint: jogalapok, alapelvek), de összességében nem váltotta be a hozzáfűzött reményeket. Az irányelvet váltó GDPR rendkívüli mértékben formálta át az adatvédelmi jogot, a védelmet kiterjesztette Európáról – extraterritoriálitása miatt – gyakorlatilag az egész világra. A harmadik generáció a német Teledienstedatenschutzgesetz 1997-es elfogadásától napjainkig tart.

3.2. Az európai adatjog léte

3.2.1. Az adatjog megítéléséről

A szabályozási megközelítések jelen korunkra három részre szakadtak, a világ három adatalapú pólusának valamelyike által meghatározott zsinórmértéknek megfelelően. A szabályozási hozzáállás ugyanis merőben eltérő Európa, az USA és Kína viszonylatában. Míg Európában az alapjogvédelem, és egyfajta biztonságos, organikus fejlődési szemlélet jellemző,[239] addig az USA és Kína az adatokkal sokkal kevesebb megkötést tart betartandónak. Az Egyesült Államok szabályozása alapvetően privatizált alapú, a vállalatok és a piac belső szabályozó erejére bízza az adatok megfelelő kezelésének kérdését. Kína ezzel szemben a centralizált megközelítést preferálja, a belső folyamatok ellenőrzésére és a külső hatásokkal szembeni védekezésre összpontosítva.[240] Gondolhatunk az „arany pajzs" projektre, ami az internetes kommunikáció totális ellenőrzésére irányul vagy az ennek keretében létrehozott „Nagy tűzfalra", ami a kínai internetet a világ többi részétől választja le.[241] Mind a Kínai, mind az USA által képviselt megközelítés pedig jelentősen igyekszik befolyásolni a világ többi részét, az adatokhoz való hozzáállás érdekeiknek megfelelő igazítása érdekében. Megemlékezhetünk a TikTok ajánló rendszerének a kínai kormányzat által támogatott politikai tartalmak szerinti működéséről[242] vagy a Schrems ügyeket kiváltó, közösségi média által gyűjtött adatokhoz az USA titkosszolgálatainak potenciális hozzáféréséről.[243] Ebben a tripoláris jogpolitikai környezetben kell tehát az európai adatjogot azonosítanunk és a jövőbeli lehetőségeit megítélnünk.

Az adatjog szóösszetétel nem új keletű, azonban az elmúlt évek európai jogalkotása annak tartalmát új szabályozó eszközökkel és az eszközök között eddig nem hangsúlyozott összefüggésekkel töltötte fel. A terület határainak meghatározása jelenleg nem mondható magától értetődőnek. Az európai jogpolitikai álláspont már 1994-ben, az un. Bangemann jelentéssel letette a voksát a „közös szabályozási megközelítés" és az „Európa szintű információs szolgáltatások piacának" létrehozása mellett,[244] amely célkitűzéseket megerősítette

[238] Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (továbbiakban adatvédelmi irányelv)

[239] Szőke Gergely László, „A közösségi oldalak működése az európai adatvédelmi szabályozás tükrében", In: Barzó Tímea, Czékmann Zsolt, Csák Csilla: „Gondolatok köztere" A közösségi média személyiségvédelemmel összefüggő kihívásai és szabályozása az egyes államokban. Miskolc, Miskolci Egyetemi Kiadó, 2021. 118 o.

[240] Tóth, 2024. 24 o.

[241] Gosztonyi, 2022. 163-165 o.

[242] John Herrman, „TikTok Is Shaping Politics. But How?" The New York Times Elérhető: https://www.nytimes.com/2020/06/28/style/tiktok-teen-politics-gen-z.html; Érdemes megjegyezni, hogy a platform adatkezelési gyakorlatainak aggályossága miatt többféle szankcióval is érintett, sőt annak teljes kitiltására is sor kerül. Lásd részletesen: Aoife Walsh, „TikTok stops working as US ban comes into force" BBC News. Elérhető: https://www.bbc.com/news/articles/cz6p1g54q85o

[243] Kis Kelemen Bence, Hohmann Balázs, „a Schrems ítélet hatásai az európai uniós és magyar adattovábbítási gyakorlatokra", Infokommunikáció és Jog, 2016/2-3. (66-67.), 64-70. o.

[244] CORDIS, „Bangemann report: Europe and the global information society". Elérhető: https://cordis.europa.eu/article/id/2730-bangemann-report-europe-and-the-global-information-society

és számottevően kiszélesítette azóta az Európai Digitális[245] és az Adatstratégia[246] bár sem ezek, sem más jelenlegi EU jogi aktusok az adatjogot, mint definiált kifejezést nem tartalmazzák. Annyi talán megállapítható, hogy Európa a közelmúltban élen járónak tekinthető az adatokkal kapcsolatos, elsődlegesen védelmi előírások megalkotásában (amelyeket sikeresen is exportál területein kívülre), azonban ez az adatjognak vélhetően mindössze egy – bár nagyon jól látható – területe. Ezt a felemás állapotot az EU egyértelműen korrigálni igyekszik az elmúlt években olyan jogszabályok megalkotásával, mint a DGA és a DA. Ezen új szabályok megjelenésével azt gondolom, hogy az adatjog elég alkotóeleme került képviseltetésre a joganyagban, ahhoz, hogy mint koherens egység beszélhessünk róla.

A szakirodalomban dedikált kutatások születtek a terület vizsgálatára. Streinz az adatjog létét, mint az európai közjog egy területét látja, amely az adatvédelmi jogot magába foglalja, de azt meg is haladja. Rávilágít arra is, hogy az adatok szabályozására (legalábbis egyes típusaira) vonatkozó egyes rendelkezések szétszórva, számos jogág és jogterület metszetében helyezkednek, ezáltal a összehangolt jogalkotás különösen nehézkes.[247] Riis szintén az adatjog léte mellett érvel, kiegészítve azzal, hogy a terület felismerésének hiánya, a digitális jogalkotás egységességén keresztül annak sikerességét veszélyezteti, ezért az adatjog lehatárolását és jogterületi klasszifikációját javasolja.[248] Hoeren és Pinelli úgy szintén létező területnek látják az adatjogot és annak definícióját is meghatározzák, e szerint „az adatjog az adatokhoz való hozzáférést, azok felhasználását és védelmét szabályozó valamennyi norma összességét jelenti, függetlenül attól, hogy személyes vagy nem személyes adatokról van-e szó.”[249]

3.2.2. Az adatjog elfogadásának lehetőségéről és szükségességéről

Egy új jogterület létrehozásának gondolatát természetesen nem szabad könnyelműen kezelni, azonban látnunk kell, hogy a technológiai folyamatok által determinált társadalmi változások láttán a jogalkotás nem maradhat tétlen. Új jogterületek szükségességének vizsgálata időről időre felmerült már a jogtudományban, a maga idejében az adatvédelem is hasonló helyzetben volt. Ezen kérdés eldöntésével kapcsolatban Honduis az alábbi három körülmény meglétét tartotta figyelembe veendőnek:[250]

- a vizsgálat (új) jogi helyzet (életviszony) vagy a meglévő jogterületek hatókörén kívül esik vagy egyidőben egynél több hatálya alá tartozik, anélkül, hogy annak szabályozottsága kielégítő lenne,
- a szabályozásra szoruló életviszony a társadalom széles rétegeit érinti, így annak jelenlegi és jövőbeni tartós rendezése lényegesnek tekinthető,
- az új jogi szabályozás az alkotmányos rendszerrel összhangban áll.

Az első körülménynek való megfelelést értékelve azt mondhatjuk, hogy az adatalapú életviszonyok jelenleg kifejezetten egy jogterület hatálya alatt sem állnak, azonban rendkívül sok kapcsolódási ponttal rendelkeznek a jogrendszer számos részével, mint a polgári jog, az adatvédelem, vagy a szerzői jog. Azonban figyelembe véve a jogpolitikai és tudományos diskurzus állását belátható, hogy kielégítő szabályozottságról nem beszélhetünk. A második kritériummal kapcsolatban a mindennapi tapasztalatok is bőséges példát hoznak arra, hogy milyen mértékben hatja át a politikai, gazdasági és szociális alrendszereket az adatalapú

[245] COM/2020/67 final
[246] COM/2020/66 final
[247] Streinz, 2021. 20-22 o.
[248] Nine Riis, „Shaping the Field of EU Data Law”, Journal of Intellectual Property, Information Technology and Electronic Commerce Law 14, no. 1, 2023. 55-56 o.
[249] Thomas Hoeren, Stefan Pinelli: European Data Law. Berlin, De Gruyter, 2025. 12 o.
[250] Frits W. Hondius, „Data Law in Europe.” Stanford Journal of International Law, 16., 1980. 89 o.

működés. Okkal következtethetünk arra, hogy a technológiai fejlődés tendenciái ezen életviszonyok tartós szabályozottságát követelik meg. Végezetül a harmadik körülménynek való megfelelést az uniós jogalkotási törekvések iránya adhatja, amelyek az adatok szabályozását az európai értékekkel és joggal összhangban állónak, sőt részben kifejezetten ezek védelmét szolgálónak tekintik. Ezek alapján igazoltnak látszik az a feltevés, ami szerint az adatjog bevezetésének feltételei fennálnak.

A terület dogmatikai megítélését tekintve, azt mondhatjuk, hogy a jogági státuszhoz a jogrendszeren belül nagyfokú elkülönültségre van szükség a tárgy, a tartalom és a módszer tekintetében is.[251] A szakirodalom egyöntetűen az adatjog „keresztülfekvő" („cross-cutting") természetét hangsúlyozza, amely miatt annak egy különösen fontos tulajdonsága a más területeken való jelenlét és ezen területekhez való praktikus alkalmazkodás. Ez alapján az adatjogot célszerűnek tűnik,[252] mint jogterület felfogni, vagyis úgy mint jogi normák olyan, többé-kevésbé összefüggő és relatíve elkülönülő, több jogágat részben átfedő összességét, amely a jogág sajátosságaival, önállóságával, elkülönültségével nem rendelkezik.[253]

A fentiek szerint tehát az adatjog, mint jogterület létrejöttének feltételei adottak lehetnek az uniós jogban. Kérdéses azonban, hogy egyáltalán szükség van-e rá. A válasz erre egy történeti párhuzammal adható meg. A szerzői jog – részben már említett és részben még a következőkben taglalt okokból – számos hasonlóságot mutat az adatjoggal, főként mert mindkettő nonriviális és immateriális entitások szabályozására vállalkozott. Ezért a szerzői jog kialakulásának feltételei mentén tűnik érdemesnek az adatjogi terület létrejöttének szükségét vizsgálni. Mezei ezzel kapcsolatban négy tényezőt határoz meg:[254]

- *a tárgyi oldal:* a könyvnyomtatás által előidézett technológiai és dologi körülmények miatt a szerzői művek száma növekedett és az olvasóknak egyre elérhetőbbé vált. Ennek hatására a szabályozásra szoruló életviszonyok száma is nőtt, ami pedig felhívta a figyelmet a szerzők jogvédelmének hiányosságaira,
- *alanyi oldal:* a szerzők a középkor végével megjelenő individualizmus terjedésével (a műveket jellemző anonimitás elhagyásával) egyre fontosabbnak érezték a jogvédelmüket,
- *a fogyasztási oldal:* a társadalom tagjaiban (az írástudás és az általános műveltség terjedésével) egyre növekedett az igény szellemi termékek élvezetére, ami keresletet generált a szerzők műveire,
- *döntéshozói oldal:* az előbbi három alulról szerveződő tényező beteljesüléséhez szükség volt a politikai döntéshozó támogató hozzáállására, annak érdekében, hogy jogalkotásra sor kerülhessen.

A négy tényezőt az adatalapú folyamatokra és az adatjogra adaptálva a következőket mondhatjuk. A digitális technológiák megjelenése az adatok észlelésében és rögzítésében (létrehozásában) rendkívül nagy előrelepésnek tekinthetők, az adatok mennyiségi és minőségi értéke ezért elérhetett egy olyan szintet, ami az ilyen egyedi életviszonyok növekedését és így a szabályozási szükség megjelenését idézheti elő. Az adatok forrásainak és azok előállítóinak sokasága ismert magára az adatalapú folyamatokban és kezdett igényt formálni a jogvédelemre,

[251] Petrétei József: Magyar alkotmányjog I. Budapest-Pécs, Dialóg Campus Kiadó, 2002. 15 o.
[252] Ezzel a szakirodalmi szóhasználata is egybevág, Riis az adatjogot, mint „autonomous legal field" azonosította, lásd részletesen: Riis, 2023. 55 o.
[253] A jogterület fogalmával kapcsolatban írt részletesen: Tamás András: Legistica, A jogalkotástan vázlata. Nemzeti Közszolgálati Egyetem, 2013. 211. és 223. o.
[254] Mezei Péter: A fájlcsere dilemma – A perek lassúak, az internet gyors. Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2012. 14-15 o.

kezdve természetes személyektől egészen a nagy platformokig.[255] Az adatvezérelt gazdaság és államigazgatás elérése magas szintű célkitűzések és az érdekelt felek jelentős része által támogatott, ez pedig a keresleti oldal igényét legitimálni látszik. Végezetül mind a globális, mind az uniós, mind a hazai policy dokumentumokból az olvasható ki, hogy a döntéshozók az adatalapú működés és ezzel együtt valamilyen adatjogi jogalkotás mellett tették le a voksukat. Összegezve mind a négy, szerzői jog létrejöttét eredményező tényező megléte igazolhatónak tűnik az adatjog vonatkozásában is, a fennmaradó nagy kérdés a szabályozás miként.

3.3. Az adatjog területei

Ahhoz, hogy az adatjog szabályozási technikáit számba vegyük és akár esetleges hiányosságokat azonosítsunk, annak jelenlegi állapotát kell felmérnünk. Ehhez pedig a terület határainak körvonalazását, az adatokra vonatkozó hatályos szabályanyag – mint az adatjog alkotóelemeinek – legalább csoportszintű vizsgálatát kell elvégeznünk. Ehhez a csoportok (kategóriák) azonosítására van legelőször is szükség. Ehhez a Riis által felvetett elméleti (jogdogmatikai) és gyakorlati (pragmatikus) kategóriaalkotás lehetőségét érdemes számba venni.[256] Előbbi a szabályozás normatív karaktere alapján jelöli ki a terület határvonalait, míg utóbbi a releváns életviszonyok jellegzetességei alapján.

3.3.1. A jogdogmatikai csoportosításról

Hoeren és Pinelli kutatásaira építkezve az adatjogot legalább két alterületre oszthatjuk.[257] Az első az adatjog horizontális szabályrendszere. Ide azok a jogszabályok tartoznak, amelyek kifejezetten az adatokra vonatkoznak (azoknak az adatok szabályozása jellegadó tulajdonságuk), ágazati szegmenstől függetlenül. Ide sorolható[258] a GDPR, a DA, a DGA, és az FFNPDR. A második alterülethez az adatjogi szektorális szabályok tartoznak, amelyeket nevezhetünk az adatjog – horizontális párját alkotó – vertikális tartományának. Ide sorolható a PSI irányelv,[259] a bűnügyi irányelv[260] és az e-Privacy irányelv,[261] valamint az EU adatterekkel kapcsolatos bizottsági javaslatok, mint a FIDAR[262] és az EHDS.[263] Az információbiztonság szabályanyagának egy része szintén a vertikális adatjoghoz sorolható, mivel az ilyen szabályok hatálya jellemzően adatkategória vagy adatkezelői státusz szerint kerül meghatározásra. Ide

[255] Természetes személyek esetén a jogvédelem a GDPR formájában kinyilvánításra is került. A nagy platformok és nem (csak) személyes adatok esetén példaként említhetjük az OpenAI és a Deepseek vitás helyzetét, aminek az egyik lényeges kérdése, hogy a Deepseek fejlesztéshez használt adatállományainak egy részét vagy egészét az OpenAI-tól szerezte meg. Lásd: Vidyut Jha, „DeepSeek vs OpenAI (2025): A Comparative Analysis", AItectonic. Elérhető: https://aitechtonic.com/deepseek-vs-openai/

[256] Riis, 2023. 57 o.

[257] Hoeren, Pinelli, 2025. 18 o.

[258] Megemlítendő, hogy a magyar jogot tekintve az Info.tv. sorolható ide.

[259] Az Európai Parlament és a Tanács 2019/1024 irányelve a nyílt hozzáférésű adatokról és a közszféra információinak további felhasználásáról

[260] Az Európai Parlament és a Tanács 2016/680 irányelve a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról (továbbiakban: bűnügyi irányelv)

[261] Az Európai Parlament és a Tanács 2002/58/EK irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (továbbiakban: e-Privacy irányelv)

[262] A pénzügyi adatokhoz való hozzáférésre vonatkozó keretről szóló EU bizottsági javaslat (COM(2023) 360 final)

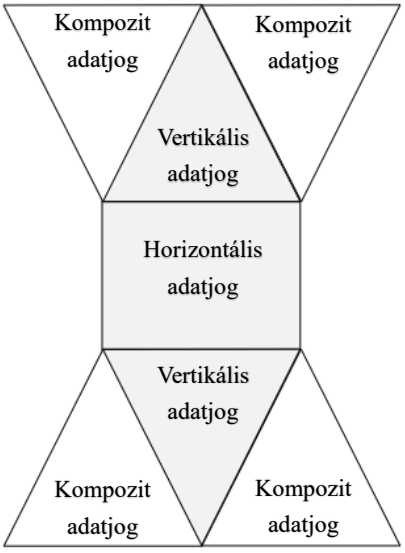
[263] Az európai egészségügyi adattérről szóló EU bizottsági javaslat (COM/2022/197 final)

tartozik[264] a DORA.[265] A CRA[266] ezzel szemben egyértelműen, mint horizontális szabályozás került megalkotásra. A szabályanyag más elemei azonban, mint a CSA,[267] és a NIS2 irányelv[268] valahol a két állapot között találhatók. Mindkettő általános jellegű és az EU joganyagának egységességét támogató szabályokat határoz meg, de – bár több ágazatra vonatkoznak (pl. energia, közlekedés, egészségügy stb.) – nem terjednek ki az egész jogrendszerre (mint pl. a GDPR). Ezeket a legpontosabban egyfajta multi-szektorális szabályozásként határozhatjuk meg, a besorolásuk pedig attól függ, hogy hogyan definiáljuk a horizontális és a vertikális szabályanyagokat. Ha a horizontális szabályok differentia sepcifica-ja, hogy azok a teljes jogrendszerre vonatkoznak, akkor a multi-szektorális szabályok vertikálisnak minősülnek. Ha viszont azt mondjuk, hogy a vertikális szabály lényegi eleme, hogy csak egy szektorra vonatkozik, akkor a CSA és a NIS2 irányelv horizontális jogi aktusok. Abból kifolyólag, hogy ezeknél a jogszabályoknál a szabályozási szemlélet nem egyetlen egy ágazati szisztémának feleltethető meg, ezért inkább a horizontális kategóriába sorolhatónak tartom őket, azzal, hogy a hatályuk korlátozottabb lehet a tisztán horizontális szabályokhoz képest. Megjegyzendő zárásképpen, hogy a horizontális szabályokra inkább jellemző az általános jelleg (lex generalis), míg a vertikálisra a specialitás (lex specialis), bár ez mint elhatárolási pont nem mindig alkalmazható következetesen.

A jelenleg hatályos európai és azon belül magyar jogrendet vizsgálva azonban az adatjog vertikális kiterjedtségének a *lehatárolhatatlansága* látszódik. A gyakorló jogalkalmazó számára ugyanis rögtön felmerül, hogy számtalan olyan norma van, amelynek fő szabályozási iránya nem az adatokra vonatkozik, azonban annak megkerülhetetlensége miatt mégis kénytelen valamilyen formában az ilyen helyzeteket is rendezni. Ezekre az adatjog tág értelmezéseként tekinthetünk, pontosabb megfogalmazással nem, mint (valódi) adatjogi szabályokra, hanem mint adatjogi előírásokat tartalmazó egyéb szabályokra. Elsők között juthat eszünkbe néhány konkrét aktus, amiket az adatalapúsággal előszeretettel hoznak összefüggésbe, mint az MI rendelet, az e-IDAS 2.0 rendelet,[269] a P2B rendelet,[270] a DSA, a DMA és a digitális tartalmakra vonatkozó irányelv.[271] Hasonlóan gyorsan felmerülő területek a szerzői jog, az iparjogvédelem és a titokvédelem (üzleti titok és minősített adat) is, hiszen ezek fő szervezőelve egy jól meghatározott, mondhatni individualizált adathalmaz (mint pl. szerzői műpéldány) kezelésére vonatkozó rendelkezések konzisztens meghatározása. Az adatokkal egyértelműen és szoros kapcsolatban álló szabályoktól távolodva sem ér azonban véget a tágan vett adatjog. Gondoljunk csak munkatörvénykönyvére,[272] amelynek 10-11/A. §-ban található előírások címe

[264] Megemlítendő, hogy a magyar jogot tekintve a Kib.tv. sorolható ide.
[265] Az Európai Parlament és a Tanács 2022/2554 rendelete a pénzügyi ágazat digitális működési rezilienciájáról (továbbiakban: DORA)
[266] Az Európai Parlament és a Tanács 2024/2847 rendelete a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről (továbbiakban: kiberrezilienciáról szóló rendelet vagy CRA)
[267] Az Európai Parlament és a Tanács 2025/38 rendelete kiberfenyegetések és -események észlelése, valamint az azokra való felkészülés és reagálás érdekében az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról (továbbiakban: kiberszolidaritási rendelet vagy CSA)
[268] Az Európai Parlament és a Tanács 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (továbbiakban: NIS2)
[269] Az Európai Parlament és a Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról és az azt módosító az Európai Parlament és a Tanács 2024/1183/EU rendelete a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról.
[270] Az Európai Parlament és a Tanács 2019/1150 rendelete az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról (továbbiakban: P2B rendelet)
[271] Az Európai Parlament és a Tanács 2019/770 irányelve a digitális tartalom szolgáltatására és digitális szolgáltatások nyújtására irányuló szerződések egyes vonatkozásairól
[272] 2012. évi I. törvény a munka törvénykönyvéről (továbbiakban: Mt.)

expressis verbis az „adatkezelés” elnevezést kapta. A köznevelési törvény[273] 41-44/A. §-nak a címe pedig „a köznevelési intézményekben nyilvántartott és kezelt személyes és különleges adatok”. Hosszasan sorolhatók még az önálló jogágak és jogterületek, amelyek az oda vonatkozó, speciális adatkezelési műveletekre maguk határoznak meg előírásokat. Ez tehát egy olyan rendhagyó helyzetet teremt, amiben az adatjog speciális szabályait nem egy adatjogi norma határozza meg. Az adatjog ezen természete a *keresztülfekvést* meglátásom szerint meghaladja. Az adatjog tartományának tágan értelmezett területeihez tartozó normákat természetesen nem lehetséges az adatjog égisze alá bevonni, hiszen akkor szinte az egész jogrendszer csak adatjogból állna. Azonban az ilyen előírások létéről sem feledkezhetünk meg, hiszen azok dogmatikailag nagyon is élő kapcsolatot ápolnak az adatjog központinak mondható, horizontális előírásaival. Gondoljunk csak a munkaügyi adatkezelések és a GDPR szoros kapcsolatára. Ezért az egyszerűség és a későbbi egyértelmű hivatkozhatóság érdekében ezeket az adatjogon kívüli adatjogi előírásokat *kompozit*[274] *adatjogi* szabályoknak nevezem. A lényege, hogy tükrözze az összeköttetést az olyan területek között, amelyeknél a kapcsolódás nem magától értetődő.



7. ábra: az adatjog dogmatikai csoportosítása

3.3.2. A pragmatikus csoportosításról

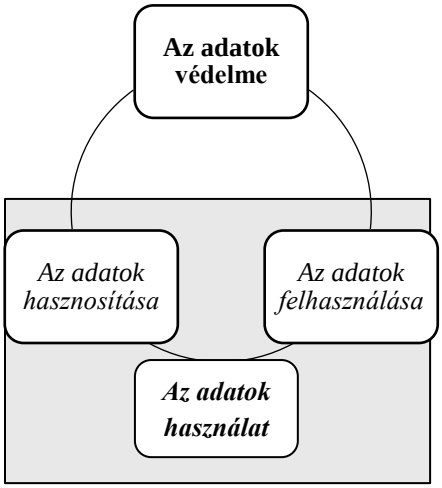
Az adatjog tényhelyzeti csoportosítását a szabályozott életviszonyok karakterisztikája adja meg. Ezt a történeti áttekintés és a jelenlegi joganyag vizsgálatával kétféleképpen tartom reálisan meghatározhatónak. Mindenekelőtt látható, hogy az adatjog egyfelől védelmi előírásokként értelmezhető. Ezeken az adatok feletti rendelkezést, az azokon való műveletvégzést[275] érintő valamilyen érdek- vagy értékvédelmi előírást érthetjük. Ez az elképzelés szerint az adatvédelmi jog kiemelt, de nem az egyetlen képviselője a védelem területének. Az ide tartozó joganyagok egy védettnek minősített érték tiszteletben tartásának biztosítása érdekében az adatok egy vagy több kategóriája vonatkozásában, bizonyos műveletek elvégzését részben vagy egészben kizárhatják, korlátozhatják vagy a jogosult döntéséhez köthetik. A terület kiemelkedő teljesítménye a GDPR (és az adatvédelem általában), de ide sorolható még az információbiztonság területe is. A védelem számomra a „hogyan” jogaként is értelmezhető, azáltal, hogy kijelöli a kereteket és a lehetséges irányokat, amelyek mentén a használat szabadon folyhat. A védelem mellett a másik nagy csoportként a használatra

[273] A nemzeti köznevelésről szóló 2011. évi CXC. törvény

[274] A kompozitanyagokat másként társított vagy összetett anyagoknak is nevezik, a lényegük, hogy két vagy több egymástól különböző szerkezetű és elkülönülő anyagkombinációból épülnek fel. Hasonlóan az adatjoghoz, amely szabályainak összessége szintén különböző, elkülönült jogágak és jogterületek előírásainak összességeként áll elő.

[275] A potenciális műveletek tekintetében kiindulópontként a GDPR terminológiáját hívhatjuk segítségül. Ez alapján azt mondhatjuk, hogy ehhez a körhöz tartozik az adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

vonatkozó előírásokat tartom azonosíthatónak. Ezek az adatokon végzet műveletekre vonatkozó szabályok a védelem „hogyanjához" képest a „mit, mikor, miért és meddig" kérdésekre adják meg a választ. Tehát a pragmatikus csoportosítás a legáltalánosabban, mint a védelem és a használat joga határolható el. A mai jogalkotási tendenciák és jogalkalmazási gyakorlat, illetve szóhasználat vizsgálata azonban egy további megkülönböztetés lehetőségét is felveti. Ez a védelem mellett a használat további két alcsoportra történő bontását jelenti, amik az adat*felhasználás* és az adat*hasznosítás*.[276] A jelen dolgozatban az alterületek között különbséget teszek, azonban ahogy látható lesz a kettő közti elhatárolás nem minden esetben indokolt vagy lehetséges. Ezért célszerű azt mindvégig szem előtt tartani, hogy mind az adatok felhasználása, mind a hasznosítása végső soron adathasználat.



8. ábra: az adatjog pragmatikus csoportosítása

A csoportosítás ezen verziója szerint a felhasználás az adatok létének tipikus területeként írható le, így nagy mennyiségű és meglehetősen szerteágazó jogi előírással szembesülünk. Ebbe a csoportba sorolhatunk ugyanis mindenfajta adatokkal kapcsolatba hozható, az azokon végzett műveletek részleteire vonatkozó előírást. Ritkább esetben lehet ezeket egy jogszabályban fellelni, a meglátásom szerint, jellemzően a vonatkozó ágazati szabályrendszer részeként jelennek meg. Személyes adatok kezelése esetén példa lehet a (későbbiekben részletesen vizsgált) munkaügyekben található számtalan adatkezelésre vonatkozó rendelkezés, valamint a személyes adatok különleges kategóriájához tartozó, egészségügyi adatok kezelésére és védelmére vonatkozó törvény[277] majd minden előírása. Nem elsődlegesen személyes adatok kezelésére vonatkozó előírások közül szemléltetésként kiemelhető a HACCP-ként ismert veszélyelemzés, kritikus szabályozási pontok elveinek megfelelő dokumentáció vezetési kötelezettsége.[278] A felhasználás joga tehát az adatokon végzett műveletek részletszabályait tudja megmutatni annak a területnek a vonatkozásában, amiben az adatok felhasználásra kerülnek. Konkrét adatfelhasználási rendelkezés lehet például a munkaszerződés kötelező tartalmi elemeinek, vagy a képalkotó diagnosztikai leletekre vonatkozó kötelező megőrzési időnek az előírása.

Az adatok hasznosítása az elképzelésem szerint a felhasználással párhuzamos rendszert alkot. Adathasznosítás esetén az adatok tipikusan, mint erőforrás kerülnek hasznosításra. A három alterület közül – jelenleg tapasztalható kiterjedtségben – ez tekinthető a legújabbnak, bár egyes, közadatok újra-hasznosítására vonatkozó részei már évek óta a jogrendszerek részét képezik. Adathasznosítás alatt tehát már korábban a felhasználás során létrejött (szekunder hasznosítás)

[276] A magyar nyelv az ilyen jellegű különbségtételre alkalmas, a „felhasználás" és „hasznosítás" szavak által, mivel jelentésükben kellően közeliek, azonban mégis képesek a különbség érzékeltetésére. Előbbi köznapi értelemben valaminek a használatát, valamilyen célra való alkalmazását jelenti, addig utóbbi egy olyan folyamatot takar, amely során egy adott erőforrást, anyagot vagy lehetőséget a legmegfelelőbb módon használják annak érdekében, hogy maximalizálják az abból származó előnyöket.

[277] Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény

[278] Az Európai Parlament és a Tanács 852/2004/EK rendelete az élelmiszer-higiéniáról

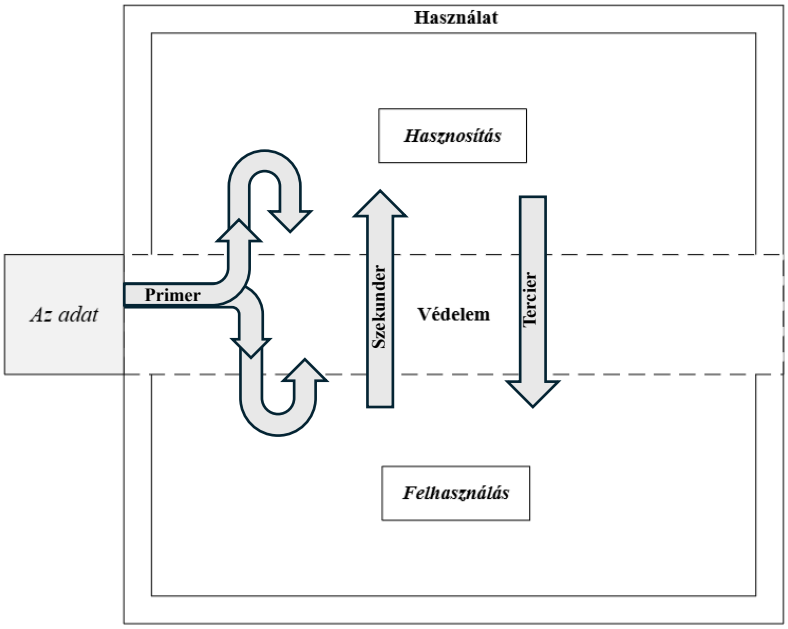
vagy kifejezetten hasznosítási célból létrehozott (primer hasznosítás) adatokon való műveletvégzést érthetjük. A felhasználáshoz képest a célok általában nehezebben megragadhatók, a folyamatok kevésbé konkrét határokkal bírnak. Az adathasznosításhoz sorolható területtel kapcsolatban a jelenleg uralkodó megközelítés szerint az elsődleges cél – jellemzően adatelemzési műveletek által – az ismeretszerzés, a tudásbővítés gyorsítása, mélyítése (vagy mesterséges úton való lehetővé tétele).[279] Az adathasznosítás jogát hosszú évekig kifejezetten a fentebb idézett, közadatokra vonatkozó előírások alkották. Ezek most is kiemelt és naprakészen tartott rendelkezésekkel operálnak, uniós és hazai szinten is számos képviselővel, így például a PSI irányelv vagy tagállami szinten a Nah.tv. említhetők. Az utóbbi időben azonban az egyéb, közszférához nem kapcsolódó adatoknak a hasznosítása is a terület homlokterébe került, a DGA mellett például a DA előírásai által.

3.3.3. Az adatfelhasználás és az adathasznosítás viszonyáról

A fentiek alapján a felhasználás és a hasznosítás területeire – hangsúlyozottan a jelenlegi tapasztalatok értelmezése alapján – az alábbiak mondhatók jellemzőnek:

Felhasználás	*Hasznosítás*
Mindennapi működéssel kapcsolatos	Innovációval kapcsolatos
Megszokott, egyértelmű célok	Szokatlan, ismeretlen vagy nehezen meghatározható célok
Az adatkezelés célja az adaton túlmutat	Az adatkezelés célja az adaton való (elemzési) műveletvégzés
Az adatra, mint eszközre tekint	Az adatra, mint erőforrásra tekint
Az érték nem kerül kifejezésre pénzben	Az adat értéke pénzben kerül kifejezésre

Az ábrán az adatjog védelmi és használati (azon belül hasznosítási és felhasználási) területeinek elhatárolása látható, az adatfolyam sematikus, de gyakorlat-orientált jelölésével (a nyilak az adatfolyam irányát jelölik). Ez alapján az adat létrejöttekor először a védelem jogának előírásai kerülnek vizsgálatra és alkalmazásra, mivel azok egy alapvetőbb, jogszerűségi előfeltételként értelmezhető viszonyrendszert képviselnek. Vagyis függetlenül attól, hogy egy adat egy munkaviszonyban vagy társadalomkutatásban kerül használatra, annak létrehozásakor (észlelés és rögzítés) – pl. személyes adatok esetén – a személyes adatok védelmére irányadó



9. ábra: a pragmatikus csoportosítás területeinek elhatárolása

[279] Lásd például a DGA (2) preambulumbekezdése

előírások feltétlenül alkalmazandók. Tovább haladva az adatfolyamon, a védelem sorompóit két irányba lehet átlépni, a hasznosítás és a felhasználás irányaiba. Ezt primer adatfolyamnak nevezhetjük, amely az adatok gyűjtésének elsődleges célja szerint kerül meghatározásra. A felhasználásból a hasznosításba tartó szekunder adatfolyam ehhez képest a már létező és felhasznált adatok másodlagos cél szerinti újra-hasznosítását fogja jelölni, tercier adatfolyamnak nevezhetjük a primer vagy szekunder adatok további (harmadlagos cél szerinti) hasznosítását. Az adatfolyam célba éréséhez az adatnak minden alkalommal át kell kelnie a védelem jogszerűségi szűrőjén. Az adatfolyammal kapcsolatban fontos azt is látni, hogy mind a hasznosítás, mind a felhasználás eredményorientált tevékenységek, azok kimeneteként új adatok jöjetnek létre, amelyekre ugyancsak először a védelem jogát kell alkalmazni (például megfelelően jött-e létre az adat, létrejöhetett-e egyáltalán stb.) és csak ezt követően térhetnek vissza a hasznosítás/felhasználás területeire.

Az adatjog fent vázolt kétféle csoportosítási megközelítése álláspontom szerint egymásnak nem mond ellent, azok egymás mellett, párhuzamosan létezhetnek. Fontos azonban, hogy ezek valójában pillanatképeket rögzítenek az adott jogi, társadalmi és technológiai állapotról, így a csoportosítás ezekkel együtt változhat. Ettől függetlenül, relatíve állandónak tekinthető a horizontális adatjogi szabályoknak a vertikális és kompozit adatjogi területekre gyakorolt összetartó ereje, amivel szó szerint igyekeznek egyben tartani az ágazati igényeknek megfelelő, speciális jog általi természetes *széttartást*. A legjobb példa erre a GDPR, amelynek de iure hatókörén túl egészen erőteljes de facto rendszerteremtő és szervező hatása van minden személyes adatkezeléssel érintett területre. Ez mostanra egy közös (európai) üzletviteli és ügyviteli zsinórmértéket és a szervezeti kultúra egyfajta minimum standardját is eredményezte.[280] Ez az összetartó hatás pedig több éves fennállása alatt sem mutat csökkenő tendenciát. Tehát a GDPR szabályozási szemlélete átszivárogni látszik, mind a hasznosítás, mind a felhasználás területeire, függetlenül az eltérő hatóköröktől, olyan alapvető rendelkezéseinek hatására, mint a célhoz kötöttség,[281] az adattakarékosság,[282] a korlátozott tárolhatóság,[283] a kockázat-arányos megközelítés[284] vagy a beépített és alapértelmezett (by design, by default) szemléletek.[285]

A csoportosítás elvégzésével, a területek azonosításával az adatjogi látkép tisztulni látszik. Azonban ezzel az újonnan jött tisztánlátással eddig rejtőzködő aggályok is felmerülnek. Ezek megtalálása és rendezése úgy gondolom az adatjogi (tényleges) tisztánlátáshoz és az adatalapú folyamatok egyensúlyi helyzetének megítéléséhez feltétlenül szükséges.

3.4. Az értékegyenlőségi elv

3.4.1. Az adatvalorizációs zavarról

A szakirodalom az adatok értékének meghatározásával kapcsolatban a „valorizáció” kifejezést használja.[286] Ez a köznapi értelemben valami értékének az azonosítását vagy valamihez értékek hozzárendelését jelenti.[287] Az értékesség az adatok esetén különösen fontos kérdés, hiszen a

[280] Second Report on the application of the General Data Protection Regulation (COM(2024) 357 final) 14-15 o.
[281] GDPR 5. cikk (1) bekezdés b) pont
[282] GDPR 5. cikk (1) bekezdés c) pont
[283] GDPR 5. cikk (1) bekezdés e) pont
[284] GDPR 32. cikk
[285] GDPR 25. cikk
[286] Lásd például: Claudio Bonvino, Marco Giorgino, „A valorization framework to strategically manage data for creating competitive value”, Int. J. Production Economics 269 (2024) 109152.
[287] Cambridge Dictionary, Cambridge University Press & Assessment 2025. Elérhető: https://dictionary.cambridge.org/dictionary/english/valorization

digitális, adatalapú működés napról napra dolgoz ki magából újabb és újabb megoldásokat, amelyek az adatok felhasználásában vagy hasznosításában rejlő potenciál kiaknázására irányulnak. Ebben az adatalapú „értékláncban”[288] pedig szinte mindannyian résztvevők vagyunk, így valójában egy mindenkit foglalkoztató kérdés lehet, hogy mikor, mit (esetleg mennyit) és kinek ér az adat?

A valorizáció – tehát az adatok értékrendelésének – zavara alatt a következő tapasztalást értem:

- Nem egyértelmű, hogy miért van az adatok jogosultjának[289] bizonyos esetekben döntési lehetősége, míg máskor tűrési kényszere az adathasználatot illetően.
- Nem egyértelmű, hogy lehetséges, hogy ugyanazon adat az egyik folyamatban pénzben kifejezhető értékkel rendelkezik, míg egy másikban nem.

Ezek a kérdések a teljes adatalapú működési spektrumon átívelő módon még nem kerültek megválaszolásra, ez pedig úgy vélem bizonytalansághoz és működési zavarokhoz vezet. A válaszadás nehézsége a valorizációs folyamat tisztázatlanságához is visszavezethető, azzal együtt, hogy az érték jogosultjának meghatározatlansága is közre játszik. Utóbbit a logikai sorban egy következő problémakörnek gondolom, ezért arra később térek vissza.[290]

A válaszok megtaláláshoz a következő feltevésből indulok ki: az adatvalorizáció zavarát egy háttérben működő, mozgató erő egyértelmű azonosításának és tudomásulvételének a hiánya okozza. Az alábbiakban ennek megtalálására teszek kísérletet.

3.4.2. Az adatok szerepéről az adatalapú folyamatokban

Az adatok szerepe alatt azok funkcióját (*viselkedését*) igyekszem meghatározni az egyes adatjogi területeken. A területek a védelem, a felhasználás és a hasznosítás, amiket az adatjog pragmatikus klasszifikációja során tudtunk elhatárolni egymástól.

- *Az adatok szerepe a védelemben*

Az adatok védelmi rendszere nem öncélú intézmény, ahogy más jogágak esetén itt is a védelem létrehozása mögött található valamilyen védett társadalmi *érték*. A büntetőjog logikájától kölcsönözve azt mondhatjuk, hogy ezen terület által védett társadalmi érték vagy érdek a védelem jogtárgya.[291] Ilyen például az adatvédelem esetén a személyes adatok védelméhez fűződő alapvető jog, mint végső soron az emberi méltóságból levezetett jogosultság. Ha ezt a gondolatmenetet folytatjuk akkor *az adatot, mint elkövetési tárgyat azonosíthatjuk* ezekben a rendszerekben. Így az adatjogi védelem az adatot azért illeti meg, mert annak nem megfelelő kezelése által a jogtárgy sérelme (vagy annak veszélye) következhet be.

- *Az adatok szerepe a hasznosításban*

Az adathasznosítás területén az adatok erőforrás alkotó tényezőkként jelennek meg,[292] amelyek gazdasági, pénzben kifejezhető értéket képviselnek és egyúttal jogügyletek tárgyai is lehetnek. Rövidebben megfogalmazva az adatokat, mint *monetizált*[293] *erőforrás* foghatjuk fel a

[288] Mayer-Schönberger, Cukier, 2014. 141 o.
[289] Jelen értelmezésben bárki, akinek valamilyen joga áll fenn egy adaton, például személyes adatok esetén az érintett.
[290] Lásd részletesen 6.2. fejezet
[291] Hornyák Szabolcs: Az emberi méltóság és egy alapvető jogok elleni bűncselekmények. In: Tóth Mihály, Nagy Zoltán (Szerk.): Magyar Büntetőjog, Budapest, Osiris Kiadó, 2014. 174 o.
[292] Lásd részletesen: ALI-ELI Principles for a Data Economy - Data Rights and Transactions - ELI Final Council Draft. 2021. (továbbiakban: ALI-ELI Alapelvek)
[293] A „pénzben kifejezhetőségre” ez a kifejezés tekinthető elterjedtnek. A monetizálás jelentése „pénzzé változtatás”

hasznosítás logikájában.[294] Ilyenkor az adat ellenértéke jellemzően pénz vagy közvetlenül pénzzé alakítható vagyoni érdekeltség. Utóbbit Tóth a „figyelemgazdaság zéróáras" megoldásaként írja le, ami azt jelenti, hogy a felhasználók a platformok használatáért pénzt nem fizetnek, hanem adatot adnak át, amelyet a platform a saját folyamatai során vált át pénzre, pl. hirdetési tevékenysége által.[295] A tényleges összegszerűsítés jelenleg egyáltalán nem egyértelmű,[296] egy egységnyi adat pénzben kifejezhető értékének meghatározására számos eltérő elgondolás létezik,[297] amelyre egyfelől hatással van a valorizáció tisztázatlansága, másfelől a terület éretlensége miatti közgazdasági háttér (pl. az átlátható piaci árazás) hiánya. A monetizációval kapcsolatban fontos megjegyezni, hogy a hatályos jog alapján az adat hasznosításba adásának egyébként nem explicit feltétele a haszon tényleges megszerzése. Ezt a DGA „adataltruizmusként"[298] aposztrofálja, ami olyan önkéntes adatmegosztást jelent, amely az érintetteknek a rájuk vonatkozó személyes adatok kezeléséhez való hozzájárulásán, vagy az adatbirtokosoknak a nem személyes adataik hasznosítására vonatkozó engedélyén alapul anélkül, hogy ezért olyan díjat számítanának fel vagy kapnának, amely meghaladja az adataiknak adott esetben a nemzeti jogban előírt közérdekű célokra való rendelkezésre bocsátása esetén felmerült költségeik ellentételezését.[299]

- *Az adatok szerepe a felhasználásban*

A védelem és a hasznosítás területén az adatok szerepének meghatározása viszonylag egyszerűnek bizonyult, mivel a területek elhatárolási szempontjaiban rejlett maga a funkció (pl. a hasznosítás lényege az adat erőforrás-jellege és pénzben kifejezhetősége). Ez azonban nincs így a felhasználásnál, hiszen azt a területek elhatárolásakor negatív megközelítéssel határoztuk meg, tehát a felhasználáshoz (többek között) azok az esetek tartoznak, ahol az adat eszközként és nem erőforrásként jelenik meg, illetve nincs pénzbeli értéke. Például egy szerződéskötéshez szükséges adatmegadásért cserébe nem gyakori pénz követelése. A monetizációt még akkor is nehéz lenne megtalálni, ha a szerződés teljesítésén keresztül megjelenő haszon realizációjával próbálnánk meg összekötni, mivel ebben az esetben az adat értéke a szerződés tárgyának értékétől függene, az érték tényleges megjelenése pedig a szerződés teljesítésétől. A magánjogi jogügyletektől eltávolodva a logika a közigazgatásban még inkább megbicsaklik, hiszen például egy hatósági eljárás lefolytatásához szükséges adatkezelés gyakorlatában egyértelműen elképzelhetetlen az eljárás alá vontnak az adataiért cserében történő pénzfizetés. Ez ugyanis első ránézésre azt jelenthetné, hogy minden közigazgatási hatóság a jogalanyok adatainak felhasználásakor (pl. egy szabálysértési eljárás lefolytatásakor) adósságot halmoz fel, ami soha nem kerül megfizetésre.

Látható, hogy – a dolgozat értelmezésében legalábbis – a felhasználás esetkörei a társadalmi működés valamelyik alapvető elemét érintik, egy olyan folyamatot, amihez adatokra van szükség. A világtörténelemben a civilizált együttélés sikerességéhez számos megoldást dolgoztak ki és nem mindnek volt vagyonmozgást előidéző aspektusa. Az adatok felhasználásban betöltött társadalmi együttélést szolgáló szerepének megragadásához használható a középkortól ismert „kölcsönös érdekrealizáción alapuló csere" intézménye.[300] Az

[294] Malgieri, Custers, 2018. 5 o.
[295] Tóth, 2024, 22 o.
[296] Custers, Bachlechner, 2017. 3 o.
[297] Lásd például: Farboodi, Veldkamp, 2021.
[298] Ezzel a szóhasználattal a monetizáció jelenlétét egyébként megerősítette, hiszen az altruizmus valamilyen önzetlen viselkedést, saját káron történő segítségnyújtást jelent.
[299] DGA 2. cikk 16. pont
[300] A feudális jogban ez például az uralkodó réteg és a jobbágyság között, egyik irányból a termékszolgáltatás, másik oldalról a terület, a közrend és jogrend védelmében nyilvánult meg. Lásd részletesen: Kajtár István: Egyetemes állam- és jogtörténet. Budapest-Pécs, Dialóg Campus Kiadó, 2005. 54 o.

elképzelés helyzetre adaptált verziója szerint az adatok a résztvevő érdekelt felek közös megegyezésével vagy egy össztársadalom által elfogadott érdekeltség kielégítése céljából lehetnek valamely felhasználási művelet részei. Ebben a konstrukcióban az adathasználat ellenszolgáltatása – bár elméletileg kifejezhető lenne – nem kerül pénzben meghatározásra, annak értékét a társadalmi együttélésben rejlő lehetőségek adják.[301] Így az adatok felhasználása vagy valamilyen jogosulti pozícióban levő beleegyezésével vagy egy olyan érdekeltség igazolásával történhet meg, amelyet az össztársadalom elfogadhatónak tart. A felhasználásban az adat tehát egy *csereeszköz*, amely az (adatalapú) társadalmi együttélés alapvető feltételeinek megteremtését szolgálja. A felhasználás a társadalmi értékek mellérendeltségéből indul ki,[302] így a csere során az érdekek valamilyen szintű egyensúlya kell megvalósuljon.[303] A felhasználásban ezért érezhető egyfajta tűrési kényszer is, ami olyan esetekben látszik meg igazán, amikor a társadalmi érdek nem esik egybe az adatok jogosultjának az érdekeivel.[304] Ezt a felhasználáshoz kapcsolódó tűrést egy „alku-alapú" megközelítésként is értelmezhetjük. Az alku-modell egyebek mellett a biztonság és a magánélet védelmének egymáshoz való viszonyával kapcsolatban szokott felmerülni, ahol e kettő jellemzően egymást kizáró értékkel összefüggő jogalkotói konfliktust oldják fel az egyén és a társadalom közötti alku bevezetésével.[305] A biztonság és magánélet alku-modelljéhez képest a felhasználás karakterisztikáját számomra célszerűbb egy kooperatív értékallokációként felfogni, ezért az alku helyett a csere kifejezés tűnik helyénvalóbbnak. Bár az adatok felhasználásához a jogkorlátozás elengedhetetlen (ami így alkuként értelmezhető), ez azonban nem kétdimenzióban, egy lineáris vonal mentén képzelhető el. Az adatjogi felhasználás az adatok nonrivalitása és másolhatósága miatt folyamatos mozgásban és a rendszeren belüli többszörösen összetett kölcsönhatásban áll az elemeivel. Vagyis a felhasználás végkimenetele nem bináris és kölcsönösen kizáró (vagy biztonság, vagy magánélet), ezek ugyanazon adat tekintetében egy időben, a tér két különböző helyén érvényesülhetnek.

3.4.3. Az értékegyenlőségi elv lényegéről

Az adat fent vázolt háromféle szerepe (elkövetési tárgy, monetizált erőforrás, társadalmi csereeszköz) a valorizáció zavarának megszüntetésére tett lépéseink környezetét adják. Mondhatnánk, hogy már látjuk a sakktáblát és a figurákat, viszont a játékszabályok egyelőre homályosak. E nélkül pedig a kiindulókérdésekre (a döntés és tűrés okára, a pénzben kifejezhetőségre) még nem kaphatjuk meg a választ. *A keresésünk tárgya egy nagy valószínűséggel nem deklarált, háttérben működő, ha nem is szabály, de legalábbis szabályszerűen érvényesülő tendencia.* Ennek be kell töltenie azt az űrt, amit az eddigiekben vázolt jogdogmatikai és pragmatikus klasszifikációs kísérletek nem tudtak. Az adatjogi területekkel összefüggő szerepkörök meghatározásai ugyanis a tényállapotot írják le (pl. a hasznosításban az adat pénzt ér, a felhasználásban nem), de azt nem magyarázzák meg.

---

[301] „[Az emberiség] fennmaradásának így tehát nincs más eszköze, mint hogy társulás által az erők olyan tömegét alkotja, amely le tudja győzni az ellenállást, s azt az erőtömeget egyetlen hatóerő révén megmozdíthatja és együttesen hatni engedi" Ld.: Jean-Jacques Rousseau: A társadalmi szerződés. Fordította és a bevezetést írta: Radványi Zsigmond. Budapest, Phönix-Oravetz-Kiadás, 1947. 28 o.

[302] „A társadalom minden egyes tagja minden jogával együtt beolvad az összességbe, azáltal, hogy különállása megszűnik, elsősorban mindenkinek a helyzete egyenlő lesz és mert egyenlő, senkinek sem érdeke a másikét megnehezíteni." Lásd: Ibid 29 o.

[303] Ezt – az adatvédelem területéről kölcsönzött példákkal – arra alapozhatjuk, hogy az érintett a hozzájárulásának visszavonásával vagy a tiltakozási jogának gyakorlásával a felhasználást akár meg is akadályozhatja.

[304] Például gondolhatunk egy munkáltatói vagyonvédelmet szolgáló kamerás megfigyelésre vagy egy cég pénzügyi átvilágítására.

[305] Székely Iván, Somody Bernadette, Szabó Máté Dániel, „Biztonság és magánélet: az alku-modell megkérdőjelezése és meghaladása, II. rész" Információs társadalom, 17. évf. 1. sz. 2017. 7-23.

Az adatjog ezen hiányzó láncszemét *értékegyenlőségi elvnek*[306] nevezem. Az elv megmutathatja a háttérben meghúzódó – jelenleg is létező, de nem azonosított – társadalmi értékallokációs mechanizmust és segíthet az adatok szerepének helyes értelmezésében, ezáltal betöltve az űrt, amit az eddigi csoportosítási lépések nem tudtak. Az elv jogdogmatikai validációját a GDPR (4) preambulumbekezdésének első fordulata adja, ami szerint „a személyes adatok kezelését az emberiség szolgálatába kell állítani. A személyes adatok védelméhez való jog nem abszolút jog, azt az arányosság elvével összhangban, a társadalomban betöltött szerepének függvényében kell figyelembe venni, egyensúlyban más alapvető jogokkal."

Az elv működése[307]
Az elv a cél szerinti szükségesség és arányosság vizsgálatán és a megfelelő érdekeltség egyensúlyának igazolásán keresztül működik. Az elv alapvetően egy háttérfolyamatként képzelhető el, ami bármilyen külső beavatkozás nélkül is lezajlik, a kiindulópontja, hogy a társadalom azokat a folyamatokat favorizálja, amelyek értékegyenlők. Az elv alapján egy teszt is létrehozható, amely az értékegyenlőség fennállását vizsgálja.[308]
Az elvben megjelenő érdekelt felek[309]
• Jogosult: bármilyen jog alapján az adatok felett rendelkezésre jogosult • Adatforrás: az adat által reprezentált tényszerűség (jelentősége akkor van, ha saját érdekeltséggel rendelkezik) • Adathasználó: de iure vagy de facto az adatokon műveletet végző • Társadalom: a folyamatokat legitimáló szerepén keresztül jelenik meg
Az alkalmazási terület
Az elv az adatok használatára irányuló területeken érvényesül. Az mind személyes, mind nem személyes adatok esetén alkalmazható. A kettő közt a lényegi különbség, hogy milyen joganyag tölti fel azt tényleges tartalommal. Előbbieknél pl. a GDPR és egyéb adatvédelmi előírások, utóbbiaknál különböző ágazati szabványok, előírások vagy szokások.
Az elv azonosítása: a csere egyenlősége
Az elv leginkább a felhasználás „össztársadalmi érdekrealizáción alapuló cseréjének" működése során figyelhető meg, mint legitimáló erő. Az értékek egyenlőségét vagy a jogosult (belátása szerint) saját maga nyilváníthatja ki beleegyezésének megadásával, vagy azt a másik – adatot használó – félnek kell bizonyítania.
Az elv, mint elhatárolási pont

[306] Az elvvel rokon fogalom a közgazdaságban ismert, ez az un. értékegyenlőségi vonal (Value Equivalance Line, vagy VEL). Lásd részletesen: Ralf Leszinski, Michael V. Marn, „Setting value, not price", The Mckinsey Quarterly 1997 Number 1. 98-115 o.

[307] Az elv a szerzői jogban ismert „három-lépcsős teszt" által fémjelzett szabad felhasználás és szerzői jogvédelem közötti „érdekkiegyensúlyozás" adatjogi leképezését is szolgálja, lásd részletesen: Gyenge Anikó: Szerzői jogi korlátozások és a szerzői jog emberi jogi háttere. Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2010.

[308] Ez gyakorlatilag, mint ex ante kötelezettség létezik az adatvédelmi jogban, mind technikai szinten (adatvédelmi hatásvizsgálat), mind jogi szinten megtörténik (érdekmérlegelési vagy szükségességi/arányossági teszt). Nem személyes adatok esetén is elképzelhető lehet, esetlegesen ex post elgondolásokként.

[309] A felek pontos meghatározásának később különös jelentősége lesz, de itt a „pozíciók megjelölése" is elégséges, azokat az 6.2. fejezetben pontosítjuk. Fontos, hogy a különböző pozíciók egymást fedhetik is, így elképzelhető lehet, hogy az adatforrás egyszerre rendelkezésre is jogosult.

A csere legitimitásának a vizsgálata megadhat egy új elhatárolási pontot a felhasználás és a hasznosítás között, ami ennek az értékegyenlőségnek a foka lesz. Tehát akkor beszélhetünk adathasznosításról, amikor az adatfelhasználás értékegyenlő cseréje nem jöhet létre.

Az értékegyenlőség fokozatai

Több olyan körülmény is említhető,[310] ami arra utal, hogy az értékegyenlőségnek különböző erősségi fokozatai lehetnek. Ez alapján az egyenlőséghez rendelt társadalmi legitimáció lehet erős vagy gyenge. A fokozatok modellezésére az adatkezelési műveletekre felhatalmazást biztosító különböző jogalapok[311] eltérő jogszerűségi feltételei jól alkalmazhatók.

- Ez alapján az adatok felhasználására két esetben van lehetőség, egyfelől, ha az értékegyenlőség *vélelmezett*, másfelől, ha az értékegyenlőség *megalapozott*.
  - Vélelmezett értékegyenlőség esetén az egyenlőséget az adathasználónak nem kell magának bizonyítania, ezt ilyenkor vagy a jogosult maga vagy a jogalkotón keresztül a társadalom teszi meg. Ide sorolhatjuk mindenekelőtt az olyan adathasználati folyamatokat, amelyek a jogosult döntésén múlnak, vagy amelyeket jogszabály tesz kötelezővé. Ezekben az esetekben az adathasználónak semmit sem kell bizonyítania, az eljárási szabályok betartásán kívül (pl. a beleegyezés megtörtént, a jogi kötelezettség ténylegesen fennállt). Szintén ide tartoznak a szerződéses alapon nyugvó felhasználási folyamatok, amelyeknél az egyenlőség vélelmének a fennállása a szerződéses viszony jogszerűségétől függ.
  - A felhasználáshoz sorolhatók az olyan értékegyenlőségi helyzetek is, amelyek nem vélelmezettek, de az adathasználó képes a megalapozásukra. Itt tehát az értékegyenlőség kétséges mindaddig, míg azt az adathasználó be nem bizonyítja technikai és jogszerűségi teszteken keresztül (magán vagy közérdek fennállása, létfontosságú érdek védelme). A teszt érvényességi vizsgálatán keresztül történhet meg a megalapozottság támadása és végeredményben az értékegyenlőtlen helyzet megszüntetése/orvoslása.
- Az adatok hasznosításakor az értékegyenlőség sem vélelmezettnek, sem megalapozottnak nem mondható. Az ilyenkor valójában ellentételezett, ez pedig azért lehet így, mert a társadalmi legitimáló erő nem elég erős ahhoz, hogy a folyamatot az együttélés alapvető feltételeként elvárja. Az ellentételezéskor az adat megosztásának ellenértéke lehet egy szolgáltatás „ingyenes” nyújtása vagy közvetlen pénzfizetés teljesítése.[312]
- Az elv végezetül megmutathatja az anyagi jogi jogellenesség helyét is az adatjogi struktúrában. Ez alapján jogellenesnek a teljesen értékegyenlőtlen adathasználatot tekinthetjük, vagyis azt, amely olyan súlyos fogyatékosságban szenved, mint az érvényes felhatalmazás (jogalap) hiánya vagy a jogellenes cél. Megjegyzendő, hogy az adatjog nem csak jogellenes adatkezeléssel, hanem eljárási szabályok be nem tartásával is megsérthető.[313]

A felhasználás tűrése

[310] Az értékegyenlőség skálázottságára utal a jogalapok mellett a GDPR érintetti jogosítványainak differenciáltsága is.
[311] GDPR 6. cikk (1) bekezdés a)-f) pontjai
[312] Ezt alátámasztani látszik, hogy amennyiben kikényszeríthető lenne az adathasználó által az adat megosztása, akkor nem lenne szükség a pénzbeliség megjelenésére.
[313] Például a GDPR III. fejezetében részletezett érintetti joggyakorlás akadályozása.

Ahogy fentebb említésre került a felhasználásban egyfajta tűréskényszer azonosítható,[314] mivel az oda bekerülő adatok egy jelentős része nem a jogosult döntésén múlik, azt a társadalmi együttélés követeli meg (erre még olyan erős jogosítványok esetén is sor kerül, mint amilyenekkel az érintett[315] rendelkezik személyes adatok esetén). Tehát még akkor is, ha szigorú jogszerűségi kritériumok vonatkoznak a folyamatra, az adatok felhasználását megfelelő érdekeltség megléte és bizonyítása mellett gyakorlatilag bárki megteheti. Az látható tehát, hogy az értékegyenlőség (jogosult vagy hatóság/bíróság általi) megdöntéséig a jogosult még a saját érdekeivel szemben is kényszerűen tűrni köteles az adatfelhasználást.[316]
A hasznosítás döntése
A hasznosításban az elv alapján a döntési szabadság jobban érvényesül, ami a társadalmi legitimáció alacsonyabb szintjére vezethető vissza. Itt a privátautonómia mellérendeltsége biztosítja a legitimáció meglétét.
Az adat monetizációja
A hasznosításban az adatok monetizációját is az alacsonyabb értékegyenlőségi szintre és az ebből eredő mellérendeltségre vezethetjük vissza. Mivel az adatokért cserében a társadalmi együttélés előnyei nem jelennek meg, ezért az adatokhoz (a valorizáció egy új formájaként) új érték hozzárendelésére van szükség. A monetizáció ezért a hasznosításban való részvétel ellentételezéseként működik.
Lehetséges érdekeltségek
Az adatalapú folyamatok mögött általában elmondható, hogy valamilyen érdekeltség áll (az érdekeltséggel kapcsolatban pedig vizsgálható a legitimáló erő). Ez közvetlenül kapcsolódhat egy vagy két személyhez (a jogosult, az adathasználó vagy harmadik fél) vagy személyek szélesebb köréhez. Az érdekeltség fakadhat közvetlenül a felek vagy a társadalom szélesebb igényeiből.

Unilaterális érdek: ez egy személy igényeinek kielégítésére irányul, amelynek azonban feltétele, hogy, mint egyéni érdeket a társadalom is méltányolhatónak tartsa. Például a munkahelyi kamerás megfigyelés a munkáltató vagyonvédelmi érdeke, azt azonban a társadalom is elismeri.	*Bilaterális érdek:* két fél közötti érdekegyezést jelentő esetkör, amelyben így a döntési autonómia egybehangzó akaratként való megnyilvánulása a legitimáló erő. Például egy szerződés teljesítésekor a felek a szerződési szabadság szerint dönthetnek bármiről, a területre vonatkozó kógens előírások határai között.	*Multilaterális érdek:* az unilaterális érdek ellentétjeként fogható fel, itt egy személy helyett egy teljes közösség érdekének kielégítése adja az adathasználat megalapozottságát. Például az adófizetést rendező hatóságok és egyéb szervezetek működését, mint az állam által szervezett társadalom egy területét és az ezzel járó adathasználatot mindenkinek el kell fogadnia.

[314] Ez alól személyes adatok esetén az érintetti hozzájárulás az egyetlen kivétel, ami a hat jogalapból egy, így az érdemi eltolódás ebből is kiolvasható.

[315] GDPR 4. cikk 1. pont szerint bármely információ alapján azonosított vagy azonosítható természetes személy

[316] Kiemelendő, hogy az egészségügyi (személyes) adatok vonatkozásában a GDPR 9. cikk (1) bekezdés szerinti általános tiltással valósul meg a legerősebb védelem, azonban itt is számos kimentési lehetőség áll az adatkezelő rendelkezésére.

<table>
<tr><td colspan="2">Példák az elv elméleti működésére</td></tr>
<tr><td>1.

• Cél: hold felszín vizsgálata távcsövön keresztül
• Érdekeltség: multilaterális - tudományos kutatás
• Szükségesség: empirikus kutatás más módon nem lehetséges
• Arányosság: nem jelent beavatkozást magánszférába vagy társadalmi rendbe
• Konklúzió: erős értékegyenlőség = adatfelhasználás</td><td>2.

• Cél: munkavállalói adatfelvételi lap kitöltetése
• Érdekeltség: bilaterális – foglalkoztatás
• Szükségesség: a munkaszerződés megkötéséhez adatokra van szükség, e nélkül a foglalkoztatás nem lehetséges[317]
• Arányosság: az adattartalmat az Mt.[318] és mint mögöttes jog a Ptk.[319] befolyásolja.
• Konklúzió: erős értékegyenlőség = adatfelhasználás</td></tr>
<tr><td>3.

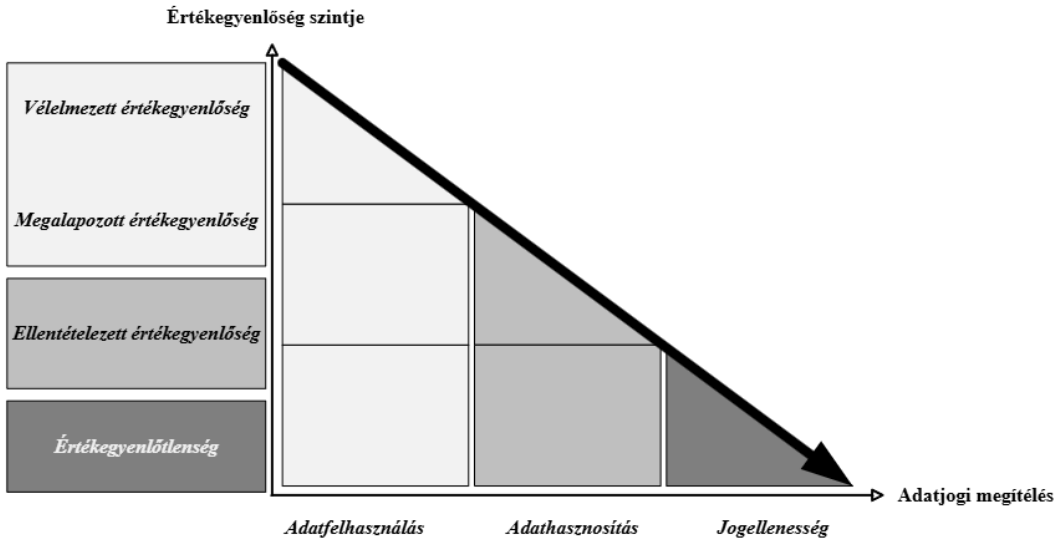
• Cél: ügyfélértékelési rendszer fejlesztése
• Érdekeltség: unilaterális – gazdasági érdekérvényesítése
• Szükségesség: folyamat automatizáció, működési költségek csökkentése (bemeneti adatok nélkül a rendszer nem fejleszthető le)
• Arányosság: az arányosság a felek megállapodásán alapulhat, a fejlesztésben való részvételért valódi előny biztosítandó, a kockázatok alapértelmezett csökkentése mellett (anonimizáció)
• Konklúzió: gyenge értékegyenlőség = adathasznosítás</td><td>4.

• Cél: államigazgatási tárhely védelmi rendszerének kijátszása, minősített adat megszerzése
• Érdekeltség: multilaterális - közfeladatot ellátó szerv által kezelt adat megismerése (információszabadság)
• Szükségesség: a lakosság tájékozódása másként nem lehetséges
• Arányosság: az arányosság nem áll fenn (korlátozó szabályba ütközés)
• Konklúzió: nincs értékegyenlőség = jogellenesség</td></tr>
<tr><td colspan="2">A elv kapcsolata a jogdogmatikai és a pragmatikus (tényhelyzeti) csoportosítással</td></tr>
<tr><td colspan="2">A kapcsolat lényegének megragadását az adathasznosítás felől érdemes közelíteni. Az ilyen folyamatok:
• vagy magas kockázatot jelentenek valamilyen védett érdekre, erős társadalmi legitimáció nélkül</td></tr>
</table>

[317] Mt. 42. § és 44. §
[318] Mt. 45. §
[319] 2013. évi V. törvény a Polgári Törvénykönyvről

- vagy ismeretlen végkimenetellel és/vagy következményekkel járnak, ami miatt (még) hiányzik az erős társadalmi legitimáció.

Az előbbi két kijelentés alapján látható, hogy a kapcsolat az értékegyenlőségi elv és a tényhelyzet között kauzálisnak mondható. Minél újszerűbb, illetve kockázatosabb az adatkezelési folyamat, annál gyengébb mögötte az össztársadalmi érdek/legitimáció. Ha gyenge, de még létező az érdek legitimitása egy folyamat mögött akkor az egyenlőséghez azt ellentételezni kell. Fontos azonban, hogy kivételek jelentős számban és folyamatosan merülhetnek fel. Egy olyan kutatási folyamat, amelynek célja a társadalom számára kiemelt fontosságú, ahhoz erős legitimáló erőt fog párosítani, így számos innovatív tevékenység kezelhető a felhasználás rendszerében (pl. egészségügyi kutatások), de a hasznosítási módszereket alkalmazva. Ezért a jogdogmatikai és pragmatikus csoportosításokat, valamint az értékegyenlőségi elvet minden estben egymás mellett, egymásra tekintettel lehetne alkalmazni és értelmezni, mivel sokszor csak együttesen képesek egy adott helyzet helyes értékelésére.



10. ábra: az értékegyenlőségi görbe

Az értékegyenlőségi elv lényege

- Az adatalapú működés folyamatainak rendezettségéhez a társadalmi legitimáló erő által diktált értékegyenlőség fenntartására van szükség. Az adatalapú folyamat értékegyenlőségének foka mutatja meg, hogy az adatfelhasználásnak vagy adathasznosításnak minősül;
- Az adatfelhasználásban a jogosultnak és/vagy adatforrásnak az értékegyenlő cserét tűrnie kell, az értékegyenlőséghez megfelelő érdekeltséget és erős társadalmi legitimációt kell bizonyítani;
- Az adathasznosításban döntési autonómia érvényesül, az értékegyenlőséghez pénzben kifejezhető ellentételezésre van szükség;
- Az értékegyenlőtlen adatalapú folyamatok jogellenesek.

Az értékegyenlőségi elv az értelmezésem szerint választ ad a valorizációs zavar kérdéseire. E szerint a felhasználásra a tűréskényszer és a csere azért jellemző, mert a társadalmi legitimáció erős (vélelmezett, megalapozott), míg az adathasznosítás esetén a legitimáció gyengébb. A tűrés

helyére ezért a döntés kerül, az adatok ellenszolgáltatásaként a társadalmi együttélés absztrakt előnyét pedig tényleges vagyoni előny váltja fel.

3.4.4. Az értékegyenlőségi elv dogmatikai hátteréről

Az adatjog létével kapcsolatos gondolatmenet következő állomásához érkeztünk. A valorizációs zavart feloldottuk, az értékegyenlőségi elv bevezetésével az adatjogi képet tovább tisztítottuk, de ismételten újabb kérdések merülnek fel. Egyáltalán lehetséges-e az értékegyenlőségi elv alapján működni? Személyes adatok esetén vitatható, hogy a védelemhez fűződő alapjog korlátozható olyan mértékben, hogy a tűrés ilyen kategorikusan megkövetelhető legyen. Felmerül továbbá, hogy az ellentételezés elképzelésének működéséhez szükséges mértékben lehetséges-e egyáltalán rendelkezni az adatok felett.

3.4.4.1. A tűréskényszer elfogadhatóságáról

Az értékegyenlőség megítéléséhez elengedhetetlen az érintett jogok alkotmányos – és később magánjogi – hátterét megvizsgálnunk. Alapjogi aggályok a természetes személyek személyes adatainak védelme esetén merülnek fel, ezért erre fogunk fókuszálni.

Kiindulópontként azt biztosan rögzíthetjük, hogy a személyes adatok védelméhez fűződő jog egy alapvető és alkotmányos jog. Ezt onnan tudhatjuk, hogy ekként szerepel az EU Alapjogi Chartájában és Magyarország Alaptörvényében.[320] Az emberi jogi megítélése kevésbé egyértelmű, sem az Emberi Jogok Egyetemes Nyilatkozata, sem az Emberi Jogok Európai Egyezménye nem tartalmazza expressis verbis, de az egyértelműen levezethető azon cikkeikből, amelyek a magán- és családi élet, valamint a lakás és kapcsolattartás tiszteletben tartásához való jogot deklarálják.[321] A természetjogi és jogpozitivista kérdéskörben való állásfoglalást kerülve, azt a szakirodalmi álláspontot érdemes legalább rögzíteni, ami szerint az alkotmányok elismerhetnek alapvető jogként olyan jogokat is, amelyek nem emberi jogok, csak legfeljebb emberi jogi tartalommal rendelkeznek.[322] Ezt egészítsük ki az Európai Adatvédelmi Biztos[323] saját álláspontjával, ami szerint az adatvédelemhez való jog (még) nem került, mint emberi jog elismerésre.[324] Így a legbiztonságosabb abból kiindulni, hogy a személyes adatok védelméhez való jog az emberi méltóság védelmének, mint alapvető emberi *anya*jognak[325] egy alapvető jogként rögzített részjogosítványa, ami a legmagasabb szintű európai és hazai jogforrásokban került deklarálásra.[326] Egyfelől fontos, hogy az anyajog mögötti értékben, az emberi méltóságban, az emberi státusz lényege kerül megjelölésre és arra a minőségre vonatkozik, amely szerint minden embert megillet a tisztelet legalább alapvető formája.[327] Másfelől az is leszögezendő, hogy az alapvető jogok sérthetetlenek és elidegeníthetetlenek, azokat mindenkinek tiszteletben kell tartani.[328] A sérthetetlenség és elidegeníthetetlenség azonban nem jelent korlátozhatatlanságot is. Az alapvető jogok más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával

---

[320] Alapjogi Charta 8. cikk és az Alaptörvény VI. cikk (3) bekezdése
[321] EJENY 12. cikk, EJEE 8. cikk
[322] Petrétei József: Az alkotmányos demokrácia alapintézményei. Budapest-Pécs, Dialóg Campus, 2009, 2011. 417 o.
[323] Továbbiakban: EDPS
[324] EDPS, „Data Protection" Elérhető: https://www.edps.europa.eu/data-protection/data-protection_en
[325] 8/1990. (IV. 23.) AB határozat
[326] Az Európa Tanács 108. Egyezménye; Az Európai Unió működéséről szóló szerződés (továbbiakban EUMSz) 16. cikk (1) bekezdése; és a már említett Alapjogi Charta és Alaptörvény. Megjegyzendő, hogy a GDPR EU rendeleti szinten, az Info.tv. magyar törvényi szinten erősíti meg ezeket.
[327] Barcsi Tamás, „Erkölcsi és emberi méltóság a középkori keresztény filozófiában", DÍKÉ. 6. 141 o.
[328] Alaptörvény I. cikk (1) bekezdés

korlátozható.[329] Koltay szerint az olyan esetekben, ahol az emberi méltóság az élethez való jogtól képes elválni, ott annak részjogosítványai – köztük az adatok védelméhez való jog – biztosan korlátozhatók. Ezek alapján az értékegyenlőségi elvben megjelenő, természetes személyek alapjogi korlátozását megvalósító *tűrés* létének, elv általi elismerése elfogadhatónak tűnik, ha a korlátozás az embernek kijáró alapvető tiszteletet megadja és az alkotmányjog által megállapított feltételeknek az megfelel. Az elv alapmechanizmusa a társadalmi érdekek keresése és kiegyenlítése, ezért az alkotmányjogi megfeleléshez arra van szükség, hogy a tűrés visszavezethető legyen egy legalább törvényi szintű előírásra és, hogy az szükséges és arányos legyen.[330] Ez az elgondolás az Alkotmánybírósági gyakorlattal összhangba állítható, a 3110/2013. (VI. 4.) AB határozat szerint ugyanis: „Az Alaptörvény az egyén-közösség közötti viszonyt az egyén közösséghez kötöttsége jegyében határozta meg, anélkül azonban, hogy annak egyedi értékét érintené. (…) Az egyénnek társadalmi lényként, szociális beágyazottsága miatt bizonyos mértékben azonban el kell tűrnie adatai kötelező kiszolgáltatását, és azok állam általi felhasználását."

3.4.4.2. Az adatokról való döntés megítéléséről

A döntés és az ezzel együtt megjelenő monetizáció megengedhetőségének vizsgálatához egyfelől a fenti alkotmányjogi okfejtést kell folytatnunk, másfelől azonban magánjogi szempontokat is figyelembe kell vennünk.

Kiindulópontként a védelem természetét kell helyesen értelmeznünk. Az adatalapúsághoz tartozó adatgazdasági folyamatokat szkeptikusan kezelő, totális védelemre alapuló koncepció az EDPS és az Európai Adatvédelmi Testület[331] állásfoglalásaiban is megjelenik. Ezek szerint egyfelől az adatok nem tekinthetők gazdasági tényezőknek, mivel azok az Alapjogi Charta és az EUMSz által konstituált alapvető jog által védettek.[332] Az EDPS szerint, ha ez mégis megtörténne akkor az adatok tömeges gyűjtése és kezelése valósulhat meg az érintettek hozzájárulása nélkül, a piaci egyenlőtlenségek kihasználásával adatmonopóliumok jöhetnek létre és ez további visszaéléseket (alapjogsértő, versenytorzító stb.) tehet lehetővé, illetve csökkentheti az adatalapú folyamatok átláthatóságát. Megjegyzi továbbá, hogy jogalkotási nehézségeket okozhat az adatalapú üzleti modellek szabályozása is.[333] Egy másik állásfoglalásában az EDPS megerősíti, hogy álláspontja szerint az adatok nem monetizálhatók és nem lehetnek tárgyai egyszerű kereskedelmi tranzakcióknak, még akkor sem, ha annak az adatalany részes fele. Az ilyesfajta ügyleteket a szervkereskedelemhez hasonlítja és leszögezi, hogy attól, hogy létező jelenség az nem jelenti, hogy a jogalkotás általi elismerésére van szükség.[334] Az EDPS álláspontját az EDPB fenntartja és megerősíti, hangsúlyozva, hogy az adatok nem lehetnek kereskedelmi tranzakciók tárgyai, az alapjogvédelem mindenkit meg kell illessen pénzügyi helyzetétől függetlenül.[335]

Mindenekelőtt fontos leszögezni, hogy az EU jogalkotása a DGA és a DA által az EDPS és az EDPB egyes felvetéseit meghaladta, így kodifikált jogi értelemben az adatokkal való kereskedelmi kapcsolatok jogszerűen létesíthetők. Gondoljunk a DGA 2. cikkére, ami szerint az adatmegosztás (személyes és nem személyes adat esetén egyaránt) *díj* ellenében történhet,

[329] Alaptörvény I. cikk (3) bekezdés második fordulata
[330] Mint a korlátozás tartalmi és formai feltételei, lásd részletesen: Kerekné Jakó Nóra, Mikes Lili, Szabó Zsolt: Alkotmányjog. Budapest, Patrocinium Kft., 2021. 38 o.
[331] Továbbiakban: EDPB
[332] EDPS, „Opinion on coherent enforcement of fundamental rights ont he age of big data" Opinion 8/2016. 7 o.
[333] Opinion 8/2016. 3, 5, 6, 10, 12 o.
[334] EDPS, „Opinion on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content" Opinion 4/2017. 7 o.
[335] EDPB Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms

illetve az adatközvetítő szolgáltatás célja *kereskedelmi* kapcsolatok létrehozása meghatározatlan számú érintett és adatbirtokos, másrészről az adatfelhasználók között. Ettől függetlenül az EDPS és az EDPB aggályai a mai napig relevánsak és az adatalapúsággal szembeni főbb ellenvetéseket jól összegzik. A dolgozat témájából fakadóan a részletes vizsgálatuk tehát indokolt.

- *A döntés alkotmányjogi szempontból*

Ahogy fentebb látható volt az adatok valóban alapvető jog által védettek, azonban az *adat*védelem – Streinz által hangsúlyozottan[336] – némileg megtévesztő elnevezés. Ahogy a védelem jogánál is láttuk, az adatok védelme valójában nem az adatokra irányul, hanem az adat mögötti érintetti érdekeltségre. Ennélfogva azt nem célszerű abszolút tilalomként értelmezni, hiszen az érintetti érdekeltség sérülésének hiányában a védelem joga nem is kell feléledjen. E körben a túl szigorú értelmezés kis túlzással ahhoz hasonlatos, mintha az ingatlanok adásvétele lenne tilalmazott a tulajdon sérthetetlenségére hivatkozással.

A védelem feléledésének szükségszerűségével kapcsolatban pedig fontos, hogy maga az alapvető jog sem egydimenziós. Mind a szakirodalomban, mint a joggyakorlatban jelentős egyetértés tapasztalható abban, hogy a terület a passzív, külső behatásokkal szembeni védelem mellett az aktív, adatalany általi cselekvési szabadságot is magában foglalja. Ezt, mint információs önrendelkezés ismerjük.[337] Az információs önrendelkezési jog az egyén *„azon joga, hogy alapvetően maga döntsön személyes adatainak kiszolgáltatásáról és felhasználásáról”.*[338] Az információs önrendelkezés léte a Német Szövetségi Köztársaság Alkotmánybíróságának 1983-as döntéséig nyúlik vissza, ahol ez először került kimondásra.[339] Azt tartalmi szempontból legalább az eltitkoláshoz való jogra és az önkifejezés jogára oszthatjuk.[340] Az eltitkolás, vagyis a passzív megismerésvédelem jogának határaival kapcsolatban az Alkotmánybíróság a következőt állapította meg: „az önrendelkezési jog azonban, mint az általános cselekvési szabadsághoz való jog, a jogérvényesítéstől való tartózkodás, a nem cselekvés jogát is magában foglalja. Mivel ez a jog az egyén autonómiájának védelmére szolgál, általában mindenkinek szabadságában áll eldönteni, hogy jogai és törvényes érdekei védelmére nyitva álló és alkotmányosan biztosított hatósági igényérvényesítési utat igénybe veszi-e vagy attól tartózkodik.”[341] A védelem ezen megfogalmazása összhangban áll az értékegyenlőségi elvnél bemutatott társadalmi legitimációs erővel, annak ugyanis artikulációjának egy megnyilvánulási formája lehet a védelem adta lehetőségek egyének általi kihasználása. Ezt megerősíti Sólyom, mikor kijelenti „amilyen a veszély, olyannak kell lennie a védekezésnek.”[342] A passzív védelmet tehát nem szükségszerű az adatalany akaratával szemben is érvényesítendő, talán túlzottan is paternalista jogintézményként felfogni. E mellett figyelembe kell venni az önrendelkezés aktív oldalát is, vagyis az önkifejezés jogát. Az Alkotmánybíróság ezzel kapcsolatban arra jutott, hogy „Az információs önrendelkezési jog szorosan kapcsolódik a magánszférához való joghoz, és az arról való döntést foglalja magában,

[336] Streinz, 2021. 3 o.
[337] Fontos, hogy az adatvédelmi jog nem azonos az információs önrendelkezési joggal, ugyanis az első adatvédelmi jogalkotás idején utóbbi még nem létezett. Ezért az adatvédelem az információs önrendelkezésnél tágabb kategória, azt mint jogelvet jelenleg azonban magába foglalja, lásd részletesen: Jóri, Soós, 2016. 21-22 o.
[338] 15/1991. (IV. 13.) Alkotmánybírósági Határozat
[339] BVerfG65.1. (69.f.)
[340] Szabó, 2012. 40 o.
[341] 1/1994. (I. 7.) AB határozat
[342] A személyiségvédelemmel kapcsolatos írásában az idézett gondolat mellett találóan a (személyiség)védelmet, mint állami szolgáltatást azonosítja, amellyel nem az állami védelmi erőt, hanem az egyén autonómiájának szerepét hangsúlyozza, lásd: Sólyom László: A személyiségi jogok elmélete. Budapest, Közigazgatási és Jogi Könyvkiadó, 1983. 318 o.

hogy az egyén mikor és milyen korlátok között fedi fel a személyéhez köthető adatokat."[343] *Vagyis az információs önrendelkezés értelmezhető egyik oldalról döntésként a védelem igénybevételéről, másfelől döntésként az adatokról való rendelkezésről.*

Összegezve az EDPS első aggályával kapcsolatban azt mondhatjuk, hogy az adatalapú folyamatok és az adatgazdaság működése alkotmányjogi szempontból kevésbé problematikus, mint az elsőre tűnik. A védelem totalitása nem az adatra, hanem az egyénre vonatkozik, ezért az abszolút tilalom megkövetelése nem feltétlenül megalapozott. E mellett az is látható, hogy az információs önrendelkezés az egyén számára szélesebb jogosítványokat biztosít az állami jogvédelemnél. Nem szabad ugyanis az információs önrendelkezés aktív oldaláról megfeledkezni, ami végső soron az egyén kezébe adja a védelem adta lehetőségek igénybe vételének vagy adatainak önkéntes megosztásáról való *döntés* jogát. Ezen álláspontot nem kell befolyásolja az, hogy a döntés jelenleg elterjedt módszertana – az un. „notice & consent" eljárás – kevésbé hatékony.[344] Az EDPS kétségtelenül helyesen látja az alapjogi kockázatokat és egyértelműen megfelelő és arányos garanciális szabályokra van szükség ezen a területen. Ez azonban úgy gondolom nem az információs önrendelkezés felülírását, hanem a módszertanok és így különösen a notice & consent eljárás újragondolását[345] kell elsősorban indokolja.

- *A döntés magánjogi szempontból*

A következő kérdéskört az EDPS szervkereskedelem-párhuzamával célszerű indítani, hiszen egy nagyon valós szabályozási kérdésre hívja fel a figyelmet. Eddig annyit mondhatunk, hogy az egyén döntési jogát – alanyi oldalról, alapjogvédelmi érvekkel – nem szükségszerű korlátozni. Felmerül azonban, hogy a döntés tárgyi oldala, vagyis az adat indokolja-e a korlátozást. Mit jelent valójában az adat az egyén oldaláról vizsgálva? Az EDPS szervkereskedelem analógiája meglátásom szerint a személy és személyiségének kifejezéseként megjelenő adatok közötti kapcsolat rendkívüli bensőségességére hívja fel a figyelmet, azzal, hogy azt az ember és belső szervei közötti kapcsolathoz hasonlítja. Ezt ezért a magánjog személyiségvédelem szemüvegén keresztül mutatkozik a legcélszerűbbnek vizsgálni, de mielőtt erre rátérünk megjegyzendő, hogy a párhuzam, bár érzékletes, de nem pontos. Az adatok létrejöttekor arra jutottunk, hogy az adat nem válik a reprezentált tényszerűséggé, annak tükörképe és nem alkotó eleme. Így a kapcsolat kétségtelenül intim, azonban az elválasztás kevésbé *végzetes*, mint a szervek esetén. Különbség van ugyanis a leválasztott testrész vagy szerv jogi megítélésében annak természete szerint,[346] így talán megfelelőbb lenne az adatokat a hajhoz hasonlítani belső szervek helyett.

A személyek magánjogi védelme értelemszerűen a személyeket illeti meg. Sárközy szerint a személy a jogban az, aki jogalany, a jogalany személyeknek pedig személyisége van és a jog ezt a személyiségvédelem intézményrendszerén keresztül védi.[347] A személyiségi jogok jelentőségét Sólyom tömören úgy összegzi, hogy azok „az ember jogállásának alapvető kifejezői".[348] A személyiség védett mivolta mellett fontos kiemelni, hogy annak un.

[343] 3110/2013. (VI. 4.) AB határozat
[344] Daniel J. Solove, „Introduction: Privacy Self-Management and the Consent Dilemma", 126 Harv. L. Rev. 1880, 2013. 1880-1881 o.
[345] Fred H. Cate, Viktor Mayer-Schönberger, „Notice and consent in a world of Big Data", International Data Privacy Law, 2013, Vol. 3, No. 2. 67 o.
[346] Menyhárd Attila, „Forgalomképes személyiség?", In: Menyhárd Attila, Gárdos-Orosz Fruzsina (Szerk.): Személy és személyiség a jogban. Budapest, Wolters Kluwer, 2016. 66-67 o.
[347] Sárközy Tamás, „Személy és személyiségvédelem", In: Menyhárd Attila, Gárdos-Orosz Fruzsina (Szerk.): Személy és személyiség a jogban. Budapest, Wolters Kluwer, 2016. 47 o.
[348] Sólyom, 1983. 10 o.

„kommercializálódása" is ismert a jogirodalomban.[349] E szerint a személyiség különös megnyilvánulási formáit nemcsak eszmei, hanem kereskedelmi (vagyoni) érdekek mentén is védelemben kell részesíteni.[350] Ezeket a megnyilvánulási formákat személyiség jegyekként is felfoghatjuk, amikhez különösen a név, a képmás, a hangfelvétel, illetve más, a jogosultra és életvitelére jellemző, a magánélethez való jog részét képező adat tartozhat.[351] Ezek Görög szerint „a személyiségnek olyan vonatkozásai, amelyek a külvilágban tárgyiasulnak, s elválnak magától az emberi személyiségtől, s ezek a személyiségvonatkozások – elválásuk okán (is) – önálló javakként vagyoni forgalom tárgyai lehetnek".[352] Az adatalapú folyamatok vizsgálatának tükrében az is láthatóvá kezd válni, hogy a személyiség (annak egyes aspektusai) adatként való leképeződésük által lehetnek kereskedelmi ügyletek tárgyai, amelynek megítélésére így a polgári jogi értelmezési szempontok jól alkalmazhatóak. Gondoljunk csak a szórakoztatóipari megjelenésekre (pl. színészek, modellek) a másodlagos kereskedelmi hasznosulást támogató merchandising szerződésekre,[353] vagy a véleményvezérek (influencer) közösségi média tevékenységére.[354]

A kommercializálódás felmerülésével kapcsolatos ok feltárására többféle megközelítés létezik. Egy mind alkotmányjogi, mind magánjogi szempontból jelentős hatást gyakorló elgondolás Locke koncepciója, ami szerint „az ember saját személye tulajdonosa", ezzel összefüggésben megjelenő gondolat, hogy aki egy jogot (a személye feletti tulajdont) bír, az a hozzá tartozó erkölcsi világ ura.[355] Szintén említhető az angolszász right to privacy szemléletének párjaként működő right to publicity megközelítés,[356] ami a személyiségi jogok vagyoni oldalát takarja és mint ilyen a személynek jogosultságot biztosít arra, hogy személyiségének egyes elemeit kereskedelmileg hasznosítsa, arról rendelkezzen (elismerve a személyiséggel összefüggő vagyoni érdekeltségeket).[357] Végezetül megemlíthetjük az információs önrendelkezés aktív oldalának magánjogba való behatását is, ami a right to publicity-hez hasonlóan az önkifejezéshez való jogot jeleníti meg, bár a vagyoni viszonyok említése nélkül. Az EDPS helyesen hívja fel a figyelmet az adatforrás és az adat intim kapcsolatára, azonban azt mondhatjuk, hogy a szervkereskedelem hasonlata túlzónak mondható, a személyiség által elérhető eredmények kereskedelmi hasznosítására – az erős magánjogi védelem ellenére – jelenleg is van lehetőség. *Ha tehát a képmással (mint adattal) való kereskedelem megengedett, akkor ésszerűnek tűnik az egyéb adatok vagyoni ellentételezésért való – szigorú garanciális szabályok közötti – megosztásának lehetővé tétele.*

- *A döntésről összegző jelleggel*

Zárásképpen az EDPS és az EDPB egyéb, eddig nem érintett aggályaira is érdemes kitérnünk. Saját meglátásom szerint is számottevő piaci egyenlőtlenség és információs egyensúlytalanság tapasztalható, ami valóban csökkenti az átláthatóságot, a visszaélések esélyét pedig növeli.

[349] A jelenség egyik korai példája az un. Dietrich ügyben jelent meg, lásd részletesen: Görög Márta, „Az általános személyiségi jog posthumus védelme a német joggyakorlatban", EJ, 2002/4., 22-26. o.
[350] Görög Márta, „Gondolatok a személyiség magánjogi védelme körében", In: Menyhárd Attila, Gárdos-Orosz Fruzsina (Szerk.): Személy és személyiség a jogban. Budapest, Wolters Kluwer, 2016. 104 o.
[351] Schultz Márton, „A vagyoni értéku személyiségi javak szabályozási problematikájának egyes kérdései. A tárgyiasulás alapú vagyoni személyiségvédelem" IJ, 2020/2. (75.). 4 o.
[352] Görög Márta, „Gondolatok a személyiségi jog egyes összetevőinek kereskedelmi értékéhez", Corvinus Law Papers CLP – 1/2018. 33 o.
[353] Görög, 2016. 106 o.
[354] Schultz, 2020. 1 o.
[355] Tattay Szilárd, „Az emberi személy, mint „önmaga tulajdonosa": a donimium siu fogalmától a self-ownerhip eszméjéig, In: Menyhárd Attila, Gárdos-Orosz Fruzsina (Szerk.): Személy és személyiség a jogban. Budapest, Wolters Kluwer, 2016. 16 o.
[356] Görög, 2018. 35 o.
[357] Schultz, 2020. 1 o.

Azzal feltétlenül egyetértek, hogy az alapjogok tiszteletben tartását nem lehet pénzfizetés ellenében biztosítani. A megjelenített álláspontok azonban a helyzeten nem feltétlenül segítenek, hanem jó eséllyel a status quo-t rögzítik. Az értékegyenlőségi elv is rámutat arra, hogy az adatok felhasználása – ami a civilizált világunktól abszolút elválaszthatatlan – a legtöbb esetben nem önkéntes, ahhoz a rendezett társadalmi együttéléshez van szükség. Azt azonban érdemes lehet szem előtt tartani, hogy ezek a folyamatok nem jelentenek számottevően kisebb behatolást a magánszférába, mint az adathasznosításban való részvétel, ami – az értékegyenlőségi elv alapján is – jellemzően döntés alapúan működik. A totális tilalomból eredő tabuként kezelés és szabályozatlanság úgy gondolom az átláthatóságot fokozatosan tovább csökkenti, míg a visszaéléseket és a nagy platformok monopol helyzetét érintetlenül hagyja. Az EDPB 2024-es véleményének alapjául a Facebook „pay or okay" megoldása szolgált, ami az adatok *jogszerűbb* kezeléséért pénzfizetést várt el a felhasználóktól. Ez azontúl, hogy a meglévő és a jelen dolgozat által felépíteni szándékozott adatjogi paradigma szerint is aggályos, arra is felhívja a figyelmet, hogy visszaélések a tilalom ellenére jelenleg is megtörténnek. Így az álláspontón való változtatás, az inkluzív, átlátható és normakövető adathasznosítás kiépítésével – DA és DGA által kijelölt úton haladva – célszerűbbnek mutatkozik.

Összegezve az adatokról való döntés és azok monetizációja több területen már érvényesül. Látható, hogy alapjogvédelmi aggályok által vezérelve a kérdés megosztónak mondható, de végeredményben létezik olyan értelmezés, ami szerint a hasznosítás döntése és az adatok monetizációja elfogadható. Hasonlóan a személyiségvédelem általános védelméhez, az adatok esetén sem mutatkozik feltétlenül szükségesnek a döntés lehetőségének talán túlzóan paternalista megközelítésű korlátozása. Görög a személyiségjegyek kommercializálódásával kapcsolatban hasonló konklúzióra jut, mikor arra az álláspontra helyezkedik, hogy „a pozitív [védelmi] megközelítés (…) nem szab gátat az érintett azon szándékának, hogy szabadon rendelkezzék személyisége felől, szabadon döntse el miként és milyen körben engedi személyiségét folyni, abba milyen körben enged belátást és behatást."[358]

[358] Görög, 2018. 38 o. Hasonló eredményre jut kifejezetten a képmáshoz és a hangfelvételhez való jog kapcsán: „Az alanyi jogok érvényesítése a jogosult akaratelhatározásától függ, a „jog rendelkezési" jogot biztosít a jogosult számára." Lásd részletesen: Görög Márta, „A képmáshoz és hangfelvételhez való jog védelmének fejlődéstörténete és a jogosultat megillető „rendelkezési jog" gyökere", In: Görög Márta, Menyhárd Attila, Koltay András: A személyiség és védelme - Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül. Budapest, ELTE Állam- és Jogtudományi Kar dékánja, 2017. 261 o.

3.5. A jelen fejezet főbb kutatási eredményei

Az adatalapú működés, mint az adatjogi szabályok életviszonya.

- Az adatalapúság az emberiség mindennapjainak mindig is része volt, de annak modern válfajának a lényege, hogy az eddigiekhez képest minőségi változást hozott az adatok *észlelésének* és *rögzítésének* módszertanában

Az analóg és digitális adatok szabályozása

- Az információkezelés és információvédelem már a korai társadalmakat szervező államokban is jelen volt (pl. népszámlások)
- Egyedi védelmi és használati szabályok közé sorolhatjuk még a titokvédelmet és a cenzúra intézményét

A magánszféra védelem az adatalapú szabályok egy kiemelkedő területe

- A magánszféra védelme a territoriális viselkedéssel hozható párhuzamba
- Az angolszász szabályozási irányra a privacy szemlélet, a kontintális jogcsaládra az adatvédelem a jellemző
- Az adatvédelmet három generációra oszthatjuk

Az adatjog léte

- Az adatokra vonatkozó szabályozásban az EU az USA és Kína mellet egy harmadik megközelítést képvisel, amit az alapjogvédelem, és egyfajta biztonságos, organikus fejlődési szemlélet jellemez
- Az adatjog életre hívása elfogadhatónak tűnik (a szabályozottság nem kielégítő, a szabályozási szükség szélesen igényelt és tartós, valamint az alkotmányos rendszerrel összhangban áll)
- Az adatjogot egy jogterületként célszerű felfogni, vagyis jogi normák olyan, többé-kevésbé összefüggő és relatíve elkülönülő, több jogágat részben átfedő összességét, amely a jogág sajátosságaival, önállóságával, elkülönültségével nem rendelkezik
- Az adatjogi szabályozás szüksége hasonlóan fennállónak tekinthető, mint a maga idejében a szerzői jognak (tárgyi, alanyi, fogyasztási, döntséhozói oldalak megléte)

Az adatjog jogdogmatikai szempontból az alábbi területekre osztható:

- Horizontális (tiszta) területre (pl. GDPR, DA, DGA, FFNPDR, CRA)
- Horizontális (multi-szektorális) területre (pl. CSA, NIS2 irányelv)
- Vertikális területre (pl. PSI és e-Privacy irányelv, FIDAR és EHDS javaslatok, DORA)
- Kompozit területre (pl. e-IDAS2.0, P2B, DSA, DMA stb.)

Az adatjog pragmatikus szempontból az alábbi területekre osztható:

- A védelem joga (pl. GDPR, CRA, CSA, DORA, NIS2 irányelv)
- A használat joga
  - A felhasználás joga (pl. munkajog, egészségügyi jog stb.)
  - A hasznosítás joga (pl. DGA, DA, FFNPDR, EHDS és FIDAR javaslatok)

Az adatjogi területek egyfajta adatjogi szabályozási konvergencia tartja össze (pl. a GDPR alapelve, érintetti jogok, jogalapok, by design, by default szemléletek stb.)

Az adatok szerepe eltérő az egyes területeken

- A védelemben elkövetési tárgy
- A hasznosításban monetizált erőforrás
- A felhasználásban társadalmi csereeszköz

Az értékegyenlőségi elv egy nem deklarált, háttérben működő szabályszerűen érvényesülő tendencia

- A cél szerinti szükségesség és arányosság vizsgálatán és a megfelelő érdekeltség egyensúlyának igazolásán keresztül működik
- A kiindulópontja, hogy a társadalom azokat a folyamatokat favorizálja, amelyek értékegyenlők
- Az elv az adatok használatára irányuló területeken érvényesül, mind személyes, mind nem személyes adatok esetén alkalmazható

Az értékegyenlőségi elv lényege

- Az adatalapú folyamat értékegyenlőségének foka mutatja meg, hogy az adatfelhasználásnak vagy adathasznosításnak minősül, előbbinél az értékegyenlőség vélelmezett vagy megalapozott, utóbbinál ellentételezett
- Az adatfelhasználásban a jogosultnak és/vagy adatforrásnak az értékegyenlő cserét tűrnie kell, az értékegyenlőséghez megfelelő érdekeltséget és erős társadalmi legitimációt kell bizonyítani
- Az adathasznosításban döntési autonómia érvényesül, az értékegyenlőséghez pénzben kifejezhető ellentételezésre van szükség
- Az értékegyenlőtlen adatalapú folyamatok jogellenesek

Az elv dogmatikai elfogadhatósága

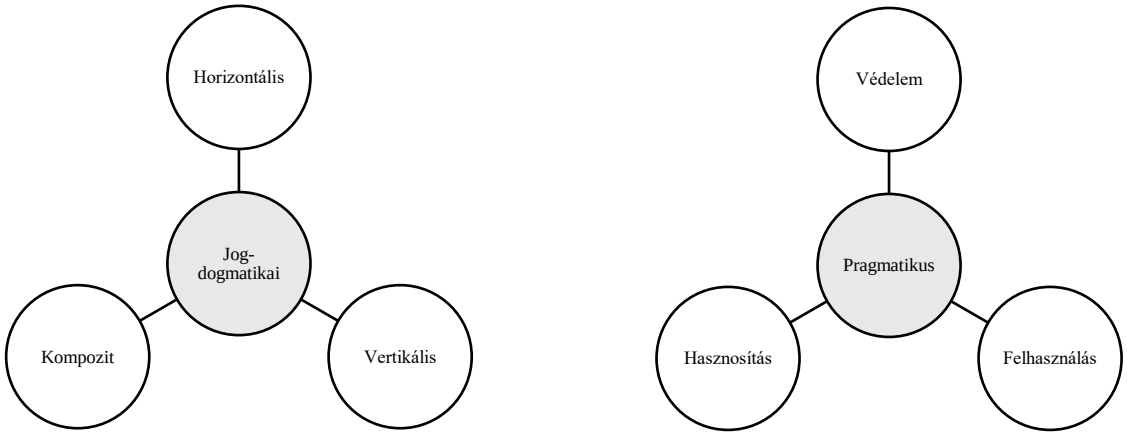
- Az alapjogi korlátozást megvalósító *tűrés* létének, elv általi elismerése elfogadhatónak tűnik, ha a korlátozás alkotmányjogi feltételeinek az megfeleltethető
- Az információs önrendelkezés értelmezhető egyik oldalról döntésként a védelem igénybevételéről, másfelől döntésként az adatokról való rendelkezésről, így az elv szerinti adatokról való döntés alkotmányjogilag elfogadható lehet
- Ha a személyiség kommercializálódását a magánjog garanciális korlátok között, de elfogadhatónak tartja akkor az az adatok monetizációja adatjogilag is elfogadható lehet

4. Az adatjog területeinek részletes vizsgálata

A jelen fejezet az adatjog alterületeinek részletes vizsgálatát végzi el annak érdekében, hogy a teljesebb képet kaphassunk a jelenleg hatályos állapotáról. Így sor kerül a védelem, a felhasználás és a hasznosítás jellegadó tulajdonságainak bemutatására és a legkiemelkedőbb joganyagok elemzésére. A fejezet zárásaként az adatjog közös pontjai feltérképzésre kerülnek, ami megalapozhatja az adatjog jelenének értékelését és így a lehetséges jövőképének feltárását.

4.1. Az adatjog területeinek kétféle csoportosítása

Az eddigiekben az adatjog kétféle csoportosítását végeztük el. A dogmatikai csoportosítás szerint a joganyagot horizontális és vertikális rendelkezésekre osztottuk, azzal, hogy az adatjogon kívüli adatjogi előírásokat kompozit adatjognak neveztük. A pragmatikus csoportosítás szerint a valós élethelyzetekhez igazodva a védelem és használat, azon belül pedig a felhasználás és a hasznosítás joganyagát különítettük el. A csoportosítás alkalmazásán keresztül az egyes területek áttekintésével az adatjog jelenének vizsgálata – a dolgozat lehetőségeihez mérten – teljessé válik, így ezt követően úgy gondolom a jövőbe tekinthetünk. A vizsgálat szervezőelveként a pragmatikus csoportosítást veszem alapul, de azt a teljesség érdekében kiegészítem a dogmatikai elhelyezkedéssel is. Az egyes jogszabályok rendelkezései lehetnek vegyes természetűek, így a területen való elhelyezést az adott jogi aktus jellegadó tulajdonsága fogja eldönteni, tehát bár a DA és a DGA is tartalmaz védelmi előírásokat, azokat egyben, a hasznosítás joga alatt fogom vizsgálni.



4.2. A védelem joga

4.2.1. A védelem jogáról általában

Az eddig azonosítható adatjogi szisztémában a védelem joga a használat mellett a másik nagy területet alkotja. Az adatok adatjogi szerepénél láttuk, hogy a védelem területén az adat gyakorlatilag egy elkövetési tárgy, így ehhez mérten tudjuk a védelem fogalmát meghatározni. Tehát, ha az adat az elkövetési tárgy akkor azonosítanunk kell a védett jogtárgyat (a társadalmi érdeket és az ide vonható életviszonyok körét), amelyet az védeni igyekszik. A szabályozás dualista szemlélete alapján az egyes aktusok között személyes adatokra vonatkozó és minden adatra vonatkozó védelemként tehetünk különbséget.

- *A személyes adatok védelme*

Ahogy fentebb említésre került az adatvédelem elnevezés némileg megtévesztő, mivel egyrészt nem az adatot védi, hanem a természetes személyt, másrészt nem minden adatot, hanem csak a

személyes adatokat.[359] Az adatvédelem tárgya így az olyan adatok védelme, amelyek összefüggésbe hozhatók természetes személyekkel,[360] ebből kiindulva az adatvédelem által védett érték a magánszféra védelme. Ez a kijelentés tágan értelmezendő, mivel beletartozik minden eszköz, megoldás és módszer, amely a védelmi cél elérésére alkalmas, legyen az jogi vagy épp jogon kívüli. Így az adatvédelmen belül az adatvédelmi jogot, a magánélet védelmét szolgáló sajátos jogi védelemként értelmezhetjük.[361]

- *Az információ biztonsága*

Az adatjogi védelem másik nagy területe az információbiztonság. Az információbiztonság az adatvédelmet magába foglaló terület, gyakorlati szempontból lényegesen tágabb annál, mivel a személyes és a nem személyes adatok egyidejű védelmét teszi lehetővé. Az adat vonatkozhat természetes vagy jogi személyre, minősülhet üzleti titokként, minősített adatként vagy állhat bármilyen egyéb korlátozószabály hatály alatt. Az információbiztonság hatóköre független attól, hogy az adat digitálisan, papír alapon vagy egy ember memóriájában kerül tárolásra.[362] Az információ biztonságára vonatkozó előírások bizonyos – közérdek által indokolt – esetekben rendelkeznek jogszabályi háttérrel (pl. Ibtv., NIS 1-2.) és számos ponton támaszkodnak jogon kívüli tényezőkre, mint amilyenek a különböző szabványok (pl. ISO/IEC 27000 szabványcsalád). A szabályozás jellege alapján az információbiztonság független az adat forrásának érdekeitől, az elsődlegesen az adathasználók műveletvégzési háborítatlanságát szolgálja. Ahogy a fogalomból is látható, az információbiztonság nem egyenlő a kiberbiztonsággal. Utóbbi ugyanis kifejezetten a kibertérben létező kockázatokkal szembeni védelemre helyezi a hangsúlyt.[363]

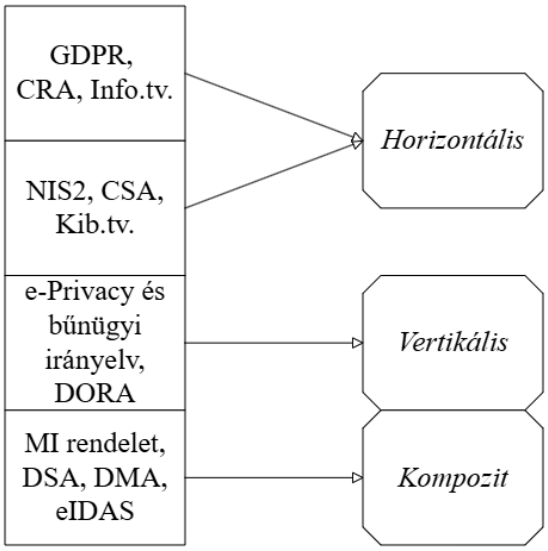
Az információbiztonságtól célszerű még megkülönbözteti az adatbiztonságot, ami az adatvédelmen belül található, de a működését tekintve erős hasonlóságokat mutat az előbbi területtel. Az adatbiztonság tárgya a személyes adat, pontosabban az adat integritása, bizalmassága és rendelkezésre állása.[364] Adatbiztonságot számos jogi vagy jogon kívüli norma írhat elő, de közös vonásuk, hogy mindig – a GDPR 32. cikke nyomán – az adott személyes adatra vonatkozó biztonsági követelményeket kell meghatározzák. Ez alapján adatbiztonsági előírás minden olyan kötelező szabály, amely a személyes adatok védelme érdekében fizikai, logikai vagy adminisztratív intézkedéseket határoz meg. Megjegyzendő, hogy adatbiztonsági előírásokat létrehozhat uniós vagy tagállami jogszabály, polgári vagy közigazgatási jogi jogviszony, de akár egy szervezet belső működésére vonatkozó szabályozó eszköz is.

Mindkét terület szabályozási természetére igaz, hogy a védelem, bár az adatra/információra vonatkozik, valójában az azokat körülvevő rendszerelemekre tud irányulni. Ez abból ered, hogy egy biztonsági esemény minden esetben a hordozón keresztül tud csak megvalósulni.

[359] Streinz, 2021. 3 o.
[360] GDPR 4. cikk 1. pont
[361] Jóri András: Adatvédelmi Kézikönyv, Elmélet, Történet, Kommentár. Budapest, Osiris Kiadó, 2005. 17 o.
[362] Bölcskei Krisztián: GDPR kézikönyv, Új Európai Uniós Adatvédelmi Szabályozás. Budapest, Vezinfó Kiadó és Tanácsadó Kft., 2018. 14 o.
[363] Tóth, 2022. 144 o.
[364] Jóri, 2005. 18 o.

- *A védelem jogának dogmatikai besorolása*

A védelem jogához EU szinten a GDPR, a bűnügyi irányelv, az e-Privacy irányelv és az információbiztonság szabályanyaga (NIS2, CSA, CRA, DORA) tartozik, míg a kiemelt hazai jogforrások az Info.tv. és a Kib.tv. A relevanciája miatt az MI rendelet, a DMA, DSA és az eIDAS néhány védelmi rendelkezése is itt kerül említésre. Az ábrán láthatóan a horizontális védelmi szabályrendszer a GDPR-ból és az Info.tv-ből álló személyes adatok védelme, valamint a CRA kibervédelme. Az un. multi-szektorálisan horizontális szabályok a NIS2, a CSA és a Kib.tv. Minden egyéb előírás vertikális és kompozit szinten jelenik meg.



11. ábra: a védelem joganyaga

4.2.2. Az általános adatvédelmi rendeletről (GDPR – 2016/678/EU rendelet), mint az adatjogi védelem archetípusáról

Elsősorban a személyes adatok védelmének, de egyúttal az adatjogi védelmi szabályozásnak is legnagyobb hatású, horizontális jellegű eleme a GDPR. Előképének tekinthető az adatvédelmi irányelv (95/45/EK irányelv), amely megalkotásakor még nem kifejezetten az alapvető jogok átfogó védelmét tűzte ki célul, sokkal inkább a belső piac működését korlátozó – személyes adatok továbbításával összefüggő – akadályok lebontását, vagyis a tagállamok közötti adatáramlás elősegítését.[365] A GDPR ellentétben az adatvédelmi irányelvvel sokkal nagyobb hangsúlyt fektet a személyes adatok védelmére irányuló előírások modernizálására és fejlesztésére, bár számos, az irányelvből átvett megoldást alkalmaz továbbra is. Legnagyobb eltérése jogforrási formájában rejlik, lévén rendeletként került megalkotásra, amelyből kifolyólag nem igényel és nincs is lehetőség átültető aktusok létrehozására a tagállamok részéről. Ettől függetlenül elmondható, hogy több mint 50 kérdésben enged kifejezetten teret a tagállami jogalkotásnak.[366] Megszövegezése egészen absztrakt, így a horizontális adatjogi szabályoknak megfelelő általánossággal rendelkezik, de ebből kifolyólag az előírásai több logikai lépést igényelnek az alkalmazásuk során. A területi hatálya kiterjedt, un. extraterritoriális jelleggel bír.[367] Tárgyi hatályát tekintve szintén meglehetősen tágan került meghatározásra, ugyanis minden esetben alkalmazandó, ha a személyes adatokat részben vagy egészben automatizált módon kezelik, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésekor, amelyek valamely nyilvántartási rendszer részét képezik. Fontos kivételszabályt állít a Rendelet, amikor kiemeli, hogy nem kell alkalmazni ezeket az adatvédelmi előírásokat, ha az adatokon végzett műveletet a természetes személyek kizárólag személyes vagy otthoni tevékenységük keretében végzik.[368]

[365] Péterfalvi Attila, Révész Balázs, Buzás Péter: Magyarázat a GDPR-ról. Budapest, Wolters Kluwer Hungary, 2018. 25-26 o.
[366] Sepsi Tibor: GDPR útikalauz adatkezelőknek. Budapest, Wolters Kluwer Hungary, 2019. 19-20 o.
[367] Eszteri Dániel, „Az Európai Uniós adatvédelem mindenhová elérő keze: a GDPR alkalmazásának kiterjesztése harmadik országokra, különös tekintettel az amerikai egyesült államokra", Állam- és Jogtudomány, 65 (2). 100 o.
[368] GDPR 2. cikk, un. „háztartási kivétel"

A fennállása óta eltelt idő alatti eseményeket a Bizottság többségében pozitívan értékelte. Ez alapján a GDPR egyenlő feltételeket teremtett a belső piacon működő vállalkozások számára, és technológiasemleges, innovációbarát megközelítése lehetővé tette a bürokrácia csökkentését és a nagyobb fogyasztói bizalom elérését.[369] Összességében az előírásaival kapcsolatban elmondható, hogy kiállták az idő próbáját, a következő felülvizsgálati ciklus lejártáig ezek alapján nem várható számottevő változás a személyes adatok védelmére vonatkozó rezsim működésében.

4.2.2.1. Az alapelvekről

- *Jogszerűség, tisztességes eljárás és átláthatóság*

A GDPR alapján a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.[370] Ezen alapelv szerint az adatkezelés csak abban az esetben tekinthető jogszerűnek, ha az nemcsak az adatvédelmi tárgyú jogszabályoknak, hanem bármely egyéb személyes adatokat érintő normának is megfelel. Ezt tekinthetjük egy párhuzamos jogszerűségi követelménynek, mivel az ágazati jog be nem tartása könnyen vezethet a GDPR által képviselt jogszerűség követelmény megsértéséhez (pl. a számlák kötelező megőrzési idejének megsértése nem csak számviteli jogi probléma, hanem adatvédelmi is).

Tisztességesség esetén különbség van eljárási vagy informatív tisztességesség és szubsztantív vagy érdemi tisztességesség között.[371] Előbbi követelménye, a téves, hiányos, félrevezető tájékoztatás hiánya, vagyis az a kívánatos állapot, amikor az érintett minden információval rendelkezik az adatkezelést illetően.[372] Utóbbi, vagyis a szubsztantív tisztességesség lényegét tekintve az eredmény tisztességességét várja el, vagyis az elfogultság és a diszkrimináció hiányát, az adatkezelési helyzet valós megértését.[373] A GDPR szellemisége alapján a szubsztantív tisztességességet várja el, amelynek immanens elemeként foghatjuk fel az informatív tisztességességet, így valójában mindkettőre szükség van.

Az átláthatóság egy alkotmányos, jogállami követelményként, jogelvként járja át a jogrendszerek többségét.[374] Adatvédelmi szempontból gondolhatunk az egyértelműen meghatározható adatkezelési folyamatok kialakítására, de emellett a szervezeten belüli gyakorlatok áttekinthetőségét, elhatárolhatóságát és nyomonkövethetőségét is jelentheti. Ennek gyakorlati megvalósulását a GDPR 12-14. cikkeinek átlátható tájékoztatási kötelezettsége jelenti elsősorban, de ide vonható még a 15. cikk hozzáférési joga is. Előbbit praktikusan proaktív tájékoztatásnak (mivel azt az érintett magatartásától függetlenül biztosítani kell), míg utóbbit reaktív tájékoztatásnak (mivel csak az érintetti kérelemre kell megtenni) nevezhetjük.

- *Célhoz kötöttség*

Személyes adatokat csak meghatározott, egyértelmű és jogszerű célból lehet kezelni vagy feldolgozni. Az adatokat az eredeti céllal össze nem egyeztethető módon tilos kezelni.[375] A személyes adatok kezelésének legfontosabb garanciája, hogy arra minden esetben pontosan meghatározott, jogszerű cél teljesítése érdekében kerüljön sor. Az alapelv egyszerre tekinthető

[369] COM(2024) 357 final, 14-15 o.
[370] GDPR 5. cikk (1) bekezdés a) pont
[371] European Parliamentary Research Service, Scientific Foresight Unit (STOA): The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (PE 641.530 – June 2020) 30 o.
[372] GDPR (60) preambulumbekezdése
[373] GDPR (71) preambulumbekezdés
[374] Hohmann Balázs: Az átláthatóság értelmezése és követelményrendszere a közigazgatási hatósági eljárások tükrében. Pécs, Novissima Kiadó, 2022. 79 o.
[375] GDPR 5. cikk (1) bekezdés b) pont

alkotmányos és speciálisan adatvédelmi követelménynek, amelynek a személyes adatkezelések során, azok teljes folyamatában érvényesülnie kell. Fontos, hogy a célhoz kötöttség követelményét a már nyilvánosságra hozott személyes adatok tekintetében is alkalmazni kell, azaz a nyilvánosságra hozatal céljától eltérő más célból azok újbóli használata új adatkezelésnek minősül, amely pl. csak megfelelő jogalappal lehetséges.[376] Az elv gyakorlati szempontból lényegi elemei tehát az egyértelmű és egyben jogszerű cél megválasztása és azt követően a személyes adatok ezen céllal összeegyeztethető kezelése.[377]

- *Adattakarékosság*

A személyes adatoknak az adatkezelés szempontjából mindig megfelelőnek és relevánsnak kell lenniük, továbbá szükséges mértékre kell korlátozódniuk.[378] Az alapelvnek megfelelően kizárólag annyi és olyan személyes adat kezelhető, ami szükséges és egyben elégséges az adatkezelés céljának eléréséhez.[379]

- *Pontosság*

Az alapelv értelmében, ha a kezelt személyes adatok körében pontatlan (hiányos, hibás, sérült) adatok merülnek fel, azokat haladéktalanul pontosítani szükséges.[380] A pontosítás meghiúsulása a pontatlan adatok törléséhez kell vezessen.[381] A pontosság elve a célhoz kötöttséghez vezethető vissza, mivel jellemzően pontatlan adatokkal az eredeti célt nem lehet elérni, tehát azok kezelése vélelmezetten jogellenes.

- *Korlátozott tárolhatóság*

Személyes adatok esetén a korlátozott tárolhatóság azt jelenti, hogy azoknak az adatkezelés szempontjából mindig megfelelőnek és relevánsnak kell lenniük, továbbá a szükséges mértékre kell korlátozódniuk.[382] Tehát az ilyen adatok tárolása csak a cél megvalósításához szükséges ideig megengedett,[383] ezáltal az ilyen adatok vonatkozásában tilos a készletező (egyértelműen meghatározott cél nélküli vagy már megvalósított cél érdekében történő) adatkezelés is.

Az adatvédelem ezen az alapelven keresztül fejt ki egyik irányból nyomást az egy adott pillanatban létező adatok globális mennyiségére, amikor maximálja a lehetséges tárolás idejét. Ezzel ellentétes irányból, de hasonló eredményt ér el a releváns adatok rendelkezésre állásának megkövetelésével.

- *Adatbiztonság*

Az alapelv által megkövetelt adatbiztonságnak ki kell terjednie mind az elektronikus és a papír alapú adatkezelésekre, mind ezek fizikai, logikai és adminisztratív védelmi intézkedéseire. Az adatok biztonsága alapelvi szinten került rögzítésre, mint adatkezelői (és adatfeldolgozói) kötelezettség annak követelményével, hogy a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket kell

[376] Jóri András, Soós Andrea Klára, Bártfai Zsolt, Hári Anita: A GDPR magyarázata. Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2018.
[377] Péterfalvi et al., 2018. 81 o.
[378] GDPR 5. cikk (1) bekezdés c) pont
[379] Péterfalvi et all., 2018. 85 o.
[380] GDPR 5. cikk (1) bekezdés d) pont
[381] Jóri et al. 2018.
[382] GDPR 5. cikk (1) bekezdés c) pont
[383] GDPR 5. cikk (1) bekezdés e) pont

végrehajtani annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.[384] A kötelezettség megfogalmazása alapján kiolvasható belőle az információbiztonságból ismert CIA triász,[385] valamint a kockázat-arányos szemlélet is.

Az adatbiztonsághoz kapcsolódóan érdemes megemlíteni az adatvédelmi incidens kategóriáját. Ezek a biztonság olyan sérülését jelentik, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezik.[386] Az incidensek 72 órás határidőjű hatósági bejelentési kötelezettség alá tartoznak, feltéve, hogy azok valószínűsíthetően kockázattal járnak a természetes személyek jogaira és szabadságaira nézve. Amennyiben nem, akkor az adatkezelőnek nyilvántartásvezetési kötelezettsége van, ha pedig az értékelése alapján a kockázatok magasak, akkor indokolatlan késedelem nélkül tájékoztatnia kell a hatóság mellett az érintettet is az adatvédelmi incidensről.[387]

- *Elszámoltathatóság*

Személyes adatoknál az alapelveknek való megfelelést minden adatkezelési és feldolgozási folyamat tekintetében garantálni kell, továbbá az ennek igazolásához szükséges intézkedéseket is meg kell tenni.[388] Az elszámoltathatóság elve adja a GDPR megfelelésből adódó legtöbb adminisztratív kötelezettséget, mivel az annak bizonyításához szükséges dokumentáció meglétét várja el. A gyakorlat ezt az alapelvet a „nem elég jónak lenni, jónak is kell látszani" frappáns megfogalmazással szokta röviden összefoglalni. Tény, hogy az ex ante jellegű jogszerűségi kellékek számos nehézséget okozhatnak, azonban a jogkövetési hajlamot is jelentős mértékben növelik. Az elszámoltathatóság alapját minden esetben már létező kötelezettségek adják, ezért attól lesz nehezen vagy könnyen teljesíthető, hogy milyen előírások „elszámoltatására" irányul.

Az elszámoltathatóság legfőbb dokumentumai a különböző nyilvántartások (pl. incidensnyilvántartás, kérés- és panasznapló stb.) és a jogszerűségi tesztek. Ezek között a 6. cikk (1) bekezdés e) és f) pont jogalapjainál említhető az érdekmérlegelési, valamint a szükségességi és arányossági teszt, továbbá az adatvédelmi hatásvizsgálat elvégzésének kötelezettsége. Előbbi kettőt a fent jelölt jogalapok alkalmazása esetén kell elvégezni, míg utóbbit akkor, ha az adatkezelés jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.[389]

Szintén ide sorolhatók azok az önkéntességen alapuló, a megfelelést a külvilág felé jelző mechanizmusok, mint a magatartási kódexek és a tanúsítás.[390]

- Beépített és alapértelmezett adatvédelem elvei

Bár nem az 5. cikkben kerültek elhelyezésre, az adatvédelmi jog és a GDPR egy különösen fontos előírása a by design és a by default szemlélet megkövetelése. A beépített adatvédelem alapján az adatkezelő a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira

[384] GDPR 32. cikk (1) bekezdés
[385] A mozaikszó jelentése: „confidentiality, integrity and availability" Lásd részletesen: Cameron Hashemi-Pour, „What is the CIA triad?", TechTarget. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA
[386] GDPR 4. cikk 12. pont
[387] GDPR 33-34. cikkek
[388] GDPR 5. cikk (2) bekezdés
[389] GDPR 35. cikk
[390] GDPR 40-43. cikkek

és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során, olyan megfelelő technikai és szervezési intézkedéseket hajt végre, amelyek célja egyrészt az adatvédelmi elvek megvalósítása, másrészt az adatvédelmi követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába. E mellett az alapértelmezett adatvédelem szerint az adatkezelő megfelelő technikai és szervezési intézkedéseket is végre kell hajtson annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.[391]

A két elv rendkívül fontos, ezeken keresztül egyfajta adatjogi összetartó erőként fűzi bele a GDPR „hogyanját" más – főként kompozit – területek joganyagába. Ebben a minőségében a beépített adatvédelem a személyes adatok védelméhez szükséges szabályoknak, mechanizmusoknak és garanciáknak a folyamatba építését jelenti elsősorban, vagyis azt, hogy az adatvédelmi szabályok nem önállóak, hanem az egyéb szabályokba épülnek, a teljes folyamatot áthatják, a ciklus elejétől a végéig, ezáltal az adatkezelési körülmények a tervezés kezdeti állapotában már rendezésre kerülhetnek. Az alapértelmezettség az adatjog „hogyanjaként" inkább az eszközök/rendszerek alapértelmezés szerinti jogszerű működését jelenti. Így a fejlesztési/beszerzési szakaszra vonatkozik, a következménye ideális esetben, hogy a felhasználói hiba és a külső támadások esélye drasztikusan csökkenhet, mivel a rendszerek és eszközök megfelelő használata nem a felhasználótól vagy szervezeti szabályoktól függ.

4.2.2.2. Az adatkezelési jogalapokról

Az adatvédelmi jogalapok már a 80-as évektől az adatvédelmi szabályozás egyik legfontosabb jellemzőjévé váltak. Kezdetekben Magyarországon egy úgynevezett dichotóm rendszert alkottak, amelyben kettő jogalap, a kötelező törvényi előírás és az érintett hozzájárulása szerepelt felhatalmazásként. Ehhez képest mára hat jogalap áll az adatkezelők rendelkezésére, a jogintézmény megkülönböztetett jelentőségét pedig a tény, hogy a GDPR „az adatkezelés jogszerűsége" cím alatt került elhelyezésre remekül bizonyítja. Ez alapján azt az uralkodó álláspontot is rögzíthetjük, ami szerint megfelelő jogalap hiányában az adatkezelés jogszerű egyáltalán nem lehet.[392] Szintén fontos kiemelni, hogy bár szabadon használható bármely jogalap, egy adatkezelésnek egyszerre csak egy érvényes jogalapja lehet, az adatkezelőnek pedig nem egy bizonyos személyes adat, hanem az azzal kapcsolatos adatkezelési folyamat vonatkozásában kell megtalálnia azt. Ezt az a tény is alátámasztja, hogy különböző célok érdekében, eltérő jogalapok alapján is lehetséges ugyanazt az adatkört kezelni (pl.: szerződésben szereplő név megegyezik a kapcsolattartáshoz használt névvel és akár a direkt marketing célú hírlevél feliratkozásban szereplő névvel).[393] A hat, jelenleg GDPR-ban szereplő jogalap az alábbiakban kerül ismertetésre.

- *A hozzájárulás alapján történő adatkezelés*[394]

[391] GDPR 25. cikk (1)-(2) bekezdés
[392] Péterfalvi et al., 2018. 29-32 o.
[393] Péterfalvi et al., 2018. 111 o.
[394] GDPR 6. cikk (1) bekezdés a) pontja

Ezen hosszú múltra visszatekintő jogalap esetén az érintett kifejezett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez. Az információs önrendelkezési jogot leginkább kiszolgáló jogalap, jellemzője, hogy bekérésének lehetséges esetei gyakorlatilag végtelenek, azonban a valódi és jogszerű hozzájárulás minden feltételének megfelelő nyilatkozatok jellemzően hézagosak, így bár ez a jogalap továbbra is sűrűn használt, számos buktatóval kell számolnia az adatkezelőnek. Mindig képes kell legyen arra, hogy a hozzájárulás megadását igazolni tudja (tehát rögzítettnek és visszakereshetőnek kell lennie), valamint azt is bizonyítania kell, hogy azt az érintett önkéntesen adta meg. Az egyetlen jogalap, amelynél speciális tájékoztatási szabályok vannak érvényben, továbbá a legerőteljesebb rendelkezési jogot adja az érintettnek, mivel lehetővé teszi számára, hogy a hozzájárulását bármikor visszavonhassa, ezzel megakadályozva az adatkezelési tevékenység folytatását.[395]

- *Szerződés megkötéséhez vagy teljesítéséhez szükséges adatkezelés*[396]

A jogalap kettő esetben használható, egyfelől a szerződést előkészítő lépések során, másfelől az érintettel kötött szerződés tényleges teljesítése alatt. A legfontosabb feltételei, hogy a (leendő) szerződő fél az érintett legyen, illetve, hogy az adatkezelésnek a szerződéses szolgáltatáshoz szorosan kell kapcsolódnia. A szerződések fogalmi meghatározására, jogszerűségére és érvényességi feltételeire a mögöttes jog (pl. polgári vagy közigazgatási jog) irányadó.[397]

- *Jogi kötelezettség teljesítéséhez szükséges adatkezelés*[398]

A c) pontban olvasható jogalap esetén az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges. Számos jogi előírás szóba jöhet, amelyek személyes adatok kezelését írják elő, vagy követelik meg. Első esetben a jogszabály konkrétan előírja, hogy milyen adatokat, milyen célból és milyen időtartamban kell kezelnie az adatkezelőnek. A második eset, amikor a jogszabály olyan jogi kötelezettséget ír elő, amelyet csak nyilvánvalóan személyes adatok kezelésével lehet betartani, azonban az Info.tv. 5.§ (3) bekezdésében megkövetelt részletességgel[399] nem írja le az adatkezelés körülményeit. Ilyen esetekben az adatkezelő (jogállásától függően) döntésén múlhat, hogy a szükségesség és arányosság vizsgálatával vagy érdekmérlegelési teszt útján fogja a törvény előírásainak betartásához fűződő közérdeket, illetve magánérdeket bizonyítani, vagy úgy ítéli meg, hogy eléggé egyértelmű maga a kötelezettség, és annak teljesítéséhez szükséges adatkezelés minden lényeges körülménye is, tehát marad a c) pont alkalmazásánál.

- *Létfontosságú érdek védelme érdekében szükséges adatkezelés*[400]

Előfordulhatnak olyan körülmények, amelyekben az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges és más jogalap a szóban forgó adatokhoz nem áll rendelkezésre. Az élethelyzetek sokfélék lehetnek, az esetek többségében az élet, testi épség és egészség védelme érdekében kerülhet sor az alkalmazására,

[395] A 29. cikk szerinti munkacsoport iránymutatása az (EU) 2016/679 rendelet szerinti hozzájárulásról, WP259 rev.01
[396] GDPR 6. cikk (1) bekezdés b) pont
[397] Jóri et al. 2018.
[398] GDPR 6. cikk (1) bekezdés c) pont
[399] Legalább a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát a kötelezettséget előíró joganyagnak kell meghatároznia.
[400] GDPR 6. cikk (1) bekezdés d) pont

de nem kizárt az alkalmazása az érintett nyilvánvaló érdekében álló, vagyoni kár bekövetkezésének elkerülésére, illetve a bekövetkezés esélyének csökkentésére.[401]

- *Közérdekű feladat ellátásához, közhatalmi jogosítvány gyakorlásához szükséges adatkezelés*[402]

A rendelkezés két fordulatra bontható, közérdekű feladat ellátásával és közhatalom gyakorlásával kapcsolatos adatkezelésre. A jogalappal kapcsolatban fontos, hogy a közszféra „szubszidiárius" felhatalmazásának tekinthető, azzal a megkötéssel, hogy a mögötte álló érdekek uniós vagy tagállami jognak kell meghatároznia. Megjegyzendő, hogy a közhatalmat gyakorló, illetve közfeladatot ellátó szervek tevékenységével összefüggésben végzett adatkezelésekkel kapcsolatban a Hatóság 2018. évi beszámolójában kiemelte, hogy ezen szervek tekintetében mind a közjogi, mind a magánjogi jogviszonyok esetén az e) pont szerinti jogalap „mintegy magába olvasztja, elnyeli a további adatkezelési jogalapokat". Ezzel a kijelentéssel kapcsolatban a gyakorlat több különböző, egymással akár szöges ellentétben lévő álláspontot is magáévá tett az elmúlt években, azonban jelenlegi – a hatósági szándékhoz talán legközelebb álló – érvelés szerint ezzel a Hatóság egy lehetséges értelmezést kívánt mindössze bemutatni és nem volt célja kizárni az alkalmazási körből minden egyéb jogalapot.

- *Az adatkezelő vagy harmadik fél jogos érdeke alapján végzett adatkezelés*[403]

A jogalap meglehetősen hasonló az előző pontban ismertetetthez, azonban ebben az esetben az alkalmazási korlátot az jelenti, ha a jogos érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek a személyes adatok védelmét teszik szükségessé. Különösen nagy hangsúlyt kell fektetni ilyen esetekben az érdekmérlegelési tesztre, amelyben alaposan körül kell járni az adatkezelés körülményeit, fel kell tárni annak okait, várható következményeit és az érintettre gyakorolt hatásait, továbbá igazolni kell azt is, hogy az adatkezelés a Rendelet – és egyéb jogszabályok – előírásainak és az adatkezelő adatbiztonsági követelményeinek megfelelően történik. A tesztben feltétlenül ki kell térni a tervezett adatkezelés szükségességére és hatásainak arányosságára, a jogos érdek fennállásának igazolására és az érintett érdekeinek vizsgálatára. Fontos, hogy ezen jogalap nem alkalmazható a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre.

4.2.2.3. Az érintetti jogokról

Az érintetti jogok az információs önrendelkezési jog elemi aspektusaiként is értelmezhetők.[404]

- *A tájékoztatáshoz való jog*

Az adatok kezelésének megkezdése előtt az adatkezelő köteles az érintettet az adatkezelés legfontosabb körülményeiről tájékoztatni.[405] Ezt az átláthatóság alapelvével összefüggésben proaktív tájékoztatásnak is nevezhetjük;

- *A hozzáféréshez való jog*

Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha igen azokhoz hozzáférjen. Ilyen esetben egyrészt a tájékoztatási kötelezettség személyre szabott megvalósítását, valamint saját

[401] Info.tv. 5. § (1) bekezdés c) pont
[402] GDPR 6. cikk (1) bekezdés e) pont
[403] GDPR 6. cikk (1) bekezdés f) pont
[404] Péterfalvi et al., 2018. 144 o.
[405] GDPR 13-14. cikk

személyes adatainak másolatát kérheti (feltéve, hogy az nem érinti hátrányosan mások jogait és szabadságait), valamint be is tekinthet azokba.[406] Ezt reaktív tájékoztatásnak nevezhetjük;

- *Helyesbítéshez való jog*

A pontatlan személyes adatokat indokolatlan késedelem nélkül helyesbíteni szükséges, ezt az adatkezelő mulasztása esetén az érintett is kérheti, az adatok kiegészítése, módosítása mellett;[407]

- *Törléshez való jog*

Az érintett bizonyos esetekben jogosult arra, hogy kérésére az adatkezelő által kezelt személyes adatait töröljék, amely az információs önrendelkezés legerősebb megnyilvánulási formájaként jelenik meg a GDPR-ban. Törlést így például a cél megvalósulása, az adatkezelés jogellenessége esetén vagy a GDPR 6. cikk 1) bekezdés a) pontja szerinti jogalap alkalmazásakor lehet kérni; [408]

- *Az elfeledtetéshez való jog*

Az elfeledtetéshez való jog értelmében, ha az adatkezelő valamilyen jogszerű okból nyilvánosságra hozta az adatot, és azt törölni köteles, akkor ésszerűen elvárható lépéseket kell tegyen annak érdekében, hogy tájékoztasson más adatkezelőket a szóban forgó adatok törlésének szükségességéről.[409] Ez a digitális adatok fentebb taglalt nonrivalitásában és másolhatóságában rejlő kockázatokat hivatott mérsékelni azáltal, hogy az adatok törlésének támogatásában az adatkezelő köteles részt vállalni;

- *Az adatkezelés korlátozásához való jog*

Az adatkezelőnek az érintett kérésére korlátoznia kell az adatkezelést, például, ha az érintett vitatja a kezelt személyes adatok pontosságát, vagy ha az adatkezelés jogellenesnek bizonyul, de az érintett ellenzi a kezelt személyes adatainak törlését, valamint akkor is, ha az érintett tiltakozott az adatkezelés ellen és ennek kivizsgálása még folyamatban van.[410] A korábban zárolásként ismert jogintézmény meglehetősen technikai, járulékos jellegű. Leginkább más jogok gyakorlását vagy kötelezettségek teljesítését támogatja.

- *Az adathordozhatósághoz való jog*

Az érintett jogosult az általa az adatkezelő rendelkezésére bocsátott adatait tagolt, széles körben használt formátumban megkapni. A kapott adatokat jogosult más adatkezelőhöz továbbítani vagy az adatkezelő által továbbíttatni, amennyiben az adatkezelés az adatkezelő és az érintett között fennálló szerződésen vagy hozzájáruláson alapul és automatizált módon történik.[411] Az adathordozhatósághoz való jog az adathasznosítás területén tehet szert nagyobb jelentőségre azáltal, hogy a személyes adatok mobilitását szolgálja, az érintett önrendelkezési jogán keresztül.[412]

- *Tiltakozáshoz való jog*

---

[406] GDPR 15. cikk
[407] GDPR 16. cikk
[408] GDPR 17. cikk (1) bekezdés
[409] GDPR 17. cikk (2) bekezdés
[410] GDPR 18. cikk
[411] GDPR 20. cikk
[412] Jó példák az adatok mobilizálására a DA 3. és 4. cikkei, továbbá ezt az elgondolást erősíti a WP29 munkacsoport WP 242 rev.01 számú iránymutatása, ahol a jogosultság egyik kiemelt célkitűzésekét jelölik, hogy az érintettek aktív szerepét támogassa az adatökoszisztémában.

Az érintett saját helyzetével kapcsolatos okokból (kivéve a közvetlen üzletszerzési célt, ahol ilyen okok bemutatására nincs szükség) tiltakozhat az adatai kezelése ellen, kiemelten, ha az adatkezelés közérdekű vagy közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához vagy, ha az adatkezelés az adatkezelő vagy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, illetve, ha az adatkezelés közvetlen üzletszerzési célra irányul. A megalapozott és megfelelő tiltakozás esetén az adatkezelő meg kell szüntesse az adatkezelést, kivéve, ha arra kényszerítő erejű jogos indokok vagy jogi igények érvényesítése miatt továbbra is szükség van.[413]

4.2.2.4. Az adatfeldolgozókra vonatkozó rendelkezésekről

Személyes adatok feldolgozása esetén a GDPR kógens előírásokat határoz meg, amelyek az ilyen tárgyú adatfeldolgozói szerződések tartalmára jelentős hatásai vannak. Így például:

- Az adatfeldolgozó az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót nem vehet igénybe.[414]
- Tagállami vagy uniós jog hiányában az adatfeldolgozó által végzett adatkezelést – az adatkezelés tárgyát, időtartamát, jellegét és célját, az adatok és adatforrások típusát, kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó – a felek között fennálló szerződésnek kell meghatároznia.[415]
- Az adatfeldolgozó a személyes adatokat kizárólag az adatkezelő utasításai alapján kezelheti,[416] az adatokhoz hozzáférők körét a szerződésben foglaltakra és az adatkezelő érdekeire tekintettel köteles korlátozni, illetve az adatok elvárt titkosságát megőrizni.[417]
- Segítenie kell az adatkezelőt az adatfeldolgozói tevékenységét értintő kérések, panaszok, illetve az ilyen adatokat érintő biztonsági incidensek rendezésében.[418]
- Az adatfeldolgozó a szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog a személyes adatok tárolását írja elő.[419]

4.2.2.5. Összegzés az adatvédelmi rendeletről

A GDPR az adatjog horizontális tartományának első és alapvető eleme, szabályozási megoldásai az utóbb megalkotott joganyagot vizsgálva azt mondhatjuk, hogy mintaadó jellegűek. A GDPR számos korábbi megközelítést szintetizált egy kiterjedt és koherens szabályanyagban, ami sok tekintetben irányadóvá vált a hasonló (digitalizációval összefüggő) jogi aktus számára. Az adatjogi összetartásban – személyes adatok esetén de iure, nem személyes adatok esetén de facto – megjelenésének a GDPR koordinatív és rendszerező szerepe évekig egyedülálló volt, azonban az egyéb horizontális szabályok, mint a DGA, DA és CRA megjelenésével jelentőségét továbbra is megtartotta.

4.2.3. A védelem további elemeiről

4.2.3.1. Az e-Privacy irányelvről (2002/58/EC irányelv)

Az irányelv a személyes adatok és a magánélet védelmét szabályozza az elektronikus hírközlési ágazatban, a célja – a GDPR-hoz hasonlóan – a tagállami rendelkezések harmonizációja a

[413] GDPR 21. cikk
[414] GDPR 28. cikk (2) bekezdés
[415] GDPR 28. cikk (3) bekezdés
[416] GDPR 28. cikk (3) bekezdés a) pont
[417] GDPR 32. cikk, 28. cikk (3) bekezdés b) pont
[418] GDPR 28. cikk (3) bekezdés e), f) pontok
[419] GDPR 28. cikk (3) bekezdés g) pont

személyes adatok védelme, valamint az ilyen adatoknak az EU-n belüli szabad mozgása terén.[420] A hatókörét tekintve az irányelvet a nyilvános hírközlő hálózaton vagy azzal összefüggésben kezelt személyes adatokra kell alkalmazni.[421] Tehát az irányelv olyan szektorális szabályokat állapít meg, amelyek a személyes adatok kezelésének biztonságát és az érintett jogvédelmét szolgálják irányelvi formában (az átültetésére nagyrészt az Eht. rendelkezései között került sor[422]).

Olyan rendelkezéseket tartalmaz, mint a közlések és forgalmi adatok titkossága[423] (vagyis lehallgatás tilalma[424]) vagy az ilyen adatok korlátozott megőrizhetősége.[425] Az irányelv hozzájárulás alkalmazására vonatkozó rendelkezései a mai napig nagy hatással vannak, pl. a weboldalak működésére (sütikezelés) és a hírlevél feliratkoztatás menetére, valamint a helymeghatározási adatok gyűjtésére. E szerint az emberi beavatkozás nélküli automatizált hívó- és távközlési rendszerek, berendezések, illetve elektronikus levelek közvetlen üzletszerzési célból történő használata kizárólag az ahhoz előzetesen hozzájáruló előfizetők vonatkozásában lehetséges. Ez a fajta hozzájárultatási kényszer értelemszerűen csak természetes személyek esetén áll fenn, azonban kivételt képeznek azok, akik a felhasznált adataikat ügyfélként korábban megadták.[426]

Az irányelv felülvizsgálata és rendeleti formába való átültetése hosszú ideje folyamatban van, de egyelőre nem jutott túl a javaslati stádiumon. Az új szabályozás célja, hogy jobban illeszkedjen az átalakult digitális környezethez és a GDPR-hoz.[427] Az e-Privacy rendeletjavaslat nagy előnye lenne, hogy a – GDPR-hoz hasonló jellegű, kiterjesztetett védelmet nem személyes adatok és így jogi személyek esetén is megerősítené.[428]

4.2.3.2. A bűnügyi irányelvről (2016/680/EU irányelv)

A bűnügyi irányelv a – GDPR mellett – az EU adatvédelmi jogi reformjának másik képviselője. A reform a korábbi szabályozáshoz képest határozottabb jogegységesítési törekvésként fogható fel, a bűnügyi irányelv – jogforrási formájából kifolyólag is – minimumharmonizációs jellegre szorítkozott, ezzel a tagállamonként eltérő követelményrendszer felállításának lehetőségét megőrizte. Az irányelv hatókörével kapcsolatban megjegyzendő, hogy nem csupán a tagállami adatcsere tárgyát képező személyes adatok kezelésére, hanem minden, a hatóságok általi, bűnügyi területen végzett adatkezelési tevékenységre kiterjed, függetlenül a kezelt adatok forrásától.[429] Az irányelv tartalmi szempontból nagy hasonlóságokat mutat a GDPR-al. A rendelkezéseinek döntőrésze az Info.tv-ben került elhelyezésre, azonban e mellett még tizenegy hazai jogszabály vesz részt a célkitűzéseinek elérésében.

---

[420] e-Privacy irányelv 1. cikk (1) bekezdés
[421] e-Privacy irányelv 3. cikk
[422] Az elektronikus hírközlésről szóló 2003. évi C. törvény
[423] e-Privacy irányelv 5. cikk
[424] Az e-Privacy irányelv 15. cikke alapján a tilalom nem vonatkozik a nemzetbiztonság (vagyis az állam biztonsága), a nemzetvédelem és a közbiztonság védelmére, valamint a bűncselekmények, illetve az elektronikus hírközlési rendszer jogosulatlan használata megelőzésére, kivizsgálására, felderítésének és üldözésének a biztosítására.
[425] e-Privacy irányelv 6. cikk
[426] e-Privacy irányelv 13. cikk (1)-(2), (5) bekezdés
[427] Európai Bizottság, „Javaslat az elektronikus hírközlési adatvédelmi rendeletre”. Elérhető: https://digital-strategy.ec.europa.eu/hu/policies/eprivacy-regulation
[428] Tóth, 2024. 96-97 o.
[429] Péterfalvi et al., 2018. 14-15 o.

Az irányelv célja a büntetőeljárásban résztvevők – tanúk, áldozatok vagy gyanúsítottak – átfogó keretetek létrehozásával történő személyes adatainak magas szintű védelme, a rendőrség és a büntető igazságszolgáltatás területe egyedi jellegének figyelembevételével.[430]

4.2.3.3. Az Info.tv-ről (2011. évi CXII. tv.)

A törvény célja az Alaptörvény VI. cikke alapján, az ott biztosított alapjogok (információs önrendelkezés/személyes adatok védelme és az információszabadság) érvényesítése érdekében, hogy meghatározza az információs jogok tartalmát és biztosítsa e jogok hatékony érvényesülését. Az Info.tv. folytatva elődje, az Avtv.[431] által kijelölt utat, rögzíti a különböző adatkezelések jogszerűségének általános feltételeit, ezen belül egyrészt a személyes adatok kezelésének garanciális szabályait és az érintett információs önrendelkezési jogait, másrészt a közérdekű adatokhoz való hozzáférés módját, valamint az e jogok érvényesítésére rendelkezésre álló jogorvoslati lehetőségeket, továbbá létrehozza a magyar felügyeleti hatóságot (NAIH[432]) és szabályozza annak feladat és hatáskörét. Az Info.tv. alapvetően követi az információs jogok magyar szabályozásában kikristályosodott rendszert, fogalmakat és elveket.[433] A GDPR rendeleti jellegéből adódóan az Info.tv. szabályozási köre lekorlátozódott a Rendelet által szabadon hagyott területekre, valamint a rendelet szövegének szükségszerinti pontosítására.

4.2.4. Az információbiztonság szabályanyagáról

Az EU információbiztonságra és kibervédelemre vonatkozó joganyaga az elmúlt évek folyamatos fejlődése által egy komplex rendszerré alakult. Ezek között találhatók horizontális és vertikális szabályok is, jogforrási formájukat tekintve mostanra többségében rendeletként kerültek megalkotásra. Az EU szabályozási megközelítése abból a felismerésből ered, hogy az ex post jellegű represszív/reparatív előírások kevésbé alkalmasak a jogszerű állapot fenntartására, mint az ex ante prevenció megvalósítása. Ezért a fő motívuma a joganyagnak az un. reziliencia vagy ellenállóképesség javítása egyfelől EU szinten, másfelől kiemelt ágazatok tekintetében.[434] A négy uniós jogszabály mellett a legfontosabb hazai jogszabály is röviden bemutatásra kerül.

4.2.4.1. A kiberbiztonsági jogszabályról (CSA - 2019/881/EU rendelet)

A CSA rendeleti formában jött létre, a célja a kiberbiztonsági kockázatok csökkentése az Európai Unióban, ehhez a belső piac megfelelő működését törekszik biztosítani és ezzel egyidejűleg az Unión belül a kiberbiztonság, a kiberellenálló képesség és a kiberbiztonságba vetett bizalom magas szintjét igyekszik elérni. Az előírásai két nagy csoportra oszthatók, az egyik az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) működésének megerősítése, a másik az uniós kiberbiztonsági tanúsítási keretrendszer létrehozása.[435] Az ENISA működésétől általánosságban az egységesen magas szintű kiberbiztonság elérését várják, többek között annak révén, hogy aktív támogatást nyújt a tagállamoknak, valamint az uniós intézményeknek, szerveknek és hivataloknak a kiberbiztonság javításához. Az ENISA-nak az uniós intézmények, szervek és hivatalok, valamint egyéb uniós érdekelt felek számára a kiberbiztonsággal

[430] EURLEX, „A rendőri és büntető igazságszolgáltatási szervek által használt személyes adatok védelme" elnevezésű dokumentum összefoglaló. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:310401_3

[431] a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (továbbiakban Avtv.)

[432] Nemzeti Adatvédelmi és Információszabadság hatóság

[433] 2011. évi CXII. törvény indokolása az információs önrendelkezési jogról és az információszabadságról

[434] Tóth, 2024. 68-69 o.

[435] CSA 1. cikk

kapcsolatos tanácsadás és szakértelem referenciapontjaként kell szolgálnia.[436] Összegezve a fő feladatai az uniós és tagállami kiberbiztonsági intézkedések támogatása, tagállamok és uniós szervek közötti együttműködés elősegítése és a kiberbiztonsági tudatosság növelése, illetve a közösségi információmegosztás.[437] E mellett részt kell vállaljon a kiberbiztonsági incidensek kezelésében,[438] kutatás és innováció támogatásában,[439] kiberbiztonsági tanúsítási folyamatban[440] és nemzetközi koordinációban.[441]

Az ENISA-ra vonatkozó rendelkezések mellett a kiberbiztonsági tanúsítási keretrendszer kiépítésében van nagy szerepe a rendeletnek. A rendszer az uniós piacra kerülő digitális termékek megfelelő biztonsági szintje érdekében az IKT-termékek,[442] -szolgáltatások és folyamatok tekintetében kerül bevezetésre. A tanúsítási keretrendszer egy mechanizmust határoz meg az európai kiberbiztonsági tanúsítási rendszerek létrehozására, valamint annak tanúsítására, hogy az e rendszerekkel összhangban értékelt IKT- termékek, IKT-szolgáltatások és IKT-folyamatok megfelelnek meghatározott biztonsági követelményeknek, a termékek, szolgáltatások és folyamatok által tárolt vagy továbbított vagy kezelt adatok, vagy az általuk ellátott funkciók vagy kínált szolgáltatások rendelkezésre állásának, hitelességének, sértetlenségének vagy titkosságának, azok teljes életciklusa alatti védelme céljából.[443] Az európai kiberbiztonsági tanúsítási rendszerek az „alap", a „jelentős" és a „magas" megbízhatósági szintek közül egy vagy több szintet határozhatnak meg. A megbízhatósági szintnek a biztonsági események valószínűsége és hatása szempontjából arányban kell állnia a termék, szolgáltatás vagy folyamat rendeltetés szerinti használatához kapcsolódó kockázat szintjével.[444]

Összegezve a CSA a (multi-szektorálisan) horizontális kibervédelem elérésére kiterjesztette és megerősítette az ENISA működési feltételeit, valamint egy általános tanúsítási rendszert vezetett be, amely a kockázat-arányos védelem egységes szintjét támogatja az egész EU-ban.

4.2.4.2. A pénzügyi kibervédelmi jogszabályról (DORA - 2022/2554/EU rendelet)

A DORA, rendeleti formában létrejött jogi aktus. A megalkotásának elsődleges célja a pénzügyi szektor digitális működési rezilienciájának megerősítése.[445] Az Európai Unió felismerte, hogy az információs és kommunikációs technológiák egyre fontosabb szerepet töltenek be a pénzügyi szolgáltatások működésében, miközben az IKT-kockázatok és a kibertámadások növekvő fenyegetést jelentenek a pénzügyi stabilitásra és a piac integritására.[446] A rendelet az információbiztonság joganyagának szektorális elemének tekinthető, így például a NIS2 irányelv (multi-szektorálisan) horizontális előírásaival szemben alkalmazási elsőbbséggel rendelkezik a hatálya alá tartozó ágazaton belül.[447]

A DORA nagy hangsúlyt fektet a belső rendszerek szabályozottságára és a szervezeti tudatosság növelésére. Az IBIR[448] területről ismert és az adatvédelemben is már alkalmazott megoldások

[436] CSA 3. cikk
[437] CSA 4. cikk
[438] CSA 7. cikk
[439] CSA 8. cikk
[440] Hoeren, Pinelli, 2024. 228 o.
[441] CSA 10. cikk
[442] Információs és kommunikációs technológia
[443] CSA 46. cikk
[444] CSA 52. cikk
[445] DORA 1. cikk
[446] Hoeren, Pinelli, 2024. 228 o.
[447] Tóth, 2024. 83-84 o.
[448] Információbiztonság-irányítási rendszer

kerültek nevesítésre, mint a szervezeti politika megalkotása, irányítási rendszer bevezetése, kötelező belső felülvizsgálatok és ellenőrzések lefolytatása, valamint a feladat- és felelősségi körök egyértelmű elhatárolásának kötelezettsége.[449] A pénzügyi szervezetektől a kockázatkezelés kiemelt szintjét várja el.[450] Nyomon kell követniük az IKT-rendszereiket érintő potenciális kockázatokat, ideértve a kibertámadásokat, rendszerszintű hibákat és egyéb fenyegetéseket. Az azonosított kockázatot dokumentálni és értékelni kell, annak a szervezet működésére és a pénzügyi stabilitására gyakorolt lehetséges hatásaival együtt. A megfelelő védelem és a válaszintézkedések megszervezése érdekében a pénzügyi szervezeteknek folyamatosan ellenőrizni kell a rendszerek és -eszközök biztonságát és működését, illetve minimalizálni szükséges az IKT-rendszereket érintő kockázat hatását megfelelő biztonsági eszközök, szabályzatok és eljárások bevezetésével. Ezek célja biztosítani az IKT-rendszerek rezilienciáját, folytonosságát, továbbá fenntartani az adatok rendelkezésre állására, hitelességére, integritására és bizalmas kezelésére vonatkozó magas szintű normákat.[451] Rögzíti továbbá az üzletmenet-folytonossági,[452] illetve az adatmentési és helyreállási[453] protokollok szükségét. Érdemes továbbá még kiemelni, hogy a DORA is bevezet egy jelentéstételi kötelezettséget, a jelentős IKT-vonatkozású eseményeket ugyanis a pénzügyi szervezeteknek be kell jelenteniük a releváns illetékes hatóságnak.[454]

Összegezve a DORA a pénzügyi szektorra dedikált ágazati szabályokat állapít meg az információbiztonság és informatikai-ellenálló képesség szintjének növelése érdekében. A szervezési-szabályozási, valamint a kifejezetten védelmi intézkedések a már létező IBIR és adatvédelmi irányokat követik, a kockázat-arányosság elvének deklarálásával,[455] fenntartva az adatjogi előírásoknál tapasztalható összetartást.

4.2.4.3. A NIS2 irányelvről (2022/2555/EU irányelv)

A NIS2 irányelvvel kapcsolatban fontos kiemelni, hogy létezett egy elődjogszabálya, a NIS1 irányelv.[456] A magyar jogba való átültetést elsődlegesen az alább tárgyalt Kib.tv. szolgálja,[457] így számos rendelkezés ott kerül értelmezésre. A NIS1 irányelvhez képest a NIS2 irányelv kibővítette az alkalmazási kört, és több gazdasági ágazatot vont be (pl. digitális szolgáltatások). Az általános keretrendszer biztosításán túl kiterjesztett és részletes kiberbiztonsági követelményrendszert és jelentéstételi kötelezettséget vezetett be. E mellett a hatósági felügyeleti intézkedéseken és a szankciós lehetőségeken szigorított, ezzel egyúttal erősebb uniós koordinációs erőt is lehetővé tett a kiberfenyegetésekkel szembeni együttes és összehangolt fellépések terén.[458]

A NIS2 irányelv kiemelt előírásai között szerepel a bizalom növekedéséhez való hozzájárulás és a tagállamok közötti gyors és hatékony operatív együttműködésben a CSIRT-ek[459] szerepének megerősítése.[460] Szintén ide tartozik a nagyszabású kiberbiztonsági események és

[449] DORA 5. cikk
[450] A DORA 28-29. cikkei a kockázatkezelési kötelezettséget kiterjesztik a pénzügyi szektorba beszállító IKT szolgáltató harmadik felekre is.
[451] DORA 8-10. cikkek
[452] DORA 11. cikk
[453] DORA 12. cikk
[454] DORA 19. cikk
[455] Hoeren, Pinelli, 2024. 272 o.
[456] 2016/1148/EU irányelv a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
[457] Kib.tv. 91. §
[458] Tóth, 2024. 80-84 o.
[459] Számítógép-biztonsági eseményekre reagáló csoportok
[460] NIS2 irányelv 10-11. és 15. cikkek

válságok operatív szintű összehangolt kezelésének támogatására, illetve a releváns információk tagállamok és az Unió intézményei, szervei, hivatalai és ügynökségei közötti rendszeres cseréjének biztosítására létrehozott Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatának (EU-CyCLONe) megalkotása.[461] A szervezetek kiberbiztonsági követelményei között olyan visszatérő kötelezettségeket találhatunk, mint a kockázatelemzés és eseménykezelés, üzletmenet-folytonosság biztosítása, kriptográfiai eszközök használata vagy a tudatosságnövelő hatású, alapvető kiberhigiéniai gyakorlatok és kiberbiztonsági képzések tartása.[462] Az említett jelentéstételi kötelezettség szintén az adatjogi jogalkotási séma szerint, pl. a GDPR incidenskezelési szabályaihoz hasonló.[463]

Összegzésként azt mondhatjuk, hogy a NIS2 irányelv is követi az adatjog szabályozási mintázatát és megjeleníti az előírásai között a koordinatív, egységes alkalmazásra való törekvést, a kockázat-arányossági kritériumot,[464] az ex ante kockázatelemzési és -kezelési, valamint jelentéstételi mechanizmusokat.[465]

4.2.4.4. A kiberrezilienciáról szóló jogszabályról (CRA - 2024/2847/EU rendelet)

A CRA, mint uniós rendelet a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelmények létrehozását szolgálja, a célja, hogy biztosítsa a digitális elemeket tartalmazó termékek magas szintű biztonságát az EU egységes piacán. Egyedülállónak mondható a maga nemében, mint az első, kötelező érvényű, expressis verbis horizontális szabályozás az EU-ban, amely minimumkövetelményeket határoz meg a digitális termékek kiberbiztonságára.[466] A CRA szabályozásának fókuszában azok a digitális elemeket tartalmazó termékek állnak, amelyek rendeltetése vagy észszerűen előrelátható használata magában foglal egy eszközhöz vagy hálózathoz való közvetlen vagy közvetett logikai vagy fizikai *adat*kapcsolatot. Ez alól például kivételt képeznek az orvostechnikai[467] és az in vitro diagnosztikai eszközök,[468] amelyekre szektorális (kompozit) szabályozás létezik.[469]

A rendelet a célját alapvetően kevesebb sebezhetőséggel rendelkező és biztonságosabb digitális termékek létrehozásának és piacra jutásának garantálásával igyekszik elérni, amihez egy standardizált kibervédelmi keretrendszert hoz létre, a termékeknek mind a szoftver, mind hardver komponensei vonatkozásában. Ezzel kapcsolatban egyfelől nagyobb átláthatóság biztosítását is várja a piaci szereplőktől, de egyúttal a fogyasztók tudatosságának a növelését is célozza, abban bízva, hogy a kiberbiztonság döntési szempont lesz számukra.[470] A gyártóknak jelentéstételi kötelezettsége áll fenn a kijelölt CSIRT és az ENISA felé olyan esetekben, amikor a digitális elemeket tartalmazó termékben található bármely aktívan kihasznált sérülékenységről tudomást szereznek. A jelentéstétel menete a NIS2 irányelvben meghatározottakkal azonosan zajlik.[471] A CRA, több más jogi aktusban (pl. MI rendelet) is látható megoldást alkalmaz, pl. az elszámoltathatóság megkövetelésére. Ilyen a műszaki

[461] NIS2 irányelv 16. cikk
[462] NIS2 iránelv 21. cikk
[463] NIS2 irányelv 23. cikk
[464] NIS2 irányelv (81)-(82) preambulumbekezdések
[465] Hoeren, Pinelli, 2024. 226 o.
[466] Hoeren, Pinelli, 2024. 230 o.
[467] 2017/745/EU rendelet az orvostechnikai eszközökről
[468] 2017/746/EU rendelete az in vitro diagnosztikai orvostechnikai eszközökről
[469] CRA 2. cikk
[470] Hoeren, Pinelli, 2024. 230-231 o.
[471] CRA 14. cikk. A CRA 21. cikke szerint ez a szabály irányadó az importőrre vagy a forgalmazóra is, ha saját neve vagy védjegye alatt hoz forgalomba digitális elemeket tartalmazó terméket, vagy jelentős módosítást hajt végre egy már forgalomba hozott, digitális elemeket tartalmazó terméken.

dokumentáció[472] megléte vagy a digitális elemeket tartalmazó termékek megfelelőségértékelési eljárásai.[473] Szintén fontos megemlíteni a CRA törekvését a GDPR-nál is látható by design és by default szemléletekhez hasonló „beépített biztonság" (secure by design[474]) elvének bevezetésére. Ezt a jogalkotó részéről tudatos döntésnek tekinthetjük, mivel kifejezett szándékának mutatkozik az egyes jogi aktusok (itt kifejezetten a GDPR) közötti szinergiák megteremtése.[475]

A CRA mellékletei számos általános előírás konkretizálását tartalmazzák. Ezek részletesen szabályozzák a digitális termékek kiberbiztonsági követelményeit, beleértve a kötelező műszaki és információs előírásokat, a biztonsági tanúsítási eljárásokat és a megfelelőségi értékelési módszereket. Az egyértelmű termékosztályozás biztosítja, hogy az eltérő kockázati szinteknek megfelelő követelmények lépjenek életbe. Fontos továbbá, hogy a kockázat-arányos megközelítés ismét kiemelten megjelenik.[476]

Összegezve a CRA nóvumnak tekinthető horizontális megközelítésében és jelentős mérföldkő a harmonizált adatjogi szabályozás létrehozásában. A szabályozási tartalmát tekintve, fenntartja és megerősíti az adatjogi védelem alapintézményeinek tekinthető előírásokat, mint a kockázat-arányosság, a by design szemlélet, vagy a jelentéstételi kötelezettség. E mellett a mellékleteiben konkretizált követelményeket állapít meg a megfelelő kibervédelem eléréséhez, ami a szereplők felkészültségi szintjének kiegyensúlyozását érheti el.

4.2.4.5. A Kib.tv-ről (2024. évi LXIX. tv.)

A törvény a már részletezett uniós jogalkotással összhangban keletkezett, így az ismert jogpolitikai célitűzéseket igyekszik elérni, illetve tagállami szinten megvalósítani.[477] Ezért a célja az elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének elérése.[478] A törvény a hatósági felügyelet rendszerét két részre osztja, a civil területen a Nemzeti Kiberbiztonsági Hatóság felügyeli a törvény végrehajtását, ellenőrzi a szervezetek kiberbiztonsági intézkedéseit és vezeti a nyilvántartásokat, míg a Honvédelmi Kiberbiztonsági Hatóság a védelmi szektorban látja el ezeket a feladatokat.[479] A NIS2 által elvártan a hazai kiberbiztonsági incidensek kezeléséért és a jelentési kötelezettségek végrehajtásáért Nemzeti Kiberbiztonsági Incidenskezelő Központ a felelős.

A törvény alapján a szervezetek kockázatkezelési rendszert kötelesek felállítani és ez alapján meg kell határozni a kockázatokkal arányos védelmi intézkedéseket,[480] el kell végezzék a biztonság osztályba sorolást,[481] és kötelesek jelentést tenni a kiberbiztonsági incidensekről.[482]

Összegezve a Kib.tv. az uniós jogalkotási irányt követve ülteti át az információbiztonság alapvető előírásait a magyar jogba.

---

[472] CRA 31. cikk
[473] CRA 32. cikk
[474] Hoeren, Pinelli, 2024. 242 o.
[475] CRA (32) preambulumbekezdés
[476] CRA I. melléklet I. rész (1) pont szerint „a digitális elemeket tartalmazó termékeket úgy kell megtervezni, fejleszteni és gyártani, hogy a kockázatok alapján megfelelő szintű kiberbiztonságot biztosítsanak."
[477] A törvény végső előterjesztői indokolása alapján a Kib.tv. NIS2 irányelv átültetése mellett, elődjének az Ibtv-nek az alkalmazási tapasztalatainak megőrzésére és jogrendbe építésére szolgál
[478] Kib. tv. preambulum [2] pontja
[479] Kib.tv. 23-24. §
[480] Kib.tv. 6. §
[481] Kib.tv. 10. §
[482] Kib.tv. 66. §

4.2.5. Egyéb védelmi előírásokról

Az egyéb előírások alatt a tágan vett (kompozit) adatjogi előírásokra lehet gondolnunk. Ezek tehát nem önálló jogszabályok, hanem más területeken található adatjogi természetű és tárgyú rendelkezések.

4.2.5.1. A mesterséges intelligenciáról szóló jogszabályról (MI rendelet - 2024/1689/EU rendelet)

A rendelet célja, hogy javítsa a belső piac működését azáltal, hogy egységes jogi keretet állapít meg az MI-rendszerek[483] az uniós értékekkel összhangban történő, Unión belüli fejlesztésére, forgalomba hozatalára, üzembe helyezésére és használatára vonatkozóan. A szabályozási megközelítése szerint elő kell mozdítsa az emberközpontú és megbízható mesterséges intelligencia elterjedését, miközben biztosítja az Unióban az egészség, a biztonság és az Alapjogi Chartában rögzített alapvető jogok magas szintű védelmét, ezáltal védelmet biztosítva az MI-rendszerek káros hatásaival szemben, miközben támogatja az innovációt.[484] Az MI rendelet által szabályozott terület rendkívül szoros kapcsolatban áll az adatokkal, ugyanis az algoritmus működése minden esetben szükségszerűen adatokkal kezdődik és adatokkal végződik. A legfontosabb védelmi előírásai az alábbiak.

- *Kockázatkezelési rendszer*[485] létrehozása, bevezetése, dokumentálása, fenntartása
- *Műszaki dokumentációnak*[486] a rendszer forgalomba hozatala vagy üzembe helyezése előtti elkészítése, és naprakészen tartása[487]
- *Pontosság, stabilitás és kiberbiztonság*[488] biztosításának követelménye
- Bizonyos nagy kockázatú MI-rendszerek alkalmazóinak egy *alapvetőjogi hatásvizsgálat*[489] (FRIA) keretében értékelniük kell azon hatást, amelyet az ilyen rendszerek használata az alapvető jogokra gyakorolhat
- *Adatok és adatkormányzás* elvárása alapján a tanító-, a validálási és a tesztadatkészleteket a nagy kockázatú MI-rendszer rendeltetésének megfelelő adatkormányzási és adatgazdálkodási gyakorlatoknak kell alávetni.[490]

4.2.5.2. A digitális piacokról szóló jogszabályról (DMA - 2022/1925/EU rendelet)

A DMA célja, hogy a digitális piacokon a kapuőrként (ún. gatekeeper) működő nagy online platformok számára egyértelmű és egységes szabályokat állapítson meg, ezáltal elősegítve a versenyképes és innovációt támogató, az üzleti felhasználók és a végfelhasználók javát szolgáló piacot,[491] a tisztesség és a támadhatóság elérésére által.[492] A DMA így alapvetően a kapuőrökre tartalmaz előírásokat, de mivel ezek jelentős szereplők az adatalapú folyamatokban a rájuk irányadó rendelkezések számottevő hatással bírnak az egész adatalapú rendszerre. A kapuőr

[483] Mesterségesintelligencia-rendszereknek
[484] MI rendelet (1) preambulumbekezdés
[485] MI rendelet 9. cikk
[486] MI rendelet 11. cikk
[487] E mellett a 18. cikk egyéb dokumentáció vezetését is elvárja, mint a minőségirányítási rendszerre, bejelentett szervezetek által jóváhagyott változtatásokra vonatkozó dokumentáció
[488] MI rendelet 15. cikk
[489] MI rendelet 27. cikk
[490] MI rendelet 10. cikk
[491] DMA 1. cikk
[492] Tóth András, Koltay András, Lapsánszky András: Nagykommentár a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról szóló, az Európai Parlament és a Tanács 2022. szeptember 14-i (EU) 2022/1925 rendelethez (digitális piacokról szóló jogszabály). Budapest, Wolters Kluwer, 2024. 1 o.

számára általában tilalmazott az üzleti felhasználók és a saját végfelhasználóinak adatait saját megfontolások alapján, korlátoktól mentesen használni.[493] Kiemelendő továbbá, hogy a DMA 5. cikke kifejezetten védelmi célú tilalmakat állít fel személyes adatok kezelésével kapcsolatban.[494]

- Tilos online hirdetési szolgáltatások nyújtása céljából végfelhasználók személyes adatait gyűjteni olyan harmadik felek szolgáltatásain keresztül, akik a kapuőr alapvető platformszolgáltatásait veszik igénybe;[495]
- Tilos alapvető platformszolgáltatásokból származó személyes adatokat összekapcsolni saját vagy harmadik fél által nyújtott szolgáltatáson keresztül gyűjtött személyes adatokkal, tilos továbbá alapvető platformszolgáltatásokból származó személyes adatokat saját, egyéb szolgáltatások, illetve saját, egyéb szolgáltatásokból származó adatokat alapvető platformszolgáltatások céljára használni;[496]
- Tilos a végfelhasználókat beléptetni a kapuőr más szolgáltatásaiba személyes adatok összekapcsolása céljából;[497]
    - A tilalmak alól kivételt jelent, ha a végfelhasználó számára konkrét választási lehetőséget kínált fel a kapuőr *és* az a GDPR alapján hozzájárulásnak minősül[498]
- Tilos az üzleti felhasználókkal való verseny során felhasználni olyan nyilvánosan nem elérhető adatokat, amelyek az érintett alapvető platformszolgáltatásoknak vagy az azokkal együtt vagy az azok támogatása céljából nyújtott szolgáltatásoknak az említett üzleti felhasználók általi használatával összefüggésben keletkeznek, vagy amelyeket az üzleti felhasználói adtak meg, beleértve az ezen üzleti felhasználók ügyfelei által generált vagy megadott adatokat is.[499]

4.2.5.3. A digitális szolgáltatásokról szóló jogszabályról (DSA – 2022/2065/EU rendelet)

A DSA rendelet átfogó szabályozást vezet be az Európai Unióban a különböző digitális szolgáltatásokra – és azok szolgáltatóira. A célja az ilyen szolgáltatások felhasználóinak védelme, az illegális tartalmakkal szembeni fellépés erősítése, valamint az online szolgáltatók átláthatóságának és felelősségvállalásának növelése.[500] A DMA „ikerrendeletének" tekinthető.[501]

---

[493] DMA 5. cikk (2) bekezdés és 6. cikk (2) bekezdés

[494] Tóth András, Szabó Endre Győző, Németh Szabolcs, Rudics Regina, Rideg Gergely, „A GDPR és a Digital Markets Act viszonyának tisztázása" IN MEDIAS RES 2023/2., 3, 2023. 49 o.

[495] DMA 5. cikk (2) bekezdés a) pont; A tilalom alatt gondolhatunk a platformok által biztosított, harmadik felek weblapjaiba integrált plugin-ek és beépülő modulokon keresztüli nagyarányú adatgyűjtésre, pl. Facebook Pixel vagy Google GA analitikai moduljai.

[496] DMA 5. cikk (2) bekezdés b) és c) pontok; Gondolhatunk pl. a Facebook és az Instagram látszólag elkülönült, de ténylegesen (vélelmezhetően) a szolgáltató által összekapcsot, komplex profiljaira.

[497] DMA 5. cikk (2) bekezdés d) pont; Ez a szolgáltatások un. „tying" vagy „bundling" formájában történő összekapcsolása, ami a GDPR jogalapjai esetén szintén felmerülő kérdés. Az adatvédelmi gyakorlat alapján is tiltott az un. „bundled consent" vagyis az összekapcsolt szolgáltatásokhoz való hozzájárultatás.

[498] DMA 5. cikk (2) bekezdés; A feltételek konjunktívnak tekinthetők, így egy jog által deklarált, kötelezően választandó GDPR 6. cikk (1) bek. a) pont szerinti hozzájárulásos jogalapot is jelent egyben. Ez alapján pl. jogos érdek mérlegelését nem alkalmazhatja a platform az adatkezelés legitimációjához.

[499] DMA 6. cikk (2) bekezdés; A rendelkezés egyedülállóan jogi személyekre tartalmaz védelmi előírásokat. Lásd részletesen: Tóth, Szabó, Németh, Rudics, Rideg, 2023. 51 o.

[500] DSA 1. cikk

[501] Tóth, Szabó, Németh, Rudics, Rideg, 2023. 55 o.

- A közvetítő szolgáltatók – legalább évente egyszer – géppel olvasható formátumban és könnyen hozzáférhető módon világos, jól érthető jelentést tesznek közzé az adott időszakban általuk végzett tartalommoderálásról.[502]
- Tilos az online platformot üzemeltető szolgátónak a kiskorúak adataival kapcsolatban, GDPR szerinti profilon alapuló hirdetéseket megjeleníteni;[503]
- Az online óriásplatformot és nagyon népszerű online keresőprogramot üzemeltető szolgáltatóknak azonosítaniuk, elemezniük és értékelniük kell a szolgáltatásaik és a kapcsolódó rendszerek – többek között az algoritmikus rendszerek – kialakításából vagy működéséből vagy a szolgáltatásaik használatából eredő rendszerszintű kockázatokat.[504] Ezzel összefüggésben a szolgáltatóknak észszerű, arányos és hatékony kockázatcsökkentési intézkedéseket kell bevezetniük az azonosított egyes rendszerszintű kockázatokra szabva, kiemelt figyelmet fordítva az ilyen intézkedéseknek az alapvető jogokra gyakorolt hatásaira.[505]

4.2.5.4. A digitális állampolgárságról szóló jogszabályról (eIDAS 2.0 - 910/2014/EU rendelet)

Az eIDAS rendelet az elektronikus azonosításra (eID), a digitális állampolgárságra és a bizalmi szolgáltatásokra vonatkozó egységes szabályozás. A célja, hogy elősegítse a biztonságos, megbízható és a tagállamokban kölcsönösen elismert elektronikus tranzakciókat, ezzel támogatva az egységes digitális piac működését.[506] A védelmi előírások alapvetően a bizalmi szolgáltatásokkal kapcsolatos technikai és szervezési intézkedésekre irányulnak, amelyek a velük kapcsolatba kerülő természetes és jogi személyes adatainak biztonságát szolgálják.[507]

- A minősített és nem minősített bizalmi szolgáltatók megfelelő technikai és szervezeti intézkedéseket kell végre hajtsanak az általuk nyújtott bizalmi szolgáltatások biztonságát fenyegető kockázatok kezelése érdekében. Ezen intézkedésekkel – figyelembe véve a legújabb technológiai fejleményeket – biztosítaniuk kell, hogy a biztonsági szint arányos legyen a kockázat mértékével. Intézkedéseket kell végrehajtaniuk különösen a biztonsági események megelőzése és azok hatásának minimálisra csökkentése, valamint az érdekelt felek bármely esemény káros hatásairól való tájékoztatása érdekében.[508]
- A szolgáltatók indokolatlan késedelem nélkül, de minden esetben az esetről való értesüléstől számított 24 órán belül értesítik a felügyeleti szervet és adott esetben más érintett szerveket a biztonság megsértéséről vagy az adatok sértetlenségének

[502] DSA. 15. cikk; Ahogy az adatjog történeti áttekintése során láthattuk a tartalommoderálás (cenzúra) és egy adatalapú folyamat keretében működik, a moderálásra vonatkozó jelentéstétel, pedig az ilyen folyamatok átláthatóságát szolgálja

[503] DSA 28. cikk (2) bekezdés; A profilalkotás kockázata abban rejlik, hogy az adatok közötti összefüggések azonosítását és konkrét csoportokra vagy személyekre történő értelmezését teszi lehetővé, ezáltal olyan kategóriák létrehozását idézi elő, amelyek azonos tulajdonságok szerint csoportosítást valósítanak meg, lásd részletesen: Pataki Gábor, Szőke Gergely László „Az online személyiségprofilok jelentősége”. In: Polyák Gábor (Szerk.): Algoritmusok, keresők, közösségi oldalak és a jog – a forgalomirányító szolgáltatások szabályozása. Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2020. 75. o.

[504] DSA 34. cikk

[505] DSA 35. cikk

[506] eIDAS 1. cikk

[507] Alessandro Mantelero, Giuseppe Vaciago, Maria Samantha Esposito and Nicole Monte, „The common EU approach to personal data and cybersecurity regulation”, International Journal of Law and Information Technology, 2020, 28, 2021. 315 o.

[508] eIDAS 19. cikk (1) bekezdés

megszűnéséről, amennyiben az jelentős hatást gyakorol a bizalmi szolgáltatásra vagy az annak keretében tárolt személyes adatokra.[509]

- A szolgáltatók kötelesek olyan munkatársakat és adott esetben olyan alvállalkozókat alkalmazni, akik megbízhatóak, rendelkeznek a szükséges szakértelemmel, tapasztalattal és képesítésekkel, valamint megfelelő képzésben részesültek a biztonságra és a személyes adatok védelmére vonatkozó szabályokkal kapcsolatban, továbbá kötelesek olyan igazgatási és ügyvezetési eljárásokat alkalmazni, amelyek megfelelnek az európai és nemzetközi szabványoknak;[510]
- A szolgáltatók kötelesek megbízható rendszereket használni és megfelelő intézkedéseket hozni az adathamisítás és az adatlopás ellen.[511]

4.2.6. Összegzés a védelem jogáról

A védelem jogának alapja – jelentősége és szabályozási megoldásainak a tekintetében is – a GDPR, e mellett a CRA horizontális szabályai szintén kiemelhetőek. Az összes vizsgált joganyag tekintetében számos hasonló megközelítés azonosítható, amelyek így az adatjogi összetartás (konvergencia) alkotóelemei lehetnek.

- Kockázat-arányos védelem
- Kockázatértékelés és -kezelés fontossága
- Jelentéstételi kötelezettség és eseménykezelés (pl. incidensek)
- By design és by default szemléletek
- Egységességre törekvő harmonizált (szinergikus) szabályok
- Információbiztonság, kiberbiztonság és adatbiztonság eredményeinek ötvözése (pl. CIA triász)
- Alkalmazói és felhasználói tudatosság növelésének fontossága
- Ex ante jogszerűségi szabályok erősödése (DPIA, FRIA, ÉMT,[512] SZAT[513])
- Folyamatszintű belső szabályozás megkövetelése (pl. irányítási rendszerek,[514] BCP,[515] DLP,[516] IRC[517] stb.)

4.3. Az adatok felhasználásának joga

4.3.1. A felhasználás jogáról általában

Az adat használatának ernyő fogalma alatt egy adat bármilyen jogszerű célból felhasználható, feltéve, hogy a szóban forgó tevékenység kellően magas fokú értékegyenlőséget mutat, ellenkező esetben már hasznosításról vagy végső esetben jogellenességről beszélnénk. A felhasználás – ahogy fentebb láthattuk is – olyan tág terület, hogy gyakorlatilag minden adaton végzett művelet ide tartozhat, függetlenül annak szintaktikai vagy szemantikai rétegbeli minőségétől. Adatfelhasználást jelent saját és más adatainak kezelése egyaránt. A használati jogosultság megalapozását az un. össztársadalmi érdekrealizáción alapuló csere fogja megadni, amely fennállását a csere egyenértékűsége adja. Így a felhasználás cseréje mindig valamilyen adat feletti uralmi viszony megosztását jelenti, valamilyen felek között fennálló, vagy a

[509] eIDAS 19. cikk (2) bekezdés
[510] eIDAS 24. cikk (2) bekezdés b) pont
[511] eIDAS 24. cikk (2) bekezdés f) és g) pontok
[512] Érdekmérlegelési teszt
[513] Szükségességi-arányossági teszt
[514] Például: ISO/IEC, ITIL, ISACA COBIT, TISAX stb.
[515] Business Continuity Protocol – üzletmenet-folytonosság
[516] Data Leak Prevention – adatszivárgás megelőzés
[517] Incident Response Plan – incidenskezelési eljárásrend

társadalom szélesebb rétege által elfogadott érdek kielégítése céljából. Egy példával érzékeltetve, egy szerződéshez szükséges adat megadása esetén az érdek a felek kölcsönös, egybehangzó akartnyilatkozatának jogszerű megtétele. A szerződés megszűnésével ez az érdek megszűnik, a szerződéses adatok további kezelése azonban ezt követően is megengedett, hiszen a szerződéses érdekeltséget a társadalom által elismert, jogi igények érvényesítéséhez és védelméhez fűződő érdekeltség fogja leváltani. Ez alapján érezhető, hogy az adatok felhasználásakor nem minden esetben az a feltétel, hogy az adat jogosultjának közvetlen érdekeltsége legyen fellelhető, az is elégséges, ha az a társadalmi együttélés szabályainak megfelel, mindaddig, amíg az adatok felhasználása által kielégített érdek és a magánszférába vagy a társadalmi rendbe való beavatkozás közötti egyenértékűség fennállónak tekinthető.

Az egyes jogi adatkategóriákra vonatkoztatva az érdemi kérdések minden esetben a felek vagy a társadalmi érdekeltség fennállásának megalapozása, illetve a csere értékegyenlőségének alátámasztása. Látható törésvonal húzódik e tekintetben a személyes és nem személyes adatok között, hiszen előbbi esetén az érdekeltségek megalapozására és az értékegyenlőség igazolására kiforrott jogintézmények vonatkoznak, amelyeket a dolgozatban részletesen tárgyaltunk. Fontos azonban, hogy az adatfelhasználás nem szűkíthető csak személyes adatok felhasználására, abba minden jogi kategóriához tartozó adat beletartozhat, mindazonáltal eltérő szabályok alapján. A közadatok esetén például a felhasználás és hasznosítás kifejezetten támogatott, míg a magánadatoknál a helyzet valamivel árnyaltabb. A cégek alapvető (indexált és attribútum, mint megnevezés és tevékenységi kör) adatai jellemzően nyilvánosak[518] azonban ezen túlmenően a magánszféra (és a közszféra által kezelt nem közadatok) adatai sok esetben korlátozó szabály hatálya alatt állnak – pl. az üzleti titok védelme – vagy ilyen szabály hiányában is a szervezet szempontjából érzékenynek minősülnek, amelyeket így védeni igyekeznek.[519] A szereplők autonómiája alapján – eltérő jogszabályi rendelkezés hiányában – az ilyen adatokról jogilag és ténylegesen saját maguk rendelkeznek. Végezetül fontos kiemelni az adatfelhasználás kiemelt csoportját, a szervezett és rendezett társadalmi együttélést biztosító intézmények működéséhez szükséges folyamatokat. Minden jogi adatkategória esetén számtalan részletesen szabályozott művelet zajlik ennek a jegyében, gondolhatunk például az állam-, és önkormányzati igazgatásra, az igazságszolgáltatási szervek munkájára vagy a köznevelés területére.

- *A felhasználás közös jellemzői*

A fentebb leírtaknak megfelelően az adatfelhasználás részleteit az ágazatra irányadó jogszabályi előírások és belső gyakorlataik határozzák meg, így ezek a szektorális határok mentén jelentősen eltérő képet mutathatnak. A kialakult adatalapú gyakorlatoknak megfelelően a személyes és nem személyes adatok felhasználásakor egyaránt az alábbi tényezők megjelenése általánosnak mondható.

- A felhasználás többnyire konkrét célzattal rendelkező tevékenység, amelyben az adat forrása vagy saját vagy harmadik fél érdekeltségére tekintettel – saját vagy össztársadalmi érdek legitimációs jelenléte mellett – vesz részt. A cél a hasznosítástól eltérően általában jól azonosítható, közelebbi a használat mindennapi körülményeihez.
- Az adathasználati műveletek végzéséhez valamilyen jogi legitimációra, vagy felhatalmazásra van szükség.
- A felhasznált adatok esetében, mivel jellemzően célorientáltak, a létrehozataluk és kezelésük pedig erőforrásigényes, általában felmerül valamilyen megőrzési idő (személyes adatok esetén kötelezően, nem személyes adatok esetén sokszor csak

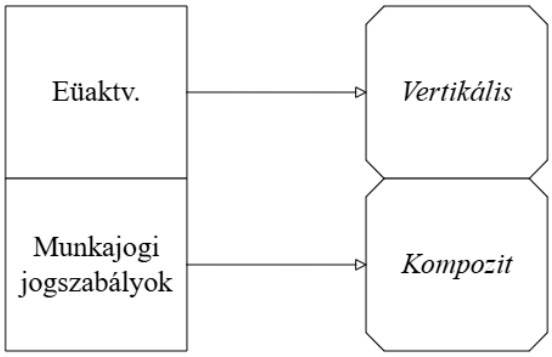
[518] 2006. évi V. törvény - a cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról
[519] Gondoljunk az un. tényleges erőhatalom estkörére

gyakorlati okokból). Erre hatással lehetnek objektív körülmények, mint a tárolási kapacitás végessége, jog által meghatározott kötelező időtartamok vagy – az előző kettő hiányában – észszerűségi okok, mint az adat felhasználásának várható szükségességi ideje. A megőrzési idő lejártával az adatok törlésre kerülhetnek vagy hasznosítási célból a további tárolásukra is sor kerülhet. Bizonyos esetekben – kevésbé prudens adathasználati gyakorlatok esetén – az adatok cél nélkül is további tárolódnak, így múlóadatként kallódhatnak az ismételt felfedezésükig vagy törlésükig.

- Az egyes felhasználási folyamatok jellemzően nem egy adattal működnek, azokban komplex állományokká vegyülnek különböző forrású, típusú és kategóriájú adatok. Egy folyamat adattartalmát jó esetben a folyamat által elérni kívánt felhasználási cél jelöli ki, amit az adathasználó vagy önállóan vagy külső tényezők hatására határoz meg. Hasonlóan a megőrzési időhöz külső tényezők lehetnek jogszabályi előírások vagy más szereplők igényei (mint hatóságok, anyavállalatok/felettes szervek vagy akár maga az adat forrása).

➢ *A felhasználás jogának dogmatikai besorolása*

A felhasználáshoz tartozó joganyagokat lehetetlen taxatíve felsorolni, hiszen ahány ágazat, annyifelé adatfelhasználási igény merül fel. Általánosságban azt mondhatjuk, hogy a felhasználás megjelenhet mind horizontális, mind vertikális adatjogi szinten, azonban egyértelműen legjellemzőbb a kompozit adatjogi szabályok alkalmazása. Ennek az oka, hogy az előírások kifejezetten és szorosan kell idomuljanak a felhasználás gyakorlati körülményeihez, amit így vagy rendkívül nehéz vagy legtöbb esetben felesleges lenne a szektoron kívülről, önálló kódexben megvalósítani. Ez alól kivétel és így az adatfelhasználásra dedikált joganyag vegytiszta példája az EHDS javaslat I. fejezete mellett az Eüaktv., amelynek a jogalkotó által deklaráltan a célja az egészségi állapotra vonatkozó különleges személyes adatok és az azokhoz kapcsolódó személyes adatok kezelésének feltételeit és céljait meghatározni.[520] Az adatfelhasználás feltárása és aktuális állapotának bemutatása egyedül egy terület kiválasztásával és részletes vizsgálatával tűnik lehetségesnek. A személyes adatok megkülönböztetett szerepére tekintettel erről a területről származó folyamaton keresztül tekintem át az adatfelhasználás sajátosságait. Példaként a munkaügyi adatkezeléseket választottam, mivel ezek kiterjedtsége sok felhasználási esetkört képes produkálni, miközben a mindennapokhoz való közelsége és gyakorlatiassága könnyen elképzelhetővé, életszerűvé teszi mindezt.



12. ábra: a felhasználás joganyaga

➢ *Példák a munkaügyi adatfelhasználás kompozit adatjogi előírásaira*

A munkaügyi adatok felhasználására vonatkozó részletszabályokat valamilyen munkajogi rendelkezés adja meg, így kivétel nélkül kompozit adatjogi szabályoknak tekinthetjük. A jellemzőjük, hogy a munkaügyi élethelyzetek igényeihez igazodnak, azonban az adatjogi konvergencia (jelen esetben legfőképpen a GDPR előírásai) által kifejtett összehangolt

[520] Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény (továbbiakban: Eüaktv.) 1. §

tartalommal rendelkeznek. Alább egy összesítő táblázatban látható néhány példa a munkaügyekre vonatkozó kompozit adatjogi elemekről (jogszabályhelyekről).

Példa adatkezelési folyamat	*Kompozit adatjogi előírás*
Munkajogviszony létesítése: a munkaszerződés megkötése	Mt. 10. §, 23. §, 45. §
Munkajogviszony létesítése: munkáltató bejelentési kötelezettsége	Art.[521] 1. melléklet az állami adó- és vámhatósághoz bejelentendő adatokról
Munkajogviszony teljesítése: munkáltató tájékoztatási kötelezettsége és a szerződő felek egyes nyilatkozatai	9. §, 38. §, 46. §, 47. §, 155. §, 185. §
Munkajogviszony teljesítése: munka és pihenőidő	Mt. 134. §
Munkajogviszony teljesítése: a munka díjazása	Mt. 42. §, 155. §, Art. 202. §
Munkajogviszony teljesítése: járulékok, levonások, letiltások kezelése	Mt. 161. §, Tbj.[522] 66. §, 74. §
Munkajogviszony teljesítése: társadalombiztosítási ellátások folyósítása	Ebtv.[523] 79. §-tól 81/B. §-ig
Munkajogviszony teljesítése: havi adó- és járulékbevallással kapcsolatos adatok továbbítása	Art. 50. §, 78. § (4) bekezdés
Munkavédelem: munkavédelmi oktatások	Mvt.[524] 55. § (1) bekezdés
Munkavédelem: munkabalesetek	Mvt. 64. § (3) bekezdés, 5/1993. (XII. 26.) MüM rendelet[525] 5. §, 27/1996. (VIII. 28.) NM rendelet[526] 5. §-tól az 5/C. §-ig
Munkajogviszony teljesítése: Igazolás tartósan beteg, vagy súlyosan fogyatékos gyermekről	Mt. 118. § (2) bek., 5/2003. (II. 19.) ESzCsM rendelet[527] 3. melléklete
Munkáltatói ellenőrzések: belső ellenőrzési rendszer, munkahelyi számítógép,	Mt. 8. §, 11. § (1) - (2) bekezdése

[521] Az adózás rendjéről szóló 2017. évi CL. törvény (továbbiakban: Art.)
[522] A társadalombiztosítás ellátásaira jogosultakról, valamint ezen ellátások fedezetéről szóló 2019. évi CXXII. törvény (továbbiakban: Tbj.)
[523] A kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény (továbbiakban: Ebtv.)
[524] A munkavédelemről szóló 1993. évi XCIII. törvény (Mvtv.)
[525] A munkavédelemről szóló 1993. évi XCIII. törvény egyes rendelkezéseinek végrehajtásáról szóló 5/1993. (XII. 26.) MüM rendelet
[526] A foglalkozási betegségek és fokozott expozíciós esetek bejelentéséről és kivizsgálásáról szóló 27/1996. (VIII. 28.) NM rendelet
[527] A magasabb összegű családi pótlékra jogosító betegségekről és fogyatékosságokról szóló 5/2003. (II. 19.) ESzCsM rendelet

elektronikus postafiók, és az internet használatának ellenőrzése	
Munkáltatói ellenőrzések: GPS nyomkövető/menetlevél	Mt. 10. §, 11.§
Munkáltatói ellenőrzések: CCTV megfigyelés végzése	Szjtv. 25. §-tól a 32. §-ig
Munkajogviszony megszüntetése: felmondás, közös megegyezés	Mt. 64. §, 66. §
Munkajogviszony megszüntetése: általános megőrzés	Tny.[528] 99/A. §

4.3.2. A munkaügyekben történő adatfelhasználásról

A technológiai fejlődés, az informatikai eszközök használatának általánossá válása a munka világán belül az adatkezelésekre is jelentős hatást gyakorolt, hiszen lehetővé tette az adatok minden eddiginél nagyobb mértékű gyűjtését és felhasználását, ennek megfelelően rendkívül nagy mennyiségű adat kerül a munkáltatók kezelésébe. Fontos továbbá, hogy a foglalkoztatás kiterjedtsége miatt az adatok felhasználására az adott foglalkoztatási jogviszonyra irányadó jog mellett számos másik jogterület előírásai is hatást gyakorolnak, ami így egy egészen komplex adatfelhasználási szisztémát keletkeztet. A lehetséges adatkategóriák tekintetében a számos személyes adat mellett természetesen fellelhetőek a munkáltató oldalán megjelenő nem személyes köz- vagy magánadatok is. Az adattípusa és az azokon végzett műveletek a munkáltató jellegétől függenek, a modernebb munkáltatók esetén a digitalizáció hatásai erősen érezhetőek, így az adatokon nagy mennyiségű és kifinomult műveleteket végeznek. Ezzel szemben a hagyományosabbnak tekinthető, méretéből vagy anyagi lehetőségeiből adódóan a digitalizációban kevésbé érintett munkáltatók a foglalkoztatást analóg adatokkal, döntően papír alapon bonyolítják le, ennek megfelelően az adatokon végzett műveletek egyszerűbbek és kevésbé kiterjedtek.

Fontos, hogy – bár a jelenlegi vizsgálat személyes adat fókuszú – a munkavállaló ugyanúgy felhasználja a munkáltató (főleg nem személyes) adatait, amelyre az adatjogi előírások ugyanúgy vonatkozhatnak. Ezért lehet, hogy a munkáltató meghatározhatja, hogy a munkavállaló milyen céges adatokhoz férhet hozzá és azokat, hogyan használhatja fel (vagyis, hogyan enged használatot a dolgozó részére), valamint hogy milyen magatartást tanúsíthat a munkáltatója vonatkozásában (a védelem enyhe megnyilvánulása, hogy a munkáltató jogos gazdasági érdekére hivatkozással megtilthatja, hogy a munkavállaló negatív színben tüntesse fel, még akkor is, ha nem minősül hitelrontásnak vagy becsületsértésnek[529]).

Egy foglalkoztatási folyamat esetén az érdekeltségek egész tárháza azonosítható az adatok felhasználásával kapcsolatban. Általában elmondható, hogy azok közvetlenül kapcsolódnak egy vagy két személyhez (felekhez vagy harmadik félhez) vagy személyek szélesebb köréhez, azonban ezek mögött minden esetben ott kell legyen az erős társadalmi legitimáció.[530] Az értékegyenlőségi elv vizsgálatakor rögzített három viszonylatban felmerülő néhány érdeket és a mögöttük álló legitimáló erőt mutatja be az alábbi táblázat. Fontos, hogy az

[528] A társadalombiztosítási nyugellátásról szóló 1997. évi LXXXI. törvény (Tny.)
[529] Mt. 8. § (1)-(2) bekezdés
[530] Mivel személyes adatok felhasználásáról van szó. Enyhébb legitimáció is elég nem személyes adatok felhasználásakor vagy személyes adatok hasznosításakor.

adatfelhasználáshoz kapcsolódó előző pontban ismertetett jogszabályhelyek elsősorban a folyamatot (célját) vagy a közvetlen érdeket határozzák meg, a szélesebb társadalmi legitimáció jellemzően magasabb rendű joganyagokban vagy nem jogi normákban lelhető fel.

	Adatkezelési folyamat	*Közvetlen érdek*	*Közvetett érdek (társadalmi legitimáció)*
Unilaterális reláció	Munkavállaló ellenőrzése (kamerás megfigyelés)	Vagyonvédelem Személyvédelem	Jogos gazdasági érdek (tulajdon védelme)[531] Az együttélés biztonságának fenntartása[532]
	Munkáltató írásbeli értékelése a munkavállalóról	A foglalkoztatási viszonyok átláthatósága A munkaerőpiacon való elhelyezkedés támogatása	Jogos gazdasági érdek (a megfelelő jelentkező megtalálása a toborzási eljárás során, a megpályázott állás megszerzése)[533]
Bilaterális reláció	Munkaszerződés megkötése	Foglalkoztatási jogviszony létrehozása	A vállalkozás és a munkavégzés keretrendszerének fenntartása[534]
	Munkavédelem	Biztonságos munkakörülmények létrehozása és fenntartása	Az emberek életének, testi épségének és egészségének védelme[535]
Multilaterális reláció	Havi adó- és járulékbevallás	Közteherviseléshez és társadalombiztosítási ellátásokhoz való hozzájárulás megfizetése	Az állami működéshez és szociális ellátórendszerhez való

[531] Alaptörvény V. cikk: Mindenkinek joga van törvényben meghatározottak szerint a személye, illetve a tulajdona ellen intézett vagy az ezeket közvetlenül fenyegető jogtalan támadás elhárításához.; Mt. 11/A. (1) bekezdés: A munkavállaló a munkaviszonnyal összefüggő magatartása körében ellenőrizhető. Ennek keretében a munkáltató technikai eszközt is alkalmazhat, erről a munkavállalót előzetesen írásban tájékoztatja.

[532] Alaptörvény IV. cikk (1) bekezdés: Mindenkinek joga van a szabadsághoz és a személyi biztonsághoz.; Mt. 51. § (4) bekezdés: A munkáltató biztosítja az egészséget nem veszélyeztető és biztonságos munkavégzés követelményeit.

[533] Alaptörvény M) cikk (1) bekezdés: Magyarország gazdasága az értékteremtő munkán és a vállalkozás szabadságán alapszik; Mt. 81. § (1) bekezdés: A munkáltató a munkavállaló kérelmére, ha a munkaviszony legalább egy évig fennállt, a munkaviszony megszüntetésekor (megszűnésekor) vagy legfeljebb az ezt követő egy éven belül a munkavállaló munkájáról írásban értékelést ad.

[534] Alaptörvény XII. cikk (1) bekezdés: Mindenkinek joga van a munka és a foglalkozás szabad megválasztásához, valamint a vállalkozáshoz; Mt. 42. § (1) bekezdés: A munkaviszony munkaszerződéssel jön létre.

[535] Alaptörvény XVII. cikk (3) bekezdés: Minden munkavállalónak joga van az egészségét, biztonságát és méltóságát tiszteletben tartó munkafeltételekhez; A munkavédelemről szóló 1993. évi XCIII. törvény 2. § (2) bekezdés: A munkáltató felelős az egészséget nem veszélyeztető és biztonságos munkavégzés követelményeinek megvalósításáért.

			hozzájárulás megtétele[536]
	Levonások, letiltások kezelése	Jogszabályban megállapított közterhek, jogszerű és megalapozott tartozások munkabérből történő levonása / letiltása	A jogügyletek teljesítésébe vetett közbizalom fenntartása (köztartozások végrehajtása, hitelezők védelme)[537]

A fentebb említett értékegyenlőség vizsgálatát minden önálló adatkezelési folyamat tekintetében el kell végezni. Az egyensúly mércéjének felállításában a területre irányadó bármely jogi vagy nem jogi szabályozó eszköz részt vehet, így figyelembe veendők a különböző alapjogokat kiszolgáló rendszerek (például az egyenlő bánásmód követelménye), a munkajog vagy az adójogszabályok. Fontos, hogy mivel személyes adatokról van szó, ezért az egyensúlyt kétséget kizáróan kell tudni bizonytani. Az adathasználat megindításához a feleknek kölcsönösen el kell tudniuk fogadni a kialakult helyzetet a felhozott érdekeltség tükrében. Ez a munkavállaló oldalán jelentheti azt, hogy megérti, hogy a munkába álláshoz szerződést kell kötni, vagy azt, hogy az állam működéséhez adót kell fizetni. Kevésbé magától értetődő, de az értékegyenlőség kimutatható azokban az esetekben is, amikor a munkavállalónak semmilyen vagy csak nagyon közvetett haszna származik a folyamatból (pl. munkáltatói ellenőrzés). Ezekben az esetekben végső soron a munkavégzés lehetősége, tágabban a társadalomban való létezés előnyei fogják az érték ellenoldalát megalapozni. Utóbbi esetben nagy jelentősége van a munkáltató helyes értékítéletének, ugyanis a túlzottan magánszférába vagy társadalmi rendbe avatkozó adatkezelési gyakorlatok jogellenesnek bizonyulhatnak. Ezt a helyzetet a nyilvánvaló adatvédelmi tételesjogi sérelem mellett úgy is értelmezhetjük, hogy az értékegyenlőség megdőlt.

4.3.3. A munkaügyi adatfelhasználás folyamatáról

Az adatfelhasználás lényege, hogy az az adatokon való műveletvégzésnek a részleteire vonatkozik. A terület szabályai vonatkozhatnak az alapvető paraméterekre, de lehetséges, hogy csak a kereteket jelölik ki. A folyamat a gyakorlat alapján három általános szakaszra osztható, a jogviszony létesítésére, teljesítésére és megszűnésére. Az adatok mindhárom szakaszban a foglalkoztatáshoz kapcsolódó érdekek által indokolt cserék eszközei, tehát az adatok monetizációja egyértelműen nem jellemző. A három szakasz külön kerül vizsgálatra (a speciálisnak mondható ellenőrzésekkel együtt) a legjelentősebb folyamatokra irányadó gyakorlaton és jogi előírásokon keresztül annak érdekében, hogy a munkaügyi adatfelhasználás sajátosságai azonosíthatók legyenek.

[536] Alaptörvény O) cikk: Mindenki felelős önmagáért, képességei és lehetőségei szerint köteles az állami és közösségi feladatok ellátásához hozzájárulni; Art. 50. § (1) a) pont: Havonként, a tárgyhót követő hónap tizenkettedik napjáig elektronikus úton bevallást tesz az adó- és/vagy társadalombiztosítási kötelezettségeket eredményező, természetes személyeknek teljesített kifizetésekkel, juttatásokkal összefüggő valamennyi adóról – ide nem értve a kamatjövedelem adót –, járulékokról és/vagy az Art.-ben meghatározott adatokról a munkáltató.

[537] Alaptörvény: XXX. cikk (1) bekezdés: Teherbíró képességének, illetve a gazdaságban való részvételének megfelelően mindenki hozzájárul a közös szükségletek fedezéséhez; Mt. 161. § (1) bekezdés: A munkabérből való levonásnak jogszabály vagy – a levonásmentes munkabérrészig – végrehajtható határozat alapján van helye; Ptk. 6:34. §: A szolgáltatást a kötelem tartalmának megfelelően kell teljesíteni (pacta sunt servanda elv)

4.3.3.1. A munkajogviszony létesítéséről

A szerződés megkötéséig vezető utat nevezhetjük toborzásnak vagy pályáztatásnak, a lényege minden esetben a munkaerő-felvétel. Az eljárás szempontjából meghatározó körülmény a szerződési szabadság, hiszen a szerződő fél döntésén múlik akar-e és, ha igen kivel és milyen tartalommal szerződést kötni.[538] A viszonyokat árnyalja a jóhiszeműség és a tisztességesség követelménye, amely mindkét fél részére teremt jogosultságokat és kötelezettségeket is.[539]

A munkáltató adatfelhasználására nagy hatással van az álláshirdetés megfogalmazása. Az abban lévő elvárásaival kapcsolatban elsősorban a mögöttes jog és a védelem előírásainak a tiszteletben tartására kell ügyelnie, így elkerülhetők a későbbi adatfelhasználási problémák is. Különösen fontos az egyenlő bánásmód követelményének betartása, hiszen ahogy fentebb megállapítottuk, a jogszerűség személyes adatok esetén párhuzamos. Az érték egyenlőségének viszonylatában különös jelentősége van, ha a pályázatban olyan feltételek kerülnek megjelölésre, amelyek a munkavégzéssel egyáltalán nem, vagy alig vannak összefüggésben,[540] illetve inkább a jelentkező személyes jellemzői közé tartoznak.[541] Az álláshirdetés tartalmi összeállítása szempontjából fontos az adattakarékosság elvének való megfelelés,[542] amely adatvédelmi alapelvi relevanciája mellett az értékegyenlőségre is jelentős hatással van.

A pályázati anyag beérkezésével elkezdődik a tényleges felhasználás, ha az adattartalom megfelelően került összeállításra, akkor, ezen a ponton az adatbiztonságra vonatkozó előírások kerülnek előtérbe. A munkáltató ugyanis az adat megszerzésével egyszerre jogosult és köteles is az adatok bizalmasságának, rendelkezésre állásának és sértetlenségének a megőrzésére.

A következő lépés súlypontja a jelentkezők személyes meghallgatásán és a belső döntési folyamaton van. Ezekkel kapcsolatban a már említett egyenlő bánásmód követelményének való megfelelés szükségessége ismét felerősödik, ugyanis az állásinterjú lebonyolítása során számos olyan kérdés tehető fel, amire a megadott válasz túlzott behatást – így az értékegyenlőség felborulását – és egyúttal akár jogellenes adatfelhasználást is eredményez.

Érdemes még az alkalmassági vizsgálatokat megemlíteni. Az Mt. 10. § (4) bekezdése szerint a munkavállalóval szemben csak olyan alkalmassági vizsgálat tehető meg, amelyet jogszabály ír elő – tehát kötelező – vagy amely a munkavégzés szempontjából különösen releváns képesség vagy készség meglétét képes igazolni.[543] Az adatfelhasználási csereérték egyensúlyának fennállásáról tehát jog által előírt esetben a jogalkotó a jogalkotási folyamat során bizonyosodik meg. A megalapozást igénylőt alkalmassági vizsgálatok ellenben jó példái az értékegyenlőség munkáltatói vizsgálatának, mivel ha a munkavállaló (vagy egy vizsgálat esetén a hatóság) számára az egyenlőség elfogadható, akkor az adatok felhasználása lehetséges jogszabályi előírás hiányában is.

4.3.3.2. A munkajogviszony teljesítéséről

A munkajogviszony teljesítéséhez értelemszerűen előbb létre kell azt hozni a felek által. A jogviszony létrehozásának és teljesítésének határterületén található maga a szerződéskötés eseménye, amely egyúttal összeköti és el is választja a két állapotot egymástól.

---

[538] Arany-Tóth Mariann: A munkavállalók személyes adatainak védelme a magyar munkajogban. Szeged, Bába Kiadó, 2008. 111 o.

[539] Mt. 6. § (2) bekezdés

[540] Mt. 10. § (1) bekezdés

[541] Az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról szóló 2003. évi CXXV. törvény (továbbiakban: Ebktv.) 21. §

[542] GDPR 5. cikk (1) bekezdés c) pont

[543] A NAIH tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről (2016). 21 o.

- *A munkaszerződésről és a kapcsolódó dokumentációról*

A felhasználás első állomása a munkaszerződés (annak mellékleteivel) megkötése, amely jelentősége, hogy minden későbbi adatkezelés kiindulópontja lesz. A munkaszerződéshez számos más folyamat is társul, amelyek attól valamelyest elkülönülnek, de önállónak mégsem nevezhetők. Mint minden szerződés, ez is kiindulópontként egy bilaterális érdekeltség mentén szerveződik, hiszen a felek egybehangzó akaratnyilatkozatát kell tükröznie, azonban látható, hogy a tartalmára számos olyan ágazati jogszabály is hatással van, amelyek a szélesebb társadalom érdekeltségének jelenlétét tükrözik.

Az Mt. szerint a munkaszerződést írásba kell foglalni,[544] amely kötelezettség a munkáltatót, vagyis az adatkezelőt terheli.[545] Az Mt. 23. § (2) bekezdése és a 45. § szerinti tartalmi elemek felvétele, a szerződés alakszerűsége, valamint annak módosítására vonatkozó szabályok kógensek, az irányadó jogszabály[546] szerint meglétük munkaügyi hatóság által ellenőrizhető. Külön említést érdemel az Mt. 45. § (1) bekezdésében említett munkaköri adat (munkaköri leírás), ami lehet a szerződés része, annak melléklete vagy akár más formátumú is (pl.: munkáltatói utasítás).[547] A szerződés és mellékleteinek adattartalmára nagy hatással van továbbá az adójogi szabályok által előírt, adóhatóság felé történő munkáltatói bejelentési kötelezettség.[548]

A szerződéskötéssel szoros kapcsolatban lehetnek egyéb megállapodások is, amelyek a munkaköri leíráshoz hasonlóan változatos formában létezhetnek, de eltérő céljuk miatt feltétlenül önálló adatkezelésnek minősülnek. Fontos, hogy ezek megkötése a felek szerződéses akaratán múlik elsősorban, így bilaterális érdekeltséget tükröznek. A teljesség igénye nélkül ilyen megállapodások lehetnek a leltárfelelősségi megállapodás,[549] a munkavállalói biztosítékról szóló megállapodás,[550] a versenytilalmi megállapodás,[551] és a tanulmányi szerződés.[552]

Szerződéskötéskor kerül sor a végzettségi és képzettségi igazolásoknak nyilvántartásba vételére is, amelyre – az Mt. módosítást követően a másolási gyakorlatot mellőzve[553] – például jegyzőkönyves hitelesítéssel kerülhet sor. Az adatok származhatnak különböző szintű iskolai végzettséget és nyelvismeretet igazoló bizonyítványokból, oklevelekből, szakképzésekről kiállított igazolásokból, de ide sorolható a jogosítvány vagy a PÁV vizsga[554] eredményének bemutatása is. Ezen adatok felhasználási céljai változatosak lehetnek, említést érdemel a munkaköri alkalmasság és a garantált bérminimum megállapítása, a munkáltató állásfelajánlási kötelezettsége,[555] valamint a kutatók után járó adókedvezmény érvényesítése,[556] valamint a vállalati vezetői engedély kiadása vagy különböző munkagépek kezelésének engedélyezése. Az adatfelhasználási érdek általában a munkakör és a tényleges feladatellátás jellegének megfelelően lehet megalapozott. Nem kérdéses ugyanis, hogy jogosítvánnyal nem rendelkező

[544] Mt. 44. §
[545] Mt. 23. §
[546] A munkaügyi ellenőrzésről szóló 1996. évi LXXV. törvény 3. § a) pont
[547] Arany-Tóth Mariann: Személyes adatok kezelése a munkaviszonyban. Budapest, Wolters Kluwer, 2016. 51 o.
[548] Art. 1. számú melléklet 3. pont
[549] Mt. 184. §
[550] Mt. 189. §
[551] Mt. 228. §
[552] Mt. 229. §
[553] Mt. 10. § (3) bekezdés szerint az okirat bemutatása követelhető, ebből következik, hogy jogszabály alapján a másolás nem indokolható
[554] Pályaalkalmassági vizsga
[555] Mt. 66. § (5) bekezdés
[556] A szociális hozzájárulásról szóló 2018. évi LII. törvény 15. §

személyt nem jó gyakorlat gépjármű vezetésére utasítani, ami mögött egyúttal megjelenik a közúti közlekedés biztonságának társadalmi motivációja is. A végzettségi és képzettségi adatok mellett szintén ezen a ponton a munkáltatói adminisztrációba kerül az orvosi alkalmassági véleményen,[557] valamint indokolt esetben az erkölcsi bizonyítványban szereplő adatkör is.[558]

A munkaszerződés megkötésekor és a jogviszony fennállása alatt a felek között a kommunikáció hivatalos és jog által szabályozott formája a tájékoztatás és a nyilatkozattétel, különös tekintettel a munkáltató hazai[559] és uniós[560] jogszabályokon alapuló tájékoztatási kötelezettségére. A névre szóló tájékoztatásokat az egyén körülményeit leíró, az egyént jellemző tulajdonságokként személyes adatként célszerű kezelni, így ezek is az adatjog hatókörébe tartoznak. Ilyen tájékoztatásnak minősül a munkavállaló munkaidőn kívüli magatartásának korlátozására irányadó szabály meghatározása,[561] valamint a munkáltató személyében bekövetkező változásról,[562] a munkáltató adatairól és a munkafeltétel változásról,[563] a 15 napot meghaladó külföldön történő munkavégzésről,[564] a kifizetett munkabér elszámolásáról[565] a leltárfelelősség feltételeiről,[566] és nem utolsó sorban a munkavállaló személyiségi jogainak korlátozásáról[567] szóló tájékoztatás.

A munkáltató tájékoztatásával párhuzamosan különféle típusú munkavállalói nyilatkozatok is megtételre kerülhetnek. Ezeknek egy része hasonlóan jog által szabályozott, de vannak olyanok, amelyeket a munkáltató saját elhatározásából követel meg, illetve léteznek a munkavállalóktól származó, önkéntes nyilatkozatok is. Példaként említhető az Mt. 6. § (4) bekezdése alapján tett bármely nyilatkozat, a munkavállaló képviselőjének meghatalmazása,[568] várandóssággal és emberi reprodukciós eljárással kapcsolatos nyilatkozat,[569] a fizetés nélküli szabadság igénybevételének bejelentése[570] és az Mt. 176. § szerinti jövedelmi viszonyokról kiállított igazolások. Az előbbiek mellett rendszerint előfordulnak utasítások és belső szabályzatok tudomásulvételéről szóló nyilatkozatok, illetve szükség esetén titoktartási nyilatkozatok.

- *Munkavédelemről és a teljesítés elszámolásáról*

Minden munkáltató alapvető kötelezettsége dolgozóinak védelme érdekében betartani és betartatni a munkavédelmi előírásokat. Ezen törekvések az esetek többségében adatok kezelésével nem járnak. Előbbi állítás alól biztos kivételt jelent a munkavédelmi oktatások dokumentálása, a munkabalesetek nyilvántartásba vétele, és az olyan ellenőrzési tevékenységek, amelyek részben vagy egészben munkavédelmi célok megvalósítására is alkalmasak (ittasság vizsgálat, kamerás megfigyelés stb.).

A munkavédelmi oktatások tartását az Mvt. írja elő, annak lényeges tartalmi elemeinek meghatározásával együtt. Ezek között szerepel az 55. § (1) bekezdésének azon előírása, amely szerint az oktatás elvégzését a tematika megjelölésével és a résztvevők aláírásával ellátva

[557] 33/1998. (VI. 24.) NM rendelet 15. számú melléklete
[558] Mt. 44/A §
[559] Mt. 6. § (4) bekezdés
[560] Az Európai Parlament és a Tanács 2002/14/EK irányelve az Európai Közösség munkavállalóinak tájékoztatása és a velük folytatott konzultáció általános keretének létrehozásáról
[561] Mt. 8. § (2) bekezdése
[562] Mt. 38. §
[563] Mt. 46. §
[564] Mt. 47. §
[565] Mt. 155. § (2) bekezdése
[566] Mt. 185. § (2) bekezdés
[567] Mt. 9. § (2) bekezdése
[568] Mt. 21. §
[569] Mt. 65. § (5) bekezdés
[570] Mt. 133. § (2) bekezdés

írásban kell rögzíteni. A munkavédelemmel kapcsolatos adatfelhasználás második tipikus esetkörét az Mvt. 64. § (1) bekezdése szabályozza, amely szerint a munkabalesetet – amely esetében a munkavállaló több mint három munkanapon át nem volt munkaképes – és a foglalkozási megbetegedést, valamint a fokozott expozíciós esetet ki kell vizsgálni, nyilvántartásba kell venni és be kell jelenteni. A munkabalesetekkel kapcsolatos nyilvántartás elemeit az 5/1993. (XII. 26.) MüM rendelet, míg a foglalkozási betegségek és fokozott expozíciós esetek bejelentésének és kivizsgálásának részletszabályait a 27/1996. (VIII. 28.) NM rendelet rögzíti, mérlegelést nem tűrő részletességgel.

A munka és pihenőidővel kapcsolatosan elsősorban a munkaidő-nyilvántartás vezetése merül fel. Jogszabályi hátterét az Mt. 134. § adja, a nyilvántartásvezetési kötelezettséghez kapcsolódó adatfelhasználás pedig egyértelműen kiolvasható belőle. Ezt a gondolatot erősítette az Európai Unió Bírósága, mikor kimondta,[571] hogy az olyan nyilvántartás, amely a munkavállalók munkaidejének kezdési és befejezési időpontját, valamint a szüneteket és a munkaidőhöz nem tartozó időszakokat rögzíti személyes adatnak minősül, függetlenül attól, hogy az adatok egy része minden munkáltatónál dolgozó személyre igaz lehet. A munkaidőnyilvántartás formájával kapcsolatban nincsenek kötelezően betartandó rendelkezések, arról minden munkáltató maga dönthet. Lehetséges papír alapú jelenléti íves vagy szoftveres megoldás is, továbbá az sem feltétel, hogy a nyilvántartás egy dokumentumban legyen fellelhető.[572] Utóbbi, tehát szoftveres megoldások esetén a felhasználás lényegi körülményei megváltozhatnak, mivel a fejlettebb technológia lehetővé tehet olyan összetett beléptető rendszerek létrehozását, amelyek lényegesen több adat gyűjtését és összehangolt feldolgozását valósítják meg.[573] Ilyen esetekben felmerül, hogy az adatkör túlterjeszkedik a munkaidőnyilvántartás elkészítésének célján és áthajlik a munkáltatói ellenőrzés területére, vagyis a vélelmezett helyett a megalapozott értékegyenlőség kategóriájába kerül át. Ezt megerősíti, hogy az adatvédelmi biztos korábbi megállapítása alapján elfogadhatatlan a nyilvántartás vezetése céljából az egyéni szükségletek teljeskörű naplózása.[574] Tehát az egyszerűbb (akár analóg), kevés adattal működő rendszerek közös érdeket alapozhatnak meg a munkáltató és a munkavállaló között, mivel ez alapján történik a szabadságok kiadása, illetve a munkában töltött idő a bérszámfejtéshez is felhasználásra kerül. Az adatok nyilvántartásvezetést meghaladó gyűjtése vagy felhasználása azonban az értékegyenlőséget gyengíti, amit így – a munkáltató unilaterális érdekeként – további vizsgálatnak kell alávetni, hogy az egyensúlyi helyzet megalapozott és igazolható legyen.

Mivel a hagyományos magyar munkajogi felfogás szerint a munkaszerződés kizárólag visszterhes szerződésként köthető meg érvényesen,[575] ezért a munkavállaló által elvégzett munka díjának megfizetése a munkáltató egyik elkerülhetetlen főkötelezettsége.[576]Az Mt. 155. § alapján a kifizetés elszámolási kötelezettséggel párosul a munkáltató oldalán, amely írásbeliséget és személyes adatokat feltételez, bár megjegyzendő, hogy amennyiben a munkabér meghatározására egyéb, a munkaszerződéstől eltérő megállapodásban kerül sor, akkor ezen megállapodásnak nem alaki kelléke az írásbeliség.[577] Az elszámolás elkészítéséhez figyelembe kell venni minden lényeges körülményt, így a munkaszerződés alapján járó alapbért, a bérformát, a munkában töltött időt, az esetleges bérpótlékokat, prémiumot, jutalmat

[571] C342/12. sz. „Worten” ügy
[572] Kúria Mfv. 10.636/2015/8.
[573] A 29. cikk szerinti munkacsoport 02/2017. számú véleménye a munkahelyi adatkezelésről (WP249), 22 o.
[574] ABI-19532/2011/P
[575] Bankó Zoltán, Berke Gyula, Kiss György, Szőke Gergely László: Nagykommentár a munka törvénykönyvéhez. Budapest, Wolters Kluwer Hungary, 2019. 578 o. (továbbiakban: Mt. Nagykommentár)
[576] Mt. 42. §
[577] BH2000. 464.

és jutalékot, valamint mindazt a terhet, amit a kifizetőnek le kell vonnia.[578] A munkabér kifizetése alapvetően a szerződés teljesítéséhez szükséges, a munkaszerződés adattartalmához hasonlóan azonban több jogszabály is hatással van a kezelt személyes adatokra. Amíg a munkaszerződés megkötésekor a felek teljes mértékben gyakorolhatták szabad akaratukat (amelynek kereteit szabta csak meg a jogszabály) jelen esetben döntési autonómiájuk lecsökkent. Az Art. pontosan meghatározza milyen adatokat kell a munkáltatónak gyűjtenie ahhoz, hogy eleget tegyen a havi adó- és járulékbevallási kötelezettségeknek.[579]

4.3.3.3. A munkáltató jogos gazdasági érdekeinek védelméről és a munkavállaló ellenőrzéséről

- *A jogos gazdasági érdek védelme általában*

A munkáltató jogos gazdasági érdekeinek védelmét az Mt. 8.§ (1) bekezdése teszi lehetővé, amely mindenekelőtt a munkavállaló által gyakorolható magatartásokra tartalmaz korlátozást. Ennek megfelelően a törvény kimondja (a joggyakorlattal összhangban[580]), hogy a munkavállaló a munkaviszony fennállása alatt nem tanúsíthat olyan magatartást, amellyel a munkáltatója jogos gazdasági érdekeit veszélyeztetné. A 8. § (2) bekezdése bizonyos esetekben a korlátozást kiterjeszti a munkavállaló munkaidején kívüli magatartására is.

Az összeférhetetlenségi vizsgálat alapját az Mt. 211. §-a adja – a Ptk. 3:115. § mellett – mivel kimondja, hogy a vezető további munkavégzésre irányuló jogviszonyt nem létesíthet, nem szerezhet részesedést a munkáltatóéval azonos vagy ahhoz hasonló tevékenységet is végző, vagy a munkáltatóval rendszeres gazdasági kapcsolatban álló más gazdálkodó szervezetben, nem köthet a saját nevében vagy javára a munkáltató tevékenységi körébe tartozó ügyletet. A vezető továbbá köteles bejelenteni, ha a hozzátartozója tagja a munkáltatóéval azonos vagy ahhoz hasonló tevékenységet is folytató vagy a munkáltatóval rendszeres gazdasági kapcsolatban álló gazdasági társaságnak, vagy vezetőként munkavégzésre irányuló jogviszonyt létesített az ilyen tevékenységet is folytató munkáltatónál. Az adatfelhasználás kiemelt jelentőségű, mivel a kialakult bírósági gyakorlat szerint a munkavállaló kötelezettségének megszegése esetén munkáltatói rendkívüli felmondásnak lehet helye.[581] Adatok kezelésére általában az adatalany által adott nyilatkozattal kapcsolatban kerül sor, amelynek adattartalmának lényeges elemeit – a fentiek tükrében – jogszabály határozza meg. Jó példát hoz az összeférhetetlenségi vizsgálat a munkavállalótól eltérő személy adatainak felhasználására, itt ugyanis semmilyen formális kapcsolat sem áll fenn a munkáltató és a munkavállaló hozzátartozója között. Megfigyelhető az unilaterális érdekeltségek működése, amely esetében az egyensúlyi helyzetet a jogalkotó állította fel, a munkáltatónak csak arra kell ügyelnie, hogy az adattartalom összeállításakor a szükségesség/arányosság mércéjét ne vétse el.

A szakirodalom álláspontja szerint a munkáltatót megilleti a munka feletti felügyeleti jog gyakorlása. A felügyelet tág értelmezése szerint kiterjed az összes fő és mellékkötelezettség teljesítésének értékelésére is. A formális értelemben vett teljesítményértékelés fogalma szerint olyan tevékenység, amely során végbemegy egy szervezet valamennyi dolgozójának adott időszakra vonatkozó teljesítményének módszeres felmérése, megítélése és értékelése. Másként megfogalmazva a teljesítményértékelés eredményeképpen megállapítható, hogy egy dolgozó

[578] Arany-Tóth, 2016. 69-72 o.
[579] Art. 50. §
[580] BH1996. 64.
[581] BH1996. 450.

milyen mértékben felel meg a munkakör elvárásainak.[582] Bár a magánszektorban nem rendelkezik jogi szabályozással, a közszférában általános gyakorlatnak mondható az eljárás.[583] A technológia adta lehetőségeket vizsgálva fontos az értékeléskor felmérni a felhasznált eszközökben rejlő kockázatokat is, amilyenek például a tisztán szoftveres – humán-közrehatás nélküli – automatizált döntéshozatalhoz vezető megoldások.[584] Függetlenül az alkalmazott eljárástól minden esetben a legfontosabb szempont, hogy az értékelés ne haladja meg a szükségesnél több adat gyűjtését vagy létrehozását, ellenkező esetben az értékegyenlőség megbomlik. Célszerű alaposan megvizsgálni az olyan részletes értékelési rendszer használatát, ami profilalkotást tesz lehetővé, hiszen a GDPR alapján az érintett bármikor tiltakozhat az ilyen adatkezeléssel szemben.[585] Az adatjogi értelemben vett tiltakozási jog különlegessége, hogy az egyik olyan jogintézménynek tekinthető, amely az adatok kezelésével kapcsolatban kifejezetten az értékegyenlőség megdöntésének eszközeként működik. Az értékeléskor különösen fontos, hogy azt kizárólag az érintettől származó és a munkavégzéssel összefüggő adatokra lehetséges alapozni, valamint a munkateljesítmény értékeléséhez szükségesnél több megállapítás kialakítására nem irányulhat. A teljesítményértékelés sajátossága, hogy kifejezetten új – sok esetben érzékeny természetű – személyes adat létrehozására irányul. A munkaügyi adatfelhasználásra kevésbé jellemző olyan adat létrehozása, amelynek teljesen új, az érintett számára is ismeretlen szemantikai rétege lenne. Az adatok jelentős része az érintettől származik (pl. személyazonosító adatok) vagy az érintett tudtával kerül létrehozásra a munkáltató által (pl. havi bér számfejtése). A teljesítményértékelés során, annak eredményeként létrejövő új adatok azonban az érintett számára teljesen ismeretlenek. Az új adatokkal kapcsolatban felmerülhet – egy kellően fejlett rendszer esetén – hogy azok olyan mértékű betekintést engednek a munkavállaló magatartásába, hogy a megismerés túlzott mélyítésére való alkalmasságán keresztül az értékegyenlőséget végérvényesen megszüntetheti. Ezáltal a teljesítményértékelést nem az adatfelhasználás, hanem már az adathasznosítás témakörénél kellene említeni. Ez kétségtelenül lehetségesnek tűnik, azonban fontosnak tartom kiemelni, hogy az adathasznosításba rendezetlenül áthajló felhasználási folyamatok valószínűleg kivétel nélkül értékegyenlőtlennek és így jogellenesnek minősülnének. Például az emberi elme működésére irányuló kutatást elsődleges tevékenységként egy munkahelyi teljesítményértékelésként lefolytatni egészen jogellenesnek hat. Az ilyen kutatást vagy eredetileg így, tehát kutatásként kell felépíteni és kommunikálni a munkavállalók felé, vagy az adatokat a valós teljesítményértékelést követően, a másodlagos hasznosításra vonatkozó jogszerűségi feltételek teljesítése után lehet valamilyen kutatásba bevonni.

- *Az ellenőrzési tevékenység részletszabályainak vizsgálatáról a kamerás megfigyelésen keresztül*

A munkáltató ellenőrzési tevékenységének kialakulása hosszú folyamat eredménye és szoros kapcsolatban áll a technológia adta lehetőségek minél nagyobb szintű kihasználásának igényével.[586] A személy, valamint a vagyonvédelmi igény a mindennapi életviszonyok keretei között jól értelmezhető, általánosan elfogadott törekvés, ennél fogva a munkáltató okkal várja el az együttműködést a védelemhez szükséges intézkedések betartásában. Fontos azonban annak a kérdésnek a vizsgálata is, hogy a személyi és vagyoni biztonság igénye mennyiben

[582] Juhász Csilla: Teljesítményértékelés a gyakorlatban. Jelenkori Társadalmi és Gazdasági Folyamatok. 3, 1 (2008). 55 o.

[583] Például: A közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény 130. §; A kormányzati igazgatásról szóló 2018. évi CXXV. törvény 96. §

[584] Hohmann Balázs, „Szempontok munkáltatói teljesítmény-értékelési rendszerek adatkezelési folyamatainak megalapozásához", Pécsi Munkajogi Közlemények 17 : 1. online különszám, 2024. 30-31 o.

[585] GDPR 21-22. cikk

[586] Kirstie Ball: Workplace surveillance: an overview. Labor History, 51:1 (2021) 87-106 o.

egyeztethető össze az érintett személyek magánszférájának védelmi igényével.[587] Tehát az ellenőrzések területén a csereérték helyes meghatározása különösen fontos. A jelenlegi gyakorlat a munkavállalók folyamatos és költséghatékony megfigyelését helyezi előtérbe, függetlenül attól, hogy azt mennyire indokolja valamilyen munkáltatói vagy társadalmi érdek. Élenjáró technológia a zárt-láncú televíziós megfigyelés (CCTV megfigyelés), a gépjárművekben GPS nyomkövető működtetése és a különféle struktúrájú beléptető rendszerek telepítése. Bizonyos szektorokban (pl.: mezőgazdaság) az előbbi három megfigyelési formát kiegészítheti a klasszikusabbnak mondható ittasság-vizsgálat, öltözőszekrény, ruházat vagy csomagátvizsgálás is. Az ellenőrzések gyűjtőfogalmaként funkcionáló „belső ellenőrzési rendszer" vagy „belső kontroll" területek vonatkozhatnak az elektronikus postafiókok, céges informatikai eszközök (telefon, laptop, PC) tartalmának, internethasználatnak, illetve céges előfizetések híváslistáinak ad hoc vagy rendszeres vizsgálatára is. Tekintve, hogy ezek mind hordozói lehetnek személyes adatoknak, és az adatokon végzett bármely műveletet adatkezelésnek tekintjük, a munkavállalók – munkáltatói unilaterális érdek alapján történő – ellenőrzése adatjogi szempontból is értékelendő. Hasonlóan az összeférhetetlenségi vizsgálathoz itt is könnyen elképzelhető, hogy olyan személyekről is adat kerül rögzítésre, akik még a munkavállaló hozzátartozójánál is távolabbi kapcsolatban állnak a munkáltatóval (pl. érdeklődök, potenciális ügyfelek vagy akár a létesítménybe más okból látogatók). Ennek következményeként általában a megfigyelési tevékenységek erős társadalmi legitimációval kell rendelkezzenek a jogszerűséghez, továbbá jellemzően szigorú garanciális szabályok is kapcsolódnak a megfelelő működéshez.

A technológiai fejlődés hatása elsődlegesen a rendelkezésre álló eszközrendszer átalakításában érzékelhető. Ennek eredményeként egyfelől a megjelenő új lehetőségek új célokat is magukkal hoztak, azonban az új eszközök a korábbi célokat is eltérő módon tették elérhetővé, ezzel kisebb-nagyobb mértékben átalakítva magát a folyamatot is. Westin magánszférával kapcsolatos kutatásai során jutott arra a következtetésre, amely szerint: *„bármely rendszernek, amely normákat teremt – miként minden emberi társadalom –, meg kell teremtenie a normák kikényszeríthetőségéhez szükséges mechanizmusokat. Mivel le kell leplezni azokat, akik megsértik a szabályokat és a tabukat, minden társadalomnak megvan a viselkedést figyelő, a normaszegést vizsgáló és a bűnt megállapító gépezete."*[588] Az idézet alapján tehát megállapítható, hogy a megfigyelés igénye egyidősnek tekinthető az emberi társadalmak normaalkotó tevékenységével, ám magának a tevékenységnek a hatékonysága – az adatalapúsággal párhuzamosan – hosszú ideig stagnált és csak az utóbbi évtizedekben indult drasztikus növekedésnek. Ennek a növekedésnek talán első és azóta is legkiemelkedőbb képviselője a térfigyelő kamera, aminek stilizált ábrája egyik elsődleges jelképévé vált az általános értelemben vett megfigyelésnek. A hatékonyság növekedése azonosítható például a távollevő személyek valós idejű megfigyelésének képességében, a felvételek rögzítésének és későbbi visszanézésének lehetőségében, valamint a technológia tömegessé válása mellett beszerzési költségének csökkenésével könnyebb elérhetőségében is.[589] A kamerás megfigyelés rövid áttekintésével lehetőségünk van további következtetéseket levonni az ellenőrzéssel megvalósított adatfelhasználás természetére vonatkozóan.

Az adatkezelő azonosítására általában nagy szükség van, azonban egy térfigyelő kamera rendszer működtetése esetén a megfigyelés technikai megvalósítása (üzemeltetés)

[587] Füzes Barnabás, Szőke Gergely László, „A technológiai változások hatása a munkavégzésre, különösen a munka-magánélet elhatárolására és annak jogi megítélésére", Pécsi Munkajogi Közlemények 17 : 1. online különszám, 2024. 44-45 o.
[588] Jóri, 2005. 13 o.
[589] Balogh Zsolt György, „Közterületi térfigyelés és adatvédelem", Vezetéstudomány XLII. ÉVF. 2011. 3. szám. 26-27 o.

szempontjából különös jelentőségre tesz szert. A megfigyelés érzékeny jellege miatt a jogosultságkezelési szabályokat a lehető legszigorúbban kell meghatározni, így függetlenül attól, hogy a munkáltató továbbra is adatkezelőként jelenik meg, a megfigyelésért felelős személy vagy szervezeti egység pontos kijelölése és a feladatainak meghatározása kiemelt jelentőségű. Az adatokhoz hozzáférők körének túl tág meghatározása ugyanis negatívan befolyásolhatja az adatkezelő és az érintettek érdekeinek egyensúlyát.

A gyűjtött – vagy gyűjthető – adatkörrel kapcsolatban mindenek előtt azt kell látni, hogy számottevő különbség van a magánterületek és közterületek megfigyelése között.[590] Az alapvető adatkezelési előírások nagyjából megegyeznek mindkét terület esetén, azonban a hatályos jogszabályok[591] csak nagyon szűk körben engedik meg közterületek elsődleges tevékenységként való megfigyelését.[592] Ehhez a szűk körhöz jelenleg biztosan a rendőrség és a közterületfelügyelet, illetve közterületfelügyelet hiányában a jegyző vagy a képviselő-testület által kijelölt köztisztviselő tartozik. Az adatfelhasználás megkezdése előtt tehát a megfigyelt területet és az annak megfigyelésére való lehetőséget szükséges tisztázni. A terület mellett a kamerarendszer telepítésekor alkalmazott technológia is befolyásoló tényező. Ennek ugyanis az elérni kívánt céllal (a célon keresztül kielégített érdekkel) arányban álló mennyiségű és minőségű adat rögzítését kell megvalósítania. Ebből kifolyólag a túl kevés adat (pl. nagyon gyenge felbontás) ugyanolyan aggályos, mint a túl sok (pl. arcfelismerésre képes kamerák[593]).

Függetlenül attól, hogy egyszerű vagy összetett technológia használatára kerül sor a jogszerű megfigyelés feltételei közül kiemelendő az adattípusával összefüggő jogalapválasztás kérdése. A képmás az emberi személyiség külső megnyilvánulása, mivel a külső megjelenésre a személyiség belső sajátosságait vetíti ki. A jogalapválasztás aggályát az okozza, hogy a Ptk. szerint a képmás vagy hangfelvétel elkészítéséhez és felhasználásához az érintett személy hozzájárulása szükséges.[594] Az előírás láthatóan nyelvtani egyezésben áll a GDPR hozzájárulás jogalapjával, azonban anélkül, hogy annak alkalmazási feltételeivel az összhangot megteremtette volna. A Ptk. miatt kötelezően alkalmazott hozzájárultatás által előidézett adatvédelmi és polgári jog párhuzamos alkalmazásának nehézségét többféleképpen próbálta a gyakorlat megoldani. Felmerült, hogy a GDPR-nak uniós jogként alkalmazási elsőbbsége van és a Ptk-t nem kell alkalmazni, illetve az is, hogy a Ptk. lex specialis, ezért a GDPR-t nem kell alkalmazni. Áthidaló megoldásként megjelent, hogy a Ptk. hozzájárulása és a GDPR jogalapjai egymás mellett kerülnek alkalmazásra, a két hozzájárulás pedig pusztán nyelvtani egyezésnek tekinthetők. A Ptk. hozzájárulása (ellentétben a GDPR-al) megadható ráutaló magatartással[595] vagy bekérése mellőzhető tömegfelvétel/közszereplés esetén.[596] A Ptk. szerinti hozzájárulás sikeres rendezésével a GDPR jogalapok közül bármelyik szabadon választható. A Hatóság álláspontja – nem érvelésében, hanem végeredményében – megerősíti ezt, mikor azt mondja, hogy „a munka világában az érintett hozzájárulása helyett más jogalap, *[például]* a munkáltató jogos érdekén alapuló adatkezelés alkalmazása indokolt.”[597] Ez alapján a jogalapok

[590] E tekintetben közterület alatt minden olyan terület érthetünk, amely az ingatlannyilvántartásban ilyen módon szerepel, magánterület pedig minden nem közterületként nyilvántartott terület, amely a szervezet tulajdonát képezi, illetve valamilyen érvényes jogcím alapján használatában áll.
[591] 1999. évi LXIII. törvény a közterület-felügyeletről (továbbiakban: Ktftv.) és 1994. évi XXXIV. törvény a Rendőrségről (továbbiakban: Rtv.)
[592] Fontos, hogy az Info.tv. 2. § (3) bekezdés szerint a megfigyelt terület jellegétől függetlenül személyes adatok bűnüldözési, nemzetbiztonsági és honvédelmi célú kezelésére nem a GDPR, hanem az Info.tv-t kell alkalmazni.
[593] Lásd részletesen: NAIH-963-10/2022
[594] Ptk. 2:48. §
[595] A Ptk. nagykommentár alapján: „A *hozzájárulás formáját* a jog nem írja elő, a mindennapi életben a ráutaló magatartással való hozzájárulás a gyakori, mikor is a hozzájárulást a tiltakozás, az elhárítás hiánya fejezi ki.”
[596] Lásd részletesen: Ptk. Nagykommentár 159-160 o.
[597] NAIH-1006-3/2022.

vonatkozásában külön kezelendők azok az adatkezelők, amelyek közhatalmat gyakorolnak vagy közfeladatot látnak el, valamint azok, amelyek nem, hiszen a GDPR 6. cikk (1) bekezdés második albekezdése szerint a 6. cikk (1) bekezdés első albekezdés f) pontja nem alkalmazható a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre, így míg előbbiek az f) pontra, utóbbiak jellemzően a GDPR 6. cikk (1) bekezdés e) pontjára támaszkodhatnak. A hozzájárulás mellőzése pedig jól tükrözi a munkáltató egyoldalú érdekeltségét.

Az adatfelhasználás céljai szempontjából kijelenthető, hogy bár a személy- és vagyonvédelem mint cél a legtöbbször jogszerű lehet, azonban a hatóság gyakorlata alapján[598] tényleges fenyegetettség fennállása szükséges konkrét helyen és időszakban ahhoz, hogy alkalmazható lehessen az adott adatkezelésre. A személy- és vagyonvédelmi célú kamerák esetén tekintettel kell lenni arra is, hogy a megfigyelni kívánt területen a települési, adott esetben a környező településekhez mért átlaghoz képest kiugróan magas-e a térfigyelő kamerák alkalmazása által kivédhető bűncselekmények előfordulása. Ez a szigorú hozzáállás érezhetően a megfigyelés mögötti társadalmi legitimációt igyekszik szűkíteni, ezáltal a elvárt értékegyenlőség eléréséhez szükséges szintet növelni. A fentiek figyelembevételével a térfigyelő kamerás megfigyelés esetén (is) igazolni kell a fennálló köz-, vagy magánérdek – célhoz mért – szükségességét és arányosságát,[599] hatásvizsgálatot[600] (DPIA) kell lefolytatni a telepíteni kívánt kamerákkal kapcsolatban, valamint a megfelelő tájékoztatási[601] pontokat szükséges beépíteni az adatkezelés folyamatába. A jogszerűségi tesztek (mint pl. ÉMT, DPIA) az értékegyenlőséget is hivatottak – a későbbi elszámoltathatóságot támogatva – vizsgálni és igazolni. A tájékoztatási rendszer a folyamat átláthatóságával az érintettek felé igyekszik érthető módon kommunikálni mindazt, ami ezen értékegyenlőség fennállásának megítéléséhez szükséges.

A munkavállalók megfigyelésére vonatkozóan általában azt mondhatjuk, hogy az átlagosnál nagyobb adatvédelmi jogi kockázattal járnak, a munkáltatói unilaterális érdek lévén az értékegyenlőség erős alapokon kell nyugodjon. Ehhez az is hozzájárul, hogy viszonylag kevés olyan kötelezően betartandó előírás létezik, ami a megfigyelési tevékenységet kellő pontossággal előírná, így annak részletszabályait általában a munkáltatónak kell kidolgoznia, ennek minden előnyével és hátrányával együtt.

4.3.3.4. A munkajogviszony megszűnéséről

A munkavállalói adatok életciklusának utolsó állomása a munkajogviszony megszűnésekor, illetve megszüntetésekor érkezik el. A munkaviszony megszűnésének eseteit az Mt.[602] rendezi, közös jellemzőjük adatkezelési szempontból, hogy a megszűnés eseménye a felek akaratától független, ezáltal csak a következményeivel kapcsolatban találhatók adatvédelmi kötelezettségek, amik megegyeznek a megszüntetés következményeivel, így az ott leírtak irányadók erre az esetre is. A megszüntetés típusaival kapcsolatban elemzésre csak az egyoldalú aktusok kerülnek, mivel a közös megegyezéssel történő megszüntetésre a szerződés megkötésére vagy módosítására vonatkozó szabályok alkalmazhatók. A jogviszony megszüntetésére irányuló lépések egyébiránt gyakorlatilag egyet jelentenek az adatfelhasználásra vonatkozó érdekek fokozatos eltűnésével, így ezen a ponton az érdekeltségek inkább a felek közötti elszámolásra, a függőben lévő folyamatok lezárására és amennyiben vannak ilyenek a vonatkozó jogszabályi előírások betartására terjednek ki.

[598] NAIH/2019/2076/11
[599] GDPR 6. cikk (3) bek.
[600] GDPR 35. cikk szerint nyilvános helyek nagymértékű megfigyelése nevesítetten magas kockázatúnak tekintendő, így hatásvizsgálat elvégzése kötelező
[601] GDPR 13-15. cikkei
[602] Mt. 63. § (1) bekezdése

- *A felmondásról és a munkáltatói jogutódlásról*

A felek részéről aktív magatartást feltételező megszüntetés eseteit az Mt. 64. §-a tartalmazza, a legnagyobb adatfelhasználási relevanciával pedig a munkáltató általi felmondás rendelkezik. Egyfelől fontos, hogy a munkaviszony megszüntetésére irányuló nyilatkozat, illetve megállapodás preferált formája az írásbeliség,[603] továbbá az, hogy a munkáltató felmondását köteles megindokolni.[604] Elsődleges szempont, hogy milyen adat kerül be a szóban forgó nyilatkozatba. Az Mt. 66. § (2) bekezdése a felhasználható adatok körét leszűkíti a munkavállaló munkaviszonnyal kapcsolatos magatartásával, képességével vagy a munkáltató működésével összefüggő körülményekre, ezen a területen belül azonban az indokolás szabadon megtehető. Az adatoknak tehát pontosnak kell lenniük, különben a felmondási ok valódisága és egyértelműsége[605] (okszerűsége[606]) kétségessé válik. Ahogy a GDPR úgy az Mt. 6. § (1) bekezdése és 7. §-a is megköveteli a felektől a tisztességes és rendeltetésszerű joggyakorlást, így figyelemmel kell lenni az adatok szükségességére az elérendő cél viszonylatában, valamint az adatok bizalmasságára is (az okok megismerésére csak a felek jogosultak). Ezen a ponton is fontos az egyenlő bánásmód elve, a diszkriminatív adatokra alapozott felmondás jogellenes adatkezelést is eredményez.[607] Fontos továbbá, hogy a felmondással megvalósuló adatfelhasználás egyik jogszerűségi előfeltételeként jelennek meg a munkáltatói felmondási tilalmak és korlátozások. Ezek körét olyan esetek alkotják, amelyek fennállása alatt a munkáltatói joggyakorlás azért tiltott vagy korlátozott, mert annak megvalósulása esetén a munkavállalónak a szokásoshoz képest nagyobb egzisztenciális nehézséget vezetne.[608]

A munkáltató személyében bekövetkező változás természetesen az adatkezelő személyében bekövetkező változást is eredményez. A jogügyleten alapuló átvétel időpontjában a fennálló munkaviszonyból származó jogok és kötelezettségek az átadóról az átvevő munkáltatóra szállnak át.[609] A törvényszöveg (és gyakorlat[610]) automatizmusa[611] adatfelhasználási szempontból is lényeges, hiszen a munkavállaló beleegyezésére nincs szükség a jogszerű átadáshoz. Ezáltal a munkaviszonyból eredő adatkezelések a munkaszerződéssel együtt szállnak át az új munkáltatóra, e tekintetben az érintett jóváhagyása nem szükséges. Nem feltétlenül vonatkozik a fenti kijelentés minden típusú – főként az önkéntességen alapuló és ellenőrzési célú – felhasználásra. Lehetséges, hogy a munkavállaló bizalma a korábbi munkáltatóban elég erős volt ahhoz, hogy jogos érdekének fennállását elfogadja a kamera rendszer működésével kapcsolatban, az új munkáltató esetén azonban ez nem feltétlenül kell, hogy így legyen. Az sem kizárt, hogy a munkavállalónak ellenérzései vannak az új munkáltatójával kapcsolatban és a továbbiakban nem kíván a cég weboldalán nevével és fényképével szerepelni, így az ahhoz adott hozzájárulásának visszavonása bekövetkezhet.

- *Az eljárásról a munkaviszony megszűnésekor*

A munkaviszony megszűnésekor a munkáltató iratkiadási kötelezettségének eleget téve különböző igazolásokat és adatlapokat kell átadjon a munkavállalónak, a későbbi

[603] BH1999. 331.
[604] Mt. 66. §
[605] BH1998. 195.
[606] MK 95. számú állásfoglalás
[607] 4/2017. (XI. 28.) KMK vélemény
[608] Bankó Zoltán, „A munkáltatói hatalom korlátai a munkaviszony megszüntetése során – a felmondási tilalmak és korlátozások a magyar munkajogban", JURA 2015/2. 5 o.
[609] Mt. 36. § (1) bekezdése
[610] MK 154. számú állásfoglalás
[611] Mt. Nagykommentár. 209-210.

jogérvényesítésének elősegítése érdekében.[612] A jelenlegi Mt. nem részletezi,[613] hogy mit kell tartalmaznia az iratoknak, e tekintetben külön jogszabályban meghatározott előírásokat kell alkalmazni, amelyek elsősorban az adó- és társadalombiztosítási igazolásokat jelentik.[614] Ezek között szerepel a biztosítási jogviszonyról és az egészségbiztosítási ellátásokról kiállított igazolvány, a munkáltatótól származó jövedelemről, az adó és adóelőleg levonásáról szóló adatlap, a levont egyéni és munkáltatói járulékalapot képező juttatásokról kiállított igazolás, az álláskeresési járadék és az álláskeresési segély megállapítását segítő igazolólap, valamint a munkáltatói igazolás a munkabért terhelő tartozásokról.

A munkáltató a munkavállaló kérelmére munkaviszony megszüntetésekor (megszűnésekor) vagy legfeljebb az ezt követő egy éven belül a munkavállaló munkájáról írásban értékelést ad (feltéve, hogy a munkaviszony legalább 1 évig fennált).[615] Az értékelésbe csak valós ténymegállapítások kerülhetnek, ellenkező esetben a munkavállaló az értékelés megsemmisítését vagy módosítását bíróságtól kérheti (amely egyértelműen az értékegyenlőtlen helyzet megszüntetésére irányuló jogintézmény).[616] Megjegyzendő, hogy valós tényállítások esetén is figyelemmel kell lenni a volt munkavállaló személyiségi jogaira.[617]

A törvény megköveteli a munkavállalótól, hogy a munkáltató által előírt rendben munkakörét átadja.[618] Különös jelentősége lehet a céges eszközök visszaadásának és a céges postafiók átadásának. Lényeges eltéréseket okozhat az, ha a belső gyakorlat megengedi a munkavállalók számára az említett eszközök és hozzáférések vegyes (magán és hivatali) használatát. Az Mt. 2019. évi módosítása óta ehhez külön megállapodást kell kötni, hiszen alapértelmezés szerint a munkáltató által biztosított eszközök csak munkavégzésre használatók.[619] Függetlenül a belső szabályozástól a munkavállaló munkavégzéssel össze nem kapcsolható személyes adatait a munkáltató nem használhatja fel, így az e-mailek, az eszközökön lokálisan és a vállalat által biztosított saját szerveren vagy felhőtárhelyen tárolt adatok ellenőrzésének végrehajtása során a fokozatosság elvét mindvégig szem előtt kell tartani.[620]

Az esetek döntő többségében jogszabályi tárolási kötelezettség írja elő vagy a magán, vagy közérdek által indokolható a munkáltató számára volt munkavállalója adatainak további tárolása, de előfordulhatnak egyedi megállapodások is. A jogviszonyt túlélő tárolás időtartama többféle lehet, annak is a függvényében, hogy milyen jog hatálya alatt áll a munkáltató. A volt munkavállalóra irányadó öregségi nyugdíjkorhatár betöltését követő 5 évig tartó megőrzést a Tny. 99/A. § írta elő 2024. december 31-éig a Tbj. 66. § (1)-(2) bekezdésében meghatározott adatkör tekintetében. Az indokolás alapján jelentős adminisztratív terhet jelentett a vállalkozások számára a biztosítottakra vonatkozó munkaügyi iratok megőrzésének ilyen kötelezettsége, ezért ez felmenő rendszerben, 2025. január 1-jétől kivezetésre került, a megőrzés így csak a 2024. december 31-ig keletkező iratokra marad fenn. Ezt követően a nyugellátás megállapításához szükséges adatokat az állami nyilvántartások tartalmazzák. Az általános megőrzést a Tny. mellett ágazati szabály is megállapíthatja, így például az

[612] Arany-Tóth, 2008. 325 o.
[613] A kiadott apasági szabadság vagy szülői szabadság tartamára vonatkozó munkáltatói igazolás kiállításán kívül
[614] Mt. Nagykommentár. 468 o.
[615] Mt. 81. §
[616] Mt. 81. § (2) bekezdés
[617] Mt. Nagykommentár. 470 o.
[618] Mt. 80. § (1) bekezdése
[619] Mt. 11/A (2) bekezdés
[620] A NAIH tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről (2016) 10 o.

önkormányzati hivatalok[621] és nevelési-oktatási intézmények[622] esetén külön rendelet határozza meg a megőrzési időket. Szintén alapot ad a megőrzésre az Mt. elévülési ideje, amely szerint az adatfelvételt vagy a jogviszony megszűnését követő 3 évvel törölhetők azok az adatok, amelyek esetlegesen a munkáltató saját jogainak védelméhez vagy azok érvényesítéséhez szükségesek lehetnek.[623] Ezt kiegészítő szabály, hogy a bűncselekménnyel okozott kár megtérítésére vagy a személyiségi jogsértéssel összefüggő sérelemdíj megfizetésére irányuló igény öt év alatt, vagy ha a büntethetőség elévülési ideje ennél hosszabb, ennek megfelelő idő alatt évül el.[624] A továbbtárolás jogszerűségi feltételeivel nem rendelkező adatot a munkáltató visszaállíthatatlan módon köteles törölni minden rendszeréből, hiszen az adatkezelés jogszerű cél és érvényes jogalap nélkül csak értékegyenlőtlen lehet.

4.3.4. Összegzés a felhasználás jogáról

Az adatok felhasználásának jogával kapcsolatban összegezve az alábbiakat mondhatjuk.

- A felhasználás joga jellemzően kompozit adatjogi előírásokban testesül meg, amelyek az adatok kezelésének alapvető paramétereit adják meg. Ilyen a konkrét adatkezelési cél, adatkör vagy megőrzési idő meghatározása. Például:
    - Mt. 11. § (1) bekezdés: a munkavállaló biometrikus adata az érintett azonosítása *céljából* abban az esetben kezelhető, ha ez valamely dologhoz vagy adathoz történő (…) jogosulatlan hozzáférés megakadályozásához szükséges (…)
    - Az Art. 1. melléklet 1. pont: az állami adó- és vámhatósághoz be kell jelenteni az adózó nevét (elnevezését), rövidített cégnevét, természetes személy adóazonosító jelét stb.
    - Tny. 99/A. § (2024. december 31-ig): a nyilvántartásra kötelezett a biztosított, volt biztosított biztosítási jogviszonyával összefüggő, a szolgálati időről vagy a nyugellátás megállapítása során figyelembevételre kerülő keresetről, jövedelemről adatot tartalmazó munkaügyi iratokat, adatokat és foglalkoztatási igazolásokat a biztosítottra, volt biztosítottra irányadó öregségi nyugdíjkorhatár betöltését követő öt évig köteles *megőrizni*.
- A felhasználás kevésbé explicit oldalához az ágazati jog által kinyilvánított célok, illetve lehetőségek megvalósítása érdekében végzett adatkezelések tartoznak, amelyeknek azonban a részleteit nem adja meg a joganyag, ezért azt általános adatjogi jogelvek mentén kell az adatkezelőnek meghatároznia. Például:
    - Mt. 11/A. § (1) bekezdés: A munkavállaló a munkaviszonnyal összefüggő magatartása körében ellenőrizhető. Ennek keretében a munkáltató technikai eszközt is alkalmazhat, erről a munkavállalót előzetesen írásban tájékoztatja.
    - Mt. 134. § (2) bekezdés: A (munkaidő-)nyilvántartásból naprakészen megállapíthatónak kell lennie a teljesített rendes és rendkívüli munkaidőnek, valamint a készenlét kezdő és befejező időpontjának is.
- Léteznek a felhasználáshoz tartozó, de felhasználási jog által egyáltalán nem szabályozott területek, amelyeknek egyetlen közös jellemzője, hogy nem létezik rájuk vonatkozóan valamilyen kifejezett tiltás. Ezeknek ilyenformán keretet nem a

[621] Az önkormányzati hivatalok egységes irattári tervének kiadásáról szóló 78/2012. (XII. 28.) BM rendelet szerint például bér- és munkaügyi kimutatásokat, nyilvántartásokat, jelentéseket 10 évig, a bérkartont 50 évig kell megőrizni.
[622] A nevelési-oktatási intézmények működéséről és a köznevelési intézmények névhasználatáról szóló 20/2012. (VIII. 31.) EMMI rendelet 1. melléklet szerint a személyzeti, bér- és munkaügyeket 50 évig kell megőrizni.
[623] Mt. 286. § (1) bekezdés;
[624] Mt. 286. § (2) bekezdés;

felhasználás, hanem a védelem összetartó-hatású rendelkezései adnak (pl. alapelvek, jogalapok stb.). Például:

- Munkavállalók képmásának weboldalra való feltöltése

4.4. A hasznosítás joga

A fentiek során az adatok fogalmi rendszere a védelem és a felhasználás vonatkozásában került vizsgálatra. Korábban azt rögzítettük, hogy az adatfelhasználáshoz olyan folyamatok tartoznak, amelyek esetén az értékegyenlőség jellemzően olyan magas, hogy az vagy vélelmezett vagy valamilyen vizsgálattal/teszttel megalapozható. Ezzel szemben az adathasznosítás alatt az olyan adatkezeléseket értjük, amelyek az értékegyenlőség szempontjából kevésbé erős alapokon nyugszanak, így az adatkezelést valamilyen formában ellentételezni kell ahhoz, hogy az jogszerűnek legyen tekinthető. Ebből az ellentételezésből származó tranzakciós jellegből következően azt mondtuk, hogy az ilyen viszonyok között az adatok elsődlegesen, mint monetizált erőforrások jelennek meg. Ilyen tulajdonságai miatt központi eleme az adathasznosításnak, hogy lényegesen nagyobb mértékben érvényesül benne a privátautonómia, a felhasználás során látott tűréskényszer itt nem tapasztalható. Ez az értékegyenlőség erejének alacsonyabb szintjéből fakad, hiszen a folyamatok mögött álló társadalmi legitimáció nem olyan erős, hogy az egyenlőséget vélelmezzük vagy pusztán egy jogszerűségi teszttel megalapozzuk. Tesztekre egyébként a hasznosításban is szükség van, tekintve, hogy az értékegyenlőségnek csak az alacsonyabb szintje megengedett, nem a teljes hiánya.

4.4.1. Az adathasznosításról általában

4.4.1.1. A fogalmáról és formáiról

Az adatokat a világ tényszerűségeit önállóan reprezentáló, de rendszert alkotó szimbólumaiként definiáltuk, amelyek így egyfelől a kognitív képességek alapját képezik, másfelől közvetítő közeget alkotnak a külvilág és az elme belső folyamatai között. Az adat ilyen módon történő definiálása és az adathasznosítás tényállapota alapján a hasznosítás céljaként a kognitív folyamatok gyorsítását és mélyítését, ezáltal az organikus elme képességeinek adatalapú megerősítését vagy a mesterséges elme létrehozására irányuló törekvéseket jelölhetjük meg.

Az adatokon végzett műveletek szempontjából az adathasznosítás legalább két – korábban részben érintett – kategóriába sorolhatók.[625] Egyfelől az adat hasznosítható elsődleges tevékenységként, ilyenkor az adat eredtileg is a hasznosítása céljából került begyűjtésre (ezeket az adatkategorizáláskor termelt adatokként jelölöm, az adatok általános kategóriái szerint pedig ezek rögzített adatoknak minősülnek). A jelenlegi adathasznosítással kapcsolatos diskurzust kevésbé köti le az elsődleges hasznosítási tevékenység, mivel a már meglévő hatalmas mennyiségű adat újrahasznosítása egy égetőbb és látványosabb jelenség.

A hasznosítás másik nagy típusa a már valamilyen egyéb célból gyűjtött és kezelt adat másodlagos hasznosítása vagy újrahasznosítása (ezek a nyers adatok kategóriáját alkotják, általános adatkategória szempontjából pedig a „lehulló adat" és a „múlóadat" köréhez tartozhatnak). Az újrahasznosítás, mint tevékenység leírható, mint adatok kereskedelmi vagy nem kereskedelmi célra való hasznosításaként, amely kívül esik az eredeti célkitűzésen, amire az adatot előállították."[626] Ilyen szekunder hasznosítás lehet például egy szerződéses

[625] Bart Custers and Helena Ursic, „Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection", International Data Privacy Law, vol. 6, no. 1. 2016. 4-15 o.

[626] A már nem hatályos Közadattv. 4. § 8. pontja alapján; Az elgondolás a DGA 2. cikk 2. pontja szerinti további felhasználáson alapul: a közszférabeli szervezetek birtokában lévő adatok természetes vagy jogi személyek általi felhasználása olyan kereskedelmi vagy nem kereskedelmi célokra, amelyek kívül esnek azon a közfeladat ellátása keretén belüli eredeti célon, amelyre az adatokat előállították, a közszférabeli szervezetek közötti, kizárólag

személyazonosító adaton, nem azonosítás, hanem például elemzés céljából történő műveletvégzés. Mielőtt a másodlagos adathasznosítás tipizálására rátérnék, megjegyezném, hogy álláspontom szerint nem tartozik ehhez a kategóriához a meglévő adatoknak pusztán a gyűjtési céltól eltérő célra történő ismételt használata. Tehát ugyanazon adat több alkalommal, azonos módon történő használatát egyszerűen adatkezelési műveletnek tekintem, amely ugyanúgy része lehet egy adathasznosítási vagy felhasználási folyamatnak. Így bár nyelvtani értelemben a szerződéses adatok a szerződő fél azonosítása mellett *hasznosíthatók* egy email címzettjének azonosítására is, de ez ettől még nem szekunder adathasznosítás. Az ilyen és egyéb adatok adatbázisba szervezése és annak elemzése által pontosabb kép kialakítása az ügyfélkör vásárlási szokásairól viszont már jó eséllyel igen. A példában is láthatóan a hasznosítás gyakorlatának visszatérő motívuma az adatelemzés, amit a következőképpen definiálhatunk: az adatok, dokumentumok emberi tevékenység kifejtésével vagy informatikai eszközökkel vagy a kettő kombinációjával való feldolgozása és a rendelkezésre álló adatokból újabb származtatott információ előállítása, valamint a feldolgozott adatokból következtetések levonása emberi tevékenység kifejtésével vagy informatikai eszközökkel vagy a kettő kombinációjával.[627]

A szakirodalom alapján a másodlagos hasznosítást az alábbi módszer szerint bonthatjuk tovább:[628]

- Az első hasznosítási módszer az adatok új célra történő ismételt használata („data repurposing"). Megjegyzendő, hogy az új – de az eredetivel kompatibilis – cél ebben az értelemben gyengébb értékegyenlőséget kell mutasson, ahhoz, hogy adathasznosításnak lehessen tekinteni. Ezt nevezhetjük újrahasznosításnak.

- A másik hasznosítási módszer az adat újra-értelmezése („data recontextualization"), ami az eredeti adatkezelési környezethez nem kapcsolódó, új cél szerinti feldolgozást jelent. Tehát míg az újrahasznosítás az eredeti céllal összeegyeztethető, addig a rekontextualizáció valószínűleg nem az. Összeegyeztethetőség mércéjéhez felhasználható a GDPR fogalomrendszere szerinti kompatibilitás.[629]

    - A kialakult gyakorlat szerint az összeegyeztethetőség létét egyedileg szükséges megállapítani, az szoros összefüggésben van egyfajta ésszerű előreláthatósággal.[630] Tehát, akkor, ha a folyamat kezdőpontján az okkal feltételezhető, hogy az adat ilyen területen/okból további hasznosításra kerül akkor az kompatibilis, amennyiben nem, akkor nem az.

Az újrahasznosítás és a rekontextualizáció között alapvetően a műveletek hatóköre (scope) tekintetében van különbség, míg előbbi a szegmensen belül marad, utóbbi nagyobb volumenű, szélesebb spektrumú hasznosítást feltételez. Zárásképpen fontos kiemelni, hogy a hasznosítás logikájában hangsúlyos a – döntően elemzés által megvalósuló – tercier (másként megfogalmazva minden további) adathasznosítás is, amely adathasznosítási kategória szempontból a finomított adatként, általános kategóriák szerint a származtatott adatként került

közfeladataik ellátása keretében történő adatcsere kivételével; Ez a Nah.tv. 2. § 35. pontjában úgyszintén megjelenik.

[627] Nah.tv. 2. § 2. pont

[628] Bart Custers, Helena U. Vrabec, Michael Friedewald, „Assessing the Legal and Ethical Impact of Data Reuse: Developing a Tool for Data Reuse Impact Assessments (DRIA), European Data Protection Law Review (EDPL), vol. 5, no. 3. 2019. 317-337 o.

[629] GDPR 5. cikk (1) bekezdés b) pont második fordulata; Hangsúlyozottan ez csak személyes adatok esetén kötelező előírás, nem személyes adatok esetén ilyen nincs, azonban, mint támpont esetlegesen alkalmazható lehet.

[630] 29. cikk szerinti munkacsoport 03/2013 sz. iránymutatása a célhoz kötöttséggel kapcsolatban (WP 203), 2013.

korábban megjelölésre. Ettől a ponttól az adat forrása az előző hasznosítási művelet és nem az eredetileg vizsgált tényszerűség.

4.4.1.2. A szereplőiről

A továbbhaladás előtt érdemes tisztázni az adatgazdaságban résztvevők jellemző pozícióit (azok, akik nem vesznek részt az adathasznosítás folyamatában természetesen léteznek, de itt nem kerülnek kiemelésre). Először is vannak olyanok, akik rendelkeznek adatokkal, de szakértelemmel/szándékkal/lehetőséggel nem, így azokat saját maguk nem hasznosítják, ezért egy másik szereplő szolgáltatásait veszik igénybe ehhez (i). Az ilyen szolgáltatók a következő résztvevők, akik saját adatokkal nem rendelkeznek, de a hasznosításhoz szükséges szakértelemmel/módszerekkel/eszközökkel igen (ii). A harmadik szereplői kör az előző kettő ötvözete, vagyis azok, akik rendelkeznek adatokkal és hasznosítják is azokat (iii).[631] A szereplők között, az adatkezelési műveletek láncolatában betöltött pozíciójuk alapján megkülönböztethetünk elsődleges (primer szereplő[632]), másodlagos (szekunder szereplő[633]) és harmadlagos (tercier szereplő[634]) feleket. Az első helyen az adatokkal direkt kapcsolatban lévő szerepel, második, aki közvetve kötődik az alapfolyamathoz, míg harmadik helyen az eredeti adatkezeléssel semmilyen kapcsolatban nem állók találhatóak.[635] Az előbbi általános pozíciók után érdemes áttekinteni a jelenleg jellemzően alkalmazott terminológiát. Az adathasznosítási folyamatnak alapvetően két oldala van, egyik a kínálati, másik a keresleti oldal, ennek megfelelően az alábbi szerepek azonosíthatók. Fontos előzetesen rögzíteni, hogy ezek a szerepek egymással szoros kölcsönhatásban vagy akár átfedésben is állhatnak az adatalapú értékláncon belül.

	Típus	*Jellemzői*
Kínálati oldal	Adatgazdák	A fő tevékenységük nem kapcsolódik adatalapú termékek, szolgáltatások és technológiák előállításához és szállításához, azonban ettől függetlenül adatok jönnek létre a működésük során.
	Adatbeszállító[636]	Fő tevékenységük adatokkal kapcsolatos termékek, szolgáltatások és technológiák előállítása és szállítása.[637]
Keresleti oldal	Adat(fel)használó[638]	Olyan szervezetek, amelyek intenzíven hoznak létre, hasznosítanak, gyűjtenek és elemeznek adatokat, és az így szerzett ismereteket az üzleti tevékenységük javítására vagy új termékek létrehozására használják fel. [639]

[631] Mayer-Schönberger, Cukier, 2014. 141-146 o.
[632] angolul „1st party", magyarul „elsőfél"
[633] angolul „2nd party", magyarul „másodfél"
[634] angolul „3rd party", magyarul „harmadfél"
[635] Sophia Bernazzani Barron, „A Basic Definition of First Party, Second Party, & Third Party Data", HubSpot.com Elérhető. https://www.bing.com/search?q=first+party+data&qs=UT&pq=first+party&sc=10-11&cvid=398B6C979C8644D8B811AF3980A74637&FORM=QBRE&sp=1&ghc=1&lq=0&ntref=1 Letöltve: 2024.01.24.
[636] European Data Market Study 2021–2023, D2.5 Second Report On Policy Conclusions. The Lisbon Council (2023).
[637] DGA 2. cikk 8. pontjában meghatározott adatbirtokos fogalommal összhangban
[638] European Data Market Study 2021–2023, D2.5 Second Report On Policy Conclusions. The Lisbon Council (2023).
[639] DGA 2. cikk 9. pontjával összhangban

	Adatfogyasztók[640]	Olyan szervezetek, amelyek adatalapú termékeket és szolgáltatásokat vesznek igénybe a tevékenységük előmozdítására.

4.4.1.3. Az adattípusairól

A hasznosítható adatokkal kapcsolatban fontos ismét leszögezni, hogy azokat alapvetően erőforrásként célszerű kezelni. Az adatok erőforrás jellegével kapcsolatban a szemiotikus adatfogalom vizsgálata során az alábbi releváns ismérveket azonosítottuk:

- nonrivális és másolható,
- egyedszinten kizárólagos,
- immateriális,
- valamint bővülő.

Ezek alapján ugyanazon adat egy időben több érdekelt fél által is hasznosítható, anélkül, hogy ezáltal megszűnne létezni. Az adatok könnyen, olcsón és gyorsan sokszorosíthatók digitális formátumukban, a megfelelő szervezés-szabályozási és technikai intézkedésekkel (tényleges erőhatalom gyakorlásával) azok egyedszinten, potenciálisan kizárólagossá tehetők. Végezetül fontos, hogy állományi szinten bővülő erőforrásnak tekinthetők jelen állapotukban.

Ezek az ismérvek rávilágítanak az adaterőforrás különleges helyzetére, amelyek a hasznosítását meglehetősen összetett feladattá és egyúttal egyedülálló gazdasági és politikai lehetőséggé teszik. A 2. főfejezetben elkezdett adatfogalom meghatározásunkat az adatoknak a hasznosítási folyamatban betöltött pozíciója alapján történő csoportosítással egészíthetjük még ki ahhoz, hogy teljes adatjogi képet kaphassunk.

- *Nyers adat*[641]

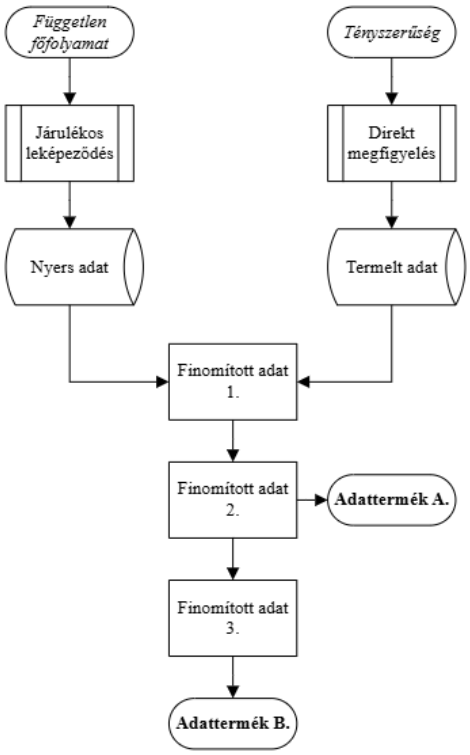
Ez egy felhasználási vagy hasznosítási főfolyamat során létrejövő adathalmazként írható le, amely így a főfolyamat „melléktermékeként" kerülhet[642] másodlagos hasznosításra. Létezhet analóg és digitális formában, bár minden bizonnyal utóbbi a jellemzőbb, tekintve, hogy a nyers adatoknak kiemelt elemei az informatikai eszközök működése során automatikusan generált adatok, illetve a szenzoros adatok. Ezek mellett ide tartozhatnak a mindennapi élet bármely eseménye/cselekménye során keletkező számtalan adat, függetlenül annak jogi megítéléstől (pl. szerződéskötés, foglalkoztatás, köznevelés stb.). Struktúra és forma tekintetében a tapasztalat alapján nagy mennyiségű strukturálatlan és kvalitatív adat fordul elő ezek között, tekintve, hogy nem a későbbi, minél hatékonyabb hasznosítás, hanem az eredeti célok elérésének szüksége dominált a főfolyamat során. A nyers adatok típusuk szerint vegyes képet mutatnak, annyi azonban elmondható, hogy az indexált és attribútum adatok mellett a metaadatok szerepe itt tesz szert a legnagyobb jelentőségre. Fontos továbbá, hogy a járulékosságuk miatt másodlagos (szekunder) hasznosíthatóság jellemzi a nyers adatokat, tehát valamilyen további feldolgozási művelet nélkül egyáltalán nem, vagy csak csökkent mértékben használhatók.

[640] European Data Market Study 2021–2023, D2.5 Second Report On Policy Conclusions. The Lisbon Council (2023).

[641] Charles I. Jones, Christopher Tonetti, „Nonrivalry and the Economics of Data", American Economic Review 2020, 110(9): 2819–2858 DOI: https://doi.org/10.1257/aer.20191330

[642] Így a korábbi Kitchin-féle általános adatkategóriák szerint a nyers adatok hasznosítás esetén un. „lehulló" adatoknak minősülnek, míg a hasznosítás elmaradása esetén un. „múlóadatnak". Részletesen lásd: 2.2.3. alfejezet

- *Termelt adat*[643]



Az adatok gyűjtése és rögzítése lehet kifejezetten az adat megszerzésére és hasznosítására irányuló folyamat. Ebben az esetben tehát nincs egy főfolyamat (pl. autó adásvétel), aminek a melléktermékeként jönnek létre az adatok, az adatrögzítés kifejezetten azért történik, hogy az adat hasznosítható legyen. Ide sorolhatók az analóg vagy digitális mérések eredményei, nyilvántartási (és elemzési) célú adatrögzítések, személyiség-profilhoz tartozó adatok és az olyan szenzoros adatok, amelyek nem tekinthetők járulékosnak egy kapcsolódó főfolyamathoz képest (pl. egy okos kazán termosztátjának adatrögzítése járulékos a kazán működéséhez képest, míg egy okos óra lépésszámlálójának elsődleges és egyetlen célja az adat rögzítése). Az ilyen adatok tehát elsődleges (primer) hasznosítás céljára szolgálnak, ennek megfelelően könnyen olvasható és használható formátumban, legalább részben strukturáltan jönnek létre. Ezek önmagukban is értékesek lehetnek, de további feldolgozással az értékük növelhető. Forma szempontjából kvantitatív és kvalitatív adatok egyenlő jelentőséggel bírnak, attól függően, hogy a megfigyelt tényszerűség reprezentálása milyen módon a legcélravezetőbb. Típusaival kapcsolatban rögzíthető, hogy ellentétben a nyers adatokkal itt az indexált és attribútum adatoknak lényegesen nagyobb szerepe van a metaadatokhoz képest (utóbbiak jelentősége a strukturáltság biztosításában rejlik).

- *Finomított adat*

Olyan származtatott adatok tartoznak ide, amelyeken már hasznosítási művelet vagy műveletek elvégzésére kerültek, az értékteremtés / értéknövelés elkezdődött / megtörtént (vagyis harmadlagos [tercier] hasznosítás ment végbe). A finomított adatok – minthogy egy megelőző folyamat kimenetei és egy következő folyamat bemenetei – jellemzően kvantitatívak, strukturáltak és attribútum típusúak. Az adatokon végzett műveletek teljes mértékben attól függenek, hogy milyen területen, milyen célok szerint, milyen adatokkal kapcsolatban kerülnek végrehajtásra. A „finomítottság foka" természetesen sokféle lehet, az elvárt minőséget az érdekelt felek jellege határozhatja meg (míg egy adatokkal foglalkozó szakember / vállalkozás alacsonyabb finomítottságú adatokat is értékesnek találhat, addig egy „végfelhasználó" mindössze eshetőlegesen meglévő szaktudása függvényében lehet rá csak képes).

- *Adattermék*[644]

Az adat végállapotát a megfelelő mélységű és minőségű finomítottsággal és egy adott szükséglet kielégítésére alkalmas egyediesítéssel érhetjük el. Ez a megfelelő adatoknak, a megfelelő helyre/személyhez történő eljuttatását, és szükség szerint az adott helyzetre értelmezését vagy a kérdéses folyamatba beépítését jelenti. Az adattermék tehát egyedi esetben értékes, egy konkrét szereplő számára hasznos adatot jelöl, így az megfelelő működés esetén a végfelhasználó

13. *ábra: a hasznosítás adattípusai*

[643] Kyu Yub Lee, Hyun Park, „Data, Privacy, and Artificial Intelligence", SSRN Electronic Journal 2022. DOI: 10.2139/ssrn.4246578

[644] „The Technology Landscape Of Data Spaces" Sitra Working Paper ISBN 978-952-347-327-0 9 o.

számára információnak minősül, míg az adattermék szolgáltatója szempontjából megőrzi adat jellegét. Ezek az újonnan létrejött, származtatott adatok ismét egy főfolyamatban fognak, mint primer adatok szerepelni, olyan formában, struktúrában és típusban, ami ezt a főfolyamatot leginkább kiszolgálja. Fontos azonban, hogy az adattermék létrejöttével az adathasznosítás folyamata véget ér, az azt követő szakaszra már az adatfelhasználás előírásai lesznek irányadók.

4.4.2. Az adathasznosítás elméleti folyamatáról

Az adatok nem a vákuumban keletkeznek, léteznek és hasznosulnak, azok szervesen kötődnek valós környezeti, politikai, gazdasági és interperszonális eseményekhez, cselekményekhez, ennek megragadása pedig egy jogi értelemben egészen széles látóteret indokol, amit célszerű az adatalapú működéshez igazíthatunk. Ennek a szemléltető bemutatására hosszú ideje az „adat az új olaj" párhuzam a legjellemzőbb megoldás, azonban ezt McCandless felvetése[645] által vezérelve mezőgazdasági példákon keresztül kísérlem meg inkább bemutatni. Remélhetőleg így láthatóvá válik az adathasznosítás emberi társadalmakra gyakorolt kiemelt hatása, továbbá a ciklikusság és az erőforrás jelleg egyaránt. Fontos még előljáróban kiemelni, hogy az adatalapúság modern megjelenésében (egyúttal az adatgazdaságban) a „forradalmiságot" a digitális technológiák általi elterjedése adja, nem maga az adatalapú működés gondolata. Egyetértve Mayer-Schönbergerrel és Cukierrel az adatok hasznosítása jóval régebb óta zajlik, mint a digitalizáció megjelenése,[646] azonban ki kell emelni, hogy annak jelentősége a digitális technológiák adta új lehetőségek miatt növekszik.

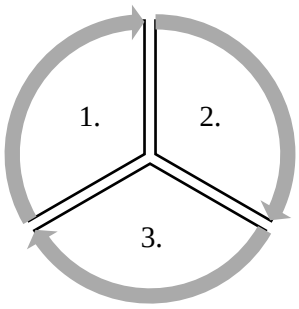
Az adatok forradalmának jelen dolgozat által követett hasonlata az „adat=termőföld" állításra épül, amelynek alappillérei az alábbiak:

- A modern (digitális) adatalapú gazdaság létrejötte hasonlóan jelentős hatással bírhat az emberi társadalmakra, mint a mezőgazdaság kialakulása és fejlődése; Az egyre hatékonyabbá váló mezőgazdaság leváltotta a gyűjtögető és vadászó életmód ad hoc produktivitását, ezáltal kiszámíthatóbb és stabilabb, egyúttal specializált feladat megosztáson alapuló, közösségi működést tett lehetővé. Ehhez hasonlóan az adatalapú működés és az algoritmizáció a korábbi – egyéni teljesítményfüggő és ezáltal eshetőleges – eredményeket új alapokra helyezi, azáltal, hogy a megismerési folyamat egy részét kiszervezi, gépesíti.
- Az adatalapúság elterjedése jelentős közvetett hatásokkal bírhat szinte minden társadalmi és gazdasági területre, továbbá új területek megjelenését idézheti elő; Hasonlóan a mezőgazdaság fejlődése következtében létrejövő felesleghez, ami meghatározta a gazdasági életben az árutermelést és a pénzgazdálkodást.[647]
- Éppúgy, mint a mezőgazdaság, az adatalapú működés is egy erőforrás hasznosító (nyersanyag előállító és feldolgozó) funkciót lát el.[648] Belátható, hogy a búzamag eredeti állapotában emberi fogyasztásra kevésbé alkalmas, a kenyér viszont igen. Csakúgy mint 2TB nyers adat nehezen értelmezhető, két gyógyszer elemzése alapján kimutatott káros kölcsönhatás viszont igen.
- Párhuzam vonható a mezőgazdaság megújulási képességével kapcsolatban is. Az adatalapúsághoz hasonlóan az un. „neolitikus forradalom"[649] óta a mezőgazdaság is egy

[645] David McCandless, The beauty of data visualization. 2010. TEDGlobal
[646] Lásd részletetesen: Mayer-Schönberger, Cukier, 2014. 90 o.
[647] David B. Grigg: A világ mezőgazdasági rendszerei. Mezőgazdasági Könyvkiadó, 1980. 152-156 o.
[648] Szénay László, Villányi László: Agrárgazdaságtan. Budapest, Mezőgazdasági Szaktudás Kiadó, 2000. 13 o.
[649] Ez az időszak fémjelzi azt a folyamatot, amely során a gyűjtögetés során a szerzett magok elszórása által elindulhatott a növénytermesztés, a vadon élő állatok domesztikációjával pedig az állattenyésztés, amelyek mind a mai napig a mezőgazdasági termelés két legfontosabb pillérét alkotják.

ciklikusságon alapuló rendszert alkot, ahol „A” év aratása, „B” év vetéséve alakítható.[650]

Az adathasznosítás rendszere ezek alapján három szakaszra osztható, az első a tényleges hasznosítást időben megelőzi, egyfajta technológiai és társadalmi előfeltételként fogható fel. A második szakasz az adathasznosítás tényleges folyamata, a harmadik pedig a hasznosítás visszahatása a társadalmi és a technológiai trendekre. Ez a mezőgazdasághoz hasonlóan szintén egy körfolyamatként fogható fel, ahol az egyes szakaszok egymással szoros kölcsönhatásban és kölcsönös függésben helyezkednek el.



4.4.2.1. Az első szakaszról

Az első szakasz az adathasznosítás háttérét adja, de valójában az adatalapú működés kiemelt folyamata. Fogalmazhatunk úgy, hogy az adathasznosítás bizonyos, rajta kívül álló feltételek hiányában nem képzelhető el. Bár a megismerhető tényszerűségek értékei állandónak tekinthetők, de azok megismerésének lehetőségei rugalmasan változnak. Ahogy a föld is állandó, az azon való gazdálkodás azonban időszakonként átalakul. Ennek a szakasznak három komponensét érdemes kiemelni.

- *Technológiai előfeltételek megléte:* A megfelelő mennyiségű és minőségű adaton alapuló működés elképzelhetetlen a szükséges technológia léte és elérhetősége nélkül (pl. rögzítés, tárolás, feldolgozás, továbbítás). Az előfeltételeket gyakorlatilag a digitalizáció létével és térnyerésével is azonosíthatjuk, amely hasonlóan a mezőgazdasági talajműveléshez, a földet a magas terméshozam elérése érdekében a vetésre előkészíti (pl. szántás, talajlazítás). A digitalizáció számottevő mérföldkövei voltak a 60-es évektől az első „nagy-gépek”, majd a személyi számítógépek (PC) elterjedése és az internethálózat megjelenése. Ezeknek a használatán jelentősen változtatott a web2 alkalmazások (2000-es évek) és az IoT eszközök tömegessé válása (2010-es évek), valamint az algoritmizáció jelentős térnyerése (2020-as évek).[651]
- *Adatgenerálási, rögzítési és felhasználási trendek erősödése:* Új vetés nélkül az aratás egyszeri esemény, a megfelelő mennyiségű és minőségű hozam pedig elérhetetlen célkitűzés. Ehhez hasonlóan a társadalom egészét átható jelenségként létező adatgenerálási és rögzítési törekvések (adatosítás), nélkül adathasznosításról – mind a keresleti, mind a kínálati oldal hiányában – nem beszélhetünk.
- *Döntéshozói elhatározás:* a termelésre alkalmas technológiai közeg, és az arra hajlamos személyek és szervezetek adatrögzítési és hasznosítási hajlama önmagában is létező és számottevő tényező. Ez azonban politikai és piaci döntéshozói reakcióktól nem mentes közeg, ezen állásfoglalások pedig jelentős hatással bírnak a folyamat egészére. Ahogy egy eltökélt gazda védi és táplálja az elvetett növényeket, úgy mutatkozik az adatalapúság táptalaját biztosító – nemzetközi, Európai Uniós és hazai szinteken is – a digitalizáció, mint elérendő cél artikulációja.[652] Ezek olykor jól kivehető, olykor láthatatlan kézként terelik az emberi közösségeket egyre fokozódó mennyiségű digitális adat rögzítésének és használatának irányába.

[650] Kovács János: Egyetemes és magyar agrárfejlődés. Budapest, Agroinform Kiadó és Nyomda, 2005. 11-14 o.
[651] Bankó, Szőke, 2015. 19-21 o.
[652] Említhető például az EU Digitális Európa Programja (2021-2027), az EU Adatstratégiája és a Mesterséges Intelligencia közös európai megközelítéséről szóló dokumentuma (COM(2021) 205 final) vagy Magyarország Nemzeti Digitalizációs Stratégiája (2022-2030) és Magyarország Mesterséges Intelligencia Stratégiája (2020-2030).

4.4.2.2. A második szakaszról

Ebben a szakaszban zajlanak az adathasznosítás központi folyamatai, ez feltételezi egyrészt az első szakasz elemeinek létét, illetve a hasznosítási szándék kellően erős megjelenését. A mezőgazdasággal való logikai kapcsolatot fenntartva, az előző szakaszban a termőföld (az adatalapú környezet) megművelésre került, így a jelen célok az adatok megszerzésére, tárolására, mozgatására és a feldolgozására irányulnak. Az alábbi műveleti kiosztás és sorrend az elérhető gyakorlati, illetve szakirodalmi tapasztalatok szintetizálásával jött létre. Az 1. és 2. szintek alkotják az adathasznosítási folyamat külső infrastruktúráját, míg a 4. és 5. szintek az adatokkal kapcsolatos értékteremtést végzik. A 3. szint áthidaló szerepet játszik az egyes szintek között, így része a külső infrastruktúrának is, de az értékteremtés folyamatában is szerepet játszik.[653]

- *Adatgyűjtés és rögzítés*

A hasznosítási folyamat megkezdéséhez természetszerűleg – mint alapanyagra – adatokra van szükség, tehát, attól függően, hogy milyen hasznosítási célzat vezérli a tevékenységet, vagy meglévő adatok begyűjtése vagy új adatok rögzítése kell, hogy megtörténjen. Ezen a szinten a cél az adatok feletti hatalom gyakorlásának megszerzése annak érdekében, hogy azokon további műveletek legyenek végezhetők. Eredeti adatrögzítés esetén a legváltozatosabbak a lehetőségek, hiszen ebben az esetben a tényszerűség közvetlen vizsgálata, kutatása zajlik. Létező adatok gyűjtésekor meglévő saját adatbázisok (vagy részeik) hasznosításra való megjelölésére vagy már létező idegen adatbázisok megszerzésére kerülhet sor.

- *Adataggregáció, kompiláció és szintetizáció*

A következő szinten az újonnan eltárolt adatok rendszerezése történhet. A kompiláció az értékteremtés megkezdésének első lépése, ilyenkor a különböző forrásokból származó, de azonos vagy hasonló típusú adatok összesítése lehet szükséges, más esetekben a meglévő adatbázisok összevonásával, kiegészítésével vagy bővítésével érhető el ugyanez. Így elmondható, hogy kompiláció során a gyűjtött adatbázisok vagy uniformizálásra vagy diverzifikálásra kerülnek a későbbi célok elérése érdekében. Egy adatbázis kompilációja során nem jönnek létre új adatok, hanem meglévő adatok alapján jön létre új adatbázis.

Ezzel ellentétben az adatok aggregációjakor olyan új adatok jönnek létre, amelyek a forrásadatok tartalmát tükrözik vissza az eredeti adatok megjelenítése nélkül. Az aggregáció a forrásadatok statisztikai elemzésére irányul. Mivel statisztikai adatok alapján jellemzően nem lehet visszaazonosítani az adatforrást ezért egyfajta anonimizációs funkciója van (a visszaazonosíthatóságot egyedileg kell vizsgálni, azt jelentősen befolyásolhatja, hogy milyen típusú adatokra épül a statisztika és milyen részletes szűrési / leválogatási opciókkal rendelkezik az adatbázis).

Az adatok szintetizációja alatt azt folyamatot értjük, amely a tényszerűséget közvetlenül reprezentáló eredeti adat algoritmizált folyamat keretében történő mesterséges reprodukciójára irányul. A szintetikus adatok[654] lényege, hogy közel azonosan viselkednek egy analitikai folyamatban az eredeti adatokkal (disztribúció, trendek, mintázatok), azonban anélkül, hogy bármilyen olyan indexáló vagy attribútum adat maradna bennük, amely visszavezethető az adat forrására.[655] Ez alapján tehát a szintetikus adat legalább egy rendkívül precízen álnevesített

[653] Ulises A. Mejias, Nick Couldry, Datafication, Internet Policy Review, Journal on internet regulation, Volume 8, Issue 4, 2019. 3 o.
[654] Fontos, hogy a szintetikus adatok nem egyenlőek a gép által előállított adatokkal.
[655] Giulia Finocchiaro, Antonio Landi, Gianluca Polifrone,Davide Ruffo, Francesco Torlontano, „The Regulatory Future Of Synthetic Data, Data synthesis as a resource for scientific research, innovation, and public policy in the

adat, de akár – a megfelelő technika alkalmazása esetén – olyan anonim adat is lehet, amelynek értéke alig – ha egyáltalán – csökkent az anonimizációs eljárás során. A szintetikus adatok jelentősége kétségtelennek látszik, ezt az is megerősíti, hogy az MI rendelet kifejezetten nevesíti a szintetikus adatokat. A 10. cikk (5) bekezdésében az anonimizálással egy sorban említi, amely a kiemelt szerepét jól tükrözi. E mellett azonban az is megfigyelhető, hogy a szintetikus adatokat nem az anonimizált adatokon belül helyezi el, a szövegezés alapján úgy tűnik, hogy önálló adattípusnak tekinti, nem az anonim adat egy fajtájának (ettől függetlenül pl. leszögezhető, ha az érintett nem azonosítható az adat alapján, akkor az nem fog személyes adatnak minősülni függetlenül attól, hogy szintetikus-e vagy sem[656]). A szintetikus adatok létrehozásának egy gyakorlati technikája az un. GAN (Generative Adversarial Network), ami egy neurális hálózati architektúraként – pontosabban két hálózat versengéseként – fogható fel. A GAN tehát egy megerősítés nélküli módszeren alapuló tanuló algoritmus, aminek a logikája, hogy a győztes változatlan marad, a vesztes pedig tanul a hibájából. A folyamata lényege, hogy egy un. „generátor-modell" eredeti bemeneti adat alapján létrehozza a szintetikus adatot, amit a diszkriminátor-modell (egy szintén eredeti adatból álló minta alapján) megítéli, hogy az eredeti vagy szintetikus. A modell célja, hogy a generátor-modell olyan állományokat hozzon létre, amik átmennek, mint eredetiek a diszkriminátor-modell szűrésén.[657]

- *Adatközvetítés és kereskedelem*

Az adatok közvetítésének és kereskedelmének értelemszerű célja, hogy egyes adatállományok és azok feletti jogosultságok egyik szereplőtől átkerüljenek egy másik szereplőhöz. Mindkét fogalom képviselői alapvetően egy áthidaló funkciót látnak el, a kettő közti különbség abban rejlik, hogy a közvetítők az adatok vonatkozásában saját célokkal nem rendelkeznek, kizárólag a felek közötti tranzakciós kapcsolat létrejöttét támogatják (a DGA nyomán nevezhetők semlegesnek), míg a kereskedők az adatok feletti jogosultságokat saját nevükben szerzik meg, azért, hogy azt valamilyen módon tovább értékesítsék.

- *Adatgondozás és adatextrakció*

Az adatok gondozásához egyfajta kísérő jellegű, közvetlenül nem értéknövelő, de ahhoz elengedhetetlen lépések is tartoznak. Ilyen például az adatokon való feltétlenül szükséges műveletek elvégzése (az adatok mobilizációja, törlése, rendezése) vagy az adatok vizualizációja, összehasonlítása.[658] Szintén ide vonható műveletek még a formátumváltás (adatkonverzió), az álnevesítés (pszeudonimizáció) és az anonimizáció. Formátumváltás során a digitális adatok megfelelő, kölcsönösen kompatibilis formátumba kerülnek átalakításra. Ennek előnye lehet, hogy az adatok könnyebben feldolgozhatók, elemezhetők és megoszthatók lesznek, hátránya lehet viszont, hogy a folyamat során sérülhet a pontosságuk vagy integritásuk. Az álnevesítés elsődlegesen adatvédelmi technikaként ismert, azonban az általánosságban is alkalmazható. Ebben az értelemben az álnevesített adat alapján – további információk felhasználása nélkül – nem állapítható meg, hogy az mely konkrét tényszerűségre vonatkozik.[659] Az álnevesítés által az adatok kezelésének kockázata jelentősen csökken, ami által az adathasznosításban való részvételi hajlam megnövekedhet. Az álnevesített személyes adat alapján a természetes személy nem azonosítható, de ez igaz az álnevesített cégadatra is,

---

European legal landscape", Italian Institute for Privacy and Data Protection, Data Intermediaries Alliance, 2024. DOI: 10.5281/zenodo.13342141

[656] MI rendelet 5. cikk (1) bekezdés b) pont szövegezése alapján anonimizált, szintetikus vagy *egyéb* nem személyes adatok léteznek. E szerint a rendelet a szintetikus adatokat nem tekinti személyes adatoknak.

[657] Martin Keen, „What are GANs?", IBM Technology. Elérhető: https://www.youtube.com/watch?v=TpMIssRdhco&t=1s

[658] Cuemat, „Data Handling". Elérhető: https://www.cuemath.com/data/data-handling/

[659] GDPR 4. cikk 5. pont

amely alapján a cég nem lesz azonosítható. Így egy vélelmezetten vagy valóban szenzitív adat nem, vagy legalábbis nehezebben vezethető vissza az adatforráshoz. Czapári és Szőke kutatásai alapján[660] az álnevesítés elterjedt technikái az egyedi értékre cserélés (pl. munkahelyi azonosító) sorszámozás vagy random számozás, a hash-elés,[661] és a szimmetrikus titkosítás.[662]

Az anonimizáció az adathasznosítás folyamatában kiemelt pozíciót tölt be, ugyanis egy lépéssel tovább megy az álnevesítésnél, amikor egy adat esetében a visszaazonosíthatóságot teljesen kizárja, az adat forrása és az adat közti kapcsolat megszüntetésével. Ennek a jelentősége meglehetősen nagy, hiszen például sikeres megvalósítás esetén a személyes adat elveszti ebbéli minőségét.[663] Anonimizációs technikák lehetnek bizonyos (főként indexáló vagy kiugró attribútum) adatoknak az adatszettből való törlése (pl. 0-ra állítással, audio és/vagy vizuális megjelenítés esetén maszkolással, mint homályosítás vagy sípolás), véletlenítéssel (pl. zajhozzáadás,[664] csere[665]), általánosítással (pl. tágabb kategória vagy tartomány megadásával[666])[667] vagy a fentebb említett szintetizációval. Adattáblák esetén elterjedt technika a három változóval működő rendszerben történő anonimizáció.[668] Ilyenkor az adatokat direkt azonosítók,[669] kvázi-azonosítók[670] és érzékeny attribútumok[671] szerint különböztetik meg. A technikák a K-anonimitás,[672] L-diverzitás[673] és T-közelség,[674] amelyeket gyakorlatilag egymásra épülő, egyre nagyobb fokú anonimitást lehetővé tevő megoldásoknak tekinthetünk. Mivel az anonimizáció lényege, hogy az azonosíthatóságot, vagyis a csoporttól való elkülönülést megszüntesse, az azonosítás ésszerű feltételezhetőségének mértékét kell csökkentenie. Az anonimizáció logikai folyamata így a következő lehet (pl. ha a cél k=3 anonimitás és l=3 diverzitás elérése): 1. direkt azonosítók törlése → 2. minimum három tagú klaszterek létrehozás a kvázi azonosítók tartományokba rendezésével vagy az egyezések törlésével → 3. háromnál kevesebb eltérő szenzitív attribútummal rendelkező klaszterek törlése.

Extrakció alatt nagyméretű adatbázisokból vagy különböző adatszettekből való, a keresés szempontjából releváns adatok kinyerését értjük. Ennek adattudományi szempontból számos

---

[660] Czapári, Szőke, 2022. 37-38 o.

[661] Algoritmizált művelet, ami az adatról fix bit-hosszúságú állományt hoz létre (egyirányú kódolás, nem visszafejthető, hasonló egy ujjlenyomatra). Ilyenkor az adatról készült hash érték kerül az álnevesített adat helyére

[662] Algoritmizált művelet, ami a teljes adatállományt kóddá alakítja (két irányú, a kulcs ismeretében visszafejthető). Ilyenkor az adatról készült kódolt állománnyal történik az álnevesítés.

[663] GDPR (26) preambulumbekezdés

[664] A pontosság csökkentése megvalósulhat, pl. ± 10 értékkel való eltolással vagy egy konstanssal való szorzással

[665] Ez az értékek adatforrások közti összecserélését (permutációját) jelenti

[666] Például életkor esetén 25-35 év közötti tartomány létrehozásával vagy születési dátum esetén az év/hónap/nap helyett csak év megadásával

[667] Czapári, Szőke, 2022. 35-37 o.

[668] Lásd részletesen: Pierangela Samarati, Latanya Sweeney, „Protecting Privacy when Disclosing Information k Anonymity and Its Enforcement through Generalization and Suppression" Technical Report SRI-CSL-98-04. Computer Science Laboratory, SRI International.; Charu C. Aggarwal, Philip S. Yu, General Survey of Privacy-Preserving Data Mining Models and Algorithms, in Privacy-Preserving Data Mining: Models and Algorithms, Springer, 2008.
1998.

[669] Olyan adatok, amelyek a tényszerűséget közvetlenül azonosítják

[670] Olyan adatok, amelyek önállóan nem, de együttesen lehetővé teszik az azonosítást

[671] Olyan adatok, amelyeket a folyamat szempontjából megőrzendőnek tekintünk

[672] A lényege a „K" számú egyénnel való csoportosítás (ez például a kvázi-azonosítók általánosításán alapuló ekvivalencia osztályokba klaszterezését jelentheti)

[673] A lényege a klaszteren belüli szenzitív attribútumok azonosságának megszüntetése, azáltal, hogy minimum „L" számú különböző attribútum kell egy csoportba kerüljön

[674] A lényege, hogy a szenzitív attribútumok klaszteren belüli értékének az egész adatszett értékének megengedett százalékos eloszlását kell tükrözniük (pl. ha T=0.1 az 10% szórást enged klaszteren belül az egész állományhoz képest)

válfaja lehet, de lényegüket tekintve mindben közös az adatállományban rejlő mintázatok (jellemzően automatizált) kutatása[675] és bizonyos esetekben referencia adatokkal való összevetése,[676] amely technikáknak különös jelentőséget ad az adatok egyre növekvő mennyisége, az egyes állományok változatossága és komplexitása. A folyamat során (pl. szövegek, képek és egyéb adatok bányászata által) jönnek létre új, származtatott (finomított) adatok, amelyek így az adathasznosításban rejlő értékteremtés létrejöttének előszobáját biztosítják.

- *Adat interpretáció és integráció*

Az adatok hasznosításának utolsó mozzanatai nélkül a folyamat meglehetősen öncélú lenne, hiszen eddig más nem történt, minthogy összegyűjtött adatok feldolgozásával hoztunk létre még több adatot. Eddig értékteremtésre szigorúan az adatgazdaság keretein belül került sor, a résztvevők munkája által. A kapott finomított adatok konkrét helyzetre (személyre vagy szervezetre) értelmezésével (interpretáció) vagy egy már létező vagy új folyamatba építésével (integráció) lehetünk képesek az adatok társadalmi és gazdasági hasznosságát beteljesíteni, vagyis az adatterméket létrehozni.

4.4.2.3. A harmadik szakaszról

Az adathasznosítás harmadik szakasza a hasznosított adatok utóéleteként írható le. Ezen belül a végfelhasználók számára *fogyasztható* formába került adattermékek értékesítése és a folyamathoz kapcsolódó egyéb kísérő tevékenységek zajlanak. Ilyen kísérő tevékenység lehet például új tanácsadási és képzési formák megjelenése, amely az adatalapú működés támogatásán keresztül hat vissza az adathasznosítás folyamatára. A célba juttatott adatterméket ezt követően már az adatfelhasználás keretei között, mint primer adat használhatják a jogi és természetes személyek, a köz- és magánszféra területein egyaránt. A harmadik szakasz zárása azonban az első szakasz nyitása is egyben, így a felhasználás eredményeként létrejövő adatok ismét hasznosíthatóvá válnak. Ezzel a három szakaszos ciklussal kapcsolatban jelenleg az látszik, hogy öngerjesztően működik, vagyis az egyre kiterjedtebb adatalapú működés növeli a hasznosítás igényét, az egyre jobban működő adathasznosítás által létrejövő eredmények pedig növelik az adatalapúságra való hajlamot. Így a folyamat minden megtett „körrel" egyre mélyül, egyre növekszik és egyre kifinomultabbá válik. Mivel a harmadik szakasz igen kiterjedt, annak elemi szintű kategorizálására jelenleg nincs lehetőség, azonban a lényegének demonstrációja érdekében a hasznosítás eredményeként előálló néhány fejlesztési terület megemlíthető.[677]

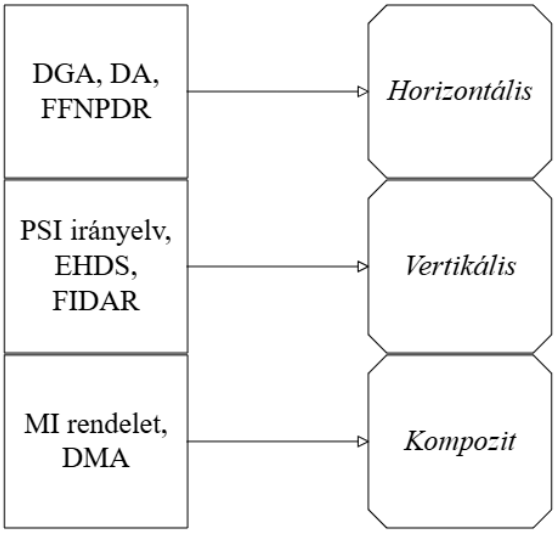
- *Hangfeldolgozás:* észleli és felismeri a különböző hangokat, ezeket rögzíti, elemzi (pl. szövegszerkesztők text-to-speech funkciója)
- *Chatbot, virtuális asszisztens, nagy nyelvi modell:* valódi emberi operátor látszatát keltve fejti ki a tevékenységét (pl. Corti,[678] ChatGPT[679])
- *Kognitív robotika:* szoftver és hardver magas szintű együttes felhasználásával elért magasabb szintű automatizáció (pl. önvezető gépjárművek)

[675] Douglas M. Kochelek, „Data Mining and Antitrust", Harvard Journal of Law & Technology 22, no. 2 (2009). 517 o.
[676] Daniel J. Steinbock, „Data Matching, Data Mining, and Due Process", Georgia Law Review 40, no. 1 (2005). 10 o.
[677] Lásd részletesen: Gianluca Misuraca, Colin van Noordt, „Overview of the use and impact of AI in public services in the EU", Publications Office of the European Union, Luxembourg, EUR 30255 EN, 2020.
[678] Corti Inc. Elérhető: https://www.corti.ai/
[679] OpenAI. Elérhető: https://openai.com/chatgpt/overview/

- *Számítógépes képalkotás:* vizuálisan észlelhető input adat alapján képes adat, illetve álló-, mozgóképek létrehozására (pl. SATIKAS[680], Midjourney[681] DALL·E 1/2/3[682])
- *Szakértői rendszerek:* döntés-automatizáló, döntéstámogató rendszerek (pl. adatbáziskezelő, ügyfélkezelő rendszerek, NAV RADAR[683])
- *Prediktív analitika:* Mintázatokat azonosít, ezeket ábrázolja, szimulálja és jövőbeni lehetséges konfigurációkat hoz létre (pl. online ajánlórendszerek, PRECOBS[684])

4.4.3. Az EU adathasznosításának hatályos szabályanyagáról

Az adathasznosítás joga a közadatok vonatkozásában régóta fennállónak tekinthető, azonban az összes lehetséges adatkategória hasznosíthatóvá tételének szándéka viszonylag újkeletű. A jogszabályi környezetet annak újszerűsége miatt érdemes, mind a *puha*, mind a *kemény* normatív eszközök tekintetében vizsgálni, így az Unió policy dokumentumai és a tényleges EU-s és hazai jogi aktusok együtt alkotják a területet. Az adatjog létező uniós forrásainak dogmatikai besorolásával kapcsolatban azt mondhatjuk, hogy a DGA, DA és az FFNPDR a horizontális, a PSI irányelv és az EU adatterekhez kapcsolódó EHDS és FIDAR javaslatok pedig a vertikális szabályokhoz tartoznak. A hazai Nah.tv. szintén vertikális adatjogi tartományba sorolható. Kompozit szabályok szintén rendkívüli számban fordulnak elő, ezek közül a DMA és az MI rendelet egyes előírásai kerülnek csak kiemelésre, szemléltetésként.



14. ábra: a hasznosítás joganyaga

4.4.3.1. EU policy dokumentumok

A 2010-es évek adatokkal kapcsolatos folyamatiban már korán fellelhetőek voltak a hasznosításra irányuló törekvések. Az „Úton a prosperáló adatközpontú gazdaság felé" c. Bizottsági közlemény[685] 2014-ben az adatok áramlását akadályozó helytelen korlátozásokkal szembeni védelemről és az adatbányászaton alapuló adatközpontú innováció javításáról beszélt. Egy évvel később az „Európai digitális egységes piaci stratégia" c. közleményben[686] pedig már az adatgazdaság építése is felmerült, az adatok szabad áramlásának, mint ötödik alapszabadságnak a felvetésével. A gondolat 2017-re forrta ki magát és „Az európai

[680] Mohammed bin Rashid Center for Government Innovation, Artificial Intelligence to Ensure Compliance with Estonia's Land Use Laws. Elérhető: https://ibtekr.org/en/cases/artificial-intelligence-to-ensure-compliance-with-estonias-land-use-laws/

[681] Midjourney. Elérhető: https://www.midjourney.com/home

[682] OpenAI, DALL·E 3. Elérhető:https://openai.com/index/dall-e-3/

[683] Adó Online, „KoKaIn-nal és RADAR-ral veszi fel a harcot az adócsalókkal az APEH" https://ado.hu/ado/kokain-nal-es-radar-ral-veszi-fel-a-harcot-az-adocsalokkal-az-apeh/ (2022.08.15.)

[684] land-der-ideen.de, PRECOBS – software for predicting crimes. Elérhető: https://Land-Der-Ideen.De/En/Project/Precobs-Software-For-Predicting-Crimes-355

[685] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Úton a prosperáló adatközpontú gazdaság felé (COM(2014) 442 final). 13 o.

[686] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Európai digitális egységes piaci stratégia (COM(2015) 192 final). 15 o.

adatgazdaság kiépítése" elnevezésű bizottsági kommunikációban[687] teljesedett ki. Ebben olyan központi elemek kerültek kiemelésre, mint az adatok szabad áramlását indokolatlanul korlátozó előírások lebontása vagy az adathozzáférés és továbbítás elősegítése. A dokumentumban a Bizottság – jelen dolgozat kiindulópontjával összhangban – arra következtetésre jutott, hogy az EU-n belüli adatkereskedelemre szabott jogi környezet hiányában nem biztosítható a nagy adatkészletekhez való hozzáférés, korlátokba ütközhet az új piaci szereplők belépése, és az innovációt megfojtó hatások érvényesülhetnek. Ezeket a gondolatokat „A digitális egységes piaci stratégia" félidős értékelését elvégző, 2017-es Bizottsági dokumentum egyértelműen megerősítette.[688] A Bizottság álláspontja szerint az adathalmazok elemzésén alapuló innováció a gazdasági növekedés és a munkahelyteremtés kulcsfontosságú eleme, amely jelentősen erősítheti az európai versenyképességet a világpiacon. Ennek érdekében un. közös európai adatterek létrehozására tett javaslatot,[689] amelyben a digitális adatok akadályoktól mentesen áramolhatnak, ezáltal serkentve új termékek és szolgáltatások létrejöttét. 2020-ban érkezett meg az „Európai adatstratégia",[690] amelyben olyan kihívásokat azonosítottak, mint az uniós tagállamok összességére vonatkozó egységes szabályozás hiánya vagy a piaci erő kiegyensúlyozatlansága, az adatokhoz való hozzáférés akadályai és a tagállamonként eltérő szintű kibervédelem.[691] A digitalizáció jelentősége kétségtelen az adatalapú működés viszonylatában, így minden intézkedés, ami erre a területre irányul, áttételesen az adatok világára is hatással van. Ezért a policy dokumentumok zárásaként a „Digitális iránytű 2030-ig" c. Bizottsági közleményt[692] szükséges említeni. A digitális transzformáció keretében megvalósuló digitális állampolgárság jövőképe sejlik fel, számos utalással az adatok általános jelentőségére. Végezetül az adatok fontosságát az európai digitális stratégia is megerősíti, ami alapvető változást sürget az adatok gazdasági, politikai és társadalmi jelentőségének felismerésében.[693] Számos ponton erősíti meg a jelen dolgozat által is képviselt egyensúlyi helyzet elérésének és fenntartásának szükségességét, kiemelve, hogy a cél megbízható technológiák fejlesztése és alkalmazása, miközben az alapvető európai értékek is védelemben részesülnek.[694]

4.4.3.2. A nem személyes adatok szabad áramlásáról szóló jogszabályról (FFNPDR - 2018/1807/EU rendelet)

A jogszabály kiemelt célja az adatjogi védelemmel nem érintett, nem személyes adatok áramlása és az azokhoz való hozzáférés előtti akadályok lebontása. A rendelet olyan nem személyes adatkezelésekre vonatkozik, amelyeket szolgáltatásként nyújtanak az Unióban tartózkodó felhasználók számára, illetve uniós természetes vagy jogi személy végez a saját szükségleteinek kielégítése érdekében. A rendelet tiltja a lokalizációs követelményeket (kivéve ha azok közbiztonsági okokból arányosan indokolhatók[695]), vagyis minden olyan jogi vagy közigazgatási intézkedést, amely kimondja, hogy az adatkezelést egy adott földrajzi területen

[687] A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Az Európai Adatgazdaság kiépítése (COM(2017) 9 final) 6-9 o.
[688] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, A digitális egységes piaci stratégia végrehajtásának félidős értékelése (COM(2017) 228 final) 11 o.
[689] A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, A közös európai adattér kialakítása felé (COM(2018) 232 final) 1 o.
[690] COM(2020) 66 final 7-13 o.
[691] Hoeren, Pinelli, 2024. 14 o.
[692] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Digitális iránytű 2030-ig: a digitális évtized megvalósításának európai módja (COM(2021) 118 final) 13-15 o.
[693] COM(2020) 67 final 1 o.
[694] COM(2020) 67 final 3-17 o.
[695] FFNPDR 4. cikk (1) bekezdés

kell végezni. A rendelet által elérni kívánt hatás, hogy könnyebbé váljon az EU-n belüli határokon átnyúló üzleti tevékenység, valamint, hogy létrejöjjön egy egységes piac az adattárolási és -feldolgozási szolgáltatásokhoz.[696] Hatókörét tekintve a GDPR-al együttes alkalmazásra lett kialakítva, tehát a személyes adatok szabad áramlására a GDPR, míg a nem személyes adatokra ezen rendelet előírásait kell alkalmazni.[697]

A rendeletben megjelenik az adathordozhatóság nem személyes adatok esetén is, valamint a ösztönözni kívánja az önszabályozó magatartási kódexek kidolgozását uniós szinten.[698] Ezek a kódexek tartalmazzák a szolgáltatóváltás gyakorlati, technikai és jogi lépéseit, valamint segítik, hogy a felhasználók könnyebben összehasonlíthassák a különböző adatkezelési szolgáltatásokat. Ennek érdekében a rendelet alapján a Bizottság kezdeményezésére több iparági érdekelt féllel közösen dolgozták ki az un. SWIPO (Switching Cloud Providers and Porting Data) magatartási kódexet. Ez két külön dokumentumban foglalkozik az IaaS („Infrastructure-as-a-Service") és a SaaS („Software-as-a-Service") szolgáltatásokra vonatkozó szabályokkal. A céljuk, hogy egységes elveket és eljárásokat biztosítsanak, ezáltal megakadályozzák az olyan nem kívánt piaci magatartásokat, mint a „vevőfogvatartás" (vendor lock-in).[699] Az adathordozhatósághoz még egy minimális tájékoztatási követelmény és a formátummal kapcsolatban az adatok strukturált, általánosan használt és géppel olvasható formátumban történő hordozásának joga kapcsolódik.[700]

Az FFNPDR kifejezetten a nem személyes adatokra irányuló adatjogi szabályozás, azoknak a „megkötési" (lokalizációs) tilalmát állítja fel, ennél tovább azonban érdemeben nem megy (leszámítva a formátumra és a minimális tájékoztatásra vonatkozó követelményeket). Az adatok lokalizációja egyfajta protekcionista mentalitásként fogható fel, ami ténylegesen elsősorban az adathordozhatóság akadályát jelenti. Az FFNPDR a hasznosítás jogához sorolható,[701] marginális jelentőségű védelmi előírásokat tartalmaz a nem személyes adatok jogosultjaira, a monetizációval, az adatokhoz való hozzáféréssel, a műveletvégzés feletti kontroll gyakorolhatóságával azonban nem foglalkozik. Végeredményben azt mondhatjuk, hogy a rendelet a mai adatalapú folyamatok és az adatgazdaság által támasztott kihívásokra nem ad kielégítő választ.

4.4.3.3. A nyílt adatokról szóló jogszabályról (PSI irányelv - 2019/1024/EU irányelv)

Annak az intézkedéscsomagnak a részeként azért jött létre, hogy az EU adatgazdaságát megerősítse, így a célja, hogy növelje a közszféra információiban rejlő társadalmi-gazdasági potenciált és meghatározza a hasznosítás jogi kereteit a közszféra adatai vonatkozásában. Az irányelv abból indul ki, hogy a közadatoknak hasznosíthatóknak kell lenniük üzleti és nem üzleti célokra egyaránt, így a nyílt hozzáférésű adatokra[702] fókuszál. Irányelvi formában létezik, így annak implementációja során a célkitűzések elérésére alkalmas intézkedések a tagállami jog részeként jöhetnek létre. Az irányelv által kitűzött célokat a magyar jogalkotó kilenc lépésben érte el, ezek közül kiemelendő a Nah.tv.

---

[696] EURLEX, „A nem személyes adatok Európai Unióban való szabad áramlása" https://eur-lex.europa.eu/legal-content/HU/LSU/?uri=CELEX:32018R1807

[697] FFNPDR 2. cikk (2) bekezdés

[698] FFNPDR 6. cikk (1) bekezdés

[699] DORDA Rechtsanwälte GmbH; Arthur Cox LLP; Ramón y Cajal Abogados SLP, „Preliminary Assessment Reports on SWIPO IaaS and SaaS Codes of Conduct", 2020. 11-15 o.

[700] FFNPDR 6. cikk (1) bekezdés a) és b) pontok

[701] FFNPDR (1) és (2) preambulumbekezdések alapján

[702] PSI irányelv 2. cikk 14. pont szerint platformfüggetlen és a nyilvánosság számára a dokumentumok további felhasználásának korlátozása nélkül hozzáférhetővé tett fájlformátumban lévő adatok

Az irányelv valójában minimumszabályokat állapít meg a nyílt hozzáférésű adatok felhasználásának előmozdítására a termékek és a szolgáltatások terén az innováció ösztönzése céljából,[703] tehát egyértelműen a közadathasznosítás alapjogszabályának tekinthető. A PSI irányelv számos adattípust kivesz a közadat kategóriából (függetlenül attól, hogy a közszféra kezelésében van), így nem vonatkozik az irányelv, például a harmadik személyek szellemi tulajdonjogával védett tartalmakra, magánéletet érintő (személyes adatot tartalmazó) dokumentumokra stb.. E tekintetben a DGA párjaként működik, amely az ilyen, közszférabeli szervezet kezelésében lévő, közadatnak nem minősülő (személyes és védett) adatok hasznosítását teszi lehetővé.

A további felhasználásnak nevezett adathasznosítás alapján induló adathozzáféréssel kapcsolatban az irányelv meghatározza, hogy milyen módon és határidővel kell a közszférabeli szervezeteknek reagálnia (vagyis 20 munkanapon belül).[704] A teljesítés formátumával kapcsolatban a közszférabeli szervezetek és a közvállalkozások dokumentumaikat (közadataikat) a meglévő formátumban és nyelven, lehetőség szerint és adott esetben elektronikus eszközök révén, olyan formátumban bocsátják rendelkezésre a hozzájuk tartozó metaadatokkal együtt, amely nyílt, géppel olvasható, hozzáférhető, fellelhető és tovább felhasználható. Megjelenik a „beépített és alapértelmezett módon nyílt adatok" elve,[705] amely a gyakorlatban azt jelenti, hogy a közszférabeli szervezetek már az adatok keletkezésének pillanatában, a technikai, jogi és adminisztratív részleteket úgy kell kialakítsák, hogy az adatok az átláthatóságot, az innovációt és a gazdasági-szociális hasznosulást szolgálják, ne utólagosan kelljen azokat hatékonyabban hasznosíthatóvá tenni. Az elvet úgy pontosítja, hogy az nem jelent kötelezettséget a közszférabeli szervezet számára arra, hogy az irányelvnek való megfelelés érdekében létrehozzon vagy átalakítson dokumentumokat, illetve azokból kivonatot készítsen, amennyiben ez aránytalan, egy egyszerű műveleten túlmutató erőfeszítést jelentene,[706] továbbá nem is kötelezhetők bizonyos típusú dokumentum előállításának és tárolásának folytatására azzal a céllal, hogy azt a magán- vagy közszféra szervezetei tovább felhasználják.[707] A díjazással (monetizációval) kapcsolatban kimondja az irányelv, hogy a hasznosításba adásnak díjmentesnek kell lennie, azonban a dokumentumok sokszorosítása, rendelkezésre bocsátása és terjesztése, valamint a személyes adatok anonimizálása és a kereskedelmileg bizalmas információk védelme érdekében hozott intézkedések során felmerült határköltségek megtérítttetését kérheti a közszférabeli szervezet.[708]

A magánadatokra jellemzőnek mondható hasznosítási kötöttségek itt nem jelennek meg, a közadatok hasznosítása nem köthető feltételekhez, kivéve, ha az ilyen feltételek objektívek, arányosak, megkülönböztetésmentesek és azokat valamely közérdekű cél indokolja. Ha a közadatok hasznosítása mégis feltételekhez kötött, a feltételek nem korlátozhatják szükségtelenül a további felhasználás lehetőségeit, és nem használhatók fel a verseny korlátozására,[709] valamint azok nem lehetnek megkülönböztetők.[710]

[703] PSI irányelv 1. cikk
[704] PSI irányelv 4. cikk
[705] PSI irányelv 5. cikk (2) bekezdés
[706] PSI irányelv 5. cikk (3) bekezdés
[707] PSI irányelv 5. cikk (4) bekezdés
[708] PSI irányelv 6. cikk (1) bekezdés
[709] PSI irányelv 8. cikk
[710] PSI irányelv 11.cikk

A közszféra adataiban nagy gazdasági és társadalmi potenciál rejlik,[711] amelynek a kiaknázására tett lépések feltétlenül üdvözlendők. Összességében a PSI irányelv előrelépésnek tekinthető[712] elődjéhez képest, amelyet a szakirodalom, mint kudarc értékelt.[713]

4.4.3.4. Az adatkormányzási rendeletről (DGA - 2022/868/EU rendelet)

A rendelet célja az európai adatmobilizáció elősegítése, annak alapvető keretfeltételeinek létrehozásával. A rendelet tehát horizontális, keretszabályokat állít az uniós adatgazdaság fejlesztéséhez és az ilyen folyamatokkal kapcsolatos bizalom erősítéséhez. A kiemelt és vizsgált előíráscsoportjai az alábbiak:[714]

- a közszférabeli szervezetek kezelésében lévő, bizonyos védett adatok további felhasználására vonatkozó feltételek,
- az adatközvetítő szolgáltatásokat nyújtó vállalatokat érintő szabályok,
- az adataltruizmusra vonatkozó keret.[715]

➢ *A közszféra védett adatainak hasznosítása*

A rendelet az olyan „nem nyílt hozzáférésű" adatok (mint: személyes adatok, üzleti titkok, szellemi tulajdonjog által védett tartalmak[716]) – további felhasználását szabályozza, amelyek felett a közszféra szervei valamilyen formában hatalmat gyakorolnak és adott feltételek mellett rendelkezésre bocsáthatnak. A rendelet meghatározza azokat a követelményeket, amelyeket a közszférabeli szervezet megkövetelhet[717] az adathoz hozzáférést kérőtől[718] annak érdekében, hogy a magánélet és az üzleti érdekek védelme adott lehessen. Ezek egyfelől az anonimizáció személyes adatok esetén és az adatok módosítása, összesítése, illetve az adatfelfedés elleni védelmet szolgáló bármely más módszer alkalmazása bizalmas üzleti adatok esetén, továbbá mindkét esetben a virtuális vagy fizikai biztonságos adatkezelési környezet[719] biztosítása.[720] A közszférabeli szervezetek által, a szerződéskötéskor felszámított díjaknak átláthatóknak, megkülönböztetésmenteseknek, arányosaknak és objektíven indokoltnak kell lenniük, és nem korlátozhatják a versenyt.[721] Fontos továbbá, hogy az adathoz hozzáférést biztosító közszférabeli szervezeteknek olyan szerződést kell kötnie az adattranzakció során, amely

---

[711] Szőke Gergely László, „Recent and Future Developments of PSI Re-use in Europe", Studia Iuridica, 155, Essays of Faculty of Law, University of Pécs, Yearbook of 2017-2018. 99 o.

[712] Thomas Margoni, „Public Sector Information Open Data Directive", Technical Report. DOI: 10.5281/zenodo.4543088

[713] Lásd részletesen: Ződi Zsolt, „Elvek és valóság Európában: a PSI-irányelv érvényesülésének problémái (miért nem szereti az európai közszféra megosztani az adatait a magán-vállalkozásokkal?) In: Sáry Pál (Szerk.): Decem anni in Europaea Unione I. - Jogtörténeti és jogelméleti tanulmányok. Miskolci Jogtudományi Műhely 6., Miskolci Egyetemi Kiadó, 2015. 175 o.

[714] DGA 1. cikk

[715] EURLEX, „Európai adatkormányzás" Elérhető: https://eur-lex.europa.eu/legal-content/HU/LSU/?uri=CELEX:32022R0868

[716] DGA 3. cikk (1) bekezdés

[717] Megjegyzendő, hogy az adatok védett jellege megóvásának biztosítása kötelező közszférabeli szervezeteknek, a döntési lehetőség a módszer megválasztásában van.

[718] A rendelet szóhasználatában továbbfelhasználó, ami jelen dolgozatban az adatokat hasznosítóval azonos

[719] DGA 2. cikk 20. pont alapján a biztonságos adatkezelési környezet olyan fizikai vagy virtuális környezet és szervezeti eljárásmód, amely az uniós jognak (pl. különösen az érintettek jogai, a szellemitulajdon-jogok, a kereskedelmi adatokra vonatkozó titoktartás és a statisztikai adatvédelem, valamint az adatok sértetlensége és hozzáférhetősége tekintetében) a GDPR és az alkalmazandó nemzeti jognak való megfelelés biztosítását és annak lehetővé tételét célozza, hogy a biztonságos adatkezelési környezetet biztosító szervezet meghatározza és felügyelje az összes adatkezelési műveletet, beleértve az adatok megjelenítését, tárolását, letöltését és exportálását, továbbá a számítási algoritmusok segítségével származtatott adatok kiszámítását.

[720] DGA 5. cikk (3) bekezdés

[721] DGA 6. cikk (2) bekezdés

megőrzi az alkalmazott biztonságos adatkezelési környezet műszaki rendszerei működésének integritását, továbbá ki kell kötnie az adatokkal kapcsolatosan végzett, hasznosítást célzó későbbi műveletek ellenőrizhetőségét, valamint a hasznosítás eredményeként létrejövő adattartalom használhatóságát.[722] A rendelkezések jelentősége egyfelől, hogy a hasznosításban adatot megszerző féllel szemben egészen szigorú követelmények támaszthatók, különös tekintettel arra, hogy a későbbi hasznosítás céljára, sőt, még az eredményeként létrejövő új (tercier) adat használhatóságára is hatással lehet a hozzáférést adó. Szintén fontos, hogy a DGA alapján a megszerzett anonim adatok visszaazonosítása de lege tilos,[723] ami az ésszerű feltételezhetőséget számottevően lecsökkenti, ezáltal az adatok anonimitásának szintjét érdemben növeli meg (mivel a visszaazonosítás jogellenes, azzal kevésbé szükséges kalkulálni).

Ugyancsak nagy horderejű változás, hogy megjelennek a nem személyes adatokra vonatkozó jogszerűségi követelmények és a jogi személyek adatjogi védelmi előírásai. Így elképzelhető például olyan helyzet, amikor nem személyes adatok hasznosításához a jogosult engedélyére van szükség.[724] Megjelenik továbbá egy tájékoztatási kötelezettség is. E szerint nem személyes adatok jogosulatlan további felhasználásának esetében az adatok hasznosítójának késedelem nélkül – adott esetben a közszférabeli szervezet segítségével – tájékoztatnia kell azokat a jogi személyeket, amelyek jogait és érdekeit ez érintheti.[725] Ezen túlmenően védett nem személyes adatok harmadik országba való továbbításának szándéka esetén, már a hasznosítás kérelmezésekor tájékoztatni kell a közszférabeli szervezetet a továbbításra irányuló szándékról, továbbá a továbbítás céljáról. Sőt olyan esetekben, amikor az adatok hasznosítása a jogosult döntésén (beleegyezésén) múlik, akkor az adatot hasznosítónak tájékoztatnia kell a továbbítási szándékáról, a célról és a megfelelő biztosítékokról azon jogi személyt, amelynek a jogait és érdekeit ez érintheti. A közszférabeli szervezet csak abban az esetben engedélyezheti a további felhasználást, ha a jogi személy engedélyt ad a továbbításra.[726] A továbbítással kapcsolatban további garanciális szabályként szerepel, hogy a közszférabeli szervezet kizárólag akkor engedhet hozzáférést nem személyes bizalmas adatokhoz vagy szellemitulajdon-jogokkal védett adatokhoz egy olyan adathasznosítónak, aki ezen adatokat (megfelelőségi minősítéssel nem rendelkező) harmadik országba szándékozik továbbítani, ha az szerződéses kötelezettséget vállal a célországban a szellemitulajdonnal kapcsolatos jogok tiszteletben tartására és a bizalmas kereskedelmi adatokkal összefüggő titoktartásra, valamint, ha a továbbító közszférabeli szervezet tagállama és joga szerinti bírósági joghatóságot elfogadja a szellemitulajdonnal vagy a titoktartással kapcsolatos bármely jogvita esetén.[727] A továbbítás témakörének zárásaként megjegyzendő, hogy a GDPR-hoz hasonlóan lehetőség van Bizottsági végrehajtási aktusok (megfelelőségi határozatok) kiadására, ami olyan harmadik országokat jelöl, ahol a jogvédelem megfelelő szintű.[728] Ezzel szemben érdekes újítás, hogy egyfajta nem-megfelelőségi értékelés is kiadható a Bizottság részéről, ami többlet felételekhez kötheti a továbbítást, ha a célországba való adatmozgás pl. az EU közpolitikai célkitűzéseit veszélyezteti.[729]

- *Az adatközvetítő szolgáltatás*

[722] DGA 5. cikk (4) bekezdés
[723] DGA 5. cikk (5) bekezdés
[724] DGA 5. cikk (6) bekezdés
[725] DGA 5. cikk (5) bekezdés
[726] DGA 5. cikk (9) bekezdés
[727] DGA 5. cikk (10) bekezdés
[728] DGA 5. cikk (12) bekezdés
[729] DGA 5. cikk (13) bekezdés

A DGA a közszféra adathasznosításán túl az újonnan létrehozott adatközvetítő szolgáltatók működését is szabályozza. Az adatközvetítő szolgáltatás egy olyan szolgáltatás, amelynek célja kereskedelmi kapcsolatok létrehozása (technikai, jogi vagy egyéb eszközök révén) egyrészről meghatározatlan számú érintett és adatbirtokos,[730] másrészről az adatfelhasználók[731] közötti adatmegosztás[732] - többek között az érintettek személyes adatokkal kapcsolatos jogainak gyakorlása – céljából.[733] Tehát az ilyen szolgáltatás kifejezetten a kereskedelmi kapcsolat létrehozására irányul a keresleti és a kínálati oldal között. A szolgáltatások magukban foglalhatják a két- vagy többoldalú adatcserét, vagy olyan platformok vagy adatbázisok létrehozását, amelyek lehetővé teszik az adatok cseréjét vagy közös felhasználását, valamint az adatbirtokosok adatfelhasználókkal való összekapcsolását szolgáló egyéb egyedi infrastruktúra létrehozását.[734] Fontos, hogy az adatközvetítő szolgáltató nem használhatja az adatfelhasználók rendelkezésére bocsátásától eltérő más célra azokat az adatokat, amelyekre vonatkozóan adatközvetítő szolgáltatásokat nyújt.[735] Ehhez kapcsolódóan további korlátként jelenik meg, hogy az adatközvetítő szolgáltatás nyújtása céljából gyűjtött adatok kizárólag a szolgáltatás fejlesztésére használhatók fel.[736] Ezen túlmenően nem szerezhet jogot az adatokon saját hasznosítási (értéknövelési) célból,[737] de bizonyos adatcserét támogató kiegészítő szolgáltatásokat elvégezhet. Ezek az ideiglenes tárolás, gondozás, átalakítás, anonimizálás vagy álnevesítés. A kiegészítő szolgáltatások azonban csak az adatbirtokos vagy az érintett kifejezett kérésére vagy jóváhagyásával használhatók.[738] A szolgáltatásnyújtás semlegességét támasztja alá továbbá és a szerződéses feltételekre (beleértve az árazást) van számottevő hatása, hogy az adatközvetítő szolgáltatásoknak az adatbirtokos vagy adatfelhasználó részére történő nyújtására vonatkozó kereskedelmi feltételek nem tehetők függővé attól, hogy az adatbirtokos vagy az adatfelhasználó igénybe vesz-e (vagy milyen mértékben vesz igénybe) más, ugyanazon adatközvetítő szolgáltató vagy egy ahhoz kapcsolt jogalany által nyújtott szolgáltatásokat.[739] A DGA a közvetítő szolgáltatók működésével kapcsolatban kiemeli, hogy

- azoknak az érintettek mindenek felett álló érdeke szerint kell eljárnia jogaik gyakorlásának elősegítésekor, akár úgy is, hogy az érintetteknek tömör, átlátható, könnyen érthető és könnyen hozzáférhető formában ad tájékoztatást, illetve adott esetben tanácsadást az adatfelhasználók általi tervezett adatkezelési műveletekkel kapcsolatban,[740]
- a személyes adatok vonatkozásában – szabályozás hiányában – általában a GDPR rendelkezéseit tartja irányadónak,

[730] „adatbirtokos”: olyan jogi személy - ideértve a közszférabeli szervezeteket és a nemzetközi szervezeteket - vagy a szóban forgó konkrét adatok tekintetében nem érintett olyan természetes személy, amely vagy aki az alkalmazandó uniós vagy nemzeti joggal összhangban jogosult hozzáférést adni bizonyos személyes adatokhoz vagy nem személyes adatokhoz, vagy jogosult azokat megosztani;
[731] „adatfelhasználó”: az a természetes vagy jogi személy, aki vagy amely jogszerű hozzáféréssel rendelkezik bizonyos személyes vagy nem személyes adatokhoz, és többek között a GDPR értelmében a személyes adatok vonatkozásában jogosult ezeket az adatokat kereskedelmi vagy nem kereskedelmi célokra felhasználni;
[732] „adatmegosztás”: valamely érintett vagy adatbirtokos általi adatszolgáltatás egy adatfelhasználó számára az érintett adatok közös vagy egyéni felhasználása céljából, önkéntes megállapodások vagy az uniós vagy nemzeti jog alapján, közvetlenül vagy közvetítőn keresztül, például - kedvezményes díjért vagy díjmentesen - nyílt felhasználási vagy kereskedelmi engedélyek alapján;
[733] DGA 2. cikk 11. pont
[734] DGA 10. cikk a) pont
[735] DGA 12. cikk a) pont
[736] DGA 12. cikk c) pont
[737] DGA 2. cikk 11. pont a) alpont
[738] DGA 12. cikk e) pont
[739] DGA 12. cikk b) pont
[740] DGA 12. cikk m) pont

- nem személyes adatok esetén azonban számos biztonsági intézkedés meghozatalát várja el a szolgáltatótól, így például: jogellenes továbbítás vagy hozzáférés megakadályozása, adatbirtokos ilyen esetben történő tájékoztatása, nem személyes adatokon való műveletvégzés során megfelelő szintű biztonság szavatolása, valamint a legmagasabb szintű biztonság nyújtása a verseny szempontjából érzékeny információk tárolása és továbbítása tekintetében.[741]

Általános követelmény, amely az adatközvetítő által kötött minden szerződés teljes tartalmát át kell hassa, hogy a szolgáltatásához való hozzáférés eljárása méltányos, átlátható és megkülönböztetésmentes kell legyen az érintettek, az adatbirtokosok és az adatfelhasználók számára egyaránt, ide értve az árakat és a szolgáltatási feltételeket is.[742] Fontos azonban, hogy az átlátható és inkluzív megközelítés mellett is rendelkeznie kell olyan eljárásokkal, amelyek megakadályozzák a adatközvetítő szolgáltatásain keresztül hozzáférést kérő felekkel kapcsolatos csalárd vagy visszaélésszerű gyakorlatokat.[743] Az adatközvetítő szolgáltatással kapcsolatban zárásképpen kiemelendő, hogy az bejelentésköteles,[744] a hazai felügyeleti szerv feladatkörének ellátására a NAIH került kijelölésre.[745]

- *Az adataltruizmus*

A DGA az adatközvetítő szolgáltatásokkal egy vonalban említi az adataltruista szervezeteket. Az adataltruizmus lényege személyes és nem személyes adatok önkéntes, díj felszámítás nélküli közérdekű célokra történő megosztása.[746] Az adataltruista szervezetet szintén hatósági nyilvántartásba szükséges vetetni. A szervezet közérdekű célok teljesítése érdekében létrehozott jogi személy formájában, nonprofit alapon kell működjön és jogilag függetlennek kell lennie minden olyan szervezettől, amely profitorientáltan működik.[747] Az adataltruista szerezetek esetén különösen fontos követelményként jelenik meg azok átláthatósága, ezért azoknak teljes és pontos nyilvántartást kell vezetniük az adatot megszerzőkről, az ilyen alapon indult adatkezelések céljáról és az esetlegesen megfizetett díjakról. A szervezet a tevékenységéről, az adatot rajta keresztül megszerzőkről, az adatszerzés alapján végbemenő adatkezelés eredményéről és saját bevételi forrásairól éves jelentést kell készítsen a nyilvántartó hatóság felé (ami hazánkban szintén a NAIH).[748]

Az adataltruista szervezetek a működésük során a jogosultak érdekeinek védelme érdekében különböző követelményeknek kell megfeleljenek. Tájékoztatást kell adniuk az adatszerzés lehetséges közérdekű céljairól nem személyes adatok esetén általában, személyes adatok esetén kifejezetten és konkrétan, továbbá arról, hogy milyen célok esetén történhet harmadik országban végzett adatkezelés. A közvetítő szolgáltatóhoz hasonlóan az adataltruista szervezet sem használhatja az adatokat közérdekű céltól eltérő célra, az érintettek és az adatbirtokosok döntését azonban támogatnia kell (hozzájárulás, beleegyezés megadása/visszavonása). Személyes adatok esetén szintén hallgat – ezzel a GDPR alkalmazására utalva – de nem személyes adatokra vonatkozóan kiköti a tárolás és kezelés megfelelő szintű biztonságát, valamint a jogosulatlan hozzáférésről vagy továbbítást / felhasználást érintően tájékoztatási kötelezettséget alapít az adatbirtokos irányába.[749] Zárásképpen megjegyzendő, hogy az

[741] DGA 12. cikk j)-l) pontok
[742] DGA 12. cikk f) pont
[743] DGA 12. cikk g) pont
[744] DGA 11. cikk (1) bekezdés
[745] Info.tv. 64/E. §
[746] DGA 2. cikk 16. pont
[747] DGA 18. cikk
[748] DGA 20. cikk
[749] DGA 21. cikk

adataltruista szervezetekre vonatkozó DGA szerinti szabályanyag jelenleg lezáratlan, mivel a Bizottság egy szabálykönyv létrehozásával kiegészítheti azt (pl. az elvárt adatbiztonság tekintetében).[750]

- *Néhány védelmi előírás*

A DGA szerint mindenkinek joga van a rendelet hatálya alá tartozó ügyben, az adatközvetítő vagy adataltruista szervezet működésével szemben, a nyilvántartó hatóságnál panaszt tenni.[751] A rendelkezés így a DGA által tipizált adatgazdasági szereplőkkel kapcsolatba kerülő természetes és jogi személyek számára keletkeztet dedikált jogot jogaik védelmére, hatósági jogorvoslati eljárás létrehozásával. Az eljárás menetéről az Info.tv. tartalmaz előírásokat, amely alapján elmondható, hogy az kérelemre és hivatalból is indulhat, illetve, hogy a rendelet megsértése esetére 100.000 Ft és 50.000.000 Ft közötti bírság szabható ki az eljárás alá vont szervezetekre.[752] A DGA szerinti hatékony bírósági jogorvoslathoz való jog az előbb említett hatósági eljárás közigazgatási bírósági felülvizsgálatát célozza, ezáltal az említett szereplők sérelmes döntésekkel szembeni védelmét teremti meg.[753]

- *Összegzés*

Összegezve a DGA előírásai nagyon fontos mérföldkőnek tekinthetők az európai adatjogban. Az adatokhoz való hozzáférést biztosító rendelkezései az adathasználatot helyezik a védelem helyett előtérbe (kiutalva a GDPR előírásaira),[754] azonban látható, hogy a nem személyes adatok és jogi személyek védelme is úttörő módon megjelenik a rendelkezések között. Az adatközvetítő és adataltruista szervezetek által az adatok jogszerű mobilizációjára for-profit és non-profit megoldásokat is létrehozott, ami fontos lépésnek tekinthető az adatszuverenitási cél elérése és az adatalapú folyamatok „megtisztítása" felé. Ezzel kapcsolatban érdemes még kiemelni az adatok monetizált (kereskedelmi) állapotának jogalkotói elismerését is. Szintén fontos, hogy a közszféra számára a már korábban is meglévő közadathasznosítási szabályrendszer mellé beemelte a közszféra által kezelt, de védett adatok hasznosításának lehetőségét.

4.4.3.5. Az adatrendeletről (DA - 2023/2854/EU rendelet)

A rendelet célja az IoT területen történő méltányos és bizonyos tekintetben kötelező adathozzáférésre és -felhasználásra vonatkozó szabályok megalkotása, egyúttal az ilyen helyzetekben történő személyes adatok védelmének pontosítása. A DA igyekszik tisztázni, hogy ki és mely adatokat, milyen feltételek mellett hasznosíthat, ezért például olyan előírásokat alkot meg, amelyek az összekapcsolt termékek[755] felhasználói számára hozzáférési jogot keletkeztetnek az ilyen termék előállítója vagy valamilyen rá épülő alkalmazás szolgáltatója vonatkozásában, a használat során előállított adatok tekintetében.[756] Tehát olyan intézkedéseket tartalmaz, amelyek növelik a jogbiztonságot az adatokhoz való hozzáférés és használat tekintetében, ilyenek például:

- megengedett felhasználási célok és irányadó feltételek,
- adattovábbítás megkönnyítése,
- észszerű ellentételezési rendszer és vitarendezési mechanizmusok,
- egyes tisztességtelen szerződéses kikötések hatásának enyhítése,

[750] DGA 22. cikk
[751] DGA 27. cikk
[752] Info.tv. 64/F. §
[753] DGA 28. cikk
[754] Hoeren, Pinelli, 2024. 147 o.
[755] Eze alatt elsődlegesen valamilyen IoT eszköz értendő
[756] DA 1. cikk

- közszféra speciális adathozzáférési jogosultsága,
- a tisztességtelen szerződési feltételek meghatározása.[757]

A DA a DGA-hoz és a GDPR-hoz hasonlóan egy horizontális adatjogi jogszabály,[758] tehát a hatóköre minden ágazatra kiterjed. A szabályozási szemlélete kifejezetten az adathasznosítási folyamatok kontraktualizációjára épít, vagyis különböző szerződéses mechanizmusokban képzeli el a megfelelő működést.[759] Fontos továbbá, hogy a jogosulti szerepek tekintetében – bár definiál pozíciókat, de – nagyrészt hallgat, kiemelve, hogy abszolút jellegű jogosultságok helyett kívánatosabbnak tartja az adathozzáférésre és -felhasználásra vonatkozó jogok átruházásával kapcsolatos általános megközelítést.[760] Kiemelésre érdemes, hogy kifejezetten nem célja felülírni a meglévő joganyagot, így különösen az adatvédelmi előírásokkal (mint egy másik horizontális szabályanyaggal) párhuzamos alkalmazást vár el. A kettő összeütközésének feloldására pedig az adatvédelmi előírások elsőbbségét rögzíti.[761] A DA szabályozási célkitűzése egy meglehetősen összetett és bonyolult eszköztárat eredményezett. Ezt a fogalommeghatározások is visszatükrözik, ahol az adatmozgásban betöltött szerep szerint három új, lehetséges jogosulti pozícióban levő szereplőt (felhasználó,[762] adatbirtokos,[763] adatátvevő[764]) és a már más kontextusban valamilyen formában definiált adat, metaadat, személyes adat és nem személyes adat fogalmak mellett további, az IoT rendszerekhez illeszkedő három adattípust vezet be (termékadatok,[765] kapcsolódószolgáltatás-adatok,[766] könnyen elérhető adatok[767]).

- *Az adatokhoz való hozzáférés szabályai*

Kiindulópontként a DA azt tartja helyesnek, ha az IoT termékeket úgy tervezik meg és gyártják, hogy azok a generált adatokhoz közvetlen hozzáférést biztosítsanak a felhasználó számára.

---

[757] EURLEX, „A méltányos adathozzáférésre és -felhasználásra vonatkozó szabályok (adatrendelet)" Elérhető: https://eur-lex.europa.eu/legal-content/HU/LSU/?uri=CELEX:32023R2854&qid=1729329473643

[758] A DA (6) preambulumbekezdésének saját megfogalmazása szerint „a rendelet horizontális szabályokról rendelkezik, amelyeket a releváns ágazatok sajátos helyzetével foglalkozó uniós vagy nemzeti jog követhet."

[759] Moritz Hennemann, Gordian Konstantin Ebner, Benedikt Karsten, Gregor Lienemann, Marie Wienroeder: Data Act – An introduction. Baden-Baden, Nomos Verlagsgesellschaft mbH & Co. KG, 2024. 26 o.

[760] DA (6) preambulumbekezdés

[761] DA 1. cikk (5) bekezdés

[762] A DA 2. cikk 12. pont szerint a felhasználó olyan természetes vagy jogi személy, aki vagy amely egy összekapcsolt termék tulajdonosa, vagy akire vagy amelyre szerződésben ideiglenes jogokat ruháztak át az adott összekapcsolt termék használatára vonatkozóan, vagy aki vagy amely kapcsolódó szolgáltatást vesz igénybe

[763] A DA 2. cikk 13. pont szerint az adatbirtokos olyan természetes vagy jogi személy, akinek vagy amelynek joga vagy kötelezettsége olyan adatokat használni és rendelkezésre bocsátani, amelyeket valamely kapcsolódó szolgáltatás nyújtása során visszanyert vagy generált

[764] A DA 2. cikk 14. pont szerint az adatátvevő olyan, valamely összekapcsolt termék vagy kapcsolódó szolgáltatás felhasználójától eltérő természetes vagy jogi személy, aki vagy amely kereskedelmi, üzleti, kézműipari vagy szakmai tevékenységével összefüggő célok érdekében jár el, és akinek vagy amelynek az adatbirtokos adatokat bocsát a rendelkezésére, ideértve az olyan harmadik felet is, aki vagy amely a felhasználó által az adatbirtokoshoz intézett vagy az uniós jog vagy az uniós joggal összhangban elfogadott nemzeti jogszabályok szerinti jogi kötelezettségnek megfelelő adatigénylés nyomán jár el;

[765] A DA 2. cikk 15. pont szerint a termékadatok egy összekapcsolt termék használata által generált olyan adatok, amelyeket a gyártó úgy tervezett, hogy a felhasználó, az adatbirtokos vagy egy harmadik fél – beleértve adott esetben a gyártót is – elektronikus hírközlési szolgáltatás, fizikai kapcsolat vagy eszközön való hozzáférés révén visszanyerhesse azokat;

[766] A DA 2. cikk 16. pont szerint a kapcsolódószolgáltatás-adatok olyan, az összekapcsolt termékhez kapcsolódó felhasználói műveletek vagy események digitalizálását képviselő, valamely kapcsolódó szolgáltatás szolgáltató általi nyújtása során a felhasználó által szándékosan rögzített vagy a felhasználói művelet melléktermékeként generált adatok

[767] A DA 2. cikk 17. pont szerint a könnyen elérhető adatok olyan termékadatok és kapcsolódószolgáltatás-adatok, amelyeket az adatbirtokos jogszerűen szerez meg vagy jogszerűen szerezhet meg az összekapcsolt termékből vagy a kapcsolódó szolgáltatásból, aránytalan, egy egyszerű műveleten túlmutató erőfeszítés nélkül

Ehhez egy összetett tájékoztatási rendszert is felállít, amiből a felhasználó számára ki kell derüljön, hogy az által használt termék vagy szolgáltatás hogyan működik (milyen adatokat rögzít, hol, meddig tárolja, kik fognak potenciálisan hozzáférni stb.).[768] Amennyiben a termék vagy szolgáltatás nem biztosít közvetlen hozzáférést az adatokhoz, akkor a felhasználó kérésére az adatbirtokos indokolatlan késedelem nélkül hozzáférhetővé kell tegye (könnyen, biztonságosan, díjmentesen, átfogó, strukturált, széles körben használt és géppel olvasható formátumban) a könnyen elérhető adatokat és a kapcsolódó metaadatokat. A hozzáférés biztosítása korlátozható szerződéses alapon, ha a hozzáférés súlyosan hátrányos hatással járhat a természetes személyek egészségére, biztonságára és védelmére, illetve akkor, ha azt az adatok üzleti titok jellege bizonyos szélsőséges esetekben indokolja.[769] A rendelkezések között szerepelnek továbbá versenyvédelmi előírások[770] és a jogi személyek nem személyes adataira vonatkozó védelmi előírások.[771] A hozzáférési kérelem alapján megszerzett adatokat – a felhasználó kérésére – egy adatátvevő harmadik fél rendelkezésére kell bocsátania az adatbirtokosnak.[772] Az adatátvevő nem minősülhet a DMA szerint kapuőr[773] vállalkozásnak,[774] az ilyen három oldalú adathozzáférés esetén pedig az előzőekben ismertetett korlátozások és garanciák továbbra is érvényesek. Ezeken túl az adatátvevő harmadik fél az így szerzett adatokat csak a felhasználóval megállapodott célokra használhatja, azokat nem adhatja át önhatalmúan további harmadik fél részére, a megállapodást nem teheti kizárólagossá, valamint annak megkötése során nem alkalmazhat olyan megoldásokat vagy eszközöket, amelyek a felhasználó általi jogok gyakorlását korlátozzák vagy megnehezítik, így pl. nem kényszerítheti, vezetheti félre vagy manipulálhatja a felhasználót, vagy áshatja alá vagy gyengítheti az autonómiáját, döntéshozatalát vagy választási lehetőségeit.[775] Szintén tilos minden esetben kapuőr részére átadni az adatokat, illetve azokat az adatbirtokossal versengő termék létrehozására, vagy az adatbirtokos saját termékére hátrányosan használni.[776] Fontos, hogy az adatbirtokos és az adatátvevő közötti szerződésben a feltételeknek méltányosnak, ésszerűnek, átláthatónak és megkülönböztetésmentesnek kell lenniük (un. FRAND feltételek).[777] Az adatok monetizációjával kapcsolatban megjegyzendő, hogy az adatbirtokos és az adatátvevő által megállapodott, az adatok vállalkozások közötti kapcsolatok keretében történő rendelkezésre bocsátásáért kompenzáció kérhető az adatbirtokos részéről, amely árrést (hasznot) is magában foglalhat. A kompenzáció számításakor így az adatbirtokos nemcsak a költségeket, hanem az adatok gyűjtésébe és előállításába történő beruházásokat is számításba veheti (kivéve kkv vagy nonprofit kutatószervezet adatátvevő esetén, ilyenkor csak a költségek számíthatók fel).[778]

- *Az adatok rendelkezésre bocsátása közszférabeli szervezetek számára*

Az ilyen rendelkezésre bocsátás csak rendkívüli igény fennállása esetén lehetséges, amelyet a közszférabeli szervezetnek, a Bizottságnak, az Európai Központi Banknak (EKB) vagy egyéb uniós szervnek kell bizonyítania.[779] Az igény időtartama és hatálya korlátozott kell legyen,

[768] DA 3. cikk
[769] DA 4. cikk (1)-(8) bekezdések
[770] DA 4. cikk (10) bekezdés szerint a felhasználó a hozzáférési kérelem alapján szerzett adatokat nem használhatja fel olyan összekapcsolt termék kifejlesztésére, amely verseng azon összekapcsolt termékkel, amelyből az adatok származnak és nem is oszthatja meg az adatokat az említett szándékkal harmadik féllel.
[771] DA 4.cikk (13), (14) bekezdések
[772] DA 5. cikk
[773] DMA 3. cikk
[774] DA 5. cikk (3) bekezdés
[775] DA 6. cikk (1) és (2) bekezdések
[776] DA 6.cikk (2) bekezdés d)-f)
[777] DA 8. cikk
[778] DA 9. cikk
[779] DA 14. cikk

annak fennállását valamilyen szükséghelyzetre való reagálás, vagy jogszabályban kifejezetten előírt, közérdekből végzett konkrét feladat indokolhat, de csak akkor, ha az adatok megszerzése céljából rendelkezésére álló minden más eszköz kimerítésre került.[780] A kérelmet az adatbirtokosnak indokolatlan késedelem nélkül kell teljesítenie, de ha azt a szükséghelyzet indokolja, akkor arra a kérelem kézhezvételétől számított legfeljebb öt-harminc munkanapon belül kell reagálni. A kérelmet az adatbirtokos bizonyos esetekben el is utasíthatja vagy módosítását kérheti, ha pl. nem rendelkezik a kért adatok felett vagy korábban ugyanazon célból nyújtottak be hasonló kérelmet. Fontos, hogy amennyiben a kért állományban személyes adatok találhatók azokat az adatbirtokosnak kell anonimizálnia, kivéve, ha a kérelem teljesítéséhez kifejezetten személyes adatokra van szükség, ilyen esetben álnevesítést kell elvégeznie.[781]

- *A DA tisztességtelen szerződési feltételei*

A tisztességtelen szerződési feltételek meghatározása nagy hatással lehet az adatjogi ügyleti viszonyokra, főként a jelenlegi szereplők és az újonnan belépők gazdasági szempontú, egyenlőtlen helyzetére tekintettel. Az első explicit előírások a DA 13. cikkében szerepelnek, amely a vállalkozások közötti adathozzáféréssel és -felhasználással kapcsolatban főszabályként kimondja, hogy az egyoldalúan megállapított kikötéseknek nincs kötelező erejük, ha azok tisztességtelenek.[782] Ez alól kivételt jelent, tehát nem tisztességtelen az olyan szerződési feltétel, amely kötelező erejű uniós jogi rendelkezést vagy az, amely olyan uniós jogi rendelkezést tükröz, ami alkalmazandó volna, ha a szerződési feltételek nem szabályoznák a kérdést.[783] A kivétel mellett a rendelet kétféleképpen igyekszik meghatározni a tisztességtelenség lényegi elemeit, egyfelől a biztosan tisztességtelen és a vélelmezhetően tisztességtelen esetek példálózó felsorolásával, az alábbiak szerint:[784]

- tisztességtelen a szerződési feltétel, ha annak tárgya vagy hatása arra irányul, hogy
  - kizárja vagy korlátozza a feltételt egyoldalúan megállapító félnek a szándékos cselekmények vagy súlyos gondatlanság esetén fennálló felelősségét;
  - kizárja azon fél, amelyre nézve a feltételt egyoldalúan megállapították, számára rendelkezésre álló jogorvoslatokat a szerződéses kötelezettségek nemteljesítése esetén, vagy kizárja a feltételt egyoldalúan megállapító fél felelősségét az említett kötelezettségek megszegése esetén;
  - kizárólagos jogot biztosítson a feltételt egyoldalúan megállapító fél számára annak meghatározására, hogy a szolgáltatott adatok megfelelnek-e a szerződésnek, vagy bármely szerződési feltétel értelmezésére.[785]
- vélelmezhetően tisztességtelen a szerződési feltétel, ha annak tárgya vagy hatása arra irányul, hogy
  - helytelenül korlátozza a jogorvoslati lehetőségeket a szerződéses kötelezettségek nemteljesítése, vagy a felelősséget az említett kötelezettségek megszegése esetén, vagy kiterjessze azon vállalkozás felelősségét, amelyre nézve a feltételt egyoldalúan megállapították;

[780] DA 15. cikk
[781] DA 18. cikk
[782] DA 13. cikk (1) bekezdés
[783] DA 13. cikk (2) bekezdés
[784] A felsorolások tükrözik a polgári jog általános elveit, azonban annál lényegesen részletesebb és gyakorlatiasabb meghatározást adnak. Lásd a Ptk. 6:102. § (1) bekezdését, ami a fogalomalkotást a következőképpen rendezi: „tisztességtelen az az általános szerződési feltétel, amely a szerződésből eredő jogokat és kötelezettségeket a jóhiszeműség és tisztesség követelményének megsértésével egyoldalúan és indokolatlanul a szerződési feltétel alkalmazójával szerződő fél hátrányára állapítja meg."
[785] DA 13. cikk (4) bekezdés

- lehetővé tegye, hogy a feltételt egyoldalúan megállapító fél a másik szerződő fél adataihoz olyan módon férjen hozzá és azokat olyan módon használja fel, amely jelentősen sérti a másik szerződő fél jogos érdekeit, különösen akkor, ha az ilyen adatok üzleti szempontból érzékeny adatokat tartalmaznak, vagy üzleti titkok vagy szellemitulajdon-jogok védik azokat;
- megakadályozza, hogy az a fél, amelyre nézve a feltételt egyoldalúan megállapították, a szerződés időtartama alatt felhasználja az általa szolgáltatott vagy generált adatokat, vagy olyan mértékben korlátozza az ilyen adatok felhasználását, hogy az említett fél nem jogosult az ilyen adatok felhasználására, rögzítésére, az azokhoz való hozzáférésre vagy azok ellenőrzésére, vagy az ilyen adatok értékének kiaknázására megfelelő módon;
- megakadályozza, hogy az a fél, amelyre nézve a feltételt egyoldalúan megállapították, észszerű határidőn belül felmondja a megállapodást;
- megakadályozza, hogy az a fél, amelyre nézve a feltételt egyoldalúan megállapították, a szerződés időtartama alatt vagy a szerződés megszűnését követő észszerű időtartamon belül másolathoz jusson az általa szolgáltatott vagy generált adatokról;
- lehetővé tegye a feltételt egyoldalúan megállapító fél számára, hogy indokolatlanul rövid határidővel felmondja a szerződést, figyelembe véve a másik szerződő fél bármely észszerű lehetőségét arra nézve, hogy egy alternatív és összehasonlítható szolgáltatásra váltson, valamint az ilyen felmondás által okozott pénzügyi hátrányt, kivéve, amennyiben az ilyen eljárásra komoly indokok szolgálnak;
- lehetővé tegye a feltételt egyoldalúan megállapító fél számára, hogy lényegesen megváltoztassa a szerződésben meghatározott árat vagy a megosztandó adatok jellegével, formátumával, minőségével vagy mennyiségével kapcsolatos bármely más lényeges feltételt, amennyiben a szerződés nem jelöl meg érvényes indokot, és nem ad jogot a másik félnek a szerződés felmondására ilyen változtatás esetén.[786]

- A tisztességtelenség mellett az egyoldalúságot is definiálja a rendelet, e szerint a szerződési feltétel akkor minősül egyoldalúan megállapítottnak, ha azt az egyik szerződő fél írta elő, és annak tartalmát a másik szerződő fél az annak megtárgyalására irányuló kísérlete ellenére sem tudta befolyásolni. Rögzíti továbbá, hogy a szerződési feltételt előíró szerződő fél viseli annak bizonyítása terhét, hogy az említett feltétel nem egyoldalúan került megállapításra, továbbá azt is kimondja, hogy a vitatott szerződési feltételt előíró szerződő fél nem hivatkozhat arra, hogy a feltétel tisztességtelen szerződési feltétel volt.[787]
- A kógenciával kapcsolatban végezetül érdemes megemlíteni, hogy a rendelet ezen cikkének előírásainak alkalmazását a felek nem zárhatják ki, nem térhetnek el attól, és nem módosíthatják annak hatásait.[788]

➢ *Néhány védelmi előírás*

A DA számos ponton keletkeztet egyedi jogosultságokat az adatgazdaságban valamilyen formában résztvevők számára, azonban a legfontosabbak az egyedi jogorvoslatra, panaszra és

[786] DA 13. cikk (5) bekezdés
[787] DA 13. cikk (6) bekezdés
[788] DA 13. cikk (9) bekezdés

közigazgatási felülvizsgálatra vonatkozó előírásai. A DA több helyen[789] rögzíti, hogy a felhasználó a szolgáltatóval felmerülő bármely vitával kapcsolatban panaszt tehet az illetékes hatósághoz vagy – megállapodásuk alapján – vitarendezési testület elé terjesztheti az ügyet. Az említett vitarendezési testület a DA sajátja, 10. cikkében részletezi, hogy általánosságban mely esetekben (az adatok rendelkezésre bocsátására vonatkozó méltányos, észszerű és megkülönböztetésmentes feltételekkel és átlátható móddal kapcsolatos ügyekben), milyen szabályok szerint (pl. díjszámítás, költségviselés, ügyintézési határidő) járhat el. Fontos továbbá, hogy a testület alávetéses hatáskör alapján működik, tehát a feleknek meg kell állapodniuk ebben ahhoz, hogy a döntésnek kötelező ereje lehessen. Részletes leírást ad az adathozzáféréssel és -felhasználással kapcsolatos tisztességtelen szerződési feltételekről, amelyekről alább még lesz szó.[790] Végezetül a DGA-hoz hasonló módon panasztételi jogot és bírósági jogorvoslathoz való jogot is tartalmaz.[791] A jogvédelem kikényszeríthetősége vonatkozásában kiemelendő, hogy az általános szankciókra vonatkozóan tagállami hatáskörbe rendeli azok meghatározását, azzal az elvárással, hogy azok hatékonyak, arányosak és visszatartó erejűek kell legyenek. Szintén rögzíti, hogy személyes adatok esetén az adatvédelmi hatóság, mint illetékes hatóság továbbra is hatáskörrel rendelkezik és a GDPR szerinti összeghatárok közötti közigazgatási bírság szabható ki.[792]

- *Összegzés*

A DA számos tekintetben valósít meg számottevő előrelépést az azt megelőző állapothoz képest, a képviselt jogpolitikai célzatot – a szakirodalmi álláspontal egyetértésben – megfelelőnek gondolom, a kivitelezés értékelése azonban nem ilyen egyértelmű.[793] A hasznosítás területén a privátautonómia (kontraktualizáció) előtérbe helyezése a jelen dolgozat által képviselt álláspontal egybevág, de a szerződési szerepkörök és lehetséges kikötések vagy nem kerülnek kifejtésre, vagy meglehetősen bonyolult szisztémában valósítja meg ezt a DA, ami a jogkövetést megnehezítheti. A jogosulti pozíciók megerősítése nélkül a jelenlegi hatalmat gyakorlók a szerződéses viszonyokat dominálhatják, aminek az eredményeként a kívánt piaci hatások nem érhetők el.[794] Ezt az elképzelést erősíti, hogy a felhasználó hozzáférési joga csak a nyers (bemeneti) adatokra vonatkozik, az azok alapján létrehozott új (kimeneti) adatokra azonban nem. Ezt a visszásságot Martens úgy fogalmazza meg, hogy ez egy olyan helyzet, mintha a Microsoft az M365 felhasználók által, az excel programmal készített dokumentumok felett szerezne jogosultságot.[795] Ha a helyzet nem is feltétlenül ennyire sarkos minden esetben, annyi megjegyezhető, hogy az adaton fennálló jogosultságok tisztázatlanságából adatbirtokosi visszaélések származhatnak. Fontos azonban, hogy a kevés kézben koncentrált adatállományok „felszabadítására" vagy legalábbis annak megkezdésére szánt és arra egyértelműen alkalmas[796] a DA, amely így az adatjog hatályos rendszerének kiemelkedő képviselője.

[789] Pl. 4. cikk (3) bekezdésben a DA hatálya alá tartozó bármely szerződéses korlátozás vagy tilalom tekintetében vagy a (9) bekezdésben az adatmegosztás megtagadására vagy visszatartására vagy felfüggesztésére vonatkozóan. Az 5. cikk (12) bekezdése alapján utóbbi esetben harmadik fél is élhet ezzel a joggal.
[790] DA 13. cikk
[791] DA 38. és 39. cikkek
[792] DA 40. cikk
[793] Hennemann et al., 2024. 13 o.
[794] Hoeren, Pinelli, 2024. 121 o.
[795] Martens, 2023. 6 o.
[796] Különösen a DA 4. cikkében nevesített, felhasználóhoz rendelet alanyi jogon keresztül

4.4.4. Az EU hasznosítási szabályanyagának tervezett fejlődési irányáráról: a közös európai adatterek

Az EU adattereket, mint az adatok egyfajta belső piacának a koncepcióját[797] az Európai Adatstratégia alkotta meg, a célja meghatározott kulcsterületeken a biztonságos és megbízható adatfelhasználás és adatmegosztás elérése, amely tiszteletben tartja az adatvédelmi és kiberbiztonsági előírásokat.[798] Az adatterek az adatjog vertikális szabályanyagát fogják alkotni, mivel kifejezetten szektoronként kerülnek megalkotásra.

4.4.4.1. Az egészségügyi adattérről szóló jogszabály-javaslatról (EHDS - COM(2022) 197 final)

Az EHDS jelenleg javaslati formában létezik, de elfogadása esetén rendeletként fog létrejönni. A Bizottság indokolása szerint az európai egészségügyi adattér egy összetett kihívásra kíván megoldást adni. A cél, hogy egyszerre erősítsék a betegek jogait az elektronikus egészségügyi adataikhoz való hozzáférésben, továbbá, hogy támogassák a kutatást, az innovációt, a politikai döntéshozatalt és a szabályozói tevékenységet. A Bizottság az európai adatstratégia részeként, valamint az európai egészségügyi unió kiépítésének egyik prioritásaként említi, hogy egységesen, Unió-szerte kötelezően alkalmazott kereteket hozzanak létre az egészségügyi adatok megosztására és kezelésére.[799]A szabályozási tárgyát tekintve a rendelet az elektronikus egészségügyi adatok elsődleges és másodlagos felhasználására (jelen dolgozatban a másodlagos felhasználást hasznosításként jelölöm) vonatkozó szabályokat, közös szabványokat és gyakorlatokat, illetve infrastruktúrákat és irányítási kereteket határozza meg.[800]

- *Az adatfelhasználásra vonatkozó előírások*

Az EHDS elsődleges felhasználásként azonosítja az egészségügyi ellátással, illetve gyógykezeléssel összefüggő adatok kezelését,[801] a rendelkezéseinek első pillére ennek a viszonyrendszernek a szabályozására irányul, ilyenformán pedig valójában az adatok felhasználására tartalmaz rendelkezéseket. Olyan jogokat rendel az érintettek részére, mint a hozzáférés, másolatkérés vagy a helyesbítés joga. Szintén ide tartozik, hogy az adataihoz való, ellátórendszeren belüli (pl. szakorvosi) hozzáférést is korlátozhatja (kivéve amennyiben létfontosságú érdekének védelme azt indokolja[802]). A hozzáférésekről tájékoztatni kell az érintettet.[803] Az adat hozzáféréssel és bevitellel kapcsolatban az egészségügyi szakemberek csak az általuk ellátott személyek adataihoz férhetnek hozzá, az ellátásuk alapján keletkező adatokkal pedig kötelesek frissíteni az állományt.[804] A javaslat meghatározza, hogy milyen minimum adatkör vonatkozásában van szükség a hozzáférés és csere biztosítására, egy elektronikus nyilvántartási rendszer vezetésén keresztül,[805] valamint, azt hogy milyen

[797] DGA (2) preambulumbekezdés
[798] Prokopios Drogkaris, Javier Gomez Prieto (Szerk.), „Engineering Personal Data Protection in EU Data Spaces", Version 1.0, ENISA, 2024. 7-8 o.
[799] EHDS javaslat 2-4 o.
[800] EHDS javaslat 1. cikk
[801] EHDS 2. cikk (2) bekezdés d) pont szerint az elektronikus egészségügyi adatok elsődleges felhasználása a személyes elektronikus egészségügyi adatoknak az egészségügyi szolgáltatások nyújtása céljából történő feldolgozása azon természetes személy egészségi állapotának felmérése, megőrzése vagy helyreállítása céljából, akire az említett adatok vonatkoznak, beleértve a gyógyszerek és orvostechnikai eszközök felírását, kiadását és rendelkezésre bocsátását, valamint a vonatkozó társadalombiztosítási, adminisztratív vagy megtérítési szolgáltatásokat.
[802] EHDS javaslat 4. cikk (4) bekezdés
[803] EHDS 3. cikk; Az (5) bekezdés alapján a hozzáférést elektronikus egészségügyiadat-hozzáférési szolgáltatás keretében kell biztosítani, amiben más személy meghatalmazására (proxy) is lehetőséget kell biztosítani.
[804] EHDS javaslat 4. cikk (1) bekezdés
[805] EHDS javaslat 7. cikk

formátumban kell mindezt biztosítani (un. európai csereformátum).[806] A nyilvántartott adatok az alábbiak:

- betegadatlapok,
- elektronikus orvosi rendelvények,
- elektronikus gyógyszerkiadás,
- orvosi képalkotási leletek és jelentések,
- laboratóriumi eredmények,
- kórházi zárójelentések.

A szinergia jegyében a javaslat a jogosultság- és azonosításkezeléshez az eIDAS által bevezetett elektronikus azonosítási mechanizmust[807] is elfogadhatónak tartja.[808] A javaslat a gyártók, importőrök és forgalmazók által elérhetővé tett elektronikus egészségügyi nyilvántartó rendszer megfelelőségére, számos egyéb jogi aktusból ismert követelményt támaszt, mint a műszaki dokumentáció,[809] az EU-megfelelőségi nyilatkozat[810] vagy a CE jelölés alkalmazása.[811] Fontos továbbá, hogy az ilyen rendszerekről a Bizottság nyilvántartást vezet.[812]

➢ *Az adathasznosításra vonatkozó előírások*

A javaslat második, és az adathasznosítás szempontjából kiemelt pillére a másodlagos felhasználásra (hasznosításra) vonatkozik. Meghatározásra kerülnek a hasznosításba adható adatok kategóriái,[813] azok a hasznosítási célok,[814] amelyek esetén az engedélyezhető, valamint azok a célok is, amelyek explicite tiltottak.[815] A hasznosítás folyamatát tekintve az egyik oldalon az elektronikus egészségügyi nyilvántartó rendszer és működtetésben résztvevő szervezet(ek) állnak (adattulajdonos[816]) a másikon pedig az adatfelhasználó[817] található. A kettő közt egyfelől az un. egészségügyi adatokhoz való hozzáférés tekintetében illetékes szervek vannak, amelyek a tagállam által kijelölt (vélelmezhetően közigazgatási) szervek. Ezeknek a

[806] EHDS javaslat 5. cikk (1) bekezdés és 6. cikk.
[807] Pl. DÁP digitális tárca
[808] EHDS javaslat 9. cikk
[809] EHDS javaslat 24. cikk
[810] EHDS javaslat 26. cikk
[811] EHDS javaslat 27. cikk
[812] EHDS javaslat 32. cikk
[813] EHDS javaslat 33. cikk alapján pl.: elektronikus egészségügyi dokumentáció, népegészségügyi nyilvántartások, klinikai vizsgálatokból származó elektronikus egészségügyi adatok, biobankokból és célzott adatbázisokból származó elektronikus egészségügyi adatok stb. A (4) bekezdés alapján a szellemitulajdonnal vagy üzleti titokkal védett adatokat is ki kell adni, azonban mindent meg kell tenni a bizalmas jelleg megőrzésére.
[814] EHDS javaslat 34. cikk alapján pl.: oktatási vagy képzési tevékenységek az egészségügyben vagy a gondozási ágazatban vagy az ágazathoz kapcsolódó tudományos kutatás, a gyógyszerek vagy az orvostechnikai eszközök magas szintű minőségét és biztonságát biztosító termékekre vagy szolgáltatásokra vonatkozó fejlesztési és innovációs tevékenységek vagy algoritmusok betanítása, tesztelése és értékelése, többek között orvostechnikai eszközökben, MI-rendszerekben és digitális egészségügyi alkalmazásokban vagy személyre szabott egészségügyi ellátás nyújtása.
[815] EHDS javaslat 35. cikk alapján pl.: olyan döntések meghozatala, amelyek kizárják a természetes személyeket egy biztosítási szerződésből, vagy módosítják járulékaikat és biztosítási díjaikat, vagy egészségügyi szakemberekre, egészségügyi szervezetekre vagy természetes személyekre irányuló reklám- vagy marketingtevékenységek, vagy az olyan folyamatok, amelyek kárt okozhatnak az egyéneknek és a társadalom egészének, ideértve többek között, de nem kizárólag a tiltott kábítószereket, alkoholtartalmú italokat, dohánytermékeket, illetve olyan árukat vagy szolgáltatásokat, amelyek kialakítása vagy módosítása a közrenddel vagy a közerkölccsel ellentétes.
[816] EHDS javaslat 2. cikk (2) bekezdés y) pont. Az angol fordításban a DGA-ból és DA-ból ismert „data holder”, amit eddig „adatbirtokosként” fordítottak a hatályos jogban.
[817] EHDS javaslat 2. cikk (2) bekezdés x) pont alapján, aki vagy amely másodlagos felhasználás céljából jogszerű hozzáféréssel rendelkezik személyes vagy nem személyes elektronikus egészségügyi adatokhoz

feladata, hogy a hasznosítás céljából történő hozzáférést biztosítsák, a folyamatot irányítsák, az azzal kapcsolatos döntéseket meghozzák, így például a hozzáféréshez szükséges kérelmeket egy „adatengedély" kiadásával elbírálják.[818] Fontos, hogy az illetékes szervek és az adatfelhasználók közös adatkezelőnek minősülnek, így az adatkezelés jogszerűségéért egyetemlegesen felelnek.[819] A folyamat köztes szereplői közé sorolhatók még a DGA szerinti adatközvetítő szolgáltatók is, amelyek a két végpont közötti kapcsolat kialakítását végzik.[820] A hozzáférési kérelmet bármely természetes vagy jogi személy benyújthatja, a kérelemben minden alapvető adatkezelési körülményt meg kell határozni (pl. cél, adatok paraméterei, adatbiztonsági intézkedések, egyéb biztosítékok).[821] Az illetékes szervek a kérelmet értékelik a cél jogszerűsége, valamint a szükségesség és arányosság szempontjai szerint. Amennyiben megfelelőnek tartják, akkor adatengedélyt adnak ki, ami tartalmazza a hasznosítás legfőbb körülményeit (pl. adatok típusa, formátuma, cél, az engedély érvényességi ideje,[822] a feldolgozási környezet műszaki jellemzői, a felhasználásra kerülő eszközök, a fizetendő díjak).[823] A díjazással (monetizációval) kapcsolatban lényeges, hogy az illetékes szervek és az egyedüli adattulajdonosok a hasznosításra történő rendelkezésre bocsátásért díjat számíthatnak fel. Ha az igényelt adatkör a közsszférabeli szervezet kezelésében van, akkor a díjazás a költségek fedezésére szolgálhat. Ha ez nem így van, akkor a felszámítható díjak magukban foglalhatják az elektronikus egészségügyi adatoknak a kifejezetten gyűjtéssel kapcsolatos költségek egy részének ellentételezését is.[824] Zárásképpen fontos a javaslat előírásai közül kiemelni, hogy mindenfajta adatádassal kapcsolatban a főszabály az, hogy annak anonimizáltan kell végbe mennie. Kivételesen, ha az adatfelhasználó által végzett adatkezelés célja anonimizált adatokkal nem érhető el, akkor azokat álnevesített formában is hozzáférhetővé lehet tenni. Az álnevesítés visszafejtéséhez szükséges adat semmilyen körülmények között sem adható át a felhasználónak, akinek a javaslat alapján tilos megkísérelnie a visszaazonosítást.[825]

A javaslat előírásainak magyarországi adaptációja tekintetében felmerül az Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) működési összhangjának vizsgálata, ami feltétlenül szükséges lehet, hiszen az EHDS által kijelölt műveletvégzésre, valamint a jogok és kötelezettségek címzésére jelenleg ez a rendszer jön elsőként számításba. Az EESZT normatív hátterét jelenleg az Eüak. és az EESZT rendelet[826] adja. A képet pedig ezek figyelembevételével árnyalja, hogy a javaslat bár nem terjed ki az egészségügyi környezetben használt általános szoftverekre,[827] azonban kiterjed minden olyan készülékre vagy szoftverre, amelyet a gyártó elektronikus egészségügyi dokumentáció tárolására, közvetítésére, importálására, exportálására, átalakítására, szerkesztésére vagy megtekintésére szánt. Így az EESZT mellett felmerülhet, hogy az egyéb nyilvántartási célú (integrált, ügyviteli) medikai rendszerek is a hatálya alatt állnak. Fontos azonban, hogy az EESZT-hez (engedélyezett informatikai rendszer útján) egyébként csatlakozásra kötelesek pl. az egészségügyi szolgáltatók, még akkor is ha saját

[818] EHDS javaslat 36-37. cikkek
[819] EHDS javaslat 51. cikk
[820] ENISA, 2024. 7-10.
[821] EHDS javaslat 45. cikk
[822] Az EHDS javaslat 46. cikk (9) bekezdés alapján az adatengedélyt a kért célok eléréséhez szükséges időtartamra kell kiállítani, amely nem haladhatja meg az öt évet, ami egyszer legfeljebb öt évvel meghosszabbítható.
[823] EHDS javaslat 46. cikk
[824] EHDS javaslat 42.cikk
[825] EHDS javaslat 44. cikk
[826] Az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról szóló 39/2016. (XII.21.) EMMI rendelet
[827] EHDS javaslat 14. cikk (2) bekezdés

medikai rendszert alkalmaznak,[828] így az adattartalom számos átfedést tartalmaz a két rendszer között.

- *Összegzés*

Az EHDS javaslatot a szakirodalom egyes képviselői egyfajta „best practice" jogalkotásnak tartják az adatjogon belül.[829] Valóban a rendelkezések vizsgálata során az látható, hogy mind a felhasználás, mind a hasznosítás számára tartalmaz jól értelmezhető és alkalmazható előírásokat. Az egészségügyi adatokhoz való hozzáférés tekintetében a szerepkörök egyértelműbben kerültek meghatározásra, az eljárás követhetőnek tűnik. Az anonimizáció megkövetelésével a személyes adatok még a hozzáférés előtt elvesztik ilyen minőségüket, így az adatokon fennálló jogosultság az érintett bevonása nélkül megosztható lehet, a jogvédelem ésszerűbb megvalósítása mellett. Fontos, hogy a joggyakorlat jelenlegi állása abba az irányba mutat, hogy az olyan álnevesített adat, amelynek a visszafejtéséhez szükséges információhoz harmadik fél semmilyen módon nem tud hozzáférni, ennek a harmadik félnek a viszonylatában anonim adatnak tekinthető,[830] így végeredményben a javaslatnak megfelelően mindkét adathozzáférési megoldás egyaránt jól alkalmazhatónak mutatkozik. A szabályozási megoldásai a terület adottságai miatt összetettek, de a meglátásom szerint a komplexitásból eredő nehézségeket jól ellensúlyozza, hogy ágazati szinten, az egészségügyi szegmens sajátosságainak megfelelően került kialakításra.

4.4.4.2. A pénzügyi adattérről szóló jogszabály-javaslatról (FIDAR - COM(2023) 360 final)

Az adatterek másik, ugyancsak javaslati szinten álló rendelettervezete a pénzügyi szektor adataihoz való hozzáférésre irányul. A rendelet célja egy általános keret létrehozása a pénzügyi intézmények ügyféladataihoz való hozzáférésre, azok megosztására és felhasználására vonatkozóan.[831] A hatálya adatkategóriánkként és szervezettípusonként került meghatározásra. Így alkalmazandó például hitelekkel kapcsolatos egyenlegekre, kondíciókra és tranzakciós adatokra, pénzügyi eszközökre, a biztosítási alapú befektetési termékekre, a kriptoeszközökre, ingatlanokra, valamint az ezekből származó bevételekre, továbbá minden olyan adatra, amit a MiFID II[832] szerinti alkalmassági és megfelelőségi vizsgálat miatt gyűjtöttek, a biztosítási termékekre és a vállalkozások hitelképességi vizsgálatához kapcsolódó adatokra. Alkalmazandó továbbá hitelintézetek, pénzforgalmi intézmények, befektetési vállalkozások, kriptoeszköz-szolgáltatók, biztosítók és viszontbiztosítók stb. által kezelt adatokra.[833]

A javaslat a DA-hoz hasonló hárompólusú rendszerben működik,[834] azzal a korlátozással, hogy az adatok mobilizációja a pénzügyi szektoron belül kell maradjon.[835] A DA mellett az EHDS megoldásaiból is kölcsönöz, amikor egy illetékes hatóság engedélyéhez köti a pénzügyi információs szolgáltatók ügyféladatokhoz való hozzáférését.[836] Az engedéllyel rendelkező

[828] Eüak. 35/B. §
[829] Martens, 2023. 4 o.
[830] Dean Spielmann főtanácsnok indítványa, Európai adatvédelmi biztos kontra Egységes Szanálási Testület ügyében (C-413/23. P.)
[831] FIDAR javaslat 1. cikk
[832] Az Európai Parlament és a Tanács 2014/65/EU irányelve a pénzügyi eszközök piacairól, valamint a 2002/92/EK irányelv és a 2011/61/EU irányelv módosításáról.
[833] FIDAR javaslat 2. cikk
[834] FIDAR javaslat 6. cikk
[835] Az adatfelhasználó csak akkor lehet jogosult arra, hogy hozzáférjen az ügyféladatokhoz, ha az adatfelhasználó pénzügyi intézményként valamely illetékes hatóság előzetes engedélyéhez kötött, vagy pénzügyi információs szolgáltatónak minősül.
[836] FIDAR javaslat 12. ikk

szolgáltatókról az EBH[837] nyilvántartást vezet. A kérelem teljesítéséhez az adatfelhasználónak speciális követelményeknek kell megfelelnie, mint a működési és üzleti terv és megfelelő belső szabályozók (pl. BCP) megalkotása, ágazati irányítási rendszer megléte.[838]

Összegezve a FIDAR javaslat a DA és az EHDS megoldásait ötvözi és értelmezi újra a pénzügyi szektor adataihoz való hozzáférés biztosításának érdekében.

4.4.5. A Magyar adathasznosítás hatályos joganyagáról

Összhangban az EU „Digitális Iránytű 2030-ig" elnevezésű stratégiájával Magyarország is rendelkezik 2022-2030 közötti időszakra Nemzeti Digitális Stratégiával. Ebben a digitális gazdaság célkitűzésének égisze alatt kiemelt helyen szerepel az adatgazdaság támogatása, a digitális állam eléréséhez pedig az adat- és felhőalapú működéshez szükséges interoperábilis adatkapcsolatok hálójának kialakítását is említi. Megemlíthető még az MI innovációt támogató hatása szempontjából értékelt adatpolitikai stratégia 2019-ből, amely helyesen emeli ki az algoritmizáció és az adatok rendkívül szoros kapcsolatát.

4.4.5.1. A Nah.tv-ről (2023. évi CI. tv.)

A hazai jogszabályok vonatkozásában a nemzeti adatvagyon hasznosításának rendszeréről és az egyes szolgáltatásokról szóló 2023. évi CI. törvényt érdemes említeni. Ez a jogszabály 2023 év végén váltotta a korábbi közadatok hasznosítására vonatkozó joganyagot, vagyis a közadatok újrahasznosításáról szóló 2012. évi LXIII. törvényt és a nemzeti adatvagyonról szóló 2021. évi XCI. törvényt. A törvény a közfeladatot ellátó szervek által kezelt, a nemzeti adatvagyon körébe tartozó adatok hasznosításával és további felhasználásával kapcsolatos minden tevékenységre kiterjed, kiemelten szabályozza, hogyan lehet a közadatokat, illetve bizonyos feltételekkel a személyes és egyéb védett adatokat további felhasználási (hasznosítás) célra igénybe venni.[839] A Nah.tv. egyszerre érvényesíti a PSI irányelv közadatokra és DGA személyes és védett adatokra vonatkozó hasznosítási előírásait. Az adatvédelemből eredő garanciális szabályokat hangsúlyozva kiemeli, például hogy a közfeladatot ellátó szerv a személyes adatok kezelése esetén adatvédelmi hatásvizsgálatot kell lefolytasson az adathasznosítási-szolgáltatásnyújtás[840] megkezdését megelőzően,[841] valamint, hogy az adatok jogosulatlan megismerésének és felhasználásának kizárására a személyes és a védett adatok kezelésével kapcsolatos kockázatok figyelembevételével, adat-, és információbiztonsági intézkedéseket kell meghozzon.[842]

A nemzeti adatvagyon körébe tartozó adatok hasznosításának alapelveit a DGA előírásaival összhangban határozza meg és az átláthatóságot, valamint a megkülönböztetés és a kizárólagosság tilalmát rögzíti.[843] A nemzetiadatvagyon-hasznosítás összehangolt megvalósítása érdekében adathasznosítás-támogatási szolgáltatásokat állapít meg, amelyeknek a megvalósításában számottevő szerepet kap a NAVÜ.[844] A szolgáltatásokat a törvény két nagy csoportba sorolja.

- Központi adathasznosítás-támogatási szolgáltatások

[837] Európai Bankhatóság
[838] FIDAR javaslat 12., 14., 16. cikkek
[839] Nah.tv. 1-3. §
[840] A Nah.tv. 2. § 3.pont szerint ez a közfeladatot ellátó szervek adattal vagy dokumentummal végzett, az adatok hasznosítását elősegítő tevékenysége
[841] Nah.tv. 3. § (3) bekezdés b) pont
[842] Nah.tv. 98. §
[843] Nah.tv. 5-7. §
[844] Nah.tv. 10-14. §, 16. §; A NAVÜ szerepével kapcsolatban lényeges, hogy az 55. § alapján erre irányuló igény esetén kapcsolatot tart a DGA szerinti belföldi és külföldi adatközvetítőkkel a belföldi adathasznosítás támogatása, valamint a DGA-ban foglaltak érvényesítése érdekében.

    - Nemzeti Adatvagyon Leltár szolgáltatás,
    - egyablakos tájékoztatási és kapcsolattartási szolgáltatás,
    - nemzeti adatvagyon köré tartozó, nem személyes és nem védett adat egyablakos közzététele szolgáltatás,
    - kormányzati tájékoztatási szolgáltatás,
    - közcélú tájékoztatási szolgáltatás,
    - piaci tájékoztatási szolgáltatás,
    - döntés-előkészítést támogató szolgáltatás,
    - Nemzeti Adatplatform szolgáltatás,
    - adatok összekészítése szolgáltatás,
    - adat-összekapcsolási szolgáltatás,
    - kulcsszolgáltatás,
    - a Kormány által rendeletben meghatározott egyéb központi adathasznosítás-támogatási szolgáltatás,
- Regisztrációköteles adathasznosítás-támogatási szolgáltatások,
    - nemzeti adatvagyon körébe tartozó, nem személyes és nem védett adat rendelkezésre bocsátása szolgáltatás,
    - nemzeti adatvagyon körébe tartozó, személyes vagy védett adat rendelkezésre bocsátása szolgáltatás,
    - adattisztítási szolgáltatás,
    - személytelenítési szolgáltatás,
    - adatelemzési szolgáltatás,
    - elemzési célú hozzáférés biztosítása szolgáltatás,
    - kutatószoba-szolgáltatás,
    - felügyelt távoli elérés szolgáltatás,
    - az adatkormányzási rendelet szerinti adatközvetítővel való kapcsolattartás szolgáltatás,
    - a Kormány által rendeletben meghatározott egyéb regisztrált adathasznosítás-támogatási szolgáltatás.

Fontos, hogy a nemzeti adatvagyon körébe tartozó személyes vagy védett adat rendelkezésre bocsátása szolgáltatás keretében a közfeladatot ellátó szerv a nem nyilvános személyes adatot vagy védett adatot hasznosítás céljából személytelenített formában, személytelenítési szolgáltatás igénybevételével bocsáthatja csak az igénylő rendelkezésére.[845] A szolgáltatások nyújtásáért a közfeladatot ellátó szerv díjat állapíthat meg, ami jogszabályi előírás esetén a jogszabályban előírt díjat és díjmegosztást, ennek hiányában pedig az együttműködési megállapodásban rögzítettet jelenti. A díj mértéke főszabály szerint nem haladhatja meg a rendelkezésre bocsátott közadatok feldolgozásának, rendelkezésre bocsátásának és terjesztésének határköltségét.[846] Kivételesen a kulturális közadatok esetén a díj mértéke nem haladhatja meg a rendelkezésre bocsátott kulturális közadatok, valamint közadatot kezelő közvállalkozások kezelésében lévő adatok gyűjtésének, sokszorosításának, előállításának, tárolásának, feldolgozásának és terjesztésének észszerű megtérüléssel megnövelt költségét.[847]

A szolgáltató (közszférabeli szervezet) a közadatok további felhasználás céljára történő rendelkezésre bocsátásáról megállapodást kell kössön az igénylővel, ami a Nemzeti Közadatportálon közzétett általános szerződési feltételek elfogadásával jön létre.[848] Az

[845] Nah.tv. 42. §
[846] Nah.tv. 67. § (1)-(3) bekezdések
[847] Nah.tv. 89. §
[848] Nah.tv. 69. § (1), (2) bekezdés

általános igénybevételi eljárásban megkötött további felhasználásra vonatkozó megállapodás tartalmazza legalább:

- a felek megnevezését;[849]
- a további felhasználás céljából rendelkezésre bocsátott adatok megnevezését, azok átadásának időpontját, az átadás módját, formátumát, további felhasználás céljából történő rendelkezésre bocsátásáért megállapított díj mértékét, megfizetésének határidejét és módját;[850]
- a további felhasználás feltételekhez kötése esetén az adatok felhasználásának részletes feltételeit, amelyek kizárólag közérdekű célból állapíthatóak meg, objektívek, arányosak és megkülönböztetéstől mentesek és nem korlátozhatják szükségtelenül a további felhasználás lehetőségeit, nem szolgálhatnak a verseny korlátozására és nem ütközhetnek a további felhasználásra vonatkozó, az e törvényben meghatározott más rendelkezésekbe.[851]

Összegezve a Nah.tv. célja az volt, hogy biztosítsa a DGA magyarországi, törvényi szintű alkalmazhatóságával együttesen a közadatok hasznosításának elősegítését (a PSI irányelv átültetését), az igénylők számára átlátható és egységes szolgáltatási rendszerének kialakítását.[852] Ezt a törvényszöveg vizsgálata alapján azt mondhatjuk elérte és így elméletileg hatékony eleme lehet az adatjognak. Természetesen az alkalmazási tapasztalatok még hézagosak, így valós értékelést a gyakorlat kialakulását követően lehet ténylegesen elvégezni.

4.4.6. Példák az EU adathasznosításának egyéb szabályaira

Az adathasznosítás kompozit szabályai között említhetjük például a DMA kapuőrökre vonatkozó rendelkezését, ami szerint ezeknek kifejezett kötelessége biztosítani a végfelhasználók és üzleti felhasználók számára az adatokhoz való hozzáférést és azok hordozhatóságát, díjmentesen és (többek között) az adataikhoz való folyamatos és valós idejű hozzáférés biztosításával.[853] Szintén ide sorolható, hogy a kapuőrnek az online keresőprogramokat nyújtó, harmadik félnek minősülő vállalkozások kérésére tisztességes, észszerű és megkülönböztetéstől mentes módon hozzáférést kell biztosítania a kapuőr online keresőprogramjával végzett díjmentes és fizetett keresések során a végfelhasználók által generált rangsorolási, keresési, kattintási és megtekintési adatokhoz. Megjegyzendő, hogy a személyes adatnak minősülő keresési, kattintási és megtekintési adatokat anonimizálnia kell a rendelkezésre bocsátás előtt.[854]

Az MI rendelet szerint az MI rendszerek fejlesztése során a releváns adatelőkészítési műveleteket el kell végezni (pl. annotálás, címkézés, tisztítás, frissítés, gazdagítás és összesítés) a forrásadatbázisok jogszerűsége érdekében,[855] valamint az algoritmizált rendszerrel kapcsolatos feltételezéseket meg kell fogalmazni, különös tekintettel azon információkra, amelyeket az adatoknak az elvárás szerint mérniük kell és meg kell jeleníteniük.[856] Szintén ide vonható, hogy az MI működésében minden olyan torzítást vizsgálni szükséges, amelyek valószínűleg hatnak a személyek egészségére és biztonságára, negatív hatást gyakorolnak az

[849] Nah.tv. 69. § (4) bekezdés a) pont
[850] Nah.tv. 69. § (4) bekezdés b)-e) pontok
[851] Nah.tv. 69. § (4) bekezdés f) pont és (5) bekezdés a)-c) pontok
[852] 2023. évi CI. törvény végső előterjesztői indokolása
[853] DMA 6. cikk (9), (10) bekezdések
[854] DMA 6. cikk (11) bekezdés
[855] MI rendelet 10. cikk (2) bekezdés c) pont
[856] MI rendelet 10. cikk (2) bekezdés d) pont

alapvető jogokra, vagy az uniós jog által tiltott megkülönböztetéshez vezetnek, különösen akkor, ha az adatok kimenetei befolyásolják a jövőbeli műveletek bemeneteit.[857]

4.4.7. Összegzés a hasznosítás jogáról

Az adathasznosítás joga az elmúlt években indult nagyarányú fejlődésnek és bővülésnek. A hasznosítás vertikális anyagának a kidolgozása a közös adatterekre vonatkozó jogi aktusokkal még csak most kezdődik, az EHDS és FIDAR javaslatokkal. A hasznosítás jogának közös vonásai az alábbiak:

- Az adathordozhatóság joga fontosságának hangsúlyozása
- Az átláthatóságot és használhatóságot (adatformátumon keresztül) támogató intézkedések bevezetése
- A by design és a by default szemlélet megjelenítése
- A díjazásra (monetizációra) vonatkozó előírások meghatározása
- A célmeghatározás szerepének hasznosításba való átmentése
- A hasznosítás korlátozhatóságának kimondása
- Az anonimizáció és álnevesítés szerepének megjelölése és a hozzáférés engedést megelőző szakaszban való elhelyezése
- Jogi személyekre és nem személyes adatokra vonatkozó hasznosítási és védelmi szabályok bevezetése
- A szektorális szabályozás előtérbe helyezése

[857] MI rendelet 10. cikk (2) bekezdés f) pont

4.5. A jelen fejezet főbb kutatási eredményei

A védelem jogának alapja – jelentősége és szabályozási megoldásainak a tekintetében is – a GDPR, e mellett a CRA horizontális szabályai szintén kiemelhetőek. Az összes vizsgált joganyag tekintetében számos hasonló megközelítés azonosítható, amelyek így az adatjogi összetartás (konvergencia) alkotóelemei lehetnek.

- Kockázat-arányos védelem
- Kockázatértékelés és -kezelés fontossága
- Jelentéstételi kötelezettség és eseménykezelés (pl. incidensek)
- By design és by default szemléletek
- Egységességre törekvő harmonizált (szinergikus) szabályok
- Információbiztonság, kiberbiztonság és adatbiztonság eredményeinek ötvözése (pl. CIA triász)
- Alkalmazói és felhasználói tudatosság növelésének fontossága
- Ex ante jogszerűségi szabályok erősödése (DPIA, FRIA, ÉMT, SZAT)
- Folyamatszintű belső szabályozás megkövetelése (pl. irányítási rendszerek, BCP, DLP, IRC stb.)

Az adatok felhasználásának jogával kapcsolatban összegezve az alábbiakat mondhatjuk.

- A felhasználás joga jellemzően kompozit adatjogi előírásokban testesül meg, amelyek az adatok kezelésének alapvető paramétereit adják meg. Ilyen a konkrét adatkezelési cél, adatkör vagy megőrzési idő meghatározása.
- A felhasználás kevésbé explicit oldalához az ágazati jog által kinyilvánított célok, illetve lehetőségek megvalósítása érdekében végzett adatkezelések tartoznak, amelyeknek azonban a részleteit nem adja meg a joganyag, ezért azt általános adatjogi jogelvek mentén kell az adatkezelőnek meghatároznia.
- Léteznek a felhasználáshoz tartozó, de felhasználási jog által egyáltalán nem szabályozott területek, amelyeknek egyetlen közös jellemzője, hogy nem létezik rájuk vonatkozóan valamilyen kifejezett tiltás. Ezeknek ilyenformán keretet nem a felhasználás, hanem a védelem összetartó-hatású rendelkezései adnak (pl. alapelvek, jogalapok stb.).

Az adathasznosítás joga az elmúlt években indult nagyarányú fejlődésnek és bővülésnek. A hasznosítás vertikális anyagának a kidolgozása a közös adatterekre vonatkozó jogi aktusokkal még csak most kezdődik, az EHDS és FIDAR javaslatokkal.

- Az adathordozhatóság joga fontosságának hangsúlyozása
- Az átláthatóságot és használhatóságot (adatformátumon keresztül) támogató intézkedések bevezetése
- A by design és a by default szemlélet megjelenítése
- A díjazásra (monetizációra) vonatkozó előírások meghatározása
- A célmeghatározás szerepének hasznosításba való átmentése
- A hasznosítás korlátozhatóságának kimondása
- Az anonimizáció és álnevesítés szerepének megjelölése és a hozzáférés engedést megelőző szakaszban való elhelyezése
- Jogi személyekre és nem személyes adatokra vonatkozó hasznosítási és védelmi szabályok bevezetése
- A szektorális szabályozás előtérbe helyezése

5. Az adatjog szabályok jelenének és lehetséges jövőjének értékelése

A jelen fejezet célja az eddigi kutatási eredmények szintetizációja, a „sein" tényleges és a „sollen" lehetséges irányainak felvázolása és értékelése.

Az adatok, az adatalapú folyamatok és az európai adatjog jelenére, vagyis a sein vizsgálatára alapozva eljött az idő a jövőbe, a sollen irányába tekinteni. Ahhoz azonban, hogy a „mi van"-ból eljussunk a „mi legyen"-ig az eddigiek szisztematikus értékelését kell elvégeznünk és kiderítenünk, hogy „mi az ami nincs, de lehetne". Az értékelés technikájaként egy kontextuselemzési módszer, a SWOT analízis tűnik jól alkalmazhatónak. Ebben az erősségek, gyengeségek, lehetőségek és fenyegetések kerülnek kvalitatív számbavételre.

Az analízist az adatjogra, mint rendszerre vonatkoztatva végzem el, annak a hátterében lévő érdekeltségeket pedig az európai döntéshozók által kinyilvánított jogpolitikai célzatok alapján ítélem meg. Tekintve, hogy nem rendelkezem naprakész ismeretekkel a jogalkotás háttérfolyamatairól, ezért a feltevéseim lehetnek tévesek. Az analízis kvalitatív jellegéből adódóan az értékelés nem objektív mérésekkel, hanem szubjektív következtetésekkel fog lezajlani, így az téves kiindulóponti feltételezések esetén is felfogható, mint gondolatkísérlet olyan fiktív politikai akarat és jogalkotói szándék meglétére, amely egybeesik a feltételezésekkel.

5.1. Az erősségek

Az adatjogi rendszer erősségei a jogpolitikai célzat elérésére való alkalmasságot jelentik. Az európai adatjog stabil alapokkal rendelkezik, az elmúlt évtizedek szervesen és fontolva haladó jogalkotási lépései miatt. Az adatvédelmi jog és különösen a GDPR eredményeinek az EU állampolgárai már ma is haszonélvezői. Ezt az EU Bizottság a GDPR értékeléséről szóló jelentésében megerősíti, mikor azt többségében pozitívan értékeli.[858] Az adatvédelem mellett kiemelendő az a számos egyéb jogi aktus és dokumentum, amelyek az EU digitális jogalkotási hullámának keretében jöttek/jönnek létre. Ide sorolhatók azok a jogi aktusok, amelyeket az adatjog területeinek vizsgálatakor elemeztünk, de ide tartozik még például a világon egyedülálló mesterséges intelligenciára vonatkozó jogalkotás (MI rendelet), valamint a digitális szolgáltatások és piacok szabályozására vonatkozó rendelkezések (DMA és DSA). Az előírások sokrétűek, lévén rendkívül összetett életviszonyok szabályozására törekszenek, a világon gyakorlatilag ilyen formában élenjáróként,[859] azonban nem egyedüliként. A „Brüsszel effektusként" elterjedt EU jogalkotási globalizációs erő feltétlenül megemlítendő, ami például utat talált Dél-Korea jogrendjébe, ahol 2026 januárjával hatályba lépő MI szabályozási keretrendszer került megalkotásra, kifejezetten az EU MI rendelettel harmonizált módon.[860] A szakirodalom alapján is kiemelendő[861] ezekkel az új jogszabályokkal kapcsolatban a kockázatalapú és arányossági szemlélet erősítése, amely vezérelvként többek között lehetővé teszi a kötelezettségek teljesítésének rugalmasságát és skálázhatóságát. Szintén említhető a szabványosítás, a by design és by default megközelítések előnyös hatásainak jogalkotói

[858] COM(2024) 357 final, 14-15 o.

[859] Az MI rendelet jó példa az EU úttörő szerepére, lásd: European Parliament, „EU AI Act: first regulation on artificial intelligence" Elérhető: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[860] Soham Jethani, Pankhuri Malhotra, Hena Ayisha és Tanvi Nimje, „The Closing Act of 2024: South Korea's AI Basic Act", TLP Advisors. Elérhető: https://techlawpolicy.com/2025/01/the-closing-act-of-2024-south-koreas-ai-basic-act/#:~:text=South%20Korea%20passed%20its%20AI%20Act%2C%20a%20comprehensive,EU%20AI%20Act%2C%20adopting%20a%20similar%20risk-based%20approach

[861] Mantelero et al., 2021. 297 o.

elismerése, valamint a jelentéstételjellegű kötelezettségek elterjedése. A téma szempontjából különösen fontosnak hat a horizontális védelem előnyben részesítése és az ex ante jogszerűségi tesztek hangsúlyozása valamint a speciális előírások (többségének) az ágazati joganyagban történő elhelyezése. A hasznosítás területével kapcsolatban külön is kiemelendő a privátautonómia (kontraktualizáció) és a célmeghatározás szerepének hangsúlyozása és a hasznosítási folyamat korlátozhatóságának elismerése.

A jelenlegi állapotból származó, meglévő erősségek mellett fontos a bennük rejlő potenciál, vagyis a későbbi előny várománya is. Az összehangolt adatjogi szabályalkotás által a használat és a védelem egymáshoz képesti hangsúlyainak helyes beállítása egyedülállóan előnyös helyzetet teremthet az Unió számára a globális versenytársaihoz képest. Jelenleg az látható ugyanis, hogy az Unió az adatok tekintetében a védelem területét (különös tekintettel a személyes adatokra) mélyrehatóan kidolgozta és eltökélten igyekszik azt betartatni a piaci szereplőkkel. Ehhez képest a versenytársak (USA és Kína) szemlélete ellenkezőnek hat, az adatok használatának elsőbbségét hirdeti inkább (akár politikai, akár gazdasági okokból). Az adatjog két oldalának egyensúlya tehát Európában a védelem, míg máshol inkább a használat irányába billen. Kezd azonban érezhetővé válni, hogy egyik vagy másik oldal negligálása inkább hátrányos, mint előnyös helyzethez vezet. A két oldalt ugyanis jutalomként és kötelességként is elképzelhetjük. Másként megfogalmazva, ha a jogalanyok betartják a védelem szabályait, akkor a használat során haszonra tehetnek szert, ezáltal mindkét oldal igényeinek kielégítésében lehet érdekeltté tenni a legkülönbözőbb köz- és magánszférabeli szereplőket. E nélkül azonban arra következtetésre is juthatunk, hogy a védelem nélküli használat a társadalom és az egyén jogainak csorbulásához vezethet, míg a használat nélküli védelem gazdasági és piaci demotiváltságot, egyúttal az adatokban rejlő erő kihasználatlanságát eredményezheti. Az adatjog egységes (szinergikus, harmonizált) kialakítása egyedülállóan támogató környezetet eredményezhetne az Unió tagállamai számára, amiben az adathasználat által a szociális és technológiai innováció megfontoltan, de folyamatosan fejlődhet, miközben az egyéni és kollektív jogok és szabadságok sem sérülnek aránytalan mértékben.

5.2. A gyengeségek

Gyengeségek alatt olyan szubjektív (adatjogban rejlő) körülményekre gondolhatunk, amelyek a jogpolitikai célzatok elérésében gátolhatják a területet.[862] Az adatjog gyengeségei annak jellegéből erednek. A technológiai jog természetes töredezettsége mellett az EDPS által felvetett jogalkotási nehézségek kétségtelenül megjelennek. A terület rendkívüli gyorsasággal változik, ezért az időtállóság különösen kényes kérdés. A technológia-specifikus pontos előírások könnyebb alkalmazhatóság mellett megmerevedhetnek és elavulhatnak. Ezzel szemben a generálklauzulák és „gumiszabályok" túlszaporodásával, bár a joganyag rugalmasan értelmezhető marad, legalább értelmezési nehézségek, de könnyen joghézagok is kialakulhatnak.

A helyzethez hozzátartozik, hogy az EU joga bármennyire is proaktív szemlélet által vezérelt, több helyen körültekintően kerüli el alapvetőnek tűnő dogmatikai kérdések megválaszolását. Példaként említhető az adat magánjogi megítélésének tisztázatlansága, amellyel kapcsolatban még az adattulajdon szóösszetétel is meg-megjelenik,[863] majd nyom nélkül tűnik el. Jelenleg az adatfogalmak szükség szerint, ágazati szinten kerülnek meghatározásra, az azokra vonatkozó alapvető jogosultságok pedig legtöbbször kimondatlanok maradnak. E helyett egy nem

[862] Ezeket akár nevezhetnénk sebezhetőségeknek is, amelyek így párban is értelmezhetők fenyegetésekkel (mint veszélyforrásokkal). Az információbiztonságból ismert fogalompár lényege, hogy a veszélyforrások a rendszertől függetlenül, objektíve léteznek, a sebezhetőségek pedig rendszer-specifikus hibák vagy gyenge pontok. Érthetjük ezt úgy, hogy kihasználható sebezhetőség nélkül egy veszélyforrás nem jelent kockázatot.
[863] COM(2015) 192 final

konfrontatív, de nehezebben is alkalmazható „hozzáférés” alapú megközelítés a jellemző, ami nem minden esetben ad biztos alapot az adatok használatával kapcsolatban. Szilágyi ezzel összefüggésben például kiemeli, hogy még ha ez a megközelítés is a preferált, akkor is szükséges azt tudni, hogy ki az, aki jogosult a hozzáférés megadására.[864] A DA szerinti szerződéses mechanizmusokra vetítve a problémát: ha mást nem is, azt biztosan tudnunk kellene, hogy milyen adatról és ki szerződhet.

Az adatokon fennálló jogosultság hiányában az adatpiac létrehozásának irányába tett lépések veszélybe kerülhetnek. Jelenleg a személyes adatok feletti kontroll részben, nem személyes adatok esetén pedig egyáltalán nem tisztázott. Menyhárd szellemi alkotásokkal összefüggő álláspontja szerint a hasznosítás privilégiumát az indokolja, hogy a kizárólagossá tétellel lehet érdekeltté tenni a különböző szereplőket a folyamatokban való részvételben.[865] Ez igaznak hat az adatok esetén is, ahol szintúgy a kontrollvesztéstől való félelem az új piaci szereplőket elrettentheti, a kizárólagosságot biztosító előírások hiánya miatt a már meglévő vállalkozások profitabilitása sérülhet.[866] A DA kontraktualizációjával az értékegyenlőségi elv mellérendeltsége összhangban áll ugyan, de a tisztességtelenségre vonatkozó előírásain kívül a szerződési részletszabályokra kevés előírást tartalmaz.[867] E mellett a nem személyes magánadatok kérdésköre emelendő ki, amelyekre az FFNPDR szabad áramlást támogató előírásain és a DGA védelmi rendelkezésein kívül kevés jogosultat támogató előírás létezik. Ezt Szilágyi akként értelmezi, mintha ezen adatokat a jogalkotó „szabad prédaként” fogná fel,[868] amely így a már kifejtett bizonytalanságot és demotiváltságot tovább erősítheti.

A jelenlegi adatjogi szisztéma szürke zónájaként és így gyenge pontjaként említhetjük, hogy a védelem és a hasznosítás szabályai – bár egyértelműen összhangra törekszenek – a két terület egymáshoz való viszonyát nem tisztázzák kellő mértékben.[869] Az adatokról való rendelkezés joga, azok monetizációjának lehetősége (pl. forgalomképessége, áru vagy szolgáltatás jellege[870]) valóban nem került eddig kifejezetten rendezésre. Az összhang tekintetében a GDPR alapelvek, adatkezelési jogalapok és az érintetti jogok, illetve az alkalmazásuk következményei merülnek fel, mint tisztázandó kérdések (pl. a hasznosításba adott adathoz tartozó hozzájárulás visszavonása által okozott kár). Ehhez a problémakörhöz tartozik, hogy a vonatkozó szabályanyag rendkívül összetett és a betartása sokszor elnehezíti az ügyviteli folyamatokat. Ez a terület komplexitása miatt önmagában nem meglepő, azonban bizonyos aktusok követhetősége a még optimálisnál is nagyobb mértékben sérül. Gondolhatunk például a DA előírásaira, amik helyenként olyan hatást keltenek, mintha egy szektorális szabály specialitását feszítenénk szét a horizontális jog általánosságába, több-kevesebb sikerrel. Ez az un. „egyszerűsítési forradalom”[871] egyébként egy új, de annál fontosabb célkitűzése az EU-nak, amit az új joganyagoknak figyelembe kell vennie. Összességében a jövő adatjogi szabályainak – az adatterek által helyesen kijelölt úton – a szektorális szintre kellene korlátozniuk a különös és részletező jellegű szabályozást. Ennek a sikerességéhez azonban a horizontális jog kellően

[864] Szilágyi Ferenc, „Kié a digitális adat? Az allokatív adatjog létjogosultsága a magánjogi (dologi jogi) megközelítés margóján. I. rész”, Polgári Jog 2022/9-10. 1 o.
[865] Menyhárd, 2016. 77 o.
[866] Martens, 2023. 2 o.
[867] Hennemann et al., 2024. 15 o.
[868] Szilágyi, I., 2022. 10 o.
[869] Hennemann et al., 2024. 17 o.
[870] Az adatok áru vagy szolgáltatás jellegének megítélésével kapcsolatban lásd részletesen: Zech, 2017.
[871] Európai Tanács sajtóközleménye a „Budapesti nyilatkozat az új európai versenyképességi megállapodásról”, 2024. Elérhető: https://www.consilium.europa.eu/hu/press/press-releases/2024/11/08/the-budapest-declaration/

absztrakt, általános és egyszerűbben betartható[872] szabályanyagának a teljesebbé tételére van szükség, ami eddig a DA és az FFNPDR által nem tekinthető megvalósítottnak.

5.3. A lehetőségek

Lehetőségek alatt a sikeres, jogpolitikai célzatoknak megfelelő adatjogi rendszer által elérhető előnyökre gondolhatunk. Az összehangolt adatjogi jogalkotás által az alapjogi védelmet és az európai értékeket tiszteletben tartó fejlődési irányok kijelölhetők és követésük betartatható lehet. Az Unió által kitűzött technológiai versenyképességet[873] és adatszuverenitás elérését az adatalapú folyamatokban szereplők jogainak és kötelezettségeinek következetes meghatározása nagyban támogathatja, azáltal, hogy az EU adatállományainak következménymentes (pl. USA-ba vagy Kínába történő) kiemelését[874] megakadályozza vagy legalábbis megnehezíti. A nagy platformok erős piaci pozíciója évtizedes múltra nyúlik vissza, az ezzel kapcsolatos versenyjogi aggályok is jól azonosíthatóak, így nem csak az adatpiac létrejöttére, hanem a szabad verseny torzulásmentességére is jótékony hatással lehet a megfelelő szabályozás biztosításával az innovatív európai szereplők szabad piacra lépésének támogatása.[875]

Jelenleg a nagy platformok maguk által jogszerűen generált és ezek mellett kétes megítélésű állományok hatalmas mennyiségét vegyítik üzleti céljaik érdekében. Ezek a vállalatok pedig – gyakorlatilag az SAP és a Spotify kivétel – mind az EU-n kívüli érdekeltségeket képviselnek. Például a Microsoft, az Apple, az Amazon, a Meta és az Alphabet (Google) az USA, míg a Tencet, Bytedance és az Alibaba Kína érdekköréhez tartoznak. Az európai adatok megtartási arányának növelése jótékony hatással lehet az EU érdekköréhez tartozó vállalkozások megerősödésére és a globális versenyre való kilépésükre. Ezenfelül megjegyzendő, hogy az említett vállalatok közül több az algoritmizált rendszerek fejlesztésében is részt vesz, amely kifejezetten adatéhes folyamatnak tekinthető, ezáltal haszonélvezője lehetne az adatjogi jogalkotásnak.

Zárásképpen fontos kiemelni, hogy az Európai adatstratégia az uniós tagállamok összességére vonatkozó egységes szabályozás hiányát és a piaci erő kiegyensúlyozatlanságának kihívásait szintén azonosította.[876] A stratégia négy pilléren nyugvó megoldási rendszert vezetett be, amelyek elérését az adatjogi előírások fejlesztése támogathatja.

- *Az adatokhoz való hozzáférésre és az adatok felhasználására vonatkozó ágazatközi irányítási keret.*

A stratégia első pillére a keretek kijelölésének és a haladási irányoknak a meghatározására vonatkozó, horizontális szabályrendszer létrehozását tűzte ki célul. Ennek egyes elemei (pl. DGA, DA) azóta már megvalósultak, azonban az adatokra vonatkozó forgalombiztonság valamilyen jogosultsági rendszer hiányában felemásnak mondható.

---

[872] Gondolhatunk például az Európai Parlament és a Tanács irányelv javaslatára a szerződésen kívüli polgári jogi felelősségre vonatkozó szabályoknak a mesterséges intelligenciához való hozzáigazításáról
(a mesterséges intelligenciával kapcsolatos felelősségről szóló irányelv), aminek a megalkotásával az EU (Bizottság) a hivatalos kommunikáció szerint az egyszerűsítés elérése érdekében hagyott fel (a vélelmezhető lobbierő nyomása mellett). Lásd részletesen: Caitlin Andrews, „European Commission withdraws AI Liability Directive from consideration", IAPP, 2025. Elérhető: https://iapp.org/news/a/european-commission-withdraws-ai-liability-directive-from-consideration

[873] EU Bizottság, „EU Compass to regain competitiveness and secure sustainable prosperity", 2025. Elérhető: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_339

[874] Tóth, 2021. 28 o.

[875] Tóth András, „A tisztességes adatkereskedelmet biztosító szabályozás szükségességéről", ÁJT, 2021/3. 103 o.

[876] COM(2020) 66 final 7-13 o.;

- *Támogató eszközök: Adatberuházások, valamint Európa képességeinek és infrastruktúráinak megerősítése az adatok tárolása, feldolgozása és felhasználása tekintetében*

A terület támogatása kétségtelenül előnyös, fontos azonban, hogy a pénzeszközök egy iránymutató keretrendszer nélkül alacsony hatékonysággal kerülhetnek felhasználásra. Az infrastrukturális fejlesztések vonatkozásában fontos megjegyezni, hogy ebben a tekintetben is számottevő kitettsége van Európának a versenytársak irányába.[877]

- *Az egyének felelősségvállalásának növelése.*

A stratégia szerint „Az egyéneket továbbra is támogatni kell jogaik érvényesítésében az általuk előállított adatok felhasználása tekintetében." Érezhetően tehát a bizottsági elképzelés is a minél inkluzívabb, horizontális rendszert preferálja, aminek a megvalósulását azonban nehéz elképzelni a szereplők általános definiálása, jogaik és kötelezettségeik pontos meghatározása nélkül. Az ésszerűen felépített, de hézagmentességre törekvő szabályozáshoz a nem személyes adatokra is nagyobb mértékben alkalmazhatóvá kellene tenni az adatjog kiterjedtebb előírásait.

- *Közös európai adatterek a stratégiai ágazatokban és a közérdekű szakterületeken.*

Az adatterek közül az EHDS és FIDAR, az egészségügyi és a pénzügyi szektor adatainak megosztására szolgáló, vertikális adatjogi aktusok már a javaslati státuszban vannak. A tervek szerint összesen 14 szektorban fognak ilyen kezdeményezések megvalósulni, köztük az agráriummal, gyártással, közlekedéssel és az energiaszektorral. Ezek nagy eredményt érhetnek el a szektorok közötti adatmegosztásban.

5.4. A fenyegetések

Ezen a területen az olyan körülményeket vehetjük számba, amelyek az adatjogi rezsimtől függetlenül, objektíve létező, a jogpolitikai célzat szempontjából negatív körülmények, amelyek az adatjogi rendszer sikerességét hátrányosan érinthetik. Ide Európán belüli és kívüli eseményeket is sorolhatunk. Gondolhatunk olyan konkrét fejleményekre, mint Donald Trump második elnökségi ciklusának megkezdése, ami könnyen hatással lehet a NATO kibervédelmi képességére,[878] illetve negatívan érintheti az elmúlt évekre jellemző EU és USA közti szabályozási közeledést. Könnyen felmerülhet az új kormányzattal kapcsolatban, hogy az EU által igényelt garanciális szabályok leépítésre fognak kerülni, ami ismét hatással lehet az adattovábbítási keretrendszerre.[879] A Kínából érkező DeepSeek startup is említésre érdemes, ami a nemrégiben történt piacra lépésével jelentős zavart okozott. Az állítások szerint a DeepSeek MI-rendszerei lényegesen olcsóbban és hatékonyabban működnek, mint az eddigi (főleg USA-beli) versenytársak.[880] Ezzel szemben az OpenAI (a ChatGPT modellek szolgáltatója) az adatainak jogellenes megszerzésével („desztillációjával") vádolja a kínai

[877] Frances G. Burwell, Kenneth Propp „The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?", Atlantic Council. 2020. 3 o.
[878] Politico, „Trump's in. Here's what it means for Europe." Elérhető: https://www.politico.eu/article/donald-trump-washington-us-elections-win-2024-kamala-harris-europe-russia/
[879] NOYB, „US Cloud soon illegal? Trump punches first hole in EU-US Data Deal" Elérhető: https://noyb.eu/en/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal
[880] Eduardo Baptista, „What is DeepSeek and why is it disrupting the AI sector?", Reuters, 2025. Elérhető: https://www.reuters.com/technology/artificial-intelligence/what-is-deepseek-why-is-it-disrupting-ai-sector-2025-01-27/

céget.[881] A helyzettel kapcsolatban rögtön kettő adatjogi kérdés merül fel, amik egyébként bármelyik adatalapú vállalkozást bármikor érinthetik (akár Európában is):

1. mire alapozza az OpenAI, hogy az adatok egésze felett rendelkezési joga van? A GPT modellek fejlesztéséhez ugyanis (egy webcrawling-ként ismert technikával[882]) az interneten elérhető és valamilyen módon hozzáférhető tartalmak kerültek használatra.[883] A kérdés, hogy ezen a személyes és nem személyes adatokat tartalmazó állományok haszonszerzési célú hasznosítására az OpenAI milyen felhatalmazással rendelkezik.

2. milyen terület jogvédelmét kívánja igénybe venni az OpenAI? A nem személyes magánadatok halmazai felett jelenleg nehéz alkalmazható védelmi előírásokat találni, ugyanis sem az USA, sem az EU szerzői joga, iparjogvédelme vagy üzleti titokvédelme nem tud minden adat vonatkozásában segítséget nyújtani.

A fenyegetések egy absztraktabb szinten is megközelíthetők. Először is említhető az un. adatok diktatúrájának rémképe.[884] Ez alatt algoritmizált és adatalapú folyamatok, főként predikciós vonulatait (azok kimeneteinek biztonságát) érhetjük.[885] Ezekben az esetekben a nagy adathalmazok alapján létrejövő valószínűségszámításra épülő előre jelzések – súlyosabb esetben manipulatív megoldások – elterjedése és emberi felügyelet nélküli végbemenetele történik. Ez aggályos lehet egyfelől az ok-okozati összefüggések háttérbe szorulása miatt, másfelől (emberekkel kapcsolatos használat esetén) súlyos beavatkozást jelenthet a magánszférába és akár a döntési szabadság kialakítására is hatással lehet. Az adatok diktatúrájának nagyon is valós veszélyével szemben a védekezés már el is kezdődött. Az MI rendelet túl magas (elfogadhatatlan) kockázatúnak minősített MI felhasználási módszereket tilalmazza. A kockázatot a természetes személyek egészségére, biztonságára vagy alapvető jogaira nézve szükséges vizsgálni, tehát az adatvédelmi logikához hasonlóan nem a szervezeti érdekekre kell tekintettel lenni. A tiltott MI-gyakorlatokról az 5. cikk rendelkezik, azáltal, hogy meghatározza az eseteket és a tilalmukat deklarálja. Így tiltottak azok, amelyek szubliminális vagy célzottan manipulatív, megtévesztő technikákat alkalmaznak vagy amelyek személyek egy meghatározott csoportjának az életkor, fogyatékosság, illetve egyedi szociális vagy gazdasági helyzet miatt fennálló valamilyen sebezhetőségét kihasználják azzal a céllal vagy olyan hatás érdekében, hogy lényegesen torzítsák egy személy vagy személyek egy csoportjának magatartását azáltal, hogy jelentősen gyengítik a megalapozott döntéshozatalra való képességüket, azt eredményezve, hogy olyan döntést hozzanak, amelyet egyébként nem hoztak volna meg, és oly módon, amely az említett személynek, egy másik személynek vagy személyek egy csoportjának jelentős károsodást okoz vagy ésszerű valószínűséggel okozhat. Az előírást enyhébb esetben a nudging,[886] komolyabb esetben az önrendelkezéshez való jog (tágabban értelmezve a szabad akarat) artikulációját korlátozó eljárások tilalmának tekinthetjük.[887] Szintén tiltottak az olyanok MI megoldások, amelyek bűncselekmények

[881] Mark Sweney, Dan Milmo, „OpenAI 'reviewing' allegations that its AI models were used to make DeepSeek", The Guardian, 2025. Elérhető: https://www.theguardian.com/technology/2025/jan/29/openai-chatgpt-deepseek-china-us-ai-models

[882] Alexander S. Gillis, „web crawler definition", TechTarget. Elérhető: https://www.techtarget.com/whatis/definition/crawler

[883] Matt Burgess, Reece Rogers, „How to Stop Your Data From Being Used to Train AI", Wired, 2024. Elérhető: https://www.wired.com/story/how-to-stop-your-data-from-being-used-to-train-ai/

[884] Mayer-Schönberger, Cukier, 2014. 25 o.

[885] Fontos azt is látni, hogy az adatok diktatúrájának nem feltétele, hogy az személyes adatokra épüljön.

[886] Ződi Zsolt: Platformok, robotok és a jog (Gondolat Kiadó, Budapest, 2018) 76. o.

[887] A befolyásolástól mentes elmeműködésre egy új alapjogi csoport, az un. „neurális jogok" kezd kibontakozni. Lásd részletesen: Eszteri Dániel, „Neurális adatok és az emberi elme sértetlensége: Az agy-számítógép interfész technológia adatvédelmi problémái Chile legfelsőbb bíróságának ítéletén keresztül", Társadalomtudományi Kutatóközpont, jtiblog. Elérhető: https://jog.tk.hu/blog/2024/10/neuralis-adatok-emberi-elme-sertetlensege

elkövetésének kockázatértékelését végzik kizárólag a természetes személyekre vonatkozó profilalkotás vagy személyiségjegyeik és tulajdonságaik értékelése alapján (kivéve az emberi értékelést támogató rendszereket). Az előírás egyfelől olyan, jelenleg scifi-be illő, rendszerek megjelenését kívánja elkerülni, amelyek a büntethetőség határait túlzottan szétfeszítenék, vagy annak megállapításának alapját aránytalanul kiterjesztenék.[888] Másfelől viszont a szabály alól kivételt képeznek azok az esetek, ahol a büntetőeljárás csak augmentálásra és nem automatizálásra kerül. Erre valós példa lehet az Angliai un. Durham HART predikciós modell, amely egy terhelt vonatkozásában, két éves távlatban becsüli meg valamilyen súlyos bűncselekmény (pl. emberölés) elkövetésének valószínűségét.[889]

Az absztrakt fenyegetésekhez sorolhatjuk még az un. technológiai feudalizmus és az azzal rokon társadalmi berendezkedések megjelenését.[890] Varoufakis a jelenlegi rendszerek – így például a kapitalizmus – teljes átalakulását sem tartja kizártnak, aminek az eredményeképpen a királyok helyett a nagy platformok – a föld helyett – uralják a virtuális teret.[891] Ha az elgondolás egészében elrugaszkodottnak is hangzik, a mögötte meghúzódó fenyegetés reálisan értelmezhető. Kiindulópontként azt kell látnunk, hogy az egyének a totális és digitális adatosítás világában – Szabó meghatározásában – virtualizálódnak.[892] Ez alatt a virtuális (jelenleg digitális) személyazonosság alatt személyek egyedi jellemzőinek a digitális világban történő, adatként való leképezését és ez alapján történő azonosíthatóvá tételét értjük.[893] A virtuális és a valódi személy közti különbség sok esetben marginális (lehetőség van álnév használatára vagy az IP cím elmaszkolására, ez azonban kevésbé elterjedt és nem is szükségszerű), ezért a virtuális személy megfigyelése egyet jelenthet a valódi megfigyelésével. Ez a gyakorlat egy un. *panoptikonná* alakítja a digitális teret, ami önmagában aggályos lehet.[894] Ezen a ponton azonban ismét felmerül a nagy platformok uralmi helyzetének a kérdése, hiszen a digitális terek és így egyúttal a virtuális személyek felett is erős alá-fölé rendeltségi viszonyt alakíthatnak ki, valóban egyfajta techno-hűbéri rendszerhez hasonlóan. Fontos ugyanis, hogy a digitális elemek (termékek, szolgáltatások) esetén a tartós jogszerzés (pl. tulajdon) egészen ritkán valósul meg. A nagy platformok üzleti modellje – amennyiben nem zéróáras – akkor jellemzően előfizetés alapú, ami így oda vezet, hogy a jogviszony – és a digitális tér használati feltételei – a platform által bármikor módosítható vagy akár megszüntethető. Egyébiránt itt is észlelhető némi áthallás a középkori dominium directum (hűbérúr tulajdona) és a dominium utile (a vazallus használati tulajdona)[895] jogintézmények irányába. Végül többször merül fel a kérdéskörrel kapcsolatban a bekerítés (enclosure) jelensége. Ez a 16-18. századra jellemző angliai folyamatra utal, amelyben a textilipar megerősödéséből eredően megnőtt gyapjú keresletet elégítették ki a földbirtokosok

[888] Például Philip K. Dick amerikai író által, 1956-ban megalkotott „Minority report" című műben leírt helyzetet, ahol a büntetőeljárás már egy un. „precrime", tehát még egy el nem követett bűncselekmény alapján is megindulhatott (azonban nem mint előkészület vagy kísérlet, hanem mint befejezett stádiumú bűncselekmény)

[889] University of Cambridge, „Helping police make custody decisions using artificial intelligence", Elérhető: https://www.cam.ac.uk/research/features/helping-police-make-custody-decisions-using-artificial-intelligence ; Lásd részletesen: Oswald, Marion, Jamie Grace, Sheena Urwin, and Geoffrey C. Barnes. 2018. "Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality." *Information & Communications Technology Law* 27 (2): 223–50. doi:10.1080/13600834.2018.1458455.

[890] Ismert még mind digitális feudalizmus és mint adatfeudalizmus is.

[891] Carole Cadwalladr, 'Capitalism is dead. Now we have something much worse': Yanis Varoufakis on extremism, Starmer, and the tyranny of big tech", The Guardian. Elérhető: https://www.theguardian.com/world/2023/sep/24/yanis-varoufakis-technofeudalism-capitalism-ukraine-interview

[892] Szabó, 2012. 30 o.

[893] Paul De Hert: Identity management of e-ID, privacy and security in Europe. A human rights view,. Information Security Technical Report, 13 sz. 71 o.

[894] Garcia, 2024. 6 o.

[895] Tattay, 2016. 19 o.

oly módon, hogy az idáig közös használatban lévő vagy mások (jellemzően gyengébb gazdasági pozícióban lévő parasztoktól) használatából igyekeztek kerítés állítással elvonni a földterületeket. Az elvont területek korábbi használóinak a rendszer jogorvoslatot nem biztosított.[896] Ha a példánkban szereplő földeket adatokkal helyettesítjük akkor láthatjuk, hogy ezeknek is, mint erőforrásoknak az elkerítése zajlik nagy adatkezelők (államok, nagyvállalatok) által,[897] amelyek vagy az online terek mindenki számára nyitva álló részein található vagy gyengébb szereplők saját állományait igyekeznek kisajátítani.[898] A hűbéri rendszerépítés és az elkerítés vízióiból annyi biztosan kiolvasható, hogy az adatok jogszerű kezelése és szabad áramlása csak akkor valósítható meg, ha minden szereplő tisztában van azzal, hogy mely adatok kihez tartoznak és milyen jogok/kötelezettségek kiket és miért illetnek meg vagy terhelnek. Ellenkező esetben az információs aszimmetriából eredő, már meglévő hatalommal rendelkezők, a saját érdekeik mentén, akadálymentesen alakíthatják az adatalapú társadalmi és gazdasági folyamatokat továbbra is.

5.5. Az adatjog szabályozási hiányterületei

A SWOT analízis alapján azonosíthatónak gondolom a jelenlegi adatjogi rendszer legfontosabb hiányosságait. Ezek az alábbiak:

- Az adatok magánjogi megítélése
- Az adatokon fennálló jogosultság
- Az adatjogi szerződések tipizálása
- A horizontális minimumszabályok

A hiányosságokat látva azok mind a horizontális adatjog befejezetlenségére utalnak. Így egyfajta szabályozási hiányterületként azonosíthatjuk azon joganyagot, amely az adatokat fundamentális szinten rendezné és így alapot adhatna komplexebb folyamatok, koherens tisztázására specializáltabb szabályok által. Úgy gondolom fontos lenne egy olyan szabályozás megléte, ami jogot ad a jogalanyoknak arra, hogy rendelkezhessenek és kontrollt gyakorolhassanak az adataik felett akkor és ott, ahol erre szükségük van és a társadalom a lehetőséget biztosítani tudja. Ezáltal eszközt és motivációt lehetne adni az európai polgárok és gazdasági szereplők számára az adatalapú folyamatokban és különösen az adatgazdaságban való részvételre. Így nem (csak) a nagy adatkezelők ex lege korlátozásával, hanem a jogalanyok közösségi erejével (is) támogatni lehetne az Unió jogpolitikai célitűzéseit, mindezt fenntartható módon, a piaci törvényszerűségeket is tiszteletben tartva, kellően rugalmas megközelítést követve.

Az uniós célmeghatározásokra figyelemmel a lehetséges haladási irányok meghatározására a dolgozat további részeiben teszek kísérletet.

6. A horizontális adatjog hiányterületeinek szabályozási lehetőségei

A jelen fejezetben az adatjog lehetséges jövőjének kutatására kerül sor. Az eddigiekben feltárt eredményekre alapozva – azoknak szintetizációs kísérletének eredményeképpen – vizsgálatra kerül a szabályozás lehetséges forrása (meglévő jog alkalmazhatóságának a vizsgálata), valamint a formája és tartalma is. Ehhez a relációs jogviszony és az ahhoz kapcsolódó

[896] Szántó György Tibor: Anglia története. Budapest, Maecenas, 1992. ISBN 963-7425-53-5. 124 o.
[897] Purtova, 2017. 11 o.
[898] Sascha D. Meinrath, James Losey, Victor Pickard, „Digital Feudalism", Advances in Computers, vol. 81. 2011. 242 o.

jogosítványok, valamint az adatjogi szerződések egy lehetséges tipizálására is sor kerül. Zárásképpen olyan horizontális minimumszabályok kialakítására is kísérletet teszek, amelyek az adatjog közös alapját adhatnák mind személyes, mind nem személyes adatok kezelése esetén.

6.1. Az új szabályozás lehetséges forrásai

Az eddigi kutatásra alapozva azt mondhatjuk, hogy a szemiotikus adatfogalom alkalmas az adatok elméleti azonosítására, egyúttal egy közös értelmezési alapot is képes létrehozni a további, gyakorlati szintű adaptáláshoz. A két adatréteg, vagyis az adat jelszintje (a szintaktikai) és az adatban rejlő értelem szintje (a szemantikai) rétegek kerültek elkülönítésre. Az adatjog jelenlegi állapotának vizsgálata során azt dogmatikai és pragmatikus szempontok szerint határoltuk el, így a horizontális, vertikális és kompozit, valamint védelem, felhasználás és a hasznosítás kategóriáihoz jutottunk. Az ezek mögött működő szervező erőt, mint értékegyenlőségi elv azonosítottuk, ami segít elhatárolni a területeket egymástól, valamint választ ad olyan kérdésekre, mint az adatok feletti rendelkezés és az adatok monetizációja.

Az egyes területek szisztematikus elemzése és értékelése alapján a hatályos adatjog hiányterületeit is megkíséreltük azonosítani, így valójában a horizontális szabályok befejezetlenségére jutottunk. Ennek egyik eleme az adatok jogi megítélésének eldöntetlensége volt. Természetszerűen adhatják magukat ugyanis az olyan – eddig érintetlenül hagyott kérdések – mint a „kié az adat, vagyis ki adhat hozzáférést az adatokhoz?", vagy a „ki végezhet műveleteket az adaton?". A joganyag a válasszal kapcsolatban hallgat, míg a szakirodalmi álláspontok erősen megosztottak.

Két út mutatkozik járhatónak tehát. A 3.2.2. alfejezet eredményei alapján arra jutottunk, hogy új jog alkotására is lehetőség van, sőt bizonyos tekintetben szükségesnek is mondhatjuk, így az egyik megoldásunk az új joganyag megalkotása lehet. A másik lehetőség, hogy egy meglévő joganyagot valamilyen módon használhatóvá teszünk. Itt felmerülhet egy jelenleg hatályos jogág vagy terület hatálya alá vonni az adatjogi kérdések rendezését, amit egyfajta kompozit jogi megoldásnak tekinthetünk. Ezzel kapcsolatban egy alkérdés lehet, hogy a létező szabályok megfelelőek-e, vagy esetlegesen azoknak a kiterjesztésére van szükség az adatokra való alkalmazhatósághoz. A kérdések megválaszolása különösen fontos lehet, hiszen jogi státusz nélkül az adat, mint entitás gazdasági megítélése, továbbá az adatról rendelkezők, az azokhoz hozzáférők köre nehezen tisztázható, aminek következménye lehet, hogy az adatok használatához szükséges tranzakciók lebonyolítása – jogszerű keretek között – aggályossá válik, a folyamatban résztvevők és nem utolsó sorban a folyamat eredményének kedvezményezetti (tényleges és potenciális) köre pedig nehezen meghatározhatóvá. Az EU Bizottsága már 2016-ban észlelte az ebből eredő kockázatokat és célul tűzte ki az adatok szabad áramlásának biztosítása érdekében az adatok feletti rendelkezési jogosultság Uniós szintű tisztázását,[899] így ennek kísérletére kerül a következőkben sor. A keresett – létező vagy létrehozandó – adatokra vonatkozó jog létjogosultságát tehát abbéli képességében kell keresnünk, hogy az európai szintnek megfelelő védelem garantálása mellett egy olyan kiszámítható és átlátható rendszert alkot, amelyben az adatok szabad áramlása és használata nem ütközik aránytalan akadályokba. De hogyan képzeljük el ezt a területet, milyen elvárásoknak kellene megfelelnie? Az eddigiek alapján azt mondhatjuk, hogy a gyakorlatnak egy szilárd alapokat biztosító, rendszerteremtő, egyúttal a területek között közvetítő funkciót is betöltő keretszabályrendszerre van szüksége. Ez alapján ennek horizontális, általános és anyagi jogi jellegű rendelkezéseket kellene alapvetően tartalmaznia, a különös és eljárási szabályokat meghagyva vertikális jogalkotásnak.

[899] Inception Impact Assessment - European free flow of data initiative within the Digital Single Market, Európai Unió Bizottsága (CONNECT.E2), 2016.

6.1.1. Az adatok magánjogi minőségéről

Ahhoz, hogy a megfelelő jog azonosítható legyen először azt kell megvizsgálnunk, hogy az adatjogi rendszeren kívül, mint milyen entitás foghatjuk fel az adatokat. Eddig azt láttuk, hogy az adatok funkciójukat tekintve a védelemben, mint elkövetési tárgy, a hasznosításban monetizált erőforrás, a felhasználásban pedig egy társadalmi csereeszköz működnek. Ezek azonban, nem mutatják meg, hogy milyen módon lehetnek az adatok egy magánjogi ügylet tárgyai, tehát arra a kérdésre keressük a választ, hogy *mi* az adat magánjogi szempontból. Ahogy az látható volt, a jelenlegi uniós jogalkotás a kérdésben kerüli az egyértelmű állásfoglalást, de a szakirodalom vizsgálata alapján egészen jól körvonalazhatóvá kezdenek válni a gondolkozás lehetséges irányai.[900] Ennek azért van különös jelentőse, mert a jogi státusz már előre kijelölheti az alkalmazandó/létrehozandó jog alaptulajdonságait. Ahogy említettem, jelenleg az adat státusza az európai gondolkozásban nem definiált, a DGA és a DA az adatokhoz való hozzáférés és a hozzáférésről való rendelkezés lehetőségeként határozza meg a feleket, illetve a felek jogait és kötelezettségeit. Ennek oka sokrétű, azonban érdemes megjegyezni, hogy a vonatkozó jogalkotást megelőző EU intézményi kommunikáció törekedett a kérdést eldönteni, azonban azzal egy ponton felhagyott. A dokumentumok alapján az Unió álláspontja egy időben dologi jogi jellegű volt, amely még az *adattulajdonhoz* hasonló szófordulatoktól sem volt mentes.[901] Ebből két következtetést érdemes mindenképpen levonni: (i) az Unió számára elképzelhető lett volna az adatokra irányadó szabályokat a dologi jog mintájára létrehozni, (ii) ezt az elhatározását azonban elvetette. A valós okok – amelyek jogkérdések mellett politikai, diplomáciai területeket is bizonyára érintettek – feltárása helyett csak egy konzervatív végkonklúziót engedjünk meg magunknak: *az adat akár dolog is lehetne*. Ez a jelenlegi erősen megosztott szakirodalmi álláspontok egyik uralkodó szereplője,[902] vagyis az adatok dologiasítása, másként megfogalmazva az adatok dologként kezelése.[903] Ez alapján először azt érdemes megvizsgálni, hogy az adat tekinthető-e dolognak vagy sem.

A valós élethelyzetekben történő működést, az említett uniós álláspontot, számos szakirodalmi megközelítést és általában a kialakuló adatgazdaság mechanizmusait figyelembe véve annyit láthatunk biztosan, hogy az adatok értékteremtő funkciójukon keresztül valamilyen *emberi szükséglet kielégítésére alkalmas entitásokként foghatók fel*,[904] amelyeknek köz- és magánjogviszonyok között is egyértelműen azonosítható egyfajta *erőforrás szerepe*.[905] Közös elnevezéssel a szükségletkielégítő tényezőket szokás *javaknak* nevezni, amely már definiált fogalom a jog és a közgazdaság területén.[906] A logikai füzéren tovább haladva szembesülhetünk a *vagyon* kifejezéssel, ami jogi értelemben egy jogalany *javainak összességét* jelenti.[907] Tehát ha elfogadjuk, hogy az adat jószág, akkor az adataink ez alapján a vagyonunk részévé is

[900] Francesco Banterle, „Data ownership in the data economy: a European dilemma", SSRN Electronic Journal, 2018. 1 o.
[901] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az európai gazdasági és szociális bizottságnak és a régiók bizottságának az Európai digitális egységes piaci stratégiáról, COM(2015) 192 final, melléklet: A digitális egységes piac megvalósításának ütemterve
[902] Banterle, 2018. 8 o.
[903] Szilágyi, I., 2022. 14 o.
[904] Herbert Zech, „A legal framework for a data economy in the European Digital Single Market: rights to use data", Journal of Intellectual Property Law & Practice, 2016, Vol. 00, No. 0. 1 o.
[905] Lsd.: 2.2.2. alfejezet és 2.4. fejezet. Az álláspontot megerősíti a Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az európai adatgazdaság kiépítéséről (COM(2017) 9 final) szóló dokumentum 1. pontja, amely szerint: „Az adatok napjainkra kulcsfontosságú erőforrássá, a gazdasági növekedés, a munkahelyteremtés és a társadalmi haladás motorjává váltak."
[906] Murray Milgate: Goods and Commodities. In: The New Palgrave Dictionary of Economics. Palgrave Macmillan, London, 2008. 1-7 o. https://doi.org/10.1057/978-1-349-95121-5_1031-2
[907] Lenkovics Barnabás: Dologi jog. Eötvös József Könyvkiadó, 2014. 49–50. o. ISBN 978-963-733-849-6

válhatnak. A vagyon egyes elemeire alkalmazandó terminus technicus a *vagyontárgy*, amelyet a hatályos Ptk. 8:1. § 5. pontja a *dologgal, joggal és követeléssel* azonosít. Ezek között szerepel a dolog, amely az adatok jogi státuszát elvileg megfelelően rendezheti. Az álláspont egyébként nem elképzelhetetlen az európai jogrendszerekben, ugyanis léteznek olyan dologfogalom meghatározások, amelyekbe akár bele is érthető az adat, mint dolog. Ilyen például az osztrák polgári törvénykönyvben szereplő definíció, amely szerint „mindaz, ami a személytől különbözik és emberi szükséglet kielégítésére szolgál, jogi értelemben dolognak minősül".[908]

A pozitív érvek mellett azonban találunk ellenérveket is az adatok dologként való kezelésével összefüggésben. Az elgondolás gyenge pontja, hogy a magyar Ptk. 5:14. §-a – sok másik kontinentális jogrendszerhez hasonlóan – a dolgot „birtokba vehető *testi tárgyként*" írja le, aminek az adatokra való alkalmazhatósága *testiség* tekintetében kétséges. Bár az adathasználat területe nem hazai jogi specifikum, így annak létjogosultsága nem feltétlenül függ a magyar Polgári Törvénykönyvtől, azonban ez a fajta ellentmondás számos helyen jelenik meg az európai jogrendszerekben, így a feloldása mindenképpen indokolt lenne. Az adatok testiségével kapcsolatban – a létrejövetel módjára alapozva – korábban arra jutottunk, hogy azokat célszerű lenne immateriális, tehát testetlen tárgyként kezelni.[909] Ez alapján pedig ténylegesen szembesülnünk kell az adat immaterialitásával, ezáltal az európai polgári jog egy részének az adat-dolog elképzeléssel szembeni ellenállásával. Bár már a római jogban is léteztek immateriális vagy testetlen dolgok (res incorporalis), ezeket alapvetően jogokként vagy követelésekként fogták fel.[910] Az angolszász jog területén említhetők olyan megengedőbb álláspontok, amik szerint a dolog független a fizikai léttől (lásd.: „a vagyon elemei a dolgok"),[911] de ezeknek nem feltétlenül kell vonatkozniuk a kontinentális jogcsalád tagjaira. A jelenleg hatályos magyar jog szerint is van egyébként kivételszabály, amely esetén a Ptk. a dologra irányadó szabályokat rendeli alkalmazni – egy fikció által – immateriális entitások, a dolog módjára hasznosítható természeti erők esetén.[912] Sem a hatályos jog, sem a gyakorlat nem tartalmaz érdemi magyarázatot a természeti erő fogalmáról, azonban a korábbi polgári törvénykönyv kommentárja igen. E szerint a természeti erő alapvetően a villamos és a vízi energia. A többi energiahordozó már tárgy, tehát dolog (pl. az ásvány, a szénhidrogén). A régi Ptk. Nagykommentárja összegzően úgy fogalmaz, hogy a *természeti erő az a természettudományos (fizikai, kémiai stb.) úton meghatározható jelenség, amely vagyoni értékű szolgáltatások alapja (hordozója).*[913] Az adatok tehát a polgári jogi meghatározás alapján nem tekinthetők természeti erőnek.

Ezen példáktól függetlenül az alkalmazandó jogi rezsim megtalálása felé mindenképpen érdemes óvatos léptekkel haladni, hiszen hasonló helyzet vált a szellemi tulajdonjog központi kérdésévé, mondhatni létrejöttének egyik indokává. A kérdéskörre irányadó, egyik polgári jogi uralkodó álláspont az immateriális javak elmélete[914] volt, amely alapján a szellemi alkotások

[908] Allgemeines bürgerliches Gesetzbuch (ABGB) 285. § szerint: „Alles, was von der Person unterschieden ist, und zum Gebrauche der Menschen dient, wird im rechtlichen Sinne eine Sache genannt."
[909] Lásd részletesen 2.2.2. alfejezet
[910] Lenkovics, 2014. 34 o.
[911] Sir Frederick Pollock: A First Book of Jurisprudence. London, Macmillan and Co., 1918. 132-133 o.
[912] Ptk. 5:14. § (2) bekezdés
[913] Gellért György (Szerk.): Nagykommentár a Polgári Törvénykönyvről szóló 1959. évi IV. törvényhez, Budapest, Complex, 2009. 279 o.
[914] Kawohl, F. (2008) 'Commentary on Josef Kohler's *The Author's Right* (1880)', in *Primary Sources on Copyright (1450-1900),* eds L. Bently & M. Kretschmer. www.copyrighthistory.org Letöltve: 2024.07.22.

pont „testetlenségük” és „nonrivalitásuk” miatt kerültek ki a klasszikus tulajdonjog égisze alól,[915] amely ismérveikben azonosnak tekinthetők az adatokkal.

Tehát az európai jogrendszerek egy része, és ezek között hazai jogunk szerint is – ragaszkodva római jogi gyökereikhez – a dolgoknak fizikai léttel kell bírniuk és az adatok nem rendelkeznek ilyennel. Ameddig ez a helyzet fennáll ezekben a jogrendszerekben az adatot csak, mint vagyonunk testetlen tárgyát képzelhetjük el, amely így nem minősülhet dolognak. Ez azonban nem azt jelenti, hogy ne létezhetnének olyan tagállamok (pl. Ausztria), ahol a magánjog ettől eltérően szabályozza a dolgot, így ott az adatokat akár ekként is lehetséges lenne kezelni. Összegezve, és az uniós álláspontot is figyelembe véve, az adatok dologként való kezelése, bár kétségkívül lehetségesnek tűnik, jelenleg nem a legmegfelelőbb megoldást jelenti. Főként, ha figyelembe vesszük, hogy ezen elgondolás EU jogi harmonizációja túl erős beavatkozást jelentene egyes tagállamok magánjogába a dologi jogi értelemben vett numerus clausus elv[916] miatt, ami szerint a tulajdon tárgyát törvénynek kell meghatároznia. Ez önmagában nem lenne az uniós jogalkotás által áthidalhatatlan feladat, de az is fontos, hogy az uniós jog (jelenleg) nem sértheti a tagállamokban fennálló tulajdoni rendet,[917] tehát minden tagállamban, egyenként kellene polgári jogilag rendezni ezt a kérdést.

Így *az első kérdésünkre megkaptuk a választ, az adatot elvben lehetséges, de jelenleg EU jogpolitikai szempontból nem célszerű dologként kezelni*. Felmerülhet még, hogy ha az adatok dologként nem is, de mint a jogok és kötelezettségek összessége (összhangban a római jogi megoldással) a Ptk. hatályos definíciója szerint vagyontárgyak lehetnének. Ezt a kérdést kétféleképpen közelíthetjük meg:

- az adat nem önmagában, hanem a rajta fennálló valamilyen jog révén, annak tárgyaként válik egy személy vagyonává,
- az adatot többnek tekintjük az azon fennálló jogoknak és kötelezettségeknek az összességénél, a vagyon tárgya így nem a jog, hanem az adat.

Az első álláspont szerint az adat vagyontárgy, a második szerint – mivel nem dolog – ezért nem az. A két értelmezés közül az adatalapú ügyletek sikeressége szempontjából érdemesnek tűnik az elsőt alapul venni, mely esetben az adatokat, mint egy *immateriális vagyontárgyat*[918] azonosíthatjuk, amely így egyébként – a szakirodalomi állásponttal összhangban[919] - a természetes és jogi személyek javai közé is tartozhat.

6.1.2. Az adatok forgalomképességéről

Az adattal kapcsolatban arra jutottunk, hogy az jelenleg nem tekinthető dolognak, de kiindulópontként vehetjük, hogy mint immateriális vagyontárgy ügyletek tárgya lehet. Azt a kérdést is azonban fel kell tennünk, hogy azontúl, hogy fogalmilag az adat lehet vagyontárgy, ténylegesen lehet-e ügyletek tárgya?

Azt, hogy az adatok a magánjogi forgalomban megjelenhetnek-e, magánjogi jogviszonyok tárgyát képezhetik-e forgalomképességnek nevezzük.[920] Bármilyen kategóriájú adattal kapcsolatban a tényhelyzet jó ideje azt mutatja, hogy azok a forgalomban részt vesznek, azonban a jogi álláspont – főként kontinentális területeken – kevésbé egyértelműnek mondható,

[915] Lontai Endre, Faludi Gábor, Gyertyánfi Péter, Vékás Gusztáv: Szerzői jog és iparjogvédelem. Budapest, Eötvös József Könyvkiadó Kft., 2015. 21-22 o.
[916] Másként a zártkörűség elveként ismert, lásd: Banterle, 2018. 8 o.; Lenkovics, 2014. 22 o.
[917] EUMSz 345. cikk
[918] Szilágyi I., 2022. 14 o.
[919] Mayer-Schönberger, Cukier, 2014. 135 o.
[920] Menyhárd, 2005. 3-11 o.

elsősorban a személyes adatok személyiségvédelmi aspektusa miatt. A forgalomképesség gátját mind az EDPS, mind az EDPB abban látta, hogy az adatvédelem célja „az érintettek számára biztosítani, hogy az őket érintő információkkal saját maguk rendelkezhessenek, a személyes adatok ezért nem tekinthetők forgalomképes árucikkeknek."[921] Ezt a szakirodalom azzal egészíti ki, hogy a személyes adatok védelméhez fűződő jog, mint alapvető emberi jog elidegeníthetetlen, ezáltal az azok feletti – pl. piaci viszonyok közötti – rendelkezés lehetetlen, mert az alapjogi védelemről még a védelem alanya sem mondhat le.[922] Mind az EDPS és EDPB, mind a szakirodalom által felvetett aggályokkal kapcsolatban személyiségvédelmi és alkotmányjogi szempontból a 3.4.4. alfejezetben foglalkoztunk, ott pedig alapvetően arra jutottunk, hogy a védelmet lehetséges kevésbé paternalista szemszögből megközelíteni, és így egy olyan differenciáltabb értelmezésre jutni, ami bizonyos védelmi mechanizmusokat a jogosult döntésétől tesz függővé. Az ott leírtakra visszautalva, itt kifejezetten a forgalomképesség kérdését vizsgálom. Menyhárd szerint, a védett jogi pozíciók forgalomképessége alapvetően társadalmi konvenció kérdése. Ezt azzal az ambivalens helyzettel magyarázza, ami szerint a személyiség védelme és a döntés szabadsága is az emberi méltóságból vezethető le, tehát a jogi védelemnek ennek megfelelően kell differenciálnia a tiltás és az engedés módszerei között.[923] A döntés jelentőségével kapcsolatban megjegyzi azt is, hogy a jogvédelemről való lemondás az, ami végső soron forgalomképessé teszi az alanyi jogot.[924] Az elgondolását kifejezetten egészségügyi adatokkal kapcsolatban is megerősíti, e szerint: „ha a jog elfogadja, hogy a jogosult a személyiségjegyeinek – köztük a személyes adatainak – a felhasználásához akár ellenérték fejében, haszonszerzési céllal hozzájáruljon, és így azt jogszerűvé tegye, nincs ok arra, hogy azt ne kezelje forgalomképes vagyoni elemként". Görög a tapasztalható extenzív adatkereskedelem tapasztalata alapján szintén arra a következtetésre jut, hogy az adat forgalomképes vagyoni jószággá, magánjogi entitássá válása megfelelő normatív környezetben indokolt lehet.[925]

A szakirodalmi álláspontok mellett a tárgyi joggal is érvelhetünk a forgalomképesség mellett. Példa lehet a DCD irányelv[926] 3. cikk (1) bekezdésének második fordulata, amely szerint (a zéróáras modellt követve) a fogyasztó saját személyes adata a digitális tartalom szolgáltatásával szemben *ellenszolgáltatásként* funkcionálhat.[927] A forgalomképességre jó példának gondolom, függetlenül attól, hogy a DCD irányelv (24) preambulumbekezdése szerint „a személyes adatok védelme alapvető jog, és ezért a személyes adatok nem tekinthetők árunak". Ugyanis az áru fogalmi eleme a forgalomképesség és nem fordítva,[928] tehát attól, hogy nem tekintjük az adatot árunak, még lehet forgalomképes. Szintén ide vonhatók a DGA 2. cikkének olyan fogalommeghatározásai is, amelyek szerint az adatmegosztás (személyes és nem személyes

[921] EDPB 2/2019 iránymutatás a személyes adatoknak az általános adatvédelmi rendelet 6. cikke (1) bekezdésének b) pontja szerinti kezeléséről az érintettek részére nyújtott online szolgáltatások összefüggésében 16 o.
[922] Dermot Groome, „Chapter 1: Overview of Human Rights Law", Handbook of Human Rights Investigation, 2nd edition 2011. Idézve: Bart Custers, Gianclaudio Malgieri, Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data. Computer Law & Security Review 45 (2022) 4 o.
[923] Menyhárd, 2016. 78 o.
[924] U.o. 80 o.
[925] Görög Márta, „"Valami mocorog a felszín alatt" - Tézis, antitézis és szintézis a személyiségi jog területén", GJ, 2023/1-2., 14-16. o.
[926] Digitális tartalom szolgáltatására és digitális szolgáltatások nyújtására irányuló szerződések egyes vonatkozásairól szóló 2019/770 irányelv
[927] Az áru fogamát nem határozza meg az uniós jog, de a szakirodalom alapján azt, mint kereskedelmi értékkel rendelkező, *kereskedelemi forgalomba hozható* tárgyat vagy terméket definiálhatjuk. Lásd részletesen: Karoliny Eszter, Komanovics Adrienne, Mohay Ágoston, Pánovics Attila, Szalayné Sándor Erzsébet: Az Európai Unió joga. Budapest-Pécs, Dialóg Campus Kiadó, 2015. 256 o.
[928] Menyhárd Attila, „Az egészségügyi adatok forgalomképessége", Információs Társadalom XXII, 3. szám (2022). 35 o.

adat esetén egyaránt) *díj* ellenében történhet, vagy az adatközvetítő szolgáltatás célja *kereskedelmi* kapcsolatok létrehozása. Ezek alapján még ha a személyes adatok forgalomképessége kimondatlan is marad, annyit mindenképpen megállapíthatunk, hogy az adatokhoz vagyoni jellegű jogosultságok tapadnak és ezek a DGA és DA mellett a GDPR alapján is megoszthatók (gondolhatunk az adathordozhatóság jogára), így az adatjogi okfejtéseinket ebből az alapállapotból érdemes indítani.

6.1.3. A létező területek alkalmazhatóságának vizsgálatáról

Ahogy fentebb megállapítottuk a hiányzó jogalkotási elemet az adatok horizontális és általános szintjére vonatkoztatva keressük. Azt is láthattuk, hogy a hiányzó szerep betöltésére több, már létező jelölt is felmerül, ezek közül a legkiemelkedőbbek a dologi jog, a szerzői jog és az üzleti titokra irányadó jog (tényleges alkalmazásuk vagy kiterjesztésük). Ennek lehetőségét az alábbiakban tekintem át röviden.

6.1.3.1. A dologi jogról

A dologi jogot a vagyoni berendezkedés jogának szokás nevezni, ez a jog az, amely megmondja, hogy milyen javak hajthatók emberi uralom alá. Ahogy a nevéből is következtethetünk a dolgok feletti uralmi viszonyokat szabályozó területről van szó, amelyet alapvetően abszolút szerkezetű rendszerként foghatunk fel. Ebben a jogosultat törvényi keretek között teljes védelem illeti meg az uralma alatt álló dolog feletti hatalom gyakorlásával összefüggésben, ebből kifolyólag a jogok kizárólagosak és (mindenki mást) kirekesztő jellegűek.[929]

Ahogy az látható volt a dologi jog – adatok dologként való kezelése által – sokak, köztük egy időben az Unió számára is kívánatos választásnak tűnt. A fentebb leírtak miatt azonban az adatok dologi minősége kérdéses, így a dologi jog jelen állapotában számos uniós tagállam számára nem alkalmazható. Olyan alapvető problémákba is ütközhetne az alkalmazása esetén a jogalkotó, mint a tulajdoni viszonyok átláthatósága. Ez alapján jelenleg az ingatlanokon fennálló tulajdont közhiteles nyilvántartás biztosítja, míg ingókon a birtok maga.[930] Ahogy azt láttuk ezeket a viszonyokat az adatok dinamikusan változó közegében (ahol ugyanazon adat egyik adatkezelő számára lehet személyes adat, míg egy másik számára nem) egyáltalán nem, vagy csak nagyon nehezen lehetne elképzelni. Szintén általában aggályos lehet a dologi jog vonatkozásában, hogy ha az adat dolog és a dologi jog hatálya alá tartozik, akkor minden, ami adatalapú (pl. a szerzői művek, információ, titkok stb.) logikailag bekerülne a dologi jog hatálya alá, ami globális szabályozási nehézségekhez vezetne (ugyanazzal az eszközkészlettel szabályozni *mindent* az autóadásvételtől az adathasznosításig nem tűnik ésszerűen megvalósíthatónak).

6.1.3.2. A szellemi tulajdonjogról

A szellemi tulajdonnal kapcsolatba említésre került, hogy hasonló okból jött létre, pontosabban megfogalmazva nyert önállóságot a dologi joghoz képest, mint amilyen helyzetben az adatok vannak. A szellemi alkotások az adathoz hasonlóan immateriális, nonriválisés másolható formában léteznek. A dologi jog mellett tehát ez is egy észszerűnek tűnő haladási irány lehet, a szabályozási hatóköre és célja azonban nem mondható ideálisnak. Az alkalmazási aggályok forrása lehet, hogy a szellemi tulajdon – pontosabban ennek két területe, a szerzői jog és az iparjogvédelem – valamilyen eredeti és újszerű szellemi alkotást vagy más oltalmi tárgyat igyekszik védeni.[931] Az adat fogalma alapján látható, hogy annak létrejöttének bár feltétele, hogy a tényszerűséget eredeti módon reprezentálja, azonban az újdonság e tekintetben csak a

[929] Lenkovics, 2014. 15 o.
[930] Purtova, 2017. 5 o.
[931] Lontai et al., 2015. 21 o.

megfigyelő oldalán kell fennálljon, ehhez nem kell globálisan újszerű legyen. Szintén érdemes megjegyezni, hogy a szellemi tulajdon területei az emberi kreativitás szellemi munkájának eredményeire, mint immateriális javakra tartalmaznak rendelkezéseket, míg az adatok esetén sem az emberi, sem a kreatív kvalitások nem lehetnek szempontok. Olyan célszerűségi problémák is felmerülhetnek, minthogy a szerzői jog szerint jogi személy nem lehet szerző,[932] ami megint csak a személyes adatokra fókuszáló jogvédelem erősödéséhez vezetne. Szintén fontos, hogy a jelen dolgozatban felépített adatjogi paradigma szerint a szerzői jog a szükséges horizontális szabályok helyett kompozit (vertikális) szabályként fogható fel. Így a hatálya és szabályozási eszközkészlete is lényegesen speciálisabb, mint amire a korábbi megállapításaink alapján szükség lenne.

6.1.3.3. Az üzleti titok védelméről

Az üzleti titok a gazdasági tevékenységhez kapcsolódó, titkos – egészben, vagy elemeinek összességeként nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető –, ennélfogva vagyoni értékkel bíró olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja.[933] Az üzleti titokra vonatkozó szabályozás előnye, hogy hatályát tekintve egészen rugalmas, nincs szükség dologi minőségre vagy szerzői jogi eredetiségre, újszerűségre.[934] Ellentétben azonban a dologi vagy szerzői joggal az üzleti titokvédelem részlegesebb védelmet nyújt, mivel az üzleti titok jogosultjától függetlenül ugyanarra az eredményre jogszerű keretek között bárki juthat. Az üzleti titok, titokjellegéből adódó fogalmi eleme, hogy az ne legyen közismert és a jogosult megtegye a titokban tartás érdekében a tőle elvárható intézkedéseket. Így az üzleti titok védelme valójában a megfelelően védett titok tényhelyzetének megváltoztatása esetén alkalmazandó védelmi rendszerként fogható fel,[935] ami adatok esetén – például a felhasználási tűréskényszer miatt – nehezen tűnik alkalmazhatónak.

6.1.4. A meglévő joganyagok kiterjesztésének lehetőségéről

A vizsgált három terület hatálya jelenlegi formájában nem tűnik alkalmazhatónak. A dologi jog esetén az adat dolog-minősége, a szellemi tulajdonnál az egyediség, újszerűség és (időnként) az emberi közrehatás, míg a titokvédelemmel kapcsolatban a titkosság az, ami hiányzik. A hatály problémáját az okozhatja, hogy az adatokra irányadó szabályozási megközelítések egy része az indokoltnál speciálisabb (nem kellően absztrakt, vagyis a jog a társadalmi viszonyt vagy vonatkozást és a benne megnyilvánuló emberi magatartást [az adatalapú viszonyokat] nem kellő általánosságában, tipikusságában ragadja meg, hanem azt konkretizálja vagy egyediesíti[936]). Gondoljunk az adatok szemantikai rétegénél taglalt jogi kategóriákra, ahol a koordináta rendszer négy dimenziója alkotta az első szintet (ezek a személyes és nem személyes, illetve a magán- és közadatok voltak), ami alatt – jellemzően specializáló vagy korlátozó szabályok által definiált – a második szint foglalt helyet (ilyenek például a titokvédelem vagy szerzői jog által meghatározott adatok).[937] A szerzői jog műre vonatkozó előírásaira ugyanis az adatok egy konkrét megjelenési formáját szabályozzák, nem az adatokat általában. A mű is adat, de annak egy speciális kontextusban megjelenő, individualizált formája.

---

[932] Grad-Gyenge Anikó: Egy modern szerzői jog. Budapest, Wolters Kluwer Hungary, 2019. 53 o.
[933] Az üzleti titok védelméről szóló 2018. évi LIV. törvény 1. § (1) bekezdés
[934] Banterle 7 o.
[935] Zech, 2015. 196 o.
[936] Visegrády Antal: Jogi alaptan. Pécs, Janus Pannonius Tudományegyetem Állam- és Jogtudományi Kar, 1996. 13 o.
[937] Megjegyzendő, hogy a koordináta rendszer térbeli kiterjedése a korlátozással érintett adatok mellett, a tengely másik végpontján egy még absztraktabb kategóriát is kijelölt, ami a jog által nem definiált adatok voltak.

Ezek alapján vizsgálható, hogy a hatály kiterjeszthető-e, illetve a szabályok módosíthatóak-e úgy, hogy az adatalapú folyamatokra *is* alkalmazhatók legyenek. A dologi jog helyzethez igazítását jelentené az immateriális dolog kategória megalkotása vagy az adatoknak a *dolog módjára hasznosítható entitások* kategóriájához történő besorolása. A szellemi tulajdonnál az adat, mint védett mű kellene megjelenjen, de ehhez a művé válás feltételeit kellene módosítani, hiszen az adatok nagyegésze szempontjából jelenleg nem felel meg (lásd: pl. az adatbázis védelem csak az egyedien összeállított gyűjteményekre vonatkozik). Az üzleti titkok szabályainak alkalmazásánál is az látszik, hogy a titokban tartás követelményét kellene megszüntetni, mivel bizonyos esetekben az adat szemantikai tartalma nem fedhető el, miközben az adat feletti rendelkezés továbbra is fenn kell álljon (pl. attól, hogy egy egészségügyi adat az ellátó számára ismert még nem szüntetheti meg az érintett fennálló jogosítványait).

Összességében azt mondhatjuk, hogy a kiterjesztés során bármely területet is vesszük alapul, a ténylegesen illeszkedő állapothoz annyi kivételszabályt kellene beépíteni, hogy a végeredmény csak igen távoli rokonságot mutatna az eredeti joggal, ezáltal mindegyik rendszer kereteit aránytalanul szétfeszíthetné.[938] Fontos azonban, hogy ha nem is alkalmazhatók egészében, de a területek tartalmaznak olyan jogtechnikai megoldásokat, amelyek jól illeszkedhetnek az adatokra.

Az alkalmazhatósággal kapcsolatban végeredményben úgy gondolom, hogy az adatjognak nem lehet célja a szerzői jog, a dologi jog vagy a titokvédelem létjogosultságának az elvétele, azonban ez fordítva is igaz kellene legyen, ezek sem törekedhetnek az adatjog létjogosultságának megtagadására. Vagyis ezek alapján az látszik, hogy egyik jelenleg létező jogterület sem alkalmas – sem jelenlegi formájában, sem alkalmazási kiterjesztése által – az adatok szükségesnek tűnő mértékű szabályozására.

6.2. Az adatokon fennálló jogosultság

A meglévő adatjogi rendszer új joganyag létrehozásával történő kiegészítését tartom megfelelő megoldásnak. A hiányosságoknál látott tényezők miatt a horizontális adatjog befejezettségéhez és így az adatok helyzetének rendezéséhez szükséges előírások rendkívül sokfélék lehetnek, azonban a saját álláspontom szerint a dologi jog fundamentális megközelítését mindenképpen érdemes figyelembe venni és azt az adatok jogi természete miatt szükség lenne a szellemi tulajdon és az üzleti titokvédelem által kidolgozott (a területek specifikumaitól mentes) eszközökkel feltölteni. Ennek a rendszernek az alábbi feltételeknek kellene megfelelnie, ahhoz, hogy működőképes lehessen:

- az adatok jogi természetére (dologként való kezelésére) vonatkozó európai törésvonalakat tiszteletben kell tartania, mindaddig, míg e tekintetben egységes álláspont nem alakul ki,
- az adatok sajátosságaihoz alkalmazkodnia kell, azt kellő rugalmassággal és absztrakcióval kell kezelnie, ahhoz, hogy relevanciáját tartósan megőrizze,
- a szabályozást az alapvető jogokkal és az EU célkitűzéseivel összhangban, a speciális és korlátozó szabályokat tartalmazó jogterületekkel való kapcsolódásra képesen kell létrehoznia,
- a horizontális megközelítés érdekében az adatjog mindhárom (pragmatikus csoportosítás szerinti) területén alkalmazhatónak kell lennie.

[938] Drexl, 2016. 27 o.

6.2.1. Az adatjogi jogosultság alapjairól

Az új horizontális szabályok egyik fókuszában az adatokon fennálló jogosultság kell álljon. A hatályos uniós joggal kapcsolatban elöljáróban kiemelendő, hogy az nem ismeri a jogosultat, csak az (adat)birtokost.[939] A DA adatbirtokos fogalma a termék gyártója vagy a kapcsolódó szolgáltatás nyújtója. Ehhez lazán és kissé aggályosan[940] kapcsolódó módon a DGA is ismeri az adatbirtokost. E szerint az egy olyan jogi személy - ideértve a közszférabeli szervezeteket és a nemzetközi szervezeteket - vagy a szóban forgó konkrét adatok tekintetében nem érintett olyan természetes személy, amely vagy aki az alkalmazandó uniós vagy nemzeti joggal összhangban jogosult hozzáférést adni bizonyos személyes adatokhoz vagy nem személyes adatokhoz, vagy jogosult azokat megosztani. A DGA hatálya alá tehát azon jogosultak fognak tartozni, amelyek – egyéb műveletek mellett – biztosan képesek az adatokhoz való hozzáférés biztosítására, illetve az adat tényleges átadására. Ez azonban nem azt jelenti, hogy más típusú jogosultsági konstellációk (például pusztán tárolást végző adatfeldolgozók vagy akár a DA által definiált szolgáltatók) ne létezhetnének. Az adatbirtokos kifejezés egyébként talán a korábbi dologi jogi elgondolások maradványának tekinthető okokra vezethető vissza – egyetértve Szilágyival[941] – mindazonáltal kevésbé szerencsés szóhasználatnak gondolom. Nem azért, mert dologi jogi áthallása van, hanem azért, mert egy erős rendelkezési jogot dedikál a „birtokláshoz", miközben a tulajdonosról nem szól, aminek a létezése így tisztázatlan marad. Végeredményben azonban kiemelendő, hogy a dologi jogi csökevény az eredeti angolnyelvű verziókban nem szerepel, a DGA és a DA is a „data holder-t" említi, ami sokkal kevesebb áthallással bír, így ez a probléma fordításbelinek mondható.

6.2.1.1. A jogosultság létéről

A jogosultság létének szükségét már jelen dolgozatban is sokszor, sokféleképpen vizsgáltuk, azt azonban Malgieri kutatásai alapján lehetne legjobban összegezni. E szerint, *amennyiben nem történik meg a jogalkotó általi jogosultság-allokáció, akkor ennek a kiosztása azzal arányban fog megtörténni, amilyen arányban az egyik fél képes kizárni a másikat az (erőforrás) használatából.* Vagyis mindenképpen létrejön a jogosultság, de ott és olyan tartalommal, ahol azt a legnagyobb hatalmi koncentráció képes megragadni[942] és ez valószínűleg mindaddig így lesz, amíg az adathoz kellően magas gazdasági érték társul.[943] Valamilyen jogosultság – mint amilyen a tulajdon is – Janecek szerint de iure és de facto módon jöhet létre, vagyis azt vagy a pozitív jog hozza létre vagy a jogosult és a jogosultság tényszerű összekapcsolódása.[944] Akár úgy gondoljuk, hogy a pozitív jog csak a természetjogot deklarálja, akár úgy, hogy a jogosultságot maga alapítja meg, a jogosultság megszerzésének valamilyen elméleti megalapozásra van szüksége, tehát tudnunk kell, hogy miért fogadjuk el a jogosultságot annak, ami. Erre többféle elmélet alakult ki. Az egyik megközelítés, a Nozick által felépített „igazságos

[939] Jelenlegi fordításában az EHDS javaslat még az adattulajdonost is ismeri, de annak is az eredeti angol kifejezése a data holder (mint az adatbirtokosé), így messzemenő következtetéseket nem érdemes a szóhasználatból levonni.
[940] Mindkét esetben az elsődleges fogalomalkotó tényező a hozzáférés adás joga vagy kötelezettsége, ez alapján észszerűnek tűnik a közös szóhasználat. A DGA adatbirtokosa azonban tágabb és sokkal inkluzívabb személyi kört fed le. A DGA alapján adatbirtokos gyakorlatilag bárki lehet, míg a DA szerint az adatbirtokos csak egy nagyon speciális szolgáltatást nyújtó személy vagy szervezet (a szolgáltatás nyújtásának [pl. IoT eszközök gyártása] pedig meglehetősen magas a bekerülési küszöbe). A DA fogalomhasználata ismét abba az irányba mutat, mintha egy szektorális szabályt húzott volna szét a jogalkotó horizontális kiterjedtségűre, hiszen a DGA-hoz képest mintha lex specialis lenne a DA fogalomalkotása.
[941] Szilágyi I., 2022. 5 o.
[942] Gianclaudio Malgieri, „'Ownership' of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?", Journal of Internet Law, Vol. 20, n.5, 2016. 7-8 o.
[943] Purtova, „The Illusion of Personal Data as No One's Property", 7 Law, Innovation and Technology 83, 2015. 28 o.
[944] Janecek, 2018. 9 o.

szerzés" modellje,[945] ami a jogosultságot (tulajdont) egy aktív magatartáshoz és a megszerzett jogosultság átruházásához köti.[946] Ezt a megközelítést a jelenleg hatályos jogi megoldásokhoz (pl. a szerzői művön a létrehozás általi jogszerzés[947] vagy a tulajdon átruházhatósága[948]) közelállónak mondhatjuk. Egy másik megközelítést is meg kell említeni, amely tiszta erőhatalomra és „foglalásra" épül („pure force/last occupation theory").[949] Egyszerűen megfogalmazva e szerint azé a jogosultság, aki képes azt megszerezni és megtartani.

Az adatalapú folyamatok vizsgálata során jelenleg azt tapasztalhatjuk, hogy a nagy állami és céges adatkezelők az adatokon fennálló jogosultságot de facto, az erőfölényük kihasználásával megragadják és ezt a helyzetet az önszabályozáson alapuló piaci mechanizmusok ezidáig nem tudták megoldani (ha megtudták volna oldani, akkor nem látnánk olyan jogi aktusokat, mint a GDPR, a DMA, DSA, DGA vagy a DA). Okkal merülhet fel ezért a Nozick-i elmélet által képviselt – és hatályos jog más területein jellemzőnek mondható – igazságos, de decentralizált elosztást biztosító, de iure jogszerzés bevezetésének gondolata. Ebben az elgondolásban ugyanis a jogosultság nemcsak, mint magánjogi, erőforrás-allokáló konstrukció, hanem, mint egy jogvédelmi garancia is felfogható.[950]

6.2.1.2. A relációs jogviszonyról

Fontos, hogy az adatjogi jogosultságot számos szerző – már évtizedes távlatban – a tulajdon szemszögéből vizsgálja,[951] ezt azonban nem gondolom feltétlenül szükségesnek. Malgieri is az adaton fennálló jogosultságot a tulajdon („propertizáció") szemszögéből közelítette, de azt helyesebbnek látta, a klasszikus elgondolásoktól eltérően dinamikus módon, mint *„jogok csokra"* felfogni.[952] Ezt a csokrot, mint kvázi-tulajdon azonosította, amit „tulajdonhoz hasonló érdekek koherens kategóriájaként" definiált. Ezzel összefüggésben a saját elgondolásom szempontjából rendkívül fontos fogalmat vezetett be, amit *relációs jogosultsági mechanizmusnak* nevezett.[953] A kvázi-tulajdon és a relációs jog mellett akként érvelt, hogy a magánszféra védelem valójában „környezetfüggő méltóságvédelemként" (másként megfogalmazva, mint kontextuális integritás) írható le. E szerint a magánszféra védelme nagymértékben eltér különböző környezetekben, valamint élethelyzetekben. Például más feltételek szerint kezelik az adatokat az oktatásban, mint a politikában vagy a kereskedelemben. Az adatok kezelésének az alapjával kapcsolatban kiemeli, hogy ezekben a különböző szférákban az *„inspiráció"* lehet a döntés, a diszkréció (más döntése), a bizalmi helyzet vagy akár a szükség, illetve valamilyen kötelezettség.[954] Malgieri ezzel a korábban felállított értékegyenlőségi elv – mint az adatjogi területek működése mögött álló szervező elv – egyes törvényszerűségeihez hasonló elgondolást vázolt fel, ami miatt kifejezetten megfelelőnek gondolom a relációs jogosultságok alkalmazhatóságát a jelen dolgozat által felépített adatjogi paradigmában.

---

[945] Lásd részletesen: Robert Nozick: Anarchy State And Utopia. Basic Books, 1974.
[946] Janecek, 2018. 15-16 o.
[947] A szerzői jogról szóló 1999. évi LXXVI. törvény (Szjt.) 9. § (1) bekezdés
[948] Ptk. 5:30. § (1) bekezdés
[949] Janecek, 2018. 16-17 o.
[950] Malgieri, 2016. 7-8 o.
[951] Yann Padova, „Data Ownership versus Data Sharing: And What about Privacy?", Lex Electronica, 26(1), 2021. 43 o.
[952] Malgieri, 2016. 12 o.; A „jogok csokra" eredeti, angol kifejezéssel „bundle of rights". Az elgondolást Paul Schwartz kutatásaira alapozza, lásd: Paul M. Schwartz, „Property, Privacy, and Personal Data." Harvard Law Review 117 (2004): 2056.
[953] U.o. 14 o. Angolul: relational entitlement mechanism
[954] U.o. 17 o.

Így Malgieri elméletére alapozva, a saját elgondolásom szerint a relációs jogosultság részjogosítványok egy csokra lenne, amelynek az egyes elemei annak megfelelően aktivizálódnak, ahogy az adatkezelés az értékegyenlőségi elv által felállított görbén halad. A relációs jogosultságok tehát több személyközt fennálló kapcsolatban (jogviszonyban) megjelenő alanyi jogokként (mint közvetlenül a jogszabályból, eredő feltétel nélküli jogokként[955]) jelenhetnek meg. Lábady kutatásai alapján a magánjogi kapcsolatok szerkezeti szempontból abszolút, relatív és öröklési jogviszonyokra oszthatók. Az abszolút szerkezetű jogviszony fő sajátosságai, hogy csak a jogosult van benne meghatározva, a kötelezettek (mindenki más) pedig nem aktív magatartásra, hanem passzív tartózkodásra kötelesek. A relatív jogviszonyban – az abszolúttal szemben – nemcsak a jogosult, hanem a kötelezett is megvan jelölve és ezúttal jellemzően aktív magatartást tanúsít. Előbbi fő képviselője a tulajdonjog, utóbbié a kötelmi jog. Fontos, hogy a magánjogi jogviszonyok szerkezeti megosztottságában van átjárás, az abszolút jog megsértése esetén például relatív joggá alakul, míg a relatív jog kinyílása által abszolút sajátosságokat vehet fel (pl. a termékfelelősség).[956] A meglátásom szerint azonban a két végponton álló archetípusok egyike sem illik az adatalapú folyamatok szabályszerűségeire. A védelem jogában a jogosult (pl. érintett) az abszolút szerkezethez hasonlóan egyedüli alany, a hasznosításban pedig (a döntési autonómia miatt) kettő vagy több fél relatív mellérendeltségét láthatjuk. A felhasználás esetén azonban egyik sem igaz. Ott kettő vagy több alá-fölé vagy akár mellérendeltségben lévő alany kell szükségszerűen megjelenjen, azonban a felmerülő érdekek rendkívül nyitottak és változatosak. Fogalmazhatnánk úgy, mintha két abszolút jogosult versengéséről lenne szó az érdekek egyenlőségének kimondásáért folytatott küzdelemben.

Így végső soron a relációs jogviszony a két szerkezeti végpont között bármi lehet, az élethelyzettől függően.[957] Nem lenne ezért talán hibás sem abszolútnak, sem relatívnak nevezni, mégis ha már létezhet e kettő mellett az öröklési jogviszony annak szukcesszív jellege miatt, úgy vélem a tisztánlátás érdekében hasznos lenne a jogviszonytípusok közé a relációs jogviszonyt is felvenni (legalább olyan mértékben, mint az abszolút és a relatív szerkezetek egyvelege). A relációs jogosultságok bizonyos helyzetekben inter alia védelmet biztosíthatnak, míg más esetekben csak inter partes valósulnának meg. Ahogy látható volt, az értékegyenlőség megállapítása sokszor a jogosulton múlik, így a relációs jogviszony egyik kulcskérdése lehet az adat feletti kontroll.[958] Ezt azonban elsődlegesen nem, mint egy konkrét adat feletti tényleges döntést értem, hanem annak a meghatározási képességét, hogy akar-e egyáltalán a jogosult döntést hozni. A másik kulcskérdés a társadalom álláspontja és legitimáló ereje. Ez az, ami meghatározhatja a jogosult számára nyitva álló relációkat, amelyekben döntést hozhat, amennyiben akar. A relációs jog jelentősége, hogy általa értelmezhető és alkalmazható lehet a főleg kontraktualizáción alapuló,[959] tehát teljesen relatív szerkezetű hasznosítási rendszer, ráadásul az abban rejlő, erőhatalommal visszaélő szereplők jogfoglalásainak visszaszorítására is esetlegesen képes lehet. Másfelől azonban az adatvédelem közel abszolút jogvédelmi és így a jog által megragadható és adott esetben az abból eredő merev és talán túlzott korlátozások

[955] Bíró György, Lenkovics Barnabás, Barzó Tímea, Pusztahelyi Réka, Juhász Ágnes: Általános tanok és személyek joga. Novotni Kiadó, Miskolc, 2014. 57-59.o.
[956] Lábady Tamás: A magyar magánjog (polgári jog) általános része. Budapest-Pécs, Dialóg Campus Kiadó, 2012. 282-286 o.
[957] A helyzet valamelyest a kvantummechanikában ismert „kvantum-szuperpozícióhoz" hasonló. A relációs jogosult valójában egyidejűleg kettő (vagy akár több) jogi helyzetben létezik. A tényleges jogviszony pedig az eset körülményeinek vizsgálata által (a relációk függvényében) „omlik" valamelyik tényleges szerkezeti állapotba.
[958] Florent Thouvenin, Aurelia Tamò-Larrieux, „Data Ownership and Data Access Rights Meaningful Tools for Promoting the European Digital Single Market?", In: Mira Burri: Big Data and Global Trade Law. Cambridge University Press; 2021. 325-326 o.
[959] DA által preferált megközelítés szerint

elkerülhetővé válhatnak.[960] Ezzel Padova által felvetett, „propertizációval" kapcsolatos ellentmondás is feloldható talán, ami szerint nem lehetséges egyszerre kiszolgálni az egyének magánszféra védelmét, illetve önrendelkezését és a piaci szereplők gazdasági igényeit.[961] A relációs jogviszony a helyzetek szerint differenciált, érdekkiegyenlítő megközelítése miatt úgy gondolom erre alkalmas lehet.

A relációs jognak ezért a fő kérdéseink, mint „ki adhat hozzáférést az adatokhoz?" és „ki végezhet műveleteket az adaton?" megválaszolása mellett, lehetőség szerint hézagmentesen kell megoldania az adatokon végzett műveletek mindennapos személyközi kérdéseit, mindezt pedig kellő általánossággal, keretszabályozás jelleggel oly módon, hogy a dologi jogi, szellemi tulajdonjogi vagy bármilyen egyéb megközelítésű jogrendszerben egyaránt alkalmazható legyen, a lehető legkevesebb zavar okozása mellet. Az adatok ilyen magánjogi jellegű területének – figyelembe véve a feltárt hiányosságokat – az alábbi szabályozási területeket kellene legalább magába foglalnia:

- a relációs jogosultság tárgya, alanya és létrejötte,
- a jogosultság tartalma (részjogosítványai),
- az adatjogi szerzőképesség,
- az adatjog korlátai,
- az adatjogi szerződésekre vonatkozó szabályok.

Az adatjog relációs jogosultságának és a relációs jogviszonynak a tartalmát magánjogi zsinórmértékek mentén kell összeállítanunk, mivel az a személyeknek mind az individuális, mind a közösségi adatalapú vonatkozásait formalizálni szándékozik. Ehhez Lábady által összegzett vezérmotívumokhoz kell visszanyúlnunk. Ezek szerint törekedni kell a gazdasági viszonyokat támogató ésszerűségre, miközben a jogalanyok számára kedvező igazságosság eszméjét sem veszítjük szem elől. E mellett meg kell felelni a jogbiztonság által elvárt stabilitásnak, kiszámíthatóságnak és előreláthatóságnak, miközben a méltányosság hajlékonysága és nyitottsága is érvényesülni képes.[962] Látható tehát, hogy a relációs jog működőképességéhez egy egyensúlyi helyzet elérésére és fenntartására van szükség, amelyet az értékegyenlőségi elv segíthet megadni.

A magánjogi szervező szerepnek megfelelően a relációs jogosultság szabályozási logikája szerint az horizontális, általános szabályként minden adat esetén felmerülő jogosultra egységesen alkalmazandó lenne. A horizontális jognak a relációs jog végső tartalmát és a háttérben meghúzódó szervező erőt (értékegyenlőségi elv) kell megadnia. Azt, hogy a relációs jogosultságból mely részjogosítványok élednek fel az adott viszonyban, a horizontális szabályok figyelembevételével az ágazati jognak vagy (ezek hiányában) szabványoknak kellene megmondania, annak megfelelően, hogy a terület érdekelt feleinek milyen igényei vannak és ahhoz a társadalom milyen legitimáló erőt társít. A horizontális szabályozási megközelítés látható előnye lehet, hogy ágazati jog hiányában is alkalmazandó, így teret engedhet a jogalanyok önszabályozásának, azokban az esetekben, ahol szektorális jog még nincs, vagy egyáltalán nem lesz megalkotva.

---

[960] A relációs jogosultság a jogirodalomban más tekintetben is felmerül, például, úgy mint a társadalmi egyenlőtlenségeket és hátrányos megkülönböztetést megszüntető, az egyéni jogokat társadalmi kontextusba helyező elgondolás. Bár számos hasonlóságot mutathat a kettő, az általam felvetett intézmény célja nem társadalmi, hanem tisztán adatjogi jogosultságok egyénhez rendelése. A relációs jog szociológiai aspektusairól lásd részletesen: Laura Beth Nielsen, „Relational rights: a vision for law and society scholarship", Cambridge University Press, 2024.

[961] Padova, 2021. 44 o.

[962] Lábady, 2012. 19 o., 130-133 o.

6.2.2. A relációs jogosultság tárgyáról, alanyáról és létrejöttéről

A relációs jogviszony Janus-arcú jogi helyzetében az adatokon való jogosultság létrejöttével természetszerűleg megjelenik tehát az adatok jogosultja, akit kiindulópontként magas fokú jogi hatalom illet meg a jogosultsága tárgyán, az adaton. A relációs jellegnek megfelelően ez közel teljes és kizárólagos uralmi jogban is megtestesülhet, de számos esetben kerülhet oly módon meghatározásra, hogy az inkább relatívnak tekinthető. Példaként vegyük a személyes adatokat, amelyeket számos garanciális szabály véd erga omnes hatállyal, ami ha nem is abszolút, de erős védelmet keletkeztet az érintett javára. Ezt azonban – a felhasználás tűréskényszerénél taglalt okokból, módon – potenciálisan bármely adatkezelő jogszerűen áttörheti és akár az érintett érdekei ellenére is adatot kezelhet. Ebben az esetben sor kerül a jogosultság relativizációjára, a konkrét adat esetében a védelem átalakul az adatkezelővel szembeni, inter partes védelemmé.

6.2.2.1. A kapcsolótényezőkről

Az egyik kiemelt kérdésünk volt a „kié az adat, ki adhat hozzáférést az adathoz?”, amelyre most már láthatóan a választ az adatok jogosultjának megtalálása fogja elhozni. Az adat leképeződésének folyamatából korábban kiolvasható volt, hogy az erőforrás igényes tevékenység. Ez azonban azt is jelenti, hogy adatok nem keletkezhetnek légüres térben, ahhoz minden esetben a megfigyelő aktív magatartására van szükség, ami által az adat észlelhető, majd rögzíthető lesz. A két mozzanat erőforrás igényéből és rögzülési kényszeréből adódóan két következtetést tehetünk:

- az adatnak a befejezett létrejövetelhez rögzülnie kell, tehát az adatjogi jogosultságnak eredeti formájában az adat létrejöttével egyidőben meg kell alapulnia a hézagmentességhez,[963]
- valakinek létre kellett hoznia az adatot, így a jogosultnak a leképeződés pillanatában megállapíthatónak kell lennie.[964]

A két következtetés alapján – összhangban a szakirodalom egyes álláspontjaival[965] – uratlan adatok nem jöhetnek létre. Az azonban már más kérdés, hogy később uratlanná válhatnak-e vagy, hogy milyen megítélés alá eshet egy adat, amelynek nem azonosítható a jogosultja. Az első esetben technikai szempontból vizsgálandó, hogy egyáltalán az uratlanná válás megtörténhet-e, tekintve, hogy például digitális adatok esetén a metaadatok alapján történő visszakövethetőség sokszor ezt lehetetlenné teszi. Hasonló lehet a helyzet egy biometrikus adat analóg módon (pl. ujjlenyomat levétele tintával és papírral) történő rögzítésével. Így a derelinkválás azt gondolom nem jogkérdés, hanem technikai, amennyiben technikailag lehetséges, úgy jogilag is annak kell lennie.

Tehát minden egységnyi új adat esetében képesnek kell lennünk a leképeződéskor megállapítani az adat jogosultját, amelyhez – Szilágyi kutatása nyomán[966] – un. kapcsolótényezők alkalmazása mutatkozik célravezetőnek. Ezeket a szemantikai (jelen dolgozatban jog-fogalmi) adatszinten ismertetett két adatjogi adatkategóriára (személyes és nem személyes adat) tekintettel tartom célszerűnek meghatározni:

---

[963] Hasonlóan a szerzői joghoz. Az Szjt. 9. § (1) bekezdés alapján a szerzőt (jogosultat) a mű (adat) létrejöttétől kezdve megilleti a szerzői (adatjogi) jogok (…) összessége.

[964] A szerzői jogi alakszerűtlenség elvéhez hasonlóan az adatok esetén sem lenne életszerű megkövetelni az adat és a jogosultság létrejöttének regisztrációját vagy valamilyen központi nyilvántartásba vételét. Az alakszerűtlenség elvével kapcsolatban lásd részletesen: Grad-Gyenge, 2019. 65 o.

[965] Szilágyi I., 2022. 14 o.

[966] Szilágyi Ferenc, „Kié a digitális adat? Az allokatív adatjog létjogosultsága a magánjogi (dologi jogi) megközelítés margóján. II. rész”, Polgári Jog 2022/11-12. 3 o.

1. az első kapcsolótényező esetében azt a kérdést kell feltenni, hogy *kire/mire vonatkozik*[967] *az adat*. Amennyiben a válasz a kérdésre, hogy egy természetes személyre, akkor az adat jogosultja a természetes személy lesz. Ebből látható, hogy – egyetértésben Zech álláspontjával[968] – amennyiben az adat személyes adatnak minősül, a kapcsolótényező alapján mindig az adat forrása, vagyis az érintett lesz a jogosult.

2. a második kapcsolótényező kérdése (amennyiben az elsőre a válasz a természetes személyen kívül bármi egyéb volt), hogy *ki hozta létre az adatot*. Ebben az esetben a jogosult az lesz, aki létrehozta vagy az érdekére tekintettel, az utasításainak megfelelően létrehozatta azt. Tehát – ugyancsak egyetértésben Zech elgondolásával[969] – nem személyes adatok esetén nem az adat forrása, hanem az adat előállítója (az aktív megfigyelő) lesz a jogosult.

A jogosulti minőség ilyen formában történő létrehozására az alábbi érvek szolgálnak:

- *Általánosságban elmondható, hogy az adat teljes leképeződése (szemantikai és szintaktikai szintek egyidőben) az eredeti létrejövetel során valósul meg.*

A jogosultság megszerzésének specialitását adja a korábban kifejtett szemantikai és szintaktikai adatszintekhez kapcsolt – leképeződés során végbemenő – észlelési és rögzülési mozzanat.[970] A létrejövetel során a szemantikai szint értelme nyilvánul meg először az észleléssel, amelyet szükségszerűen a rögzülés követ. A nonrivalitással kapcsolatban arra is utaltam, hogy a másolás során a szintaktikai szint ismétlődik, azonban a szemantikai szint változatlan marad. Bár végeredményben a konklúzió az volt, hogy mind az eredeti, mind a másodpéldány adatként jelenik meg, a jogosultság megszerzése tekintetében ennek a kérdésnek új aspektusa látható. Mivel az adatban rejlő értelem észlelése csak egyszer, a tényszerűség eredeti vizsgálata során mehet végbe, így indokoltnak tűnik a jog létrejöttét mindkét mozzanat egyidejű megvalósulásához, tehát az eredeti létrejövetelhez kötni.

- *Személyes adatok esetén az érintett alapvető és elidegeníthetetlen emberi jogának érvényesülése a jogosulti pozíción keresztül tud megvalósulni.*

A Nozick-i teóriának megfelelően mind a dologi, mind a szerzői jogi logika alapján csak a 2. számú kapcsolótényezőre lenne szükség. A tulajdon eredeti szerzésmódjai között szerepel a gazdátlan javakon való tulajdonszerzés, amely esetkör lefedi az új dolog létrehozatalát is. A jogosultság a tulajdonszerzési szándékú birtokbavétellel történik meg, amelyet értelmezhetünk úgy, hogy a létrehozó – ha akarja ezt – tulajdont szerez azon, amit létrehozott.[971] Ehhez hasonlóan a szerzői jog alaptétele, hogy a szerzői jog azt illeti, aki a művet megalkotta.[972] Elkerülhetetlen azonban kivételt tennünk a személyes adatok esetén. A már vizsgált információs önrendelkezési és adatvédelmi jog olyan erős közjogi védelmi mechanizmusokat hozott létre az érintett jogainak védelmére és érvényesítésére, amelyeket az adatjogi kapcsolótényezőknek is tükröznie kell. Gondoljunk bele, a törléshez való jog vagy a tiltakozáshoz való jog gyakorlása a jogosult abszolút jellegű védelmének dologi vagy a szerző személyhez fűződő védelmének jogi eszközeihez hasonlatos azokban az esetekben, amikor az adatok jogellenes kezelése valósul meg az érintettől eltérő személy által. Továbbá ugyanezek a jogok kötelmi viszonyok között a szerződésszerű teljesítés egyoldalú kikényszeríthetőségét is szolgálják. Ezt az is alátámasztja,

[967] A vonatkozik itt azt jelenti, hogy kit/mit reprezentál, mint szimbólum az adat
[968] Zech, 2015. 195-196 o.
[969] Uo. 196 o.
[970] Ökölszabályként fogalmazhatunk így: rögzülés nélkül nem jön létre adat, észlelés nélkül nem jön létre új adat.
[971] Gárdos Péter, Vékás Lajos (szerk.): Nagykommentár a Polgári Törvénykönyvről szóló 2013. évi V. törvényhez (továbbiakban: Ptk. Nagykommentár) 1060 o.
[972] Szjt. 4. § (1) bekezdés

hogy személyes adatok esetén mindig olyan megkülönböztetett helyzet áll elő, amiben az adat forrása (a tényszerűség) és a jogosult egybeesik. Ez pedig az ember már említett virtualizációja miatt különösen fontos kérdés, hiszen, ami a fizikai valóságban az emberi személyiség, az a digitális térben az adatokból összeálló virtuális személyeséget jelentheti.[973] Összességében tehát látható, hogy a jelenlegi alapjogi védelmi szint mellett értelmetlennek tűnik a személyes adatok feletti jogosultságot az érintetten kívül máshoz rendelni.

- *Nem személyes adatok esetén a létrehozó elsődleges jogosulti pozícióját az aktív magatartás és az erőforrások befektetése indokolja.*

Másként megfogalmazva az adatot létrehozó tette meg a szükséges lépéseket az eredmény elérésére, így célszerűnek és egyúttal méltányosnak hat, hogy az adat feletti hatalmat is ő gyakorolhassa. Ez egyébként a fentebb leírt Nozick-i teóriával és így a dologi és szerzői jogi megközelítéssel azonos, így az ott leírt indokok erre is vonatkoznak.

6.2.2.2. Az árva adatokról

A kapcsolótényezők láthatóan csak a létrejövetel pillanatában jelölik ki a jogosultat, kérdéses hogy milyen szabályok vonatkoznak azt követő időszakra. Az azonosítható jogosult nélküli – szerzői jogi szóhasználattal[974] – árva adatok kezelésének jelentőségét a hézagmentesség fenntartásának igénye adja, hiszen az adat keletkezésekor a jogosult létezett, csak annak kiléte a vizsgálat pillanatban nem állapítható meg. Kiindulópontként azt mondhatjuk, hogy személyes adatok esetén az „elárvulás" az azonosíthatóság mértékével függ össze, tehát az objektíve azonosíthatatlan adatalanyra vonatkozó adat biztosan nem tekinthető személyes adatnak. A joggyakorlat állása alapján – a relatív azonosíthatatlanság elfogadásával – a „találó" vonatkozásában fennálló azonosíthatatlanság sem fog személyes adatot eredményezni. Felmerülhet a későbbi visszaazonosítás kérdése (ami megvalósulhat pl. egy új adat állományhoz kapcsolásával, vagy új típusú technológia megjelenésével). Álláspontom szerint ebben az esetben is csak akkortól számít személyesnek az adat, amikortól az alapján egy természetes személy azonosíthatóvá válik, így a nem személyes adatként töltött időt nem tekinteném „árvaságnak".

Nem személyes adatok esetén más a helyzet, itt ugyanis nem fogalmi elem az adatforrás és egyben a jogosult azonosíthatósága. A kérdés, hogy ki hozta létre az adatot – ami hasonlóan a szerzőhöz – könnyebben merülhet feledésbe. Az ilyen esetben is azonban, mivel az adat valójában létrejött, a hézagmentességhez legalább egy jogosult kijelölésére mindenképpen szükség van. Ennek az azonosításához kisegítő elvként alkalmazhatónak mutatkozik a személyes adatok esetében bevált módszer, vagyis az adat forrásának jogszerzése. Amennyiben az adatok több forrásból származnak, azokon akár egy időben több jogosultság létesülhet. Ha az előbbi lépés nem megvalósítható (pl. lehetetlen vagy érdeksérelmet okozna) vagy az adat forrása nem szerezhet jogosultságot, mert pl. egy természeti jelenségről (mint egy égitest) van szó, akkor ultima ratioként az adat dologi jogi megfogalmazással a „res omnium communes"[975] kategóriába kerülhet, azaz közkincsé válhat. Ennek a feltétele, hogy nem állhat olyan speciális vagy korlátozó szabály hatálya alatt, ami ettől eltérő eljárást ír elő (pl. szerzői jog árva művei). A közkincsé vált adatokra a nem személyes közadatokra irányadó, de megismerési korlátozásoktól mentes szabályok lehetnek alkalmazhatóak. Ezek kezelésére jelenleg Magyarországon – törvény általi kijelölése esetén – a már említett NAVÜ lehetne a megfelelő szerv. Az ilyen adatok kezelője a NAVÜ-n keresztül az állam, mint szükségképpeni

[973] Szabó, 2012. 31 o.
[974] Grad-Gyenge, 2019. 148 o.
[975] Helyesnek tűnik ebben az esetben „datum omnuim communes" elnevezés használata, hiszen a jelen értelmezés szerint az adat nem dolog.

adatkezelő[976] lépne fel, az adat közérdekű célokra történő használata és a harmadik felek részére történő hozzáférhető tétele érdekében. A NAVÜ ilyen jellegű működése az egyéb közadatokra vonatkozó jogköreiben merülhetne ki, így pl. leltárba veheti, közzé teheti vagy rendelkezésre bocsáthatja azokat.[977] Az eljárása az SZTNH[978] árvaműveknél fennálló eljárásával látható hasonlóságokat mutat, így az SZTNH gyakorlata is támpontul szolgálhat az ilyen jellegű működésére.[979]

Az árva, nem személyes adatokkal kapcsolatban is felmerülhet a jogosult későbbi megkerülése. Amennyiben az árvaság harmadik fél jogellenes magatartására vezethető vissza, akkor a jogosult és a harmadik fél közötti kárkötelemként folytatódhatna az eljárás, azzal, hogy a közkincs minőség a NAVÜ által megszüntethető a jogosult előkerülésével. Abban az esetben, ha az elárvulás a jogosult közrehatása által valósult meg, valamilyen információbiztonsági, illetve kibervédelmi hiányosság miatt, akkor úgy vélem bármilyen megtérítési igénye legfeljebb az olyan harmadik felekkel szemben merülhet fel, akik nem a NAVÜ-n keresztül, hanem önhatalmúan szereztek hozzáférést az árva adatokhoz. Fontos, hogy a jelenlegi szabályok szerint nincs ex lege díjfizetési kötelezettsége senkinek, semmilyen adat használatáért cserében, a monetizáció épp ellenkezőleg a jogosult általi díjszámítás lehetőségében áll, ami egy árva adat esetén nem történhet meg.

6.2.2.3. A relációs jogosultakról

Fontos, hogy az eredeti jogosulti pozíció mindig egy egységnyi új adaton alapulhat. Ahogy fentebb láttuk az adat eredetisége és újdonsága a szemantikai szint észlelésétől és nem a szintaktikai szint technikailag ismétlődő rögzülésétől függ, így álláspontom szerint – ahogy a művek többszörözése sem tekinthető új mű létrehozatalának[980] – nem minősül új adatnak a másolt vagy továbbított adat a másolás céljaként funkcionáló adathordozón, illetve az adattovábbítás címzettjénél. Vagyis ezekben az esetekben új jogosulti pozícióról sem beszélhetünk, függetlenül attól, hogy ki hajtotta végre a másolási műveletet vagy ki az adattovábbítás címzettje. Új adat jön viszont létre – amin ennek megfelelően új és eredeti jellegű jogosultság szerezhető – ha például a címzett a megszerzett adaton olyan műveletet végez, aminek eredményeként az eredetitől eltérő, új szemantikai minőség is előáll. Ezt értelmezhetjük hasonlóan a szerzői jogi művek átdolgozásának ahhoz a formájához, amelynek eredményeképpen az eredeti műből származó más mű jön létre.[981] Ez a mű módosításának, megváltoztatásának olyan szélső esete, amikor a változtató, kiegészítő vonások önmagukban is olyannyira lényegiek, hogy megfelelnek az egyéni és eredeti mű követelményének (alkotó jellegűek).[982] Fontos azonban, hogy az átdolgozás sem alkalmazható parttalan „jogfoglalásra", mivel a szerzői jog szerint ehhez is a szerző engedélyére van szükség.[983]

---

[976] Hasonlóan a Ptk. 7:74. § szerinti állam általi örökléshez az állam csak a jogosult kétséget kizáró azonosíthatatlansága esetén válhatna az adatok kezelőjévé, az adatkezelést pedig nem utasíthatná vissza.
[977] Nah.tv. 16. §
[978] Szellemi Tulajdon Nemzeti Hivatala
[979] SZTNH, „Árva művek" tájékoztató anyaga, 2023. Elérhető: https://www.sztnh.gov.hu/sites/default/files/10_arva_muvek_2023.pdf#:~:text=%C3%81rva%20m%C5%B1vek nek%20nevezz%C3%BCk%20az%20ismeretlen%20vagy%20ismeretlen%20helyen,%28Szjt.%29%2041%2FB. %20%C2%A7-41%2FE.%20%C2%A7-ai%2C%20a%20138%2F2014.%20%28IV.%2030.%29
[980] Szjt. 18. §; Ahogy a szerzői jogban, itt sincs jelentősége annak, hogy a másolás milyen módon valósul meg, ide tartozik az analóg adat digitalizálása és a .pdf dokumentum email csatolmányként való küldése is. Lásd részletesen: Gyertyánfy Péter, Legeza Dénes (szerk.): Nagykommentár a szerzői jogról szóló 1999. évi LXXVI. törvényhez 167 o. (továbbiakban: Szjt. Nagykommentár)
[981] Szjt. 29. §
[982] Szjt. Nagykommentár 250 o.
[983] Grad-Gyenge, 2019. 102 o.

Érezhetően összesen egy uralkodó joggal rendelkező pozíció kontraproduktívnak és irreálisnak tűnik az adatokkal kapcsolatban, egyfelől az adathasználat természete, másfelől az adatok nonriválisés másolható jellegére tekintettel. Az eddig említett jogosultat így tekintsük elsődleges jogosultnak (eredeti módon szerzőnek, amely személyes adatok esetén az érintett, nem személyes adatok esetén az adat létrehozója), amely így egy személyben egyesít minden – relációs helyzet szerint aktivált – adattal kapcsolatos jogosítványt. Az elsődleges jogosult a relációs szerkezetű jogviszony első alanya, így párhuzamba állíthatjuk a dologi jogi tulajdonossal és a szerzői jogi szerzővel. Az elsődleges mellett azonban szükségesnek látszik egy vagy több másodlagos (származékos módon szerző, ilyen személyes adat esetén pl. az adat létrehozója, illetve bármilyen adat esetén pl. felhatalmazással rendelkező adathasználó) jogosult is, akik az adaton fennálló jogosítványok egy részével rendelkeznek. Az adatjog másodlagos jogosultjához hasonló pozíciók a tulajdonostól eltérő birtokos vagy a használati joggal rendelkező a dologi jogban, valamint a felhasználó a szerzői jogban.

Az elképzelésem szerint az elsődleges jogosult jogát tehát eredeti módon szerzi, míg a másodlagos az elsődlegesre vezeti azt vissza. Megjegyzendő ismét, hogy az eredeti szerzés újszerűsége szubjektív, nem objektív kvalitás. Ugyanannak a fának több személy általi lefényképezése például több eredeti adatszerzést kell eredményezzen, függetlenül attól, hogy az első fénykép után az objektív újszerűség nagymértékben megszűnik. Ez igaz az adattovábbítás címzettje vonatkozásában is, számára hiába számít „újdonságnak” az adat, mivel hiányzik a leképeződés első mozzanata az észlelés, így eredeti módon jogot nem tud szerezni, tehát elsődleges jogosultságot sem kaphat. Ez alapján fontos a jogosultságokkal kapcsolatban felismerni egy implicit, de mégis megkerülhetetlen védelmi mechanizmust. E védelem alapján a személyes adatoknak a forrástól vagy más szereplőktől függetlenül történő, eredeti létrehozása láthatóan nem fog új elsődleges jogosulti pozíciót létrehozni, hiszen a kapcsolótényező alapján az mindig az érintett lesz. Ennek az ellenkezőjét is fontos azonban kiemelni, mert nem személyes adatok esetén nem beszélhetünk ilyen védelemről. Ezek esetében ahány eredeti megfigyelő, annyi jogosultság jön létre. Ez azt jelenti, hogy egy tényszerűségről bárhány egymástól független szereplő képezhet le nem személyes adatokat, ami által önálló, teljes körű jogot szerezhet. Ezt a jelenséget az üzleti titok titokgazdától független megszerzéséhez hasonlíthatjuk.[984]

A két jogosulton alapuló elképzelés szerint tehát a másodlagos jogosulti pozíció mindig limitáltan jön létre, minden jogszerű tevékenysége az elsődleges jogosult jogára kell visszavezethető legyen. A jogosultak egy un. antecedens[985] viszonyrendszerben képzelhetők el, amelyben egymáshoz képesti elhelyezkedésük mindig állandó, az elsődleges mindig megelőzi a másodlagosat, a másodlagos jogosultság pedig mindig visszautal az elsődlegesre.

A relációs jognak egy különös jellegzetessége ennek a jogosulti kettősségnek a megjelenése. Ez a relatív, mellérendeltségen alapuló esetekben könnyen értelmezhető, ott egyébként is két félre van szükség. Azonban sokszor a két jogosult abszolút-jellegű védelme egyidőben vagy felváltva jelenik meg ugyanabban az adatkezelési folyamatban. Gondoljunk csak arra, hogy a felhasználás tűréskényszere során a másodlagos jogosult (pl. egy jogszabály által előírt adatkezelés esetén) erősebb jogosítványokkal rendelkezhet, mint az elsődleges, hiába a kiindulópontban valóban létező elsődleges jogosulti uralmi állapot, azt az adott helyzet (a

[984] 2018. évi LIV. törvény 5. § (1) bekezdés szerint nem minősül az üzleti titokhoz fűződő jog megsértésének az üzleti titok megszerzése, amennyiben az pl. a jogosulttól független fejlesztés, felfedezés vagy alkotás útján valósul meg.

[985] A nyelvészetben antecedensnek nevezik azt a nyelvi entitást, amelyre egy utána álló másik entitás utal. Lásd részletesen: Tolcsvai Nagy Gábor: Szöveg és típus - Szövegtipológiai tanulmányok. Budapest, Tintakönyvkiadó, 2006. 54 o.

reláció) felülírja. A relációs és az abszolút szerkezetű jogok különbségét jól mutatja, ha a felhasználás tűréskényszerének terjedelmét[986] összevetjük a dologi jogi kisajátítással és a szerzői jog szabad felhasználásával (mint rokon területekkel). A kisajátítás egy drasztikus beavatkozást jelent a tulajdoni viszonyokba, mivel egy kényszerű alanyváltozást idéz elő azáltal, hogy a tulajdon (ingatlan) tárgyát elvonja a tulajdonostól.[987] Fontos azonban, hogy tulajdonjog csak kivételesen vonható el, törvényben meghatározott közérdekű célból, feltételekkel és módon, teljes, azonnali és feltétlen kártalanítás mellett.[988] A kisajátítást tehát korlátozott esetekben és e mellett korlátozott személyi kör által lehet megtenni,[989] ami az adatalapú folyamatokra egyáltalán nem jellemző.[990] A szerzői jogi szabad felhasználás körében a felhasználás díjtalan, és ahhoz a szerző engedélye nem szükséges. A felhasználás azonban csak annyiban megengedett, illetve díjtalan, amennyiben nem sérelmes a mű rendes felhasználására és indokolatlanul nem károsítja a szerző jogos érdekeit, továbbá amennyiben megfelel a tisztesség követelményeinek és nem irányul a szabad felhasználás rendeltetésével össze nem férő célra.[991] Fontos továbbá, hogy arra csak négy általános cél megvalósítása érdekében van mód, ezek az oktatás, a művelődés, a tudományos kutatás és az információ szabad áramlásának biztosítása.[992] Látható, hogy a szerzői jog szabad felhasználás esetén garanciális szabályokkal védi a szerző érdekeit, továbbá a lehetséges célokat jelentősen beszűkíti. Ehhez képest az adatok érintettje legfeljebb célhoz kötöttségre tarthat igényt, az adatjogi garanciális szabályok pedig egyáltalán nem tilthatják meg az adatalany érdekeit sértő adatkezeléseket (pl. jogi igény érvényesítéséhez szükséges adatkezelés).

6.2.2.4. A többes adatjogi jogosultságról

A jogosulti pozíciók tisztázását követően, rögtön felmerülhet az adatok feletti többes jogosultság megszerzésének kérdése. Az adatokról való közös rendelkezés gyakorlása, azok közösen történő hatalomban tartása mind a polgári jogi, mind a kialakuló adatjogi logika alapján lehetségesnek tűnik. Gondolhatunk a közös tulajdonra vagy társszerzőségre (mint elsődleges megosztott jogosultságra) a polgári jogon belül vagy a közös adatkezelői viszonyra (mint többes másodlagos jogosultságra) és az osztott adat jelenségére (ami mindkét jogosultság esetén felmerülhet) az adatvédelmi jogban.

Közös tulajdon esetén a fennálló tulajdonjog meghatározott hányadok szerint több személyt illet meg, ilyenkor a tulajdonostársak mindegyike jogosult a dolog birtoklására és használatára, a hasznai és költségei a tulajdonostársakat tulajdoni hányaduk arányában illetik meg, illetve terhelik.[993] Több szerző közös műve esetén, ha annak részei nem használhatók fel önállóan, a szerzői jog együttesen és – kétség esetén – egyenlő arányban illeti meg a szerzőtársakat, ha azonban a közös mű részei önállóan is felhasználhatók (összekapcsolt művek), a saját rész tekintetében a szerzői jogok önállóan gyakorolhatók.[994] A közös adatkezelői minőség akkor jön létre, ha a személyes adatok kezelésének céljait és eszközeit két vagy több adatkezelő közösen határozza meg. A közös adatkezelők átlátható módon, a közöttük létrejött megállapodásban kell meghatározzák a személyes adatok kezelésével kapcsolatos kötelezettségeik teljesítéséért fennálló, különösen az érintetti tájékoztatással kapcsolatos feladataikkal összefüggő

[986] Lásd 3.4. fejezet
[987] Lenkovics, 2014. 105 o.
[988] A kisajátításról szóló 2007. évi CXXIII. törvény 1. §
[989] U.o. 1. § (2) bekezdés, 2. §
[990] Gondoljunk csak arra, hogy a törvényi szinten szabályozott közérdek mellett alacsonyabb rendű közfeladatok ellátásához szükséges és tisztán magánérdekeket kielégítő adatkezelések sokasága történik.
[991] Szjt. 33. § (1)-(2) bekezdés
[992] Grad-Gyenge, 2019. 154 o.
[993] Ptk. 5:73. §, 5:75. §
[994] Szjt. 5. §

felelősségük megoszlását.[995] Osztott adat esetén egy adathordozón több személy adata is megtalálható, vagy egy adat egyszerre több személyt is azonosít(hat) (pl. az „anyja születési családi és utóneve" fordulat, ami egyszerre azonosítja a gyermeket és az anyát is),[996] amely így indokolt esetben az egyik érintett vonatkozásában fennálló jogosultságot a másik érintett vonatkozásában is fennállónak tekinti (a gyermek szükségszerűen jogosult anyja családi és utónevének kezelésére). Ez alapján arra következtethetünk, hogy ha egy komplex adatállomány létrejöttekor arra bármelyik kapcsolótényező egynél több személyt vagy szervezetet jelöl ki (mert egy adat több személyre vonatkozik, vagy a nem személyes adatot tartalmazó adatállományt egyszerre többen hozták létre) akkor a megfelelő indokoltság esetén elképzelhető lehet a közös, eredeti adatjogi jogosultság megjelenése (pl. egy dolgozat esetén, ahol a vizsgázó és a vizsgáztató személyes adatai szükségszerűen egyszerre kell szerepeljenek[997]). Az adat megalapozott osztott minőségének hiányában – szintén a fennálló gyakorlatnak megfelelően – a potenciális többes jogosultság megszüntethető a kérdéses adat anonimizálásával vagy az adatállományból való törlésével. Az adatok természetéből adódóan a komplex adattartalmak megoszthatósága technikailag viszonylag könnyen megoldható, azonban ennek célszerűségi akadályai merülhetnek fel. Egy több személyt ábrázoló fotó például szoftveresen és mechanikailag is megvágható, azonban annak következtében az adatállomány kohéziója szükségképpen megbomlik, amelynek egy kép esetén könnyen belátható. Ezzel szemben egy adatbázis esetén már nehezebben megbecsülhető következményei lehetnek a kohézió megbomlásának, ezért a többes joggyakorlás kérdését érdemes szilárd alapokra építeni.

A példák alapján is látható, hogy többes jog létrejöhet elsődleges és másodlagos jogosultsággal kapcsolatban is. Az elsődleges jogosultak (érintettek és a nem személyes adatot létrehozók) esetén a komplex állománnyal kapcsolatos többes adatjogi jogosultság kifelé egységes kellene legyen, a vonatkozó jogokat pedig együttesen kellene gyakorolhatóvá tenni. A többes jogosultak belső viszonyaira elsődlegesen a felek egymásközti megállapodása lehet irányadó,[998] aminek, ha az állomány egyértelműen szétválasztható és a felekhez rendelhető, akkor erre az arányra tekintettel kellene lennie. Amennyiben erre nincs lehetőség az arányt célszerű lehet egyenlőnek tekinteni. Másodlagos jogosultak ugyanazon adaton, egymástól függetlenül is szerezhetnek jogot, az egymásközti viszonyuk lehet lazább vagy akár egyáltalán nem létező, így a többes jog gyakorlásának alapja az elsődleges és másodlagos jogosultak egybehangzó akarata vagy kógens jog lehet (szabályozott többes másodlagos jogra jó példák a közös adatkezelői státuszra vonatkozó előírások).

A többes jogosultsággal kapcsolatban fontos visszautalni az FFNPDR 2. cikke vonatkozásában tárgyalt alkalmazási szabályokra. E szerint amíg a személyes és a nem személyes adat szétválasztható az adatbázison belül, addig a két adatkategóriára vonatkozó joganyag párhuzamosan, egymás mellett alkalmazandó, és csak, ha a két adat elválaszthatatlanul összekapcsolódott, akkor kell egyszerre, egyidőben azokat alkalmazni. Bár nincs olyan jogszabályi kötelezettség, hogy az adatok szétválasztásra kell kerüljenek (un. un-bundling), a magam részéről azoknak az elválaszthatatlan összekapcsolódási lehetőségét kerülendőnek gondolom. Az adat alapján vagy azonosítható egy természetes személy vagy nem. Amennyiben nem az, akkor az nem személyes adat, amennyiben az, akkor személyes adat. Bizonytalanság esetén nem gondolom, hogy megoldást jelent az összekapcsoltság kérdését vizsgálni, célszerűbb lenne az azonosíthatóság mértékével foglalkozni. A kérdés, hogy mekkora bizonyosságra, illetve körültekintésre van szükség az adatkezelő részéről annak a kijelentéséhez, hogy az adat alapján nem azonosítható egy természetes személy. Ezzel

[995] GDPR 26. cikk
[996] Péterfalvi et al., 2018. 57 o.
[997] C-434/16 sz. ügy (Nowak-ítélet)
[998] ALI-ELI Alapelvek 84-85 o.

kapcsolatban az abszolút megközelítés szerint akkor nem azonosítható az érintett, ha objektíve lehetetlen bárki által az azonosítás. A relatív megközelítés szerint elégséges már az, ha csak az adatkezelő számára nem lehetséges.[999] Tehát elképzelhető egy olyan értelmezés, amelyben, ha az adatkezelő számára az adat alapján nem azonosítható senki, akkor az adat az ő tekintetében nem személyes adat, függetlenül attól, hogy mivel van tartalmilag összekapcsolódva.

- *Többes jogosultság IoT eszközök esetén*

Összetett szolgáltatások esetén, mint amilyenek például az IoT eszközök, az adatjogi jogosultságok rendelésének, illetve a többes jogosultságszerzésnek a kérdése különösen kiélezetté válhat. Még személyes adatok esetén a kapcsolótényező viszonylag hézagmentesen alkalmazható, hiszen személyes adatok per definitionem csak olyan adatok lehetnek, amelyek alapján azonosítható egy természetes személy, így az elsődleges jogosult (vagy jogosulti kör) szükségszerűen kijelölhető kell legyen. Amennyiben több (azonosítható) jogosult merül fel akkor a többes adatjogi jogosultságnál leírtaknak megfelelően külső viszonyokban egységes és együttes joggyakorlás, belső viszonyokban pedig az állomány szétválaszthatósági arányának figyelembevételével a felek önrendelkezésének és magánautonómiájának alkalmazása megvalósíthatónak mutatkozik. Nem tűnik aggályosnak az elsődleges jogosult mellett egy másodlagos jogosulti pozíció automatikus keletkeztetése a szolgáltató oldalán, amelynek az elsődleges jogosulttól származtatott jogosítványait a szolgáltatással kapcsolatos jogi vagy szerződéses előírások rendezhetik. Több mellérendelt szolgáltató esetén a többes másodlagos jogosultságszerzés úgyszintén megvalósítható, amelyek egymásközti viszonyait kötelmi keretek tisztázhatják.

Nem személyes adatok esetén a kapcsolótényező alapján az elsődleges jogosult az adatot létrehozó vagy a nevében, érdekeire tekintettel *létrehozató*. Fontosnak tartom kiemelni, hogy – a kapcsolótényező alapján – személyes adatok elsődleges jogosultja minden esetben csak természetes személy lehet, azonban nem személyes adatok esetén ezt a szerepet mind jogi, mind természetes személyek is betölthetik. Az olyan összetett rendszerek, mint az IoT szolgáltatások esetén az eszköz rendeltetése és az általa gyűjtött adatok típusa lehet jelentős hatással a jogosulti pozíciókra. A kapcsolótényezőnél ugyanis az aktív (célzatos) magatartást és az erőforrások befektetését adtuk meg az elsődleges jogosulti pozíció kijelölésének alapjaként. Egy ilyen rendszer esetén tehát a szolgáltatást igénybe vevő és a szolgáltató kiindulópontként azonosított céljait és az azokhoz szükséges adatokat kell tisztázni, mivel az elsődleges jogosult az lesz, aki az adat vonatkozásában ezt az aktív magatartást és a befektetést eszközölte a saját érdekeire tekintettel. Képzeljük el például, hogy egy kifutópályákat automatikusan takarító hókotró berendezés[1000] által folyamatosan generált adatok közül melyek azok, amelyek a szolgáltatást igénybe vevő (berendezés tulajdonosa, üzembentartója) és a szolgáltatást nyújtó (a hókotró gyártója, IoT rendszereinek működtetője) tevékenységére és érdekköreire tekintettel megkülönböztethetők. Az adatjog relációs szerkezete miatt az elsődleges jogosultat kell először meghatározni, így megállapítható lesz, hogy hozzá képest ki a másodlagos, így származtatott jogokkal bíró szereplő. A szolgáltatást igénybe vevő azért fizette ki a hókotró vételárát és a működési költségeit, hogy azt a repülőtér kifutópályájának takarításához használni tudja. Így az olyan adatok tekintetében, amik ehhez szorosan kapcsolódnak, mint a geolokációs adatok, útvonal információk vagy a jármű környezetére vonatkozó pl. képi adatok elsődleges jogosultságát neki kellene megszereznie. Ezzel szemben az olyan adatok, amelyek kifejezetten a berendezés megfelelő működésével vannak összefüggésben, mint az algoritmus döntési mintázatai, a motor státusza, az akkufeszültség vagy a fékbetétek állapota a szolgáltatót, mint

[999] Czapári, Szőke, 2022. 28 o.

[1000] A példánkban szereplő hókotró teljes mértékben önvezető, utas fogadására nem is képes így személyes adatok nem jöhetnek létre.

elsődleges jogosultat kellene illessék. Tehát a tény, hogy az adatot minden esetben a szolgáltató által gyártott berendezés hozta létre nem azt jelenti, hogy minden adat a szolgáltatóé kellene legyen. Egyúttal az, hogy minden adat létrejötte az igénybe vevő használatára vezethető vissza sem jelentheti, hogy minden adat feletti jog őt illeti. Például nem mondhatjuk, hogy a működéssel kapcsolatos adatok azért jönnek létre, mert a repülőtér be akar szállni az hókotrógyártó üzletágba. Az egy másik kérdés, hogy az adatokra, mint másodlagos jogosult a repülőtér igényt tarthat a javítások, karbantartások megfelelő elvégzéséhez. Tehát az elsődleges jogosult kijelölése nem jelenti, hogy más felek potenciálisan ne férhetnének hozzá valamely adathoz, mint másodlagos jogosult, a kérdés e tekintetben, hogy kihez kerülnek az erősebb jogosítványok és nem mellékesen az adatrögzítésből eredő jogi megfelelésre vonatkozó kötelezettségek.[1001]

Szintén kiemelendő, hogy mivel az IoT eszközök egyre szélesebb skálájával és a nyújtott szolgáltatások egyre bővülő lehetőségeivel kell számolnunk a hézagmentesség érdekében az olyan (hangsúlyozottan nem személyes) adatok esetén, amelyeket a kapcsolótényezők a fent kifejtettek alapján egyik félhez sem tudják egyértelműen rendelni, célszerű lenne un. közösen generált adatokként[1002] kezelni és többes jogosulti pozíciót létrehozni. A területet elsősorban szabályozó joganyag jelenleg a DA, amely a jogosultsági kérdéseket nem részletezi, hasonlóan az amúgyis óvatos jogi megközelítéshez csak részlegesen definiált, adatokkal kapcsolatos sui generis jogosítványokkal operál, amelyek látszólag nem részei egy nagyobb egésznek.

6.2.3. A jogosultság tartalmáról (részjogosítványairól)

A jogosultak azonosítását követően azok jogait is érdemes áttekinteni. Az elsődleges jogosult kiindulópontként minden jogosítvánnyal rendelkezik az adat létrejöttének pillanatától, ehhez képest a másodlagos jogosult a megszerezhetőnek tekintett (és ténylegesen megszerzett) részjogosítványokkal bírhat. Az adatjogi jogosítványok az alábbiak szerint alakulhatnak. Fontos, hogy a relációs jognak megfelelően ezeknek a *csokra* mindig dinamikusan változik az adatalapú helyzet környezetének és a résztvevő érdekelt feleknek megfelelően. A relációs jog lényege, hogy a részjogosítványok teljességének nem kell minden esetben, egy időben, egy jogosult vonatkozásában megjelennie. A jog megmutathatja, hogy a jogosult más magatartására milyen hatást gyakorolhat, meghatározhatja egy célzott joghatás kiváltására irányuló döntés lehetőségét vagy akár egyfajta tevés alóli mentesülést is előidézhet.[1003]

6.2.3.1. Az adat hatalomban tartásának (adattartás) jogáról

Az adat tartása az adat feletti tényleges hatalmat jelenti, így az adattartó az a személy, akinek valódi lehetősége van arra, hogy az adatot hatalmában tartsa. Ez az adatok vonatkozásában ténykérdésként kezelhető, így de facto adattartó az, aki az adaton (bármilyen okból, módon, célból) műveleteket végez vagy végezhet.[1004] Ez kiindulópontként az elsődleges jogosulti

[1001] A relációs joggal Wiebe felvetésében szereplő túl sok érdekelt fél jelenléte által előidézett allokációs probléma részben bizonyosan feloldhatónak tűnik. Ehhez ugyanis csak arra van szükség, hogy az elsődleges jogosult tisztázott legyen, akihez képest a másodlagos jogosultak az érdekeiket felsorakoztatva vehetnek részt a folyamatban, az értékegyenlőségi elv által diktált feltételek mentén és adatkör tekintetében. Tehát semmilyen érdekelt fél sincs kizárva a folyamatból, de csak a helyzetnek (relációnak) megfelelő jogokkal rendelkezhet. Lásd részletesen a problémafelvetéssel kapcsolatban: Andreas Wiebe, „Protection of industrial data – a new property right for the digital economy?", Journal of Intellectual Property Law & Practice, 2017, Vol. 12, No. 1. 69-70 o.

[1002] Az ALI-ELI Alapelvek 22 o. Az un. co-generated data fogalma e szerint: olyan adatok, amelyek előállításához az adatkezelőtől eltérő személy is hozzájárult, például azáltal, hogy ő az adat alanya vagy (…) az adatgeneráló eszköz tulajdonosa vagy üzemeltetője (…).

[1003] Blutman László, Görög Márta, „Alapvető alanyi jogi pozíciók a Polgári Törvény könyvben (2013)", JK, 2013/6., 273-274. o.

[1004] A GDPR 4. cikk 2. pontja alapján például művelet lehet a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés

pozícióval együtt jön létre, de a másodlagos jogosultak is rendszerint szükségszerűen rendelkeznek ezzel a joggal. Azokban az esetekben, amikor az adatot létrehozó és az elsődleges jogosult eltérő személyek, az adatot létrehozó másodlagos jogosultként adattartói minőséget kell szerezzen párhuzamosan a jogosultság létrejöttével (pl. munkahelyi azonosító [személyes adat] kibocsátásakor, ahol az elsődleges jogosult a munkavállaló, de az adat létrehozója, a munkáltató, másodlagos jogosult és adattartó is egyben).

Az adattartó intézménye több ponton hasonlóságot mutat a dologi jogi birtokkal. Ennek oka, hogy az adatokon végzett műveletek fajtái rendkívül sokrétűek és a végzésük indokoltsága változatos. Elképzelhető (főként Big Data alapú rendszerek esetén), hogy még a műveletek végzésének megvalósulása is kérdésként merül fel. Amennyiben az adattartói jog mindig az elsődleges vagy másodlagos jogosult érdekkörében maradna, nem lenne értelme külön részjogosítványként említeni. Azonban a sokszor zavaros adatalapú életviszonyok rendszeresen hozhatnak létre olyan helyzeteket, amelyekben az adattartói minőség bár jogellenesen áll elő, az adattal való kapcsolatot ténybelileg ilyenkor is létrehozza. Adatjogi felhatalmazás hiányában az adattartói jog másodlagos jogosultságként nem jöhet létre, így önálló szabályoknak kell rá vonatkoznia. Hasonlóan a jogalap nélküli birtokláshoz a felhatalmazás nélküli adattartónak csak harmadik felek irányába állhatnak fenn jogosultságai, aminek oka az elsődleges jogosult érdekeinek védelme, tekintve, hogy a felhatalmazás nélküli adattartó sérelme végső soron az elsődleges jogosult (adatainak) sérelmét is jelentené. Így végeredményben a felhatalmazás nélküli adattartót meg kell illesse a védelem mindenkivel szemben, kivéve az elsődleges jogosultat, aki felé kötelezettsége jön létre a jogellenes állapot valamilyen módon történő helyreállítására.[1005]

6.2.3.2. A használathoz (felhasználáshoz és hasznosításhoz) való jogról

Az eddigiek alapján látható talán, hogy az adatok jellemzően céllal keletkeznek (legfeljebb a cél csak később jelentkezik). Ebből következik, hogy az adatoknak valamilyen célra felhasználhatónak, illetve hasznosíthatónak kell lenniük. Ide tartozik például a lakcímünk használata a hazataláláshoz vagy saját cégünk – nem nyilvános – eladási statisztikájának elemzése. Ezek bár triviálisnak tűnnek, az adat és az elsődleges jogosult közötti kapcsolatot egyértelműen kiolvashatóvá teszik. Örülnénk-e például, ha egy másik, ismeretlen személy is a mi címünket tekintené lakcímének vagy esetleg egy versenytárs elemezné a mi cégünk titokban tartott eladási adatait?[1006] A használat tehát alapvetően a saját célzattal bíró műveletek végzését foglalja magába. A használathoz elengedhetetlen az adat hatalomban tartása, azonban az adat tartható anélkül is, hogy a használata megtörténne, amennyiben az nélkülözi a saját célt (pl. a megbízó utasításainak megfelelő adattárolás, ahol az adaton műveletet végzünk, de saját célunk nincs vele).

A használat láthatóan történhet vagyoni és nem vagyoni érdekeltségből egyaránt. A használat joga teljességében mindkét területen (felhasználás, hasznosítás), való alkalmazásra kiterjed, azonban az megbontható, korlátozható. Származékos szerzés esetén elképzelhető, hogy a használat csak egy területre és azon belül csak meghatározott műveletekre vagy tágabban folyamatokra terjed ki. Átemelhetőnek mutatkozik a Ptk. 5:22. § szerinti dologi jogi axióma, ami szerint a használat során a jogosult köteles tartózkodni minden olyan magatartástól, amellyel másokat szükségtelenül zavarná, vagy amellyel jogaik gyakorlását veszélyeztetné. Ide

[1005] Hasonlóan a birtokhoz, lásd részletesen: Ptk. Nagykommentár 958-959 o.

[1006] Az adatjog ezért csak harmonizált szabályrendszer keretében működhet. A hamis lakcím megadása közokirathamisításként büntetőjog által büntethető, míg a titkos céges statisztika elemzése üzleti titkot sérthet. Az adatjog az ilyen közrehatások kezelésére alkalmas kell legyen úgy is, hogy közben jogvédelmet biztosít a hasonló, de mégsem tényállásszerű helyzetekre (pl. az eladási statisztika titokban tartása érdekében a jogosult nem tett eleget, így azt nem lehet üzleti titokként kezelni, mégis adatjogi szempontból sérelmes).

vonható példa az osztott adatok esetköre, amikor bár saját adatainkat korlátlanul használhatjuk, ha azok összeköttetésben állnak mások adataival ugyanezt nem tehetjük már meg.

6.2.3.3. A hasznok szedésének jogáról

A használat logikus következménye, hogy az adatok által valamilyen eredmény, egyfajta haszon jön létre. Haszon alatt érthetjük mindazt az előnyt, amely az adatból, mint immateriális jószágból származik.[1007] Ez az előny azonban nem csak vagyoni előnyt jelenthet. Az adattal kapcsolatos hasznok szedésére eredendően az elsődleges jogosultnak van lehetősége. Haszon lehet például egy művészi fotó értékesítéséből befolyt vételár, de ugyanígy a haszon várományaként foghatjuk fel a gyógyulás reményében megadott egészségügyi személyes adatainkat. Szintén az adatból származó haszon lehet saját cégünk brand értékkel bíró neve alatt szerződést kötni, valamint éves értékesítési statisztikáit elemezni és ez alapján jobb üzleti döntéseket hozni.

Kiemelendő, hogy az adathasznosítás az adatokban rejlő haszon kinyerésének elsődleges terepe, ahol ez egészen a monetizáció állapotáig jutott. Azonban a hasznok szedésének fenti klasszikus példái mellett a hasznosításban felmerül a harmadik fél általi, adatalapú eredményekből való részesedés kérdése.[1008] Ebben az esetben tehát nem az elsődleges jogosult a saját eredménye által éri el a haszon keletkezését, de ahhoz feltétlenül szükség volt a jogosult adatának a használatára.

6.2.3.4. A rendelkezéshez való jogról

Ezen jog alapján van lehetősége a jogosultaknak az adattal kapcsolatban jogviszonyokat létesíteni. Az adathasználat szempontjából különösen fontos részjogosítvány, hiszen ez fogja meghatározni, hogy az adatokhoz a jogosult milyen módon tud hozzáférést adni/szerezni. A rendelkezés egy lényeges kérdése a magánjogi forgalomképesség, amelyet fentebb az adatok vonatkozásában részletesen vizsgáltunk, e tekintetben annyit kell leszögeznünk, hogy megalapozottan gondolhatunk az adatokra, mint forgalomképes vagyontárgyakra. De vajon mi a helyzet az adaton fennálló jogosultság forgalomképességével? Ahhoz, hogy az adat ügyleti forgalom tárgya legyen, ahhoz a jogoknak is valamilyen formában annak kell lennie, de ez nem zárja ki, hogy valamilyen szintű megkötéseket a rendszer tartalmazzon. A műpéldány forgalomképességétől függetlenül a szerzői jog a szerző személyhez fűződő[1009] és vagyoni jogai[1010] között tesz különbséget, amelyekkel kapcsolatban a magyar jog kifejezetten az átruházás tilalmát, és a két jog oszthatatlan összekapcsolását állítja fel (ez a monista felfogás). Az angolszász területek itt is sokkal megengedőbbek, egy un. „copyright-rendszert" követnek, ahol a szerző és a jogosult személye el is válhat egymástól. A kettő között átmenet is létezik, amely szerint a személyhez fűződő jogok nem, de a vagyoni jogok átruházhatóak (dualista felfogás).[1011] Ebben a rendszerben elképzelve a relációs jogosultságot azt mondhatjuk, hogy a kapcsolótényezők szigorúan kijelölik az elsődleges jogosultat, amelynek lehetnek olyan jogai, amelyek a személyéhez kötődnek, így átruházhatatlanok. E mellett azonban az adat

---

[1007] Lenkovics dologi jog, 82 o.

[1008] Dirk Bergemann , Jacques Cremer , David Dinielli , Carl-Christian Groh , Paul Heidhues , Maximilian Schafer , Monika Schnitzer , Fiona M. Scott Morton, Katja Seim, Michael Sullivan, „Market Design for Personal Data", Yale Journal on Regulation, 40(3). 1058 o.

[1009] Az Szjt. II. fejezete szerint a mű nyilvánosságra hozatala, a név feltüntetése, a mű egységének védelme

[1010] Az Szjt. 16. § szerint a vagyoni jog kiterjed a mű egészének vagy valamely azonosítható részének anyagi formában és nem anyagi formában történő bármilyen felhasználására és minden egyes felhasználás engedélyezésére. A 17. § alapján felhasználás különösen a többszörözés (18–19. §), a terjesztés (23. §), a nyilvános előadás (24–25. §), a nyilvánossághoz közvetítés sugárzással vagy másként (26–27. §), a sugárzott műnek az eredetihez képest más szervezet közbeiktatásával a nyilvánossághoz történő továbbközvetítése (28. §), az átdolgozás (29. §) és a kiállítás (69. §).

[1011] Grad-Gyenge, 2019. 64 o.

használhatóságát (akár vagyoni, akár nem vagyoni érdekek mentén) az egyes részjogosítványok feletti szabad rendelkezés adná meg, így ennek a rendszernek a szerzői jog dualista felfogása felelne meg leginkább.

Tehát az adatjogi jogosultság (forgalomképessége) a rendelkezési jog keretében az adaton való műveletek végezhetőségéről, a használatról, a hasznok szedéséről, mint részjogosítványokról való döntést foglalja magában, mivel az elsődleges jogosulti pozíció a dualista felfogás alapján a személyhez kötődik, csak korlátozottan lehet átruházható.

A lehetséges rendelkezési módokat érdemes kiindulópontként tisztázni. Az egyik az átruházás, ami egy jog jogosulti pozíciójában történő alanycserét jelenti, aminek következtében az átruházott jog az eredeti jogosultnál megszűnik. Ez dologi jogi kontextusban, testi tárgyak esetén valóban így kell legyen, azonban nonriválisimmateriális javak esetén nem szükségszerűen.[1012] Így a rendelkezési jog körében az átruházás mellett feltétlenül gondolnunk kell a jog megosztására is, amely esetben potenciálisan az elsődleges és akár több másodlagos jogosult egyidőben rendelkezhet ugyanazzal a jogosítvánnyal, ugyanazon adat tekintetében.[1013] Valamely jog megosztása esetén tehát pozíció csere nem valósul meg, a másodlagos jogosult az elsődleges jogosult jogának megosztásával jön létre. Ezek tudatában az alábbiakat mondhatjuk:

- *Személyes adatok esetén az elsődleges jogosulti pozíció átruházása, illetve (a személyes adat létezésének megszűnésén kívül) bármely okból való megszűnése kizárt kell legyen, az arról való lemondás pedig érvénytelen.*[1014] Ennek oka, hogy a „kire vonatkozik az adat" kérdés valójában az adat által reprezentált tényszerűséget keresi. Látható továbbá, hogy személyes adatok esetén a tényszerűség maga a természetes személy. Vagyis ebben az esetben (mikor az elsődleges jogosult megegyezik a tényszerűséggel) a jog átruházása egyet jelenthet a tényszerűség és az adat közti kapcsolat megszüntetésének lehetőségével. Így végeredményben olyan helyzet alakulhat ki, amelyben egy személy neve felett jogot szerzett másik személy a név (mint adat) használati jogát elveheti, ezáltal a név használatától is megfoszthatja a korábbi jogosultat.

- *Nem személyes adatok esetén az átruházás lehetséges lehet, kivéve, ha az elsődleges jogosult egyúttal az adat forrása is.*[1015] A személyes adatokhoz hasonló helyzet alakulhatna ki, amennyiben a szervezet a saját magára vonatkozó adatokkal kapcsolatos jogosultságokat teljes egészében elidegenítené. Itt is ugyanis a tényszerűség maga a szervezet, az adatok eredeti jogának átruházása pedig értelmezhetetlen helyzethez vezethet mindaddig, amíg az adat-adatforrás kapcsolat fennáll. Fontos, hogy nem személyes adatok esetén nem beszélhetünk ilyen erős személyhez-kötöttségről vagy olyan erős védelmi rendszerről, mint az adatvédelmi jog, így azt elméletileg nem zárja ki semmi, hogy ugyanolyan vagy hasonló szemantikai tartalmú adat (pl. egy cégre

[1012] A Ptk. Nagykommentár alapján „az információ (adat) átengedése mások számára valójában annak többszörözését jelenti, és nem azt, hogy az átruházó hatalma megszűnik a jószág felett egy másik személy hatalmának a keletkezésével, hiszen az információ 'átruházásával' az információt 'átadó' személynél az információ továbbra is fennmarad." Ezt érdemes kiegészíteni azzal, hogy a relációs jog nem merül ki az adat hatalomban tartásában, még ha ez de facto meg is marad, más jogosultság nem biztos, hogy gyakorolható lesz. Lásd részletesen: Ptk. Nagykommentár, 975 o.

[1013] Ezért is tűnik helyesebbnek az abszolút jog helyett a relációs jog előnyben részesítése, hiszen, ahány különféle környezetben létrejövő jogosulti pozíció, annyiféle (rész)jogosultsági konstelláció képzelhető el.

[1014] Purtova, 2017. 8 o.

[1015] A gyakorlatban lehet például jelentősége magas brand értékű cégek esetén a név megvásárlásának, amely kétségtelenül a cégre vonatkozó adat, a vásárló a tranzakciót követően viszont okkal várja el, hogy azt az eladó már ne használhassa a későbbiekben. Ilyenkor az adat elsődleges jogosulti pozíciója oly módon kerül átruházásra, hogy az eredeti jogosultnál megszűnik, míg az újnál megjelenik.

vonatkozó indexáló adat) vonatkozásában párhuzamosan többen szerezzenek elsődleges jogosultságot. Tehát az átruházási korlátozás inkább arra vonatkozik, hogy amíg az adat-adatforrás kapcsolat fennáll, a rendkívül erős személyhez kapcsoltság miatt, addig az adat forrásánál nem szűnhet meg az elsődleges jogosultság, ellenkező esetben – ad absurdum – a cég lenne a világon az egyetlen, aki saját nevét nem használhatná jogszerűen.

Az átruházási tilalomra tehát azért van szükség, hogy a relációs jogviszonyban rejlő egy ellentmondást megszüntessen. Ugyanis az erga omnes jog inter partes joggá alakulásával az eredeti jogosult nem egy abszolút, hanem egy relatív tilalom miatt záródhat ki a saját magára vonatkozó adat használatából. Ez pedig jogsértő és nonszensz helyzet lenne.

A fentiek alapján az elsődleges jogosulti pozíció átruházhatósága (ezáltal a relációs jogviszony alanyi jogainak összessége) korlátozottan történhet csak meg, de hogyan alakul a helyzet az egyéb jogosítványok esetén? Ezzel együtt vizsgálhatjuk az elsődleges jog megosztásának és a másodlagos jog átruházhatóságának és megosztásának kérdéseit is, hiszen ezek egyébként is minden esetben csak egyes részjogosítványok tekintetében történhetnek meg.

Az adat hatalomban tartásának joga, mivel ténykérdés – az adattal együtt – átruházható és megosztható kell legyen. Az adatokon végzett műveletek döntő többségben célzatos tevékenységek, így az adat hatalomban tartásával együtt a használat jogának szintén átruházhatónak és megoszthatónak kell lennie (ennek hiányában ugyanis az adat hatalomban tartása sok esetben értelmetlenné válna). Az adatok hasznainak szedése ugyancsak sokszor kapcsolódhat vagy éppen motivációt biztosíthat más adatokon végzett műveletekhez, így annak szintén megoszthatónak vagy akár átruházhatónak kell lennie. Fontos továbbá, hogy az adatok nonrivalitásából adódóan a megosztási jogügyletek korlátlan alkalommal, korlátlan személy számára megvalósíthatóak ugyanazon adat vonatkozásában, míg az átruházás fogalmilag csak egyszer eredményezheti a jogosítvány átadását.

A rendelkezési jog az előbbiekhez képest lényegesen erősebb, teljességében kizárólagosságot is jelentő jogosítvány, így annak egészében történő átruházása valójában az elsődleges jogosulti pozíció átadásával jelentene egyet (ennek feltételeire a fentebb leírtak irányadóak). A rendelkezés megosztása ezzel ellentétben sokkal egyszerűbben kivitelezhető[1016] hiszen pl. a másodlagos jogosult által az adattartás jogának megosztása nem jelenti, hogy az adat megszűnt volna létezni nála vagy az elsődleges jogosultnál. Így ezen megosztási jog (megfelelő körülmények között) érdeksérelem nélkül gyakorolható nemcsak az elsődleges, hanem a másodlagos jogosult által is. A rendelkezési jog tehát csak azokban az esetekben lehet átruházható, ha maga a jogosulti pozíció is átruházható, de annak teljes vagy részleges megosztása egyértelműen megvalósíthatónak tűnik. Ez a jogmegosztás pedig az elsődleges mellet a másodlagos jogosultat – társadalmi érdek, jog vagy az elsődleges jogosult döntése alapján – is megilletheti a (nemo plus iuris elvének figyelembe vételével) saját jogosítványainak terjedelmében.[1017]

6.2.3.5. A jogvédelemhez való jogról

Az adatjogi védelemnek jogi és ténybeli pozíciók számára egyidőben, a lehető legtöbb irányból érkező káros behatással szemben kell védelmet nyújtania, azonban mindössze egy egészen

[1016] A másodlagos jogosult a rendelkezési joggal felruházva hasonló helyzetbe kerül, mint a szerzői jogi felhasználó, aki a felhasználói jogot tovább engedélyezheti.

[1017] Ez szükségszerűen így kell legyen például egy munkáltató általi, adóhatóság felé történő bejelentés esetén, ahol a munkavállaló (elsődleges jogosult) akaratától függetlenül az adat megosztásra kell kerüljön. Ebben az esetben a társadalmi érdek felülírja a jogosult saját döntési jogát, az adattovábbításhoz pedig a jog általi kötelezővé tétellel biztosítja a szükséges terjedelmű rendelkezési jogot a munkáltató számára.

alapvető szinten, amely nem ütközik vagy verseng más, speciálisabb előírásokkal (pl. szerzői jogi védelem).

- *Az elsődleges és másodlagos jogvédelem.* Az elsődleges és másodlagos jogvédelem célja az adatjog jogszerű résztvevőinek erga omnes védelme valamilyen jogellenes hatással szemben. Ezen felül szolgálhatja az elsődleges jogosult inter partes védelmét a másodlagossal szemben, valamint a másodlagos jogosultakat egymással szemben. Ez a típusú jogvédelem tehát az adatjogi jogosultsággal járó részjogosítványok (tartás, használat, hasznok szedése, rendelkezés) gyakorlásával áll összefüggésben, így csak azokat illeti meg, akik valamilyen jogosulti pozícióban állnak. A részjogosítványok átruházhatósága és megoszthatósága miatt a védelem így objektívnek, vagyis az alany személyétől függetlennek tekinthető. A védelem jellege miatt a szankciórendszere a jogszerű állapot helyreállítására, a háborítatlanság megőrzésére és végső esetben kártérítésre, illetve kártalanításra irányulhat.

- *Az adatforrásvédelem.* Az adatforrás egy speciális pozícióként azonosítható az adatjogon belül, ami minden esetben a tényszerűséget jelöli, amelyet az adat szimbolizál. Ez így ténykérdésnek tekinthető, a kapcsolódó védelem ezért személyhez kötődő (szubjektív) és (amíg az adat-adatforrás kapcsolat fennáll) nem idegeníthető el. Az adatforrásvédelem fenntartásához a legközelebb álló szankciórendszer elsődlegesen a jogellenes magatartástól való eltiltásban, illetve az ilyen magatartásokkal kapcsolatos represszióban valósulhat meg.

Leszögezhető, hogy a legkiforrottabb védelem a természetes személyek jog- és adatforrásvédelmére irányul és az adatvédelmi jogon keresztül valósul meg. Az információbiztonság szabályanyaga erős elsődleges és másodlagos jogvédelemként fogható fel mind személyes, mind nem személyes adatok esetén. E mellett az adathasznosítási jog, az adatok szabad áramlásának megteremtéséhez szükség mértékben, elkezdett egyedi szerepkörökhöz, egyedi jogokat kreálni, ami bár fragmentáltan, de a horizontális általános jogvédelem és adatforrásvédelem eszközrendszerét kezdte el felépíteni. Az eddigi kutatások alapján megállapítható, hogy nem személyes adatokra és a jogi személyekre kevés dedikált jogvédelmi és adatforrásvédelmi rendelkezés található.

6.2.4. Az adatjogi szerzőképességről

Az adattal kapcsolatos szerzőképesség feltételeit érdemes még tisztázni. A szerzőképesség egy konkrét jogtárgy megszerzésére való alkalmasságot jelenti, ennek előfeltétele lehet a jogképesség, de az adat kognitív folyamatban betöltött alapvető funkciója miatt úgy gondolom a cselekvőképesség nem.

Tehát mindenki, aki jogot szerezhet és kötelezettséget vállalhat az jogosult lehet, de ez ahogy láttuk elsődleges formájában mindig csak egy egységnyi új adaton szerezhető, amihez az észlelési és rögzítési mozzanatok egyidejű lefutására van szükség. Fontos azonban, hogy az új adat létrejötte és a kapcsolótényezők alkalmazása csak a potenciális elsődleges jogosult kijelölésére lehet képes, de nem eredményezheti automatikusan a jog megszerzését is. Ehhez ugyanis az adott adatra vonatkozó, mögöttes jog által keletkeztetett jogszerűségi előfeltételeknek a teljesülésére van szükség.[1018] Így például személyes adatok esetén a házassági név felvételére érvényes házasságkötést követően van lehetőség, az érvényes házasságkötés feltételeit pedig a családjog határozza meg az eljárás menetével és a megkívánt bemeneti adatokkal együtt. Nem személyes adatok vonatkozásában pedig hiába kellene az adatok előállítójának elsődleges jogot szereznie, ha az adatok előállítására eredendően nem volt

[1018] ALI-ELI Alapelvek 191 o.

lehetősége. Így például piackutatás során olyan cégadatok, mint a foglalkoztatottak száma vagy a székhely, megkötések nélkül összegyűjthetők, ezekből akármilyen következtetés levonható. Ezt azonban nem értelmezhetjük úgy, hogy ha egy cég a versenytársai nem nyilvános ügyfél-adatbázisainak kifürkészése által egy új, mindegyiknél nagyobb és jobb ügyfél-adatbázist hoz létre, azon jogszerű adatjogi jogosultságot szerezhet.[1019] Hiába volt meg az aktív magatartás, az erőforrások befektetése, hiába nem minősül az eredmény személyes adatnak, elsődleges jogosultság jogsértő módon létrejött adaton nem lehet megszerezhető, az adaton a jogsértőnél legfeljebb de facto adattartás jöhet létre. Az ilyen esetben a hézagmentességhez szükséges jogosult kijelölésére az árva adatoknál leírtak lehetnek irányadóak.

Az adatok hatalomban tartása vonatkozásában – ahogy említésre is került – lehetséges az adattartás megszerzése jogszerűen és jogellenesen is, gyakorlatilag bármilyen módon, ami lehetővé teszi az adatokon tényleges műveletek végzését. A jogszerűséghez a vonatkozó jogi vagy szerződéses feltételeknek való megfelelésre van szükség, így például személyes adat hatalomban tartása lehetséges, ha az adatkezelés megfelel az adatvédelmi előírásoknak (különösen alapelveknek való megfelelés, az adatkezelési jogalap megléte) és a területre érvényes ágazati szabályoknak (pl. magánszemélynek szóló számlakiállítás esetén az Áfa tv.[1020] és a számviteli törvény[1021] előírásainak).

A szerzőképesség tisztázásával és a fejezet többi tanulságával együttesen egy jelen állás szerint a gyakorlatban is alkalmazhatónak tűnő relációs jogosultsági rendszert építettünk fel, ami szerint az adatokat, mint immateriális vagyontárgyakat tudjuk kezelni. Polgári jogi (dologi, szellemi tulajdonjog, üzleti titokvédelmi) és adatvédelmi jogi alapokra tudtunk támaszkodni, ami által talán mind a köz, mind a magán jellegű viszonyokban a rendszer adaptálása a legkisebb akadályokba ütközne. Ez a jogosultsági szerkezet így a kiindulópontként szolgáló kérdések megválaszolását is lehetővé teszi:

Kié az adat, ki adhat hozzáférést az adathoz?	→	Az elsődleges jogosulté	→	Az elsődleges jogosult az a természetes személy, akire az adat vonatkozik és bárki, aki a nem személyes adatot létrehozta.
Ki végezhet ténylegesen műveleteket az adaton?	→	Az adattartó (elsődleges vagy másodlagos jogosultként)	→	Az adat hatalomban tartásának joga eredendően megilleti az elsődleges jogosultat, de az megosztható/átruházható. De iure adattartó a személyes adatot létrehozó. De facto adattartó, aki felhatalmazás nélkül tartja hatalmában az adatot.

6.2.5. A jogosultság korlátairól

Az eddig leírtak alapján az adatjogi jogosultságok gyakorolhatóságának számos korlátja azonosítható, ezért is volt részben indokolt a relációs szerkezetű jogviszony megjelölés

[1019] Az elsődleges jogosultság megszerezhetőségével kapcsolatban támpontként szolgálhat a szerző fél tudati kapcsolata a tevékenységével. Így az megszerezhető lehet, amennyiben a fél jóhiszeműen, abban a tudatban volt, hogy az adat létrehozatalára jogszerű lehetősége van.

[1020] Az általános forgalmi adóról szóló 2007. évi CXXVII. törvény 169. § e) pont szerint a számla kötelező személyes adattartalma a „termék beszerzőjének, szolgáltatás igénybevevőjének neve és címe”

[1021] A számvitelről szóló 2000. évi C. törvény 169. § (1) bekezdés szerint a gazdálkodó az üzleti évről készített beszámolót, az üzleti jelentést, valamint az azokat alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá a naplófőkönyvet, vagy más, a törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 8 évig köteles megőrizni.

alkalmazása. Az adatjog külső korlátai a mögöttes jog által támasztott, az egész jogrendszert átható elvárások, ilyenek például az alkotmányossági és emberi jogi kontrolleszközök. Konkrét példaként hozhatjuk a rendeltetésszerű joggyakorlást vagy a versenyjognál látható erőfölénnyel való visszaélés tilalmát. Szintén ilyen korlátokként foghatjuk fel a speciális, korlátozó szabályok előírásait, mint a szerzői jog vagy a titokvédelem. Ezekben mind közös, hogy nem a szűken vett (horizontális vagy vertikális) adatjogi jogalkotás termékei, így mint külső tényezők fejtik ki a hatásaikat.

Az adatjogi jogosultságok az adatjog által kijelölt belső korlátok között gyakorolhatók. Ezeket az alterületek viszonylatában érdemes vizsgálni.

- *A védelem jogának hatása a jogosulttá válásra:* a szerzőképesség pontjában leírtaknak megfelelően, ahhoz, hogy jogosulti pozícióba kerülhessen bárki, teljesíteni kell a védelmi jog által diktált jogszerűségi feltételeket.
- *Az érdekrealizáció alapú korlátok és a felhasználás tűrése:* a hosszasan vizsgált, társadalom által elfogadott magán vagy közérdekek jelentős korlátozó hatással bírnak a jogosultak lehetőségeire.
- *A hasznosítás önkorlátai:* a hasznosítás a jogosulti autonómia teljesebb állapotából indul ki a felhasználáshoz képest. Az eddigiek alapján azt mondhatjuk, hogy fogalmilag kizárt bárki adatát hasznosítani az akarata ellenére. Ha lehetne akkor, a megfelelő érdekek fennállása esetén azt felhasználásnak neveznénk. Ezért a hasznosításban rejlő korlát valójában maga a jogosult által vállalt, és a hasznosításra irányuló szerződéses viszonyok között kerül artikulációra.

6.3. Az adatjogi szerződések tipizálása

6.3.1. Létező szerződéstípusok alkalmazhatóságának vizsgálatáról

Az adatjog relációs jogosultságainak számbavétele nem lehet teljes a mellérendeltségen alapuló, kötelmi viszonyokat rendező jog egyes aspektusainak vizsgálata nélkül, amely másodlagos vagy többes elsődleges jogot eredményező jogmegosztást vagy ezek (bizonyos esetekben lehetséges) átruházását kellene megvalósítsa. A jogosultságokhoz hasonlóan érdemes kiindulópontként a meglévő, az adatjoggal határos területeken már bevált szerződéstípusokkal kezdeni a vizsgálódást.

6.3.1.1. A tulajdonátruházó és használati szerződésekről

Fentebb arra jutottunk, hogy az adat nem dolog és a dologi jogi szabályok nem alkalmazhatók rá, egyúttal így tulajdonjog sem alapulhat rajta. Ebből kifolyólag a tipikusan ezen a területen alkalmazott szerződések sem mutatkoznak megfelelőnek. Mind az adásvételi, mind a bérleti szerződés esetén a Ptk. dolgok tulajdonjogának átruházásáról vagy azok időleges használatának átengedéséről beszél.[1022] Megjegyzendő, hogy a Ptk. az adásvételi és a bérleti szerződések kiterjesztett alkalmazását írja elő jogok időleges gyakorlásának más személy részére, ellenérték fejében történő átengedésének, továbbá visszterhes, illetve ingyenes átruházásának esetére.[1023] Fontos emlékezni azonban, hogy az adatjogi relációs jogviszonyok jogmegosztó és jogátruházó vállfajai esetén sem csak jogokról, hanem kifejezetten az adatok, mint immateriális vagyontárgyak és az azokhoz kapcsolódó jogosítványok ideiglenes/végleges átruházásáról/megosztásáról van szó. Ezért a Ptk. tulajdonátruházó és használati szerződésekre vonatkozó rendelkezéseit, mint háttérnormát azzal a fenntartással kell figyelembe venni, hogy az adatjogi szerződések nem tekinthetők tisztán jogok átruházásának vagy bérletének. Ezek a szerződések ugyanis, pont annyira értelmezhetetlenek adat nélkül, mint az adásvétel vagy a

[1022] Ptk. 6:215. § és Ptk. 6:331. §
[1023] Ptk. 6:331. § (2) bekezdés, Ptk. 6:215. § (3) bekezdés, Ptk. 6:234. §, Ptk. 6:235. § (3) bekezdés

bérlet dolog nélkül (a jogbérlet egy tipizált szerződés, amellyel alább részletesebben foglalkozom). Így hasonlóan a szerzői jog esetéhez, ahol az oltalmi tárgyak sem definiálhatók *csak* jogokként,[1024] úgy vélem az adatok sem.

6.3.1.2. A felhasználási szerződésről

A szerzői jogban ismert felhasználási szerződés alapján a szerző engedélyt ad művének a felhasználására, a felhasználó pedig köteles ennek fejében díjat fizetni.[1025] Ez egy sajátos sui generis szerződéstípusnak tekinthető, amelynek közvetlen tárgya a felhasználási cselekményre vonatkozó engedély, közvetett tárgyai a mű szellemi természetének jellegzetességei és a hozzá kapcsolódó egyes érdekek specifikumai.[1026] A szabályozott területek hasonlósága miatt a felhasználási szerződésre vonatkozó szabályok különösen hasznosak, azonban magának a szerződéstípusnak az adatjog területén való teljeskörű alkalmazhatósága – hasonlóan a szerzői jogi előírások egészéhez – kétséges. Elsődleges azért, mert kifejezetten egy szerzői műre kell vonatkozzon, az előírásai pedig a szerzői jog személyhez fűződő és vagyoni aspektusaihoz igazodnak, ami az adatalapú folyamatok tekintetében csak jelentős módosításokkal lenne alkalmazható. E mellet azonban fontos, hogy a szerzői jogi felhasználás kifejezetten egy engedélyezési szemléletet követ,[1027] bármennyire is legyen az kiterjedt. Például a felhasználás kizárólagossá tételekor a szerző saját magát is adott esetben kizárhatja művének felhasználásából,[1028] de még ekkor is – a tartós jogviszony miatt – a szerződés felmondható,[1029] valamint annak szükségszerűen valamilyen megállapodott térbeli kiterjedtséghez és időbeli tartamhoz kell igazodnia.[1030]

Az adatok rendezett, de szabad áramlásához bizonyos esetekben a véglegességhez közeli kiszámíthatóságra van szükség, ami az engedélyezés tartós jogviszonyon keresztül megvalósuló logikájához nem minden esetben képes megfelelően igazodni. Az adatalapú működés esetén az adatok vagy eszközökként vagy erőforrásokként foghatók fel, amelyeknek a megbízható használhatóságához olyan gazdasági és társadalmi igény társulhat, ami a tranzakciók visszafordíthatatlanságát és lezártságát követelheti meg. Az ilyen igény kielégítéséhez ezért sok esetben az egyszeri ügylet alapján történő végleges jogszerzésre lehet szükség (un. fire-and-forget elv). A helyzet gyakorlati alkalmazhatósága is kérdésessé válhat, ha azt is számításba vesszük, hogy az adatok jellemzően valamilyen transzformatív folyamatban kerülnek használatra, amiben az „elvegyülést" követően az egyes állományok jogosulthoz való visszakövetése csak nehézkesen kivitelezhető. Ehhez tartozik, hogy a tartós szerződésből eredő felmondás alkalmazása vagy más okból való megszűnés pedig érdeksérelmet okozhat.[1031] Az engedélyezéssel együtt járó kontroll gyakorolhatóságát így reálisan az adatalapú folyamatnak a megosztást követő egy (legfeljebb kettő) lépéseben lehet elvárni, azt követően nem. Ezért a felhasználási szerződés olyan esetekben lehet mintaadó szerződéstípus, ahol a jogosult tartós kapcsolatban kíván (és tud) az adatokkal maradni.

[1024] Lontai et al., 2015. 159-160 o.
[1025] Szjt. 42. § (1) bekezdés
[1026] Lontai et al. 159-160 o.
[1027] Az Szjt. Nagykommentár szerint: „a felhasználási szerződés tárgya, tehát lényegi ismérve az, hogy a szerző valamely műre (művekre) nézve a felhasználási jog gyakorlására engedélyt ad, és az engedélyt tükröző jog keletkezik a felhasználó oldalán" Az engedélyezés egyébként a díjfizetési kötelezettséggel (mint ellenoldallal) együtt alkotják a felhasználási szerződés alapvető építőelemeit. Lásd részletesen: Szjt. Nagykommentár, 355 o.
[1028] Grad-Gyenge, 2019. 123 o.
[1029] U.o. 129-130 o.
[1030] Fodor Klaudia Franciska, Gubicz Flóra Anna, „Szerzői jogi felhasználási szerződés", in Jakab András – Könczöl Miklós – Menyhárd Attila – Sulyok Gábor (szerk.): Internetes Jogtudományi Enciklopédia (Szerzői jog és iparjogvédelem rovat, rovatszerkesztő: Grad-Gyenge Anikó, Pogácsás Anett), 2024. 14-15 o.
[1031] A felhasználási szerződés engedélyezési logikájához hasonló az adatvédelmi jog hozzájárulási jogalapja, amit – egyebek mellett – ebből az okból kifolyólag nem tartok a hasznosításban kiterjedten alkalmazhatónak.

6.3.1.3. A jogbérleti (franchise) szerződésről

A jogbérleti szerződés alapján a jogbérletbe adó szerzői és iparjogvédelmi jogok által védett oltalmi tárgyakhoz, illetve védett ismerethez kapcsolódó felhasználási, hasznosítási vagy használati jogok engedélyezésére, a jogbérletbe vevő termékeknek, illetve szolgáltatásoknak a szerzői és iparjogvédelmi jogok által védett oltalmi tárgyaknak, illetve védett ismeretnek a felhasználásával, hasznosításával vagy használatával történő előállítására, illetve értékesítésére és díj fizetésére köteles.[1032] A jogbérleti szerződés elsősorban a magánszféra védett tartalmainak (know-how, üzleti titkok) kezelési körében felmerülő szerződés, amelynél az előbbi esetben vázolt aggályokhoz hasonlók merülhetnek fel. Így például szerzői és iparjogvédelmi jogok által védett oltalmi tárgyakra, illetve védett ismeretekre vonatkoznak, valamint ismét egy engedélyezési konstrukcióra építkezik.

6.3.2. Az új tipológiáról

A fentiek alapján arra a következtetésre juthatunk, hogy egyik létező, vizsgált szerződéstípus sem alkalmas jelenlegi formájában a relációs adatjogi jogviszonyokat rendezni. Hasonlóan ezért a szerzői jogi megoldáshoz, itt is célszerűnek mutatkozik egy immateriális jószágra (vagyontárgyra) jól alkalmazható, a terület sajátosságait figyelembe vevő sui generis szerződési tipizálást felvázolni. A már létező szerződések vizsgálata alapján látható – követve a szakirodalmi álláspontot is – a tipológia transzfer-célzatú szerződései vagy az átruházási vagy a licencia (használati) kategóriák sajátosságait fogják magukon viselni.[1033]

A tipizált adatszerződések szerepe az alapvető adatmozgások és adatkezelési műveletek elvégzésének felek általi rendezése, ezért három szerződési alaptípussal kezdhetjük a vizsgálatunkat. Ezek az egyirányú adatmozgáshoz szükséges adattovábbítási szerződések, a műveletvégzés kiszervezését megvalósító adatfeldolgozói szerződések és a több irányú, kölcsönös adatmozgást lehetővé tevő adatvegyítési és egyesítési szerződések. A jelenleg ismert gyakorlat alapján e három alaptípus használatával mind az adatok szükség szerinti mobilitása, mind a kellő mértékű jogmegosztás vagy jogátruházás végrehajtható lehet. Ezt a kijelentést támasztja alá, hogy a három alaptípus a GDPR által alkalmazott kötelmi viszonyokra építkezik és egyébként ebből fakad az is, hogy az adatfelhasználás és az adathasznosítás közös szerződési bázisát is ez a három alaptípus adhatja.

Az alaptípusok egyes tulajdonságainak a speciális igényekhez való igazításával vegyes típusú szerződések hozhatók létre a gyakorlati elvárásoknak megfelelően. Jelen dolgozatban ezek közül kettőt vizsgálok, a bizalmi adatkezelési és az adatközvetítői szerződést. Mindkettő az adatok áramlásának serkentését és az adatgazdaság szereplőinek jogérvényesítésének megkönnyítését szolgálják, bár eltérő megközelítések mentén. Szintén közös bennük, hogy mindkettőben vegyesen szerepelnek a három alaptípus tulajdonságai.

Végezetül fontos, hogy a jelenleg hatályos adatjog is tartalmaz előírásokat egyes kötelmi helyzetekre, amelyeket az ilyen helyzetben lévőknek be kell tartani. A tipizáláshoz az ALI-ELI Alapelvekben szereplő tipológiára építkezve a létező polgári, szerzői és adatjogi szerződéstípusok – és az azokra irányadó előírások és joggyakorlat – kerültek felhasználásra.

6.3.2.1. Az adattovábbítási szerződésekről[1034]

Az adattovábbítási szerződések alapvetően egyirányú adatmozgásra és jogmegosztásra alkalmazhatók a továbbító és címzett között, amely az adatok címzett tárhelyére való küldésével

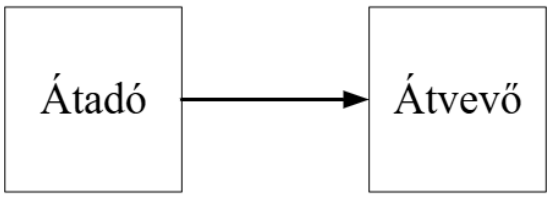
[1032] Ptk. 6:376. § (1) bekezdés
[1033] Görög Márta, „A technológia-, tudástranszfer jogi eszközei”, In: Bajmócy Zoltán – Elekes Zoltán (szerk.): Innováció: a vállalati stratégiától a társadalmi stratégiáig. Szeged, JATEPress, 2013. 281. o.
[1034] ALI-ELI Alapelvek 52-79 o.

vagy az adatok tárolására szolgáló hordozó átadásával valósulhat meg (átadással járó adattovábbítás) vagy az adatokat tároló berendezéshez vagy az adatokat létrehozó eszközhöz való hozzáférés létrehozásával teljesülhet (hozzáférés biztosításával járó adattovábbítás).

Az adatvédelmi jogi előírások az ilyen megállapodások megkötését elsődlegesen az EU szempontjából harmadik országok irányában teszik kötelezővé,[1035] de az általános gyakorlat alapján az adatok EU-n belüli továbbítására két önálló fél (adatkezelő) között is alkalmazásra kerülhet. A szerződés horizontális szabályozáshoz adaptált verziójában a lehetséges felek közé még bele kell értenünk az érintettet is, aki saját adatait továbbíthatja, valamint nem személyes adatok ilyen jellegű továbbítását. A személyes adatokra irányadó gyakorlat alapján a szerződésre vonatkozó minimum tartalmi elemek a felek megjelölése, a továbbítás célja, időpontja, az adatokra vonatkozó paraméterek leírása, a bevezetett védelmi intézkedések megjelölése és az adattovábbítás módszere lehet.[1036] Általában szintén jó megoldás a szerződésben a továbbító adatgyűjtési/rögzítési gyakorlatának, illetve a címzett általi tervezett adathasználat jogszerűségének kötelmi jogi rendezése.

Az adattovábbítási szerződések a dolgozat horizontális adatjogi megközelítésében az alábbiak szerint bonthatók altípusokra.

- *Átadással járó altípusok*



15. ábra: adattovábbítás átadással

Az átadást megvalósító szerződési altípus a jogi és reálaktust egyszerre valósítja meg, azáltal, hogy az adat feletti – a megállapodás alapján *átruházott* vagy *megosztott* – jogot és magát az adatot is a címzetthez eljuttatja. A befejezett átadáshoz mindkét körülmény bekövetkezésére szükség van. Szintén fontos körülmény azonban, hogy a technológia állásából kifolyólag az adatokhoz a legtöbb esetben távoli eléréssel is hozzá lehet férni, így az átadást online körülmények közötti is meg lehet valósítani.[1037] A tárhely helyének kisebb jelentősége azonban nem csökkenti az adatok pontos beazonosításának szükségét, így a szerződési formák elkülönítése szempontjából annak van jelentősége, hogy az átadás fizikai vagy online adatmozgásának jellege megállapítható legyen.

Az átadással járó adattovábbítási szerződések lezártságuk miatt a tulajdonátruházó szerződésekhez állnak közel, a Ptk. kiterjesztés által, a már említett fenntartással, de, mint háttérnorma a Ptk. előírásai alkalmazandók lehetnek, mind visszterhes, mind ingyenes adatátadás esetén.[1038] A szabályozás hatóköréből adódó eltérések racionalizálása érdekében fontosnak tartom, hogy az adatjogi előírások alkalmazási elsőbbséggel kell bírjanak a polgári jogival szemben.

[1035] GDPR V. fejezet

[1036] Information Commissioner's Office, „International data transfer agreement and guidance" Elérhető: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/ Letöltve: 2024.09.24.

[1037] ALI-ELI Alapelvek 48 o.

[1038] Ptk. 6:215. § (3) bekezdés szerint „a dolog adásvételére vonatkozó szabályokat kell megfelelően alkalmazni arra a szerződésre is, amelyből jog vagy követelés visszterhes átruházására vonatkozó kötelezettség fakad."; Ptk. 6:234. § szerint „ha a felek dolgok tulajdonjogának, más jogoknak vagy követeléseknek kölcsönös átruházására vállalnak kötelezettséget, az adásvétel szabályait kell megfelelően alkalmazni"; Ptk. 2:235. § szerint „a dolog ajándékozására vonatkozó szabályokat kell megfelelően alkalmazni jog vagy követelés ingyenes átruházására történő kötelezettségvállalás esetén."

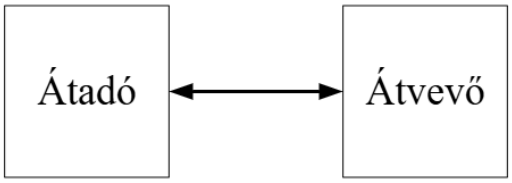
- *Fizikai adatmozgás megvalósításával*

  A fizikai adatmozgáshoz azok az esetek tartoznak, amikor az átadás az adathordozóval együtt történik. Az adathordozó az adat típusától függően bármi lehet, így digitális adat esetén külső merevlemez vagy analóg adat esetén egy papírlap. Fizikai átadáskor az adatkör egyértelműen lehatárolt és azonosított a hordozó által, az átadás (és a szerzés) pedig egyszeri. Az adatmozgás jelentősége a ténybeli erőhatalom[1039] gyakorlási szándéka esetén növekedhet számottevően. Például a felhőtárhelyen való tárolás, az interneten keresztül történő továbbítás a kérdéses adatállományhoz hozzáférők potenciális körét drasztikusan megnövelheti, az online továbbítás kockázatai,[1040] másfelől a tárolás módja, a másolhatóság alacsony ellenőrizhetősége és a későbbi visszaállítás magas valószínűsége miatt. Így a címzett számára különösen érzékeny, új adatok esetén az egy (lokális) tárhelyen való rögzítés és a hordozó fizikai átadása a kellő biztonsági intézkedések mellett a tényleges erőhatalom gyakorolhatóságát jelenti. Az ilyen esetekben fontos, hogy az átadónak gondoskodnia kell a hordozó tulajdonjogának vagy az olvasáshoz és másoláshoz szükséges használati jogának (és ha így állapodtak meg, akkor a birtokának) a címzettnek való átadásáról is.

- *Online adatmozgás megvalósításával*

  Az online adatmozgással járó esetekben is mind a jog- mind a tényhelyzet megváltozik a megállapodásnak megfelelően, azzal a különbséggel, hogy az átadás módja nem fizikai adathordozón, hanem online környezetben történik. Ebben az esetben a ténybeli erőhatalom gyakorlásának esélye csökken, de ez nem kell jelentse az általános biztonság drasztikus esését is egyben. Az online adatmozgás történhet elektronikus levél csatolmányaként való küldés formájában, vagy akár egy interneten elérhető tárhelyen való letölthetővé tétellel, illetve az adat streamelésével. A biztonság ebben a környezetben is megvalósítható, még ha az adatok feletti definitív kontroll kifejtése kevésbé életszerű.

➢ *Hozzáférés biztosításával járó altípusok*



16. ábra: adattovábbítás hozzáféréssel

Hozzáférés biztosításakor az adatok szó szerinti értelemben vett átadása nem történik meg, ez sokkal inkább a kérdéses állományba való betekintést, az állományon való műveletvégzést jelentheti. Láthatóan az ilyen jellegű folyamatok az adatok szemantikai szintjében rejlő lehetőségek kiaknázására szolgálnak, anélkül, hogy azok felett a címzett oldalán a hatalom kiterjedt formájának megszerzésére sor kerülne. Így elmondható, hogy az érintett adatállományon elsődleges jog nem jöhet létre hozzáférés biztosítása esetén.[1041] Ilyenkor lényeges, hogy a corpus megszerzésére egyáltalán nem kerül sor, mivel az adatok hordozója nem változik, tehát az adatok mobilizálásra nem kerülnek. Magának a tárhelynek elképzelhető, hogy polgári jogi értelemben átmenetileg a birtokviszonya megváltozik, de ez az

[1039] Lásd részletesen 2.2.2.

[1040] Jessica Groopman, „7 common file sharing security risks", TechTarget, 2022. Elérhető: https://www.techtarget.com/searchcontentmanagement/tip/7-common-file-sharing-security-risks

[1041] Megjegyzendő, hogy az állományról való másolatkészítés esetét átadásnak tekinthetjük, mivel csak az adatmozgás kezdeményezésének iránya változik a többi ilyen esethez képest. Itt is kiemelendő, hogy tercier adaton való elsődleges jog megszerzésére a szerződéses kikötések alapján van lehetőség.

adatok feletti jogosultságra nincs hatással (a hordozó és az adatok technikai és jogi értelemben is megőrzik önállóságukat[1042]).

A hozzáférés biztosításával járó altípusok használati jellegűek, így a bérleti szerződésekhez állnak közel, így a Ptk. ismét, mint háttérnorma vehető figyelembe a fentebb jelzett eltérésekkel. A jogviszony használati jellegéből adódó tartósság és engedély-alapúság miatt a szerzői jogi felhasználás ehhez a szerződési altípushoz kapcsolódik a legszorosabban. A jelen dolgozat által felépített adatjogi paradigmában a szerzői jog az adatjoggal lex generalis - lex specialis kapcsolatban áll, így rendszertani okokból a felhasználási szerződésre vonatkozó joganyagot nem tekinteném háttérnormának. Ettől függetlenül akár kodifikált, akár szokásjogi alapon átvehetők a szerződésre vonatkozó rendelkezések és joggyakorlati eredmények. A szerződési altípust az alábbiak szerint tudjuk tovább bontani az adatjogi sajátosságok szerint.

- *Fizikai jelenléttel / távoli eléréssel*

  A hozzáférésre sor kerülhet a címzettnek a létesítménybe való beengedésével és a tárhelyhez/szerverhez/irattárhoz biztonságos belső interfészen keresztüli csatlakozásának engedélyezésével. Távoli elérés esetén online kapcsolat kerül létesítésre a belső tárhelyeken eltárolt adatállományokhoz, amelyeket így minimum olvasni, legfeljebb feldolgozni lehet. Egyszerű példája lehet az adattovábbítási szerződéseknek a hozzáférést fizikai jelenléttel biztosító altípusainak a klasszikus könyvtári szolgáltatások, míg a távoli elérést alkalmazó válfaja például az online repozitórium[1043] kategóriát foglalhatja magába (természetesen csak olyan kérdések tekintetében, amiket a szerzői jog nem rendez).

- *Felelősségvállalással / felelősségvállalás nélkül[1044]*

  Ennek kapcsán a szolgáltatói oldal felelősségvállalásáról vagy annak hiányáról beszélünk. Ezt a különbségtételt akkor lehet érdemes bevezetni, amikor a szolgáltató nagy mennyiségű adathoz kínál hozzáférést, de az eredményért való helytállás tőle észszerű okokból nem elvárható (ez pl. előfordulhat nagy mennyiségű történeti adatot tartalmazó állomány esetén vagy sok forrásból származó adatból létrehozott, kompilált adatbázis esetén). A használhatóságra vonatkozó felelősségvállalástól való mentesülés által elkerülhető lehet potenciálisan nagy értéket hordozó, de magas ráfordítást igénylő adatállományok elveszése, oly módon, hogy a szolgáltató azt piaci viszonylatban átlagon aluli értéken kínálja, míg a címzett vállalja annak a kockázatát, hogy a befektetése csekély mértékben vagy egyáltalán nem térül meg. A felelősségvállalás alóli mentesülés azért került a hozzáféréssel történő adattovábbításhoz, mert jellemzően a szolgáltatói állományok unikálisak és/vagy a függetlenségük megőrzéséhez valamilyen (köz)érdek fűződik.

- *Tárhelyhez / eszközhöz biztosított hozzáféréssel*

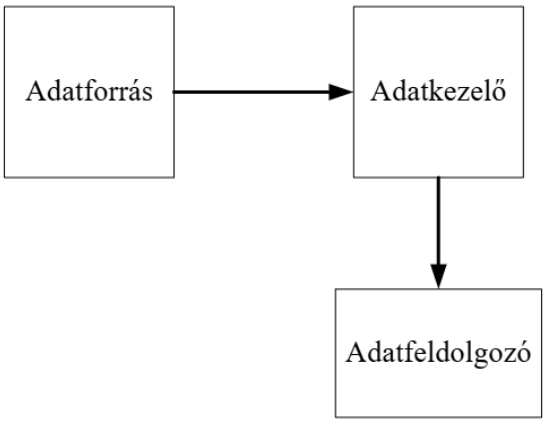
  A hozzáférés esetén szükségszerű azt tisztázni, hogy pontosan mihez kerül megadásra. A két lehetőség, hogy az adatok tárhelyéhez vagy azok gyűjtéséhez/rögzítéséhez alkalmazott eszközhöz tud közvetlenül a címzett hozzáférni. Előbbi esetén a tárhely beállításaitól függ, hogy a hozzáférés során milyen adatokhoz meddig lehet hozzáférni, tehát a folyamatra sokkal erősebb kontroll gyakorolható a szolgáltató által, ezért egy statikus hozzáférésről van szó. Az eszközhöz való hozzáférés esetén (ahol technikai

[1042] Lásd: 2.2.2. fejezet
[1043] Így például az MTA könyvtárának repozitóriuma ide tartozhat https://real.mtak.hu/
[1044] ALI-ELI Alapelvek 79 o.

értelemben egyébként ugyancsak van egy tárhely) a lényegi különbség, hogy a pontos adatkör az adott eszköztől függ, nem a szolgáltató (kivéve, ha a szolgáltató és az eszközt használó megegyezik) azon akaratától, hogy milyen adatokat helyez el a tárhelyen. Az eszközzel való közvetlen kapcsolat esetén a hozzáférés dinamikus, akár olyan mértékig, hogy sem a címzett, sem a szolgáltató nem tudhatja egészen pontosan milyen adatok kerülnek az eszköz által rögzítésre (ezt a gyakorlatban az eszköz maga tudja a legjobban előre jelezni, pl. a sportoló karján lévő okosóra és a precíziós növénytermesztéshez szükséges szenzorokkal rendelkező traktor geolokációs adatai eltérő következtetések levonását teszik lehetővé). Ennek a dinamikus környezetnek az előnye a közvetlen és gyors (akár valós idejű) kapcsolat az adatforrással, hátránya lehet a cél elérésére való esetleges alkalmatlanság vagy az alacsonyabb szintű adatminőség.

6.3.2.2. Az adatfeldolgozói szerződésekről[1045]

Az adatfeldolgozói szerződésre az adatokon végzett műveletek önállótlan formájának archetípusaként tekinthetünk. A GDPR szerint a szerződés névadó alanya bárki lehet, aki az adatkezelő nevében személyes adatokat kezel. Összhangban továbbá az eddig kialakult gyakorlattal adatfeldolgozói tevékenység mindenfajta műveletre kiterjedhet, a lényegi eleme az, hogy a szolgáltatás kifejezetten az adatokra irányuljon és, hogy az adatfeldolgozó ne rendelkezzen saját céllal a folyamatban. Az adatfeldolgozás összes körülménye alapján kijelenthető, hogy az adatfeldolgozó elsődleges jogosulti pozícióba nem kerülhet a feldolgozott adatkör tekintetében. Különös ismertetőjegye az ilyen szerződéseknek, hogy sokszor töltenek be kísérő szerepkört egy főtevékenység mellett. Ez jellemzően adatalapúan működő szolgáltatások esetén fordul elő, ahol az ágazati jog szerint érvényesen létrejövő szerződés mellett – annak gyakorlatilag elválaszthatatlan részét képező, de különálló – szerződésben szabályozzák az adatfeldolgozói tevékenységet. A potenciális műveletvégzési repertoár a tág hatókör miatt – személyes és nem személyes adatok esetén is – gyakorlatilag végtelen, így a szerződés további tipizálása nehézkes. A fentebb bevezetett műveleti struktúrát követve az adatfeldolgozói tevékenység kiterjedhet:



17. ábra: adatfeldolgozás

- a gyűjtésre, rögzítésre és törlésre,
- aggregációra, kompilációra, szintetizációra,
- gondozásra, extrakcióra, illetve
- interpretációra, integrációra.

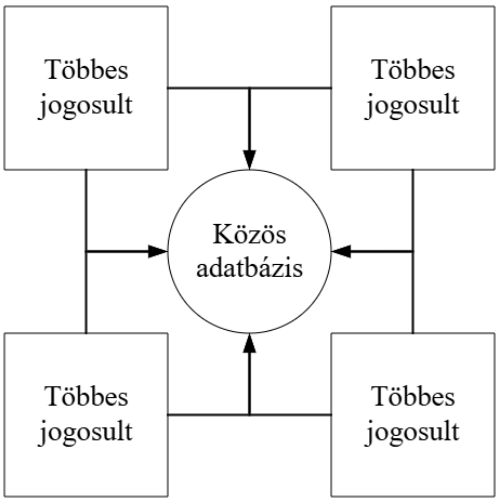
Kiemelendő, hogy a fenti területek közül egynél több is – pl. egy szolgáltatás vagy szolgáltatáscsomag részeként – felkínálható ugyanazon szereplő által. Például egy tárhelyszolgáltató a nála tárolt adatokat rendezheti vagy álnevesítheti, valamint akár valamilyen analitikai megoldást is kérésre elvégezhet, anélkül, hogy a magasabb kompetencia szintet átlépné és adatkezelővé válna.

[1045] ALI-ELI Alapelvek 91-99 o.

Az adatfeldolgozói tevékenység megbízási vagy vállalkozási típusú szerződésekhez áll közel, attól függően, hogy egy gondossági vagy egy eredménykötelmi jellegű műveletvégzést várnak el az adatfeldolgozótól.

6.3.2.3. Az adatvegyítési vagy adategyesítési szerződésekről (data pooling)[1046]

Ez a szerződéstípus alapvetően a kettő vagy több fél által közös elhatározásból épített diverz (adatvegyítés) vagy uniform (adategyesítés) adatbázisok létrehozására irányuló tevékenységet foglalja magába. A szerződő felek az együttműködés során egymás viszonylatában kölcsönösen átadnak és fogadnak adatokat, azzal, hogy a célokat és eszközöket közösen határozzák meg. Ilyenformán csak önálló adatkezelők lehetnek részes felek, az adatkezelő és az adatfeldolgozó közötti együttműködésre ennek keretében nem kerülhet sor (ennek oka a mellérendeltségi helyzet hiánya).



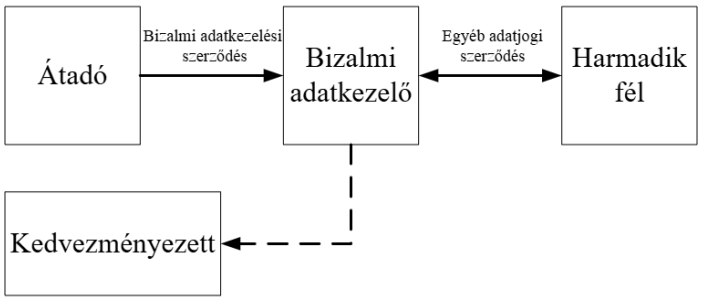
18. ábra: adatvegyítés vagy adategyesítés

A jelenlegi adatjogi alapját a közös adatkezelői konstrukciók adják, amelyek létrejöttéhez a felek közötti megállapodásra (vagy uniós vagy tagállami jogra) van szükség.[1047] A szerződés gyakorlati szempontból új közös adatállomány vagy adatbázis létrehozására vagy meglévő adatbázisok összevonására szolgálhat,[1048] ezáltal az adatkezelés megosztásának eszköze. Tartalmilag ezért kiemelt eleme a felek belső és külső viszonyainak átlátható rendezése,[1049] illetve a jogszerzés körülményeinek szabályozása. A relációs jogoknál látható volt, hogy a személyes adatok felett a természetes személyek, míg a nem személyes adatok felett az adatot létrehozók többes elsődleges jogot szerezhetnek, minden más esetben a szerződésnek (vagy más módon kinyilvánított akaratnak) megfelelő másodlagos jog jön létre.[1050] Ezáltal a szerződésnek a két adatkategória esetén létrejövő kétféle többes elsődleges jog belső viszonyait[1051] és általában az összes szereplő (elsődleges és másodlagos jogosultak, mint amilyen például az adatbázis létrehozója lehet) egymáshoz való kapcsolatát is rendeznie kell.

A szerződéstípus hátterét ezúttal nem egy polgári jogi szerződés, hanem egy szerzésmód, az egyesítés és vegyítés[1052] adja. A szerzésmód különböző tulajdonosok ingó dolgainak "elválaszthatatlan" egyesítését (összekeverése, összeolvasztása) vagy egyéb módon történő összevegyítését írja le,[1053] a lényege pedig, hogy a dolgok értéke arányában közös tulajdon keletkezik. Az adatjogi szerződésnek ez alapján a lényege, hogy a felek által, egy közös cél érdekében történő adatok egymásközti megosztását rendezze.[1054]

[1046] ALI-ELI Alapelvek 84-91 o.
[1047] GDPR 26. cikk
[1048] ALI-ELI Alapelvek 84 o.
[1049] EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR
[1050] Lásd részletese 6.2.2.1. alfejezet
[1051] Lásd részletesen 6.2.2.4. alfejezet
[1052] Ptk. 5:56. §, 5:67. §
[1053] Lenkovics Barnabás, „A tulajdonszerzés-módok eredeti, illetve származékos jellege", PJK, 2003/3.. 14-29. o.
[1054] ALI-ELI Alapelvek, 84-85 o.

6.3.2.4. A bizalmi adatkezelési szerződésekről[1055]



19. ábra: bizalmi adatkezelés

Bizalmi adatkezelési szerződés alapján az adatkezelő az elsődleges jogosult által kezelésébe adott adatok, ezzel kapcsolatos jogok és követelések (a továbbiakban: kezelt adatvagyon) saját nevében a kedvezményezett (elsődleges jogosult vagy általa megjelölt harmadik fél) javára és érdekeinek megfelelően történő kezelése történhet.[1056] A bizalmi adatkezelésbe adott adatvagyon feletti – akár teljeskörű – jogok gyakorlásához az ilyen szerződés felhatalmazást biztosíthat, anélkül, hogy az az adatkezelő saját adatvagyonának részévé válna.[1057] A bizalmi adatkezelés lényegét tekintve egy olyan általános megbízás valamilyen adatállományon való műveletvégzésre, aminek alapvető irányvonalait az elsődleges jogosult határozza meg a szerződéskötéskor, azonban a mindennapi kérdések tekintetében, az eredeti cél/érdek megvalósításához/védelméhez szükséges lépésekről a bizalmi adatkezelő dönt. E tekintetben hasonlóságot mutat egy adatfeldolgozó pozíciójával, mivel azonban a célt és az eszközt maga határozza meg a mindennapi ügyvitelben ezért adatfeldolgozó nem lehet.

A szerződés kiemelt adatjogi relevanciája a szerzői jogi közös jogkezeléshez[1058] hasonló megoldás biztosítása, amelyen keresztül a lehetőség vagy képesség hiányában hátrányosabb pozícióban lévő szereplőknek az adathasznosítási folyamatokba való bevonása könnyebben elérhető lehet. A bizalmi adatkezelői jogviszony alapján nagyobb adathalmazok feletti joggyakorlás kiszervezésére is sor kerülhet, így az ügyviteli vagy technikai nehézségek feloldhatók anélkül, hogy az elsődleges jogosultra túlzottan nagy teher hárulna. E mellett kiemelt lehetőség rejlik több elsődleges jogosult adatjoghoz kapcsolódó jogainak közös kezelésében és képviseletében[1059] egy adatkezelő által. Erre akkor lehet szükség, ha a hasznosításra irányuló folyamat vagy adatkör jellege, illetve körülményei miatt az elsődleges jog egyedileg hatékonyan nem gyakorolható.[1060] Ilyen eset lehet kisebb méretű vagy gyengébb igényérvényesítési helyzetben lévő (pl. civil szervezet, kis önkormányzat, kkv) szervezetek vagy természetes személyek közös fellépése egy bizalmi adatkezelőn keresztül. Előnyös lehet, hogy így nagyobb piaci erő képviseletére van lehetőség, a bizalmi adatkezelő a közös igényérvényesítéshez szükséges tudással rendelkezhet, illetve ez irányú megállapodás esetén közös adatállományok is létrehozhatók (data pooling szerződéssel kombinálva), amellyel így az elsődleges jogosultak adatainak összértéke növelhető.[1061]

[1055] ALI-ELI Alapelvek, 99-110 o.
[1056] Ptk. 6:310. §
[1057] Ptk. 6:312. §
[1058] A szerzői jogok és a szerzői joghoz kapcsolódó jogok közös kezeléséről szóló 2016. évi XCIII. törvény (továbbiakban: Kjkt.) 4. § 7. pont szerint a közös jogkezelés: egyes szerzői vagyoni jogok és a szerzői joghoz kapcsolódó vagyoni jogok több jogosult érdekében és közös javára közös jogkezelő szervezet által történő gyakorlása és érvényesítése
[1059] Grad-Gyenge, 2019. 140 o.
[1060] Kjkt. 1. §
[1061] Kimberly A. Houser, John W. Bagby, „The Data Trust Solution to Data Sharing Problems", Vanderbilt Journal of Entertainment & Technology Law, 25(1), 2023. 140-141 o.

A bizalmi adatkezelés a Ptk. bizalmi vagyonkezelési szerződésével[1062] rokon, így az háttérnormaként az eddigieknek megfelelően alkalmazható lehet.

6.3.2.5. Az adatközvetítői szerződésekről

Az adatközvetítés intézményesítése a DGA alkalmazandóvá válására vezethető vissza. Ez alapján az adatközvetítő szolgáltatás olyan szolgáltatás, amelynek célja kereskedelmi kapcsolatok létrehozása egyrészről meghatározatlan számú érintett és adatbirtokos, másrészről az adatfelhasználók közötti adatmegosztás - többek között az érintettek személyes adatokkal kapcsolatos jogainak gyakorlása – céljából. Az adatközvetítő a szolgáltatás nyújtásához technikai, jogi vagy egyéb eszközöket alkalmazhat.[1063] Erre alapozva azt mondhatjuk, hogy az adatközvetítői szerződés az adatközvetítő megbízója (elsődleges vagy másodlagos jogosult) és harmadik személy között szerződés megkötésének elősegítésére irányuló tevékenység folytatása.[1064] A bizalmi adatkezelési helyzethez hasonlóan a jelen szerződés is egy speciális adatjogi konstrukciót hoz létre. Ezt támasztja alá, hogy a DGA például kizárja az olyan szolgáltatásokat a közvetítés alól, amelyek az adatokkal kapcsolatosan értéknövelő műveleteket foglalnak magukba.[1065]

20. ábra: adatközvetítés

Az adatközvetítő a Ptk. közvetítői szerződésével rokon, így az a megszokott módon háttérnormaként hívható fel.[1066]

Az adatközvetítői szerződések négy altípusra oszthatók, attól függően, hogy milyen módon működik közre a közvetítő.

- *A direkt-közvetítő*

A direkt-közvetítő egyedileg meghatározott, konkrét adatállománynak – a megbízója pozíciójának megfelelően – valamilyen módon történő hasznosításba adását vagy hasznosításba vételét támogatja, kifejezetten a felek közötti üzleti kapcsolatok előmozdításán keresztül. Így tehát a direkt-közvetítésnek két iránya lehetséges. Ha a megbízó a jelenlegi jogosult, akkor az általa kijelölt állomány megosztására vagy átruházására alkalmas szerződések megkötését közvetíti a direkt-közvetítő lehetséges érdeklődők (jövőbeli jogosultak) felé. Az is lehetséges, hogy a megbízó a leendő jogosult, akinek meghatározott adatokra van szüksége saját céljainak eléréséhez. Ilyen esetben a közvetítő olyan jogosultakat kutat fel, akik ilyen adatok felett rendelkezhetnek. A direkt-közvetítőt az adatpiactértől az határolja el, hogy konkrét felek között, konkrét ügyben, jellemzően személyes erőfeszítés keretében jár el. Azonban hasonlóan az adatpiactérhez – és ellentétben egy adatokkal saját jogon kereskedő piaci szereplővel – megőrzi a folyamatban a semlegességét, az adatok tekintetében saját céllal nem rendelkezhet, csak a szerződéses közvetítés teljesítésének mértékéig. Megjegyzendő, hogy a közvetítő folyamatbéli döntési kompetenciájának szintje szerint elképzelhető az is, hogy adatkezelőként és az is, hogy adatfeldolgozóként jelenik meg. Felmerülhet továbbá, hogy a DGA adatközvetítő szolgáltatás

[1062] Ptk. XLIII. fejezet
[1063] DGA 2. cikk 11. pont
[1064] Ptk. 6:288. §
[1065] DGA 2. cikk 11. a) pont
[1066] Ptk. XLI. fejezet

fogalmában[1067] szereplő „meghatározatlan számú" kitétel miatt a direkt-közvetítő – mivel konkrét megbízóval rendelkezik – a rendelet hatályán kívül helyezkedik el. A 10. cikkben – amely a bejelentésköteles adatközvetítői szolgáltatásokat határozza meg – ez a kitétel már nem szerepel, azonban azt rögzíti, hogy szolgáltatások két- vagy többoldalú adatcserét foglalhatnak magukban, amelynek már a direkt-közvetítő is meg tud felelni. Végső soron, ha a DGA szabályozási célkitűzése a semlegesség volt, akkor ameddig ezt a közvetítő bizonyítani tudja azzal, hogy potenciálisan korlátlan számú fél között közvetít, akkor elméletben megfelelhet a DGA előírásainak (még akkor is, ha egy adott időszakban csak egy megbízója van).

- *Az adatpiactérként működő közvetítő*

Az adatpiactér egy olyan online platform,[1068] amely az adatközvetítést egy előzetesen felépített, általános jellegű informatikai keretrendszeren keresztül valósítja meg. Az adatpiactér a különböző adatjogi pozícióban levő ügyfelei által meghirdetett/keresett adatok vonatkozásában, automata vagy fél-automata eszközökkel hozhatja létre az üzleti kapcsolatot. Így az adatpiactér nem látja el egyedi igények szerinti adatoknak a felkutatását, csak azoknak az adatoknak a közvetítését végzi, amelyeket a jogosulti oldalon lévő felhasználók már előzetesen a felületen meghirdettek. Visszafelé is igaz a kijelentés, az adatpiactér – marketing tevékenységén felül – nem keres meg kifejezetten potenciális érdeklődőket egy hirdető felhasználója érdekében. A piactér ezért jellemzően adatfeldolgozói minőségben járhat el.

- *Az adatszövetkezetként működő közvetítő*

Az adatszövetkezet érintettekből, egyszemélyes vállalkozásokból vagy kkv-kból álló olyan szervezeti struktúra, amelynek az említettek a tagjai, és amelynek fő céljai, hogy támogassa a tagjait bizonyos adatokra vonatkozó jogaik gyakorlásában.[1069] Az adatszövetkezet így egy polgári jogi személyegyesülés formájában létező, adatközvetítő tevékenységet ellátó szervezet, amelynek kifejezett célja az egyesülést alkotó tagok adatjogi érdekeinek érvényesítése. Az adatszövetkezet e szerint egyszerre működik speciális adatközvetítőként és speciális, (data pooling-al vegyes) bizalmi adatkezelőként is, ahol az adatkezelő nem mások, hanem saját tagjainak adatait kezeli és közvetíti.

- *Az adataltruista szervezetként működő közvetítő*

A közvetítés legspeciálisabb esete az adataltruista szervezet által végzett tevékenység, amely alapvetően arra irányul, hogy közérdekű célokat támogasson releváns adatok adataltruizmuson alapuló, széles körű rendelkezésre bocsátásával. Az adataltruizmus egy olyan önkéntes adatmegosztás, amely az érintetteknek a rájuk vonatkozó személyes adatok kezeléséhez való hozzájárulásán, vagy az adatbirtokosoknak a nem személyes adataik felhasználására vonatkozó engedélyén alapul anélkül, hogy ezért a költség fedezésén felüli díjat számítanának fel vagy kapnának.[1070] Az adataltruista szervezetnek közérdekű célok teljesítése érdekében létrehozott jogi személy formájában, nonprofit alapon kell működnie és jogilag függetlennek kell lennie minden olyan szervezettől, amely profitorientáltan működik.[1071]

6.3.2.6. Az adatjogi szerződések alkalmazására vonatkozó általános javaslatokról

- Az adatjogi szerződések szerinti adatmozgás módjának és az adatállomány alapvető technikai paramétereinek meghatározásakor a címzett fél feldolgozási lehetőségeit és

[1067] DGA 2. cikk 11. pont
[1068] DGA 10. cikk a) pont
[1069] DGA 2. cikk 15. pont
[1070] DGA 2. cikk 16. pont
[1071] DGA 18. cikk

képességeit érdemes figyelembe venni (pl. formátum, szoftveres környezet és verzió, operációs rendszer), ellenkező esetben a megszerzett adatállomány használhatatlannak bizonyulhat. Ezért annak formátumával kapcsolatban egyértelmű és teljeskörű tájékoztatás lenne elvárható az adatokat megosztó fél részéről.[1072]

- Ha az adatot megosztó szerződéses vállalásai – főként előzetesen biztosított mintával (sample) igazolt módon – kiterjednek a felhasználhatóságra/hasznosíthatóságra való alkalmasságra, az átadások számára, gyakoriságára, vagy meghatározott eredmény kiváltása szempontjából visszamérhető adatminőségre, azokat a szerződés viszonylatában lényeges kérdésnek érdemes tekinteni.
- Amennyiben a megosztott adat valamilyen korlátozó szabály hatálya alatt áll (pl. szerzői jog), az adatot megosztó a címzettet olyan jogi és ténybeli helyzetbe kellene hozza, hogy az adatok a szerződéskötéskor kinyilvánított célzat szempontjából használhatóak legyenek a számára. E mozzanat nélkül az adat megosztásának lényege kiüresedhet, hiszen a gyűjtésben részt nem vevő, szerző fél valószínűleg csak aránytalanul nagy erőfeszítés árán kerülhet ilyen helyzetbe.[1073]
- A jogszerű megosztáshoz az állománynak a címzett által meghatározott és kinyilvánított célzat szerinti, és az azzal szoros összefüggésben előrelátható vagy járulékos használatra rendelkeznie kell minden jogszerűségi kellékkel, amelyek meglétéről alapvetően a szolgáltató tud gondoskodni. Ilyen kellékek lehetnek pl. személyes adatok esetén az érvényes jogalap és annak megfelelő adatgyűjtés, illetve az elszámoltathatóságot biztosító dokumentáció. Ez egyfelől a gyűjtött adat gyűjtéskori jogszerűségét, a jogszerűség címzett általi ellenőrizhetőségét és végső soron a jogellenes adatállományok terjedésének meggátolását szolgálhatná. A jogszerűségi kellékek meglétének részletes vizsgálatát a címzettől egyébként nem tűnik életszerűnek elvárni, de azok nyilvánvaló hiányának figyelmen kívül hagyása a címzett számára a jogellenes adatkezelésből eredő következmények alóli mentesülés megszűnését eredményezheti.
- Az átadott állománnyal kapcsolatban célszerűnek mutatkozik, ha a szolgáltató – ha ilyenek vannak, akkor a szolgáltató által képviselt személyek érdekeire, álláspontjára tekintettel – a tranzakciót megelőzően használati feltételeket állapíthatna meg vagy a címzett előzetesen bemutatott használati céljait jóváhagyhatná.[1074] Ezen kötelezettség a címzettet időbeli korlát nélkül kellene kösse.[1075] A kötelezettség ilyen szerződési kikötés esetén vonatkozhat az átadott állomány alapján létrehozott új, származtatott adatokra is.[1076]
- Jó gyakorlatnak tűnik, a megosztás során megszerzett állomány feldolgozása tekintetében a címzettet a szerződésben rögzített célokhoz kötni. Annak érdekében, hogy ez ne jelentsen aránytalan terhet a szerző fél számára a feldolgozás következtében esetlegesen létrejövő új adat esetén (tercier adatszerzés) a szolgáltatótól megkövetelhető lehetne, hogy a címzett jogszerzését aránytalanul nem korlátozza. A feldolgozás formája, módja és időtartama a szerződés lényeges körülményének minősülhetne.
- A DGA, az EHDS javaslat és a Nah.tv. által bevezetett anonimizálási/pszeudonimizálási eljárások lefolytatását célszerű lenne az adatokhoz hozzáférést biztosító félhez telepíteni, ezzel pl. a szükségtelen személyes adatok mozgását meg lehetne gátolni
- Az adatjogi szerződések tartalmi elemei közül az alábbiakat lehet érdemes rögzíteni:

[1072] A használható formátum jelentőségét számos elírás hangsúlyozza, például az FFNPDR 6. cikke
[1073] Felfogható egyfajta jogszavatossági kikötésként is
[1074] Hasonlóan a DGA és a Nah.tv. előírásaihoz
[1075] ALI-ELI Alapelvek 52 o.
[1076] Elsődleges jogtól függetlenül létező, egyfajta szerződéses önkorlátozásként az ilyen kikötés érvényes lehet.

- Az érdekelt feleket: szerződő feleket, az adatforrás legalább csoport szerinti, legfeljebb pszeudonim azonosítását;
- A szerződés tárgyát:
  - a szerződésnek megfelelő adatmozgás és műveletvégzés pontos meghatározását (feldolgozás formája, módja és időtartama), a felhasználási és hasznosítási korlátozásokat és/vagy a tervezett műveletek cél szerinti meghatározását;
  - az adatkör azonosítását, paramétereit (különösen típusát, kategóriáját), a forrásadatkezelés paramétereit (cél, felhatalmazás, tárolási idő [ha van]), az átadás módját (pl. email csatolmányként) és formáját (átruházás vagy megosztás) a szerzés jogalapját/jogcímét.

6.4. A horizontális minimumszabályozás lehetőségei

Az eddigiekben javaslat szintjén tisztáztuk az adat jogi megítélését, a horizontálisan érvényesülő relációs jogokat és az adatjogi szerződések lehetséges tipológiáját. A hiányterületeknél a horizontális adatjogi befejezetlenség utolsó okozójaként a nem személyes magánadatokra irányadó szabályanyag elégtelensége került megjelölésre. Személyes adatok esetén ugyanis a jogvédelem és az adatforrásvédelem is részletesen szabályozott az adatvédelem által, közadatok esetén a védelem pedig eljárási jellegű (pl. döntéselőkészítő adat kiadásának[1077] és ismételt adatigénylés megtagadhatósága[1078]) a nyílt közadatok jogpolitikai célzatának megfelelően. Ez a helyzet nem személyes magánadatoknál kevésbé egyértelmű. A DGA egyik mérföldkő jellegű jogalkotási lépése, hogy nem személyes adatokra és jogi személy jogosultakra is védelmi előírásokat vezetett be, de ezt csak közszférabeli szervezetek hasznosítási tevékenységében tartja irányadónak. Így a jogalkotói elhatározás azt gondolom azonosítható, de az ilyen adatokra vonatkozó rendelkezések koherenciája mellett az adatjogi konzisztencia is növelhető lenne, az egyes szabályozási területek egységes, jogpolitikai célokkal arányos szintre hozásával. Ez egyrészt az önszabályozásnak teret engedő, erős piaci szereplők önvédelmének túlnövekedését – tehát a globális használat serkentését – is szolgálhatja, de az előírások harmonizációján keresztül könnyebb, átláthatóbb jogalkalmazást is eredményezhetne. Ennek érdekében olyan szabályokra teszek javaslatot, amelyek a nem személyes magánadatok horizontális védelmével és kezelésével kapcsolatos minimumkövetelményekre irányulnak, ezzel a GDPR valódi párjaként a meglévő adatjogi aktusok (különösen az FFNPDR és a DA) gyenge pontjaiból eredő problémákat orvosolhatják. A szabályozási keretek megerősítésére meglévő előírások tovább gondolása – elsősorban a GDPR rendelkezései – mutatkoznak célszerűnek. A GDPR szabályanyaga (mint az EU digitális jogának sarokköve,[1079] és az adatjogi konvergencia központi eleme) által inspirált megoldások eszközt adhatnak arra, hogy egy skálázott és hézagmentesebb adatjogi szisztémát kaphassunk. Még akkor is, ha nem személyes adatok esetén egyértelműen enyhébb előírásokra van szükség, úgy gondolom, hogy szükséges valami, ami irányt mutat és végső esetben határt szab az adatalapú folyamatoknak. A GDPR egyes előírásainak szervező és rendszerteremtő ereje erre megoldást jelenthet, mivel nemcsak több szinten rétegzett védelmi előírásokat tartalmaz, hanem az operatív adatfelhasználási és adathasznosítási működésre is számottevő közvetett hatással bír (ezért is említettük a védelmet, mint a *hogyan* jogát). Ez kiindulópontként egy általános szemléletű adatjogi keretrendszer kialakításával és a jogi személy adatforrások legalább alapszintű védelmének kialakításával lehetne elérthető, melyeknek kevésbé az erős garanciákat,

[1077] Info.tv. 27. § (5)-(6) bekezdések
[1078] Info.tv. 29. § (1a) bekezdés szerint az adatigénylésnek az adatot kezelő közfeladatot ellátó szerv nem köteles eleget tenni abban a részben, amelyben az azonos igénylő által egy éven belül benyújtott, azonos adatkörre irányuló adatigényléssel megegyezik, feltéve, hogy az azonos adatkörbe tartozó adatokban változás nem állt be.
[1079] COM(2024) 357 final, 16 o.

sokkal inkább az „adatjogi tisztánlátást” kellene szolgálniuk, lehetőséget biztosítva arra, hogy a már létező szabályok (pl. DA, DGA) kibontakozhassanak. Az újonnan javasolt minimum szabályozásnak az adatjogi egyensúlyt felállítva, a személyes adatok és természetes személyek *mellett*, a nem személyes adatokra és jogi személyekre *is* irányadónak kellene lennie. Tehát a javasolt horizontális szabályok mindkét adatforrásra és adatkategóriára irányadóak lehetnének, azzal, hogy ahol az adatvédelem szigorúbb szabályt már létrehozott, ott az alkalmazási elsőbbséggel rendelkezik.

6.4.1. A horizontális minimumszabályok megalkotásának lehetséges okairól

6.4.1.1. A magánszféravédelem lehetőségéről jogi személyek esetén

Röviden áttekintve a szabályozás indokoltságát, először érdemes visszagondolni a magánszféravédelemnél leírtakra. Westin kutatásai nyomán a magánszféra védelmét a territoriális viselkedéssel állítottuk párhuzamba, ami továbbélésével a civilizált létezésnek is egy egészen alapvető funkciójává alakult. Erre alapozva azt is mondhatjuk, hogy az egyfajta szociális immunrendszer[1080] szerepét is ellátja a mindennapjaink során. A modern társadalmak, bár a kezdeti törzsi szintet már rég meghaladták, az együttélés szabályait továbbra is hasonló logika mentén határozzák meg, amire akár a COVID járványra adott állami reakciók is példaként hozhatók. A pandémia idejében a rendkívüli jogalkotás által szintén egyéni, családi/háztartási és közösségi szintek mentén kerültek létrehozásra a járvány terjedésének megelőzését szolgáló intézkedések, mint például a karantén vagy a kijárási tilalom. Ezek az intézkedések egy össztársadalmi védekezőrendszerként szolgáltak és ezzel analóg módon képzelhetjük el a magánszféravédelem szociális immunitás jellegét is. A COVID alatt a védelem azokra irányult, akiknek a jogaira (élethez és egészséghez való jog) a járvány veszélyt jelentett, ez alapján a társadalmi immunreakciók azokat fogják védeni, akik a társadalom tagjai és az érdekeikre jelentett veszélyek enyhítésre szorulnak. Bár emberi méltósággal értelemszerűen nem rendelkezhetnek, mint a társadalom – jog által létrehozott – tagjai akár a jogi személyek is igényt tarthatnak a privátszféra valamilyen szintű védelmére, ha az érdekeikre jelentett veszélyek enyhítésre szorulnak (amilyen érdekeket pl. a versenyjog is elismer és védendőnek tart[1081]).

6.4.1.2. A személyiségvédelem lehetőségéről jogi személyek esetén

Magánjogi szempontból azt mondhatjuk, hogy a jogi személy jogképes,[1082] tehát jogalany.[1083] A Ptk. szerint a jogi személy jogképessége ráadásul abszolút, mivel az kiterjed minden olyan jogra és kötelezettségre, amely jellegénél fogva nem csupán az emberhez kapcsolódhat,[1084] továbbá a személyhez fűződő jogaira a személyiségi jogokra vonatkozó általános szabályokat rendeli alkalmazni, minden olyan esetben, amikor a védelem a jellegénél fogva nem csupán az embert illetheti meg.[1085] Az látható, hogy a hatályos polgári jog a jogi személyt jogalanyként a

---

[1080] A szociális immunrendszer alapvetően egy csoport patogénekkel szembeni kollektív védekezési mechanizmusaként írható le. A jelenség főként államalkotó életmódot folytató rovarok esetében került vizsgálatra, lásd részletesebben: Sophie Van Meyel, Maximilian Körner, Joël Meunier, Social immunity: why we should study its nature, evolution and functions across all social systems, Current Opinion in Insect Science, Volume 28, 2018, 1-7 o.

[1081] Lásd például: a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról szóló 1996. évi LVII. törvény 3. § szerint „tilos valótlan tény állításával vagy híresztelésével, valamint valós tény hamis színben való feltüntetésével, úgyszintén egyéb magatartással a versenytárs jó hírnevét vagy hitelképességét sérteni, illetőleg veszélyeztetni.”

[1082] Ptk. 3:1. § (1) bekezdés

[1083] Sárközy, 2016. 47 o.

[1084] Ptk. 3:1. § (2) bekezdés

[1085] Ptk. 3:1. § (3) bekezdés

természetes személlyel egy sorba hozza, így az ésszerűség határain belül, de azzal egyenlővé tette.[1086] A polgári jogi személyiség létének tekintetében azonban a megkülönböztetett pozíció ellenére nincs konszenzus, mivel annak fizikai világban való manifesztációja (a személy- és vagyonegyesítő jelleg, illetve a képviselethez kötöttség miatt) számottevően eltér az emberétől. A személyiségük részleges megléte a hatályos jog és a szakirodalom alapján is elfogadhatónak tűnik,[1087] amit a joggyakorlat is megerősíteni látszik. Szalai szerint a jogi személyek személyiségvédelmének terjedelme egyre bővül, ami által értelemszerűen szűkül azon jogok köre, amelyek „természeténél" vagy „jellegénél" fogva csak az embert illethetik meg.[1088] A modern folyamatok erre pedig egyértelműen erősítő hatással bírnak. Fontos azt látni, hogy nem csak a természetes személyek virtualizációja történik a kibertérben, hanem a jogi személyeké is. Az állami szervek és a vállalatok online megjelenései és a közösségi média tevékenyége már sokkal kevésbé tér el az emberekétől, mint a fizikai valóságban. Attól függetlenül, hogy nem egy, hanem akár több ember munkájának eredménye, egy jogi személy is önálló karakterisztikát, egyedi – szinte antropomorf – személyiségjegyeket szerez és hordoz miközben pl. posztol vagy kommentel.[1089] Így végső soron érdemes lehet a jogi személyeket, mint emberek kollektívája által életre keltett, virtuálisan (jog általi fikcióként) létező, személyhez fűződő jogi jogalanyisággal rendelkező[1090] személyiségeket kezelnünk.

6.4.1.3. Nem személyes adatok védelmének lehetőségéről

A jogi személyek mellett fontos lehet a nem személyes adatokra külön fókuszáló (további) előírások megfogalmazása is. Ennek a szükségét alapvetően a már korábban a kimenetek biztonsága körében kifejtett „adatok diktatúrájának" a lehetősége és az a felismerés kell adja, hogy az egyénekre káros hatással járó adatkezelési műveletek nem csak személyes adatokkal végezhetők, így a védelem egy része a nem személyes adatokra is ki kellene terjedjen. Erre jó példákat találhatunk az algoritmizáció területén. Ebben általában megbúvó aggályok az algoritmizált elfogultság és a fekete doboz jelenség. Előbbi az un. „algorithmic bias" jelensége, amiben szoftverhiba vagy a fejlesztéskor használt tanítóadat torzítása / torzulása az MI rendszer diszkriminatív működéséhez vezet. Ez jóhiszeműséget feltételezve nem tekinthető szándékolt hatásnak a fejlesztők részéről, hiszen könnyen elképzelhető (főleg történelmi adatbázisok esetén[1091]), hogy egy olyan régóta meglévő, de addig azonosítatlan megkülönböztető gyakorlat az ok, amit az algoritmus mindössze felerősített.[1092] Adatvédelmi szempontból (az egyéb alapjogsérelem mellett) súlyos következményekkel járhat az ilyen diszfunkcionális működés – függetlenül az októl és a szándéktól – hiszen egy hátrányosan megkülönböztető módon működő

[1086] Rácz Lilla, „A jogi személyek személyiségvédelme – képzelet vagy valóság?", In: Görög Márta, Menyhárd Attila, Koltay András (Szerk.): A személyiség és védelme. Budapest, Felelős kiadó az ELTE Állam- és Jogtudományi Kar dékánja, 2017. 354 o.

[1087] Sárközy, 2016. 49 o. „A személyiségi jogok, illetve ezek jogvédelmi eszközei a jogi személyeket is megilletik, (…) így például a jóhírnév védelme kapcsán, az emberhez hasonlóan ebben a körben is lehetne személyiségről beszélni."

[1088] Szalai Ákos, „A szervezetek jogi személyiségének mennyiségi elmélete", In: Menyhárd Attila, Gárdos-Orosz Fruzsina (Szerk.): Személy és személyiség a jogban. Budapest, Wolters Kluwer, 2016. 84 o.

[1089] Kétségtelen, hogy ennek egyértelmű marketing céljai vannak. Lásd részletesen: Abas Mirzaei, Dean Charles, Hugh Wilkie, Amelie Jay Burgess, „Does human value-expressive brand anthropomorphism on social media lead to greater brand competitiveness?", Journal of Retailing and Consumer Services, Volume 81, 2024; Carlos Eduardo Lourenco, Juliana Correa Ferreira, Vanessa Martins dos Santos, „Humanizing brands in social media: The impact of anthropomorphism on brand identification, engagement, and advocacy", Journal of Marketing Communications, 1–22.

[1090] Görög Márta, „A jogi személy személyi értéke", JK, 2011/11., 572-573. o.

[1091] Edwards, Lilian „Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?" IEEE Security & Privacy (2018) 16(3), 46-48 o.

[1092] Chander, Anupam „The Racist Algorithm?" *Michigan Law review, Volume 115, Issue 6.* (2017) 1028-1030 o.

algoritmus szerinti adatkezelés óhatatlanul jogellenességet fog megvalósítani.[1093] Az algoritmizált elfogultsághoz hasonló, generálisan jelenlévő aggály a legtöbb fejlett MI rendszer immanens részét képező, un. fekete doboz (black box) jelenségből ered. A jelenség lényege, hogy az algoritmus működése során az input oldal és az output oldal közötti követhető kapcsolat megszűnik a külső szemlélő számára. Vagyis ezekben az esetekben tisztázott a bemeneti és kimeneti oldal adattartalma (az, hogy milyen adatok alapján, milyen eredmény jött létre), de a kettő közötti ok-okozati összefüggés (miért ez az eredmény jött létre a megadott adatok alapján) nem, vagy csak nagyon nehezen ismerhető meg.[1094] Ez adatvédelmi szempontból alapelvi szinten okoz problémákat az átláthatóság hiánya miatt, de az érintetti jogok tiszteletben tartása és a jogérvényesítés elősegítése is komoly akadályokba ütközhet. Az adatjogi megfontolások mellett egyéb alapvető emberi jogok (emberi méltóság, egyenlő bánásmód) is veszélyeztettek lehetnek, továbbá ágazati és eljárási szabályok is sérülhetnek.[1095]

6.4.2. A horizontális minimumszabályozás elemeiről

6.4.2.1. A szabályok módszeréről

Az említett okokból az adatjog horizontális zártságát és hézagmentességét, az érdekek kiegyenlítését és az említett adatjogi tisztánlátást biztosítani lehetne a személyiségre és a fennálló érdekeltségre tekintettel megvalósuló szabályok létrehozásával. Így személyükre tekintettel védettek lehetnének a természetes személyek mellett a jogi személyek is[1096] és egy személyi vagy társadalmi érdekeltségre tekintettel védelmet kaphatnak olyan adatforrások is, amelyek jogtárgyak, tehát nem rendelkeznek jogképességgel (épített és természetes környezet, élettelen tárgyak, állatok). Jogtárgyak esetében a védelemnek csak akkor és annyiban szabadna megvalósulnia, amikor és amennyiben azt a jogképtelen adatforrás felett rendelkezni képes személy vagy a társadalom szélesebb érdekei megkövetelik. Itt gondolhatunk pl. egy ingatlanra vagy haszonállatokra, amelyeket így áttételesen a tulajdonosra tekintettel illethet meg valamilyen szintű adatjogi védelem. A jogképes, de nem természetes személyek alapvetően képviselőik útján jogi értelemben cselekvők, így a védelem ebbéli minőségüknek megfelelően alakulhat.

A horizontális védelem befejezettségét az alábbi irányvonalak mentén lehetne elérni:

- a természetes személyeket az alapjogoknak és az adatvédelmi jognak megfelelően,
- a jogképes, nem természetes személyeket a korlátozott, de létező személyiségvédelemnek megfelelően,
- a jogtárgyakat közvetve, az őket hatalomban tartók érdekeire tekintettel.

Érezhetően a természetes személyek védelme már létezik, de a koherensebb jogosulti és a teljesebb adatforrásvédelem eléréshez az alábbi konkrét megoldások járulhatnak hozzá:

- közös adatjogi fogalomrendszer megalkotása,
- az adatkezelésre való felhatalmazás általános előírásainak (jogalapok és jogcímek) létrehozása,

---

[1093] „Artificial intelligence: Algorithms face scrutiny over potential bias” BBC NEWS (2019) https://www.bbc.com/news/technology-47638916

[1094] Agencia Española Protección Datos (AEPD): Technologies and Data Protection in Public Administrations (2020)

[1094] Misuraca, Gianluca – van Noordt, Colin: Overview of the use and impact of AI in public services in the EU, (Publications Office of the European Union, Luxembourg, 2020) 36-37. o.

[1095] Mohay Ágoston, „A mesterséges intelligencia szabályozási perspektívái az Európai Unióban”, Kis Kelemen Bence – Mohay Ágoston (Szerk.): A technológiai fejlődés jogi kihívásai: Kézikönyv a jogalkotás és jogalkalmazás számára (Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2021) 72. o.

[1096] Megjegyezhető, hogy a magyar adatvédelem kialakulásának kezdetén, az Avtv. tervezeteiben még szerepelt olyan elgondolás, ami szerint a védelem kifejezetten kiterjedt volna a jogi személyekre és a jogi személyiséggel nem rendelkező szervezetekre. Lásd részletesen: Jóri, Soós, 2016. 53 o.

- személyiséggel rendelkező adatforrások általános minimumvédelmének szabályozása,
- értékegyenlőségi vizsgálat bevezetése (szükségesség és arányosság, hatásvizsgálat elvégzésének szabályai).

6.4.2.2. A közös fogalomrendszerről

A deklaráltan és rendszertanilag érvényesített közös, horizontális fogalmak használatának előnye lenne, hogy a bonyolultan kialakított vagy túlzottan részletekbe menő definíciók legfeljebb az ágazati szinten kellene megjelenjenek.

A GDPR alapján az *érintett* bármely információ alapján azonosított vagy – közvetlenül, vagy közvetve – azonosítható természetes személy. *Adatkezelés*nek minősül az adatokon végzett bármely művelet vagy a műveletek összessége, függetlenül az alkalmazott eljárástól. Ilyen művelet – a GDPR példálózó felsorolásában – az adatok gyűjtése, rögzítése, rendszerezése, tagolása, tárolása, átalakítása vagy megváltoztatása, lekérdezése, az azokba való betekintés, a felhasználás, a közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, az összehangolás vagy az összekapcsolás, a korlátozás, a törlés, illetve a megsemmisítés.[1097] Az a természetes személy vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza, és e döntéseket – maga vagy egy adatfeldolgozó megbízásával – végrehajtja, az *adatkezelő*.[1098] Az *adatfeldolgozás* fogalmát a GDPR nem, de az Info.tv. meghatározza, mely szerint az az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége.[1099] Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelő nevében személyes adatokat kezel, az *adatfeldolgozó*.[1100] Az adatkezelő és az adatfeldolgozó közötti jogviszonyból következően az adatfeldolgozó az adatkezelő utasításainak megfelelően végzi a tevékenységét, ő maga az adatkezelést érintő érdemi döntést nem hozhat. Felelőssége a saját tevékenységéért és a szerződésben vállalt szolgáltatásért, illetve annak színvonaláért áll fenn. Az általa az érintettnek okozott kárért az érintettel szemben az adatkezelő felel.[1101]

Az adatjogban az adatokon való műveletvégzés kardinális kérdés, a műveletek definiálása ezáltal szintén az. A GDPR adatkezelés fogalmának tág megfogalmazása és példálózó felsorolása rendkívül jól alkalmazható, nemcsak személyes adatok esetén, így ennek csak kiterjesztő értelmezésére lenne szükség. Az adatkezelési folyamatok és az adatkezelésben résztvevők esetén valamivel nagyobb szükség van a harmonizációra. A GDPR által nevesítettek az adatjog közjogias szabályozásának körébe sorolhatók és jelenleg kiemelten[1102] a személyes adatok esetén alkalmazandók. A fogalomrendszer harmóniája az adatjog GDPR szerinti és a jelen dolgozatban vázolt magánjogi szerepköreinek egymáshoz való viszonyán alapszik. Ezzel kapcsolatos magyarázó táblázat alább látható:

GDPR szerepkörök		*Új (magánjogi) szerepek*
Érintett, adatalany	↔	Elsődleges jogosult, adatforrás

[1097] GDPR 4. cikk 2. pont
[1098] GDPR 4. cikk 7. pont
[1099] Info.tv. 3. § 17. pont
[1100] GDPR 4. cikk 8. pont
[1101] GDPR 28-29. cikk
[1102] A közös fogalomhasználat nem példanélküli, az Info.tv. a közadatokat kezelő közfeladatot ellátó szervet is adatkezelőnek jelöli, lásd pl.: Info.tv. 28. § (3) bekezdés szerint ha a (közérdekű) adatigénylés nem egyértelmű, az *adatkezelő* legfeljebb 15 napos határidő tűzésével felhívja az igénylőt az igény pontosítására.

Adattárgy	↔	Adatforrás
Adatkezelő	↔	Elsődleges vagy másodlagos jogosult, adathasználó, de facto adattartó
Adatfeldolgozó	↔	Másodlagos jogosult (adattartó)
Harmadik fél	↔	Relációs kötelezett

Az ábra bal oldalán a GDPR által definiált szerepkörök láthatók, egy kiigazítással. Az angol szövegverzió az érintettet, mint adatalanyt (data subject) ismeri, ezt a kettőséget személyes adatok esetén a két kifejezés szinonímakénti használatával oldja meg a magyar adatvédelmi szókészlet. A kiigazítás – így mind magyar, mind angol nyelven – az adattárgy bevezetése (data object), ami a nem személyes adatok forrását jelöli, ezáltal az adatalany párját adja. Az adatkezelő magánjogi multipozíciója a tág GDPR definíciós határokból ered, mivel bárki annak tekinthető, aki (személyes) adatok kezelésének célját és eszközeit meghatározza. Mivel a használat részjogosítványánál a saját célból történő műveletvégzést adtuk meg, ezért az adatkezelő minden esetben adathasználó is. Az adatkezelői minőség objektív kritériumokat vesz figyelembe, ezért annak minősül a felhatalmazás nélküli adattartó is, ha az kellő autonómiával rendelkezik az adatokkal kapcsolatos döntések meghozatala tekintetében, függetlenül attól, hogy a folyamat jogellenes. Az adatfeldolgozó mindig feltételez egy rajta kívül álló adatkezelőt, akinek az érdekében adatokon műveleteket végez, ezért minden adat esetén csak mint másodlagos jogosult jelenhet meg. Az adatfeldolgozók az adatokon jellemzően valamilyen műveletet is végeznek, ezért szükségszerű adattartók is lehetnek egyben. A harmadik felek az adatkezelési folyamatban nem vesznek részt, ennek a magánjogi oldala az adatjog relációs jogvédelmi rendszerében a meg nem jelölt kötelezetti kör, vagyis mindenki más, aki az adott pillanatban nem jogosult. Megjegyzendő, hogy harmadik felek esetén sem az adatvédelmi, sem más jog nem zárja ki, hogy a folyamatba valamilyen formában belépjenek és maguk is jogosulttá váljanak.

A közös fogalomhasználat által az egységes jogalkalmazás könnyebbé válhat, mivel a szereplők fogalmi háttere állandó tartalommal rendelkezik. E mellett a részjogosítványok kiemelésével a szerepkör egyedivé tehető és részletezhető, de a közös dogmatikai alapok miatt az értelmezési nehézségek alacsonyabb szinten tarthatók.

6.4.2.3. Az adatjogi felhatalmazásról

Felhatalmazás alatt azt a jogilag és erkölcsileg helytálló hivatkozást vagy engedélyt érthetjük, amely ahhoz kell, hogy egyáltalán adatok kezelése történhessen. Ennek gyökere egyértelműen az adatvédelmi jogalapokban található, de az új adatjogi paradigmánkban a polgári jogi szerzésmódokkal is párhuzamba állíthatjuk. A polgári jog a szerzés eredeti és származékos válfajait ismeri, a kettő közti különbség, hogy származékos szerzéskor a jogot egy korábbi jogosult jogából eredezteti a szerző fél, míg az eredeti esetén ilyen jogról nem beszélhetünk.[1103] Az adatjogi felhatalmazásokat is ilyen módon két részre oszthatjuk.

- *Az adatjogi (GDPR szerinti) jogalapok*

A GDPR szerinti hat jogalap a másodlagos jogosultak adatkezelésre való felhatalmazását biztosítja, és így mint származékos szerzésmódok jelennek meg. Ennek elsődleges oka, hogy személyes adatokon az érintetten kívül más személy elsődleges jogot nem szerezhet. Azonban ez a tény nem azt jelenti, hogy nem személyes adatok feletti másodlagos jogosultság

[1103] Lenkovics, 2014. 110 o.

gyakorlására ne adhatnának ugyanezen típusú jogalapok felhatalmazást, tehát mindkét adatkategória esetén alkalmazhatók lehetnek.

Az adatok létrejötténél azt rögzítettük, hogy jogosultságot csak új adat felett lehet szerezni, a kapcsolótényezőknél pedig az volt látható, hogy nem személyes adatok esetén az azokat létrehozó vagy létrehozató szerez elsődleges jogosultságot. Ezekből kifolyólag a már létrejött nem személyes adat átvétele (másolása) nem vezethet elsődleges jog létrejöttéhez, mégis az ilyen adatmozgások rendszeresen előfordulnak a gyakorlatban. Vegyük példaként egy cég éves pénzügyi beszámolóját. Ezt a cég – vagy az érdekében eljáró könyvelő iroda – hozta létre, így az elsődleges jogot a cég szerzi meg. A beszámoló adattartalmának egy részét a cégnyilvánosság értelmében egy kormányzati oldalra fel kell tölteni, amelyhez így bárki hozzáférhet. A nyilvános adatokat ezáltal bárki kezelheti, de azon csak másodlagos jogot szerezhet, például a jogos érdeke vagy a fennálló közérdek szerint. Így végeredményben a tényhelyzet nem változik meg, viszont egy eszköz kerül az elsődleges jogosult kezébe arra az esetre, ha a nyilvános adatokkal kapcsolatban visszaéléseket tapasztal (pl. versenyjogilag még nem értékelt, de számára mégis sérelmes módon való feltüntetésük esetén).

A jogalapok alkalmazási kiterjesztése jótékony hatással lehetne a nem személyes adatokhoz való hozzáférésre és az ilyen adatok mobilizációjára. A GDPR hat jogalapját a szakirodalom egy része az alapjogvédelem szintjének csökkentésével azonosította,[1104] mivel lehetőséget adott személyes adatok kezelésére pl. az érintett hozzájárulása vagy törvényi előírás hiányában. Az álláspontom szerint ezt nem személyes adatok esetén fordítva kell értelmeznünk. A jogalapok lehetőséget adhatnának arra (a relációs jogosultsággal együttesen), hogy egy magánérdek vagy közérdek fennállásának bizonyításával bárki, bármilyen adatot kezelhessen, ezáltal megnyitva az utat (pl. platformok kezelésében lévő) nagy méretű adatkoncentrációk megbontására, és az azokhoz való hozzáférés lehetővé tételére.[1105] Gondoljunk csak bele, jelenleg a nem személyes magánadatok – a szabályozatlanság miatt – erősebben védhetők, mint a személyes adatok, hiába az alapjogi minőségük.

- *Az adatjogi jogcímek*

A származékos szerzésnél írtakkal szemben – ami legalább személyes adatok esetén biztosan létezik – eredeti jogosulti pozíció megszerzését lehetővé tevő, eredeti módon szerzett adatkezelésre való felhatalmazást biztosító jogintézményről jelenleg nem beszélhetünk. Ezeket a jogalapoktól való elhatárolás érdekében, mint *jogcímeket* jelölhetjük és alapvetően nem személyes adatok esetén tennének nagyobb jelentőségre szert, hiszen személyes adatoknál az elsődleges jogosultság megszerzése a kapcsolótényező alapján megtörténik az érintett vonatkozásában.

A jogalapok és jogcímek közti alapvető különbség tehát, hogy a jogalapok másodlagos (származékos) adatjogi jogosultság, míg a jogcímek elsődleges (eredeti) jogosultság létrejöttéhez vezetnek. A jogcímek célja, hogy igazolható felhatalmazást biztosítsanak a nem személyes adatok megszerzésére, ezzel támogatva az adatalapú folyamatokban részvevőket mindkét irányban felmerülő érdekeik védelmében. Tehát védelmet nyújthatnak az adatot jogcímesen szerzőnek, ezzel kiszámíthatóságot biztosítva az adatgazdasági folyamatokban

[1104] Arra alapozva, hogy a hozzájárulás szolgálja ki az érintett információs önrendelkezési jogát a leginkább, ezért, minden olyan eset, amihez nem szükséges az érintett döntése csökkenti a védelem szintjét. Megjegyzendő, hogy a hat jogalapból mindössze ez az egy igényli az érintett kifejezett döntését. Lásd például: Jóri András, „Adatvédelem: az alapjogvédelmi teszttől az érdekmérlegelésig", ABSz, 2018/1. 16-21. o.

[1105] A DA ehhez nagyon hasonló megoldást alkalmaz az IoT adatok rendelkezésre bocsátásának megkövetelésével a közszférabeli szervezetek, a Bizottság, az Európai Központi Bank és uniós szervek számára, egy rendkívüli igény (érdek) alapján. Lásd: DA V. fejezet.

érdekeltek számára. Másfelől támadhatóvá tehetik azokat, akik nem megfelelően szerzett adatokon végeznek műveleteket, így újabb – alulról szerveződő – lehetőséget biztosítva a versenyellenes adatkoncentrációk felszámolására.[1106]

A jogcímeket két részre oszthatjuk: kettő általános jogcímre és hat különös jogcímre.

- *Az érintett jogszerzése*

A jogcímek között szerepel az érintett saját személyes adatai vonatkozásában történő ipso iure jogszerzése, mint az egyetlen olyan jogcím, amely személyes adatok felett eredeti, elsődleges jog megszerzését teszi lehetővé. Erről már a kapcsolótényezőknél részletesen esett szó, így itt további magyarázatra nem kerül.[1107]

- *A tilalom hiánya*

Az adatgyűjtés és megosztás támogatását szolgáló, nem személyes adatok esetére vonatkozó általános jogcím a tilalom hiányaként jelölhető meg, tehát minden tényszerűségről rögzíthető és kezelhető nem személyes adat, amelyet valamilyen normatív előírás kifejezetten nem tilt és nem jár más jogalany sérelmével. Ez elsődlegesen az adatalapú működés szabadságát és az adatgazdasághoz szükséges akadálytalan adatáramlást hivatott biztosítani. A tilalom hiányával támasztható alá tehát nem személyes adatok esetén az alapértelmezett, eredeti adatszerzés.

- *Az átruházás*

Az átruházó jogügylet célja az elsődleges adatjogi jogosultság elidegenítése, amelynek következtében az, az eredeti jogosultnál megszűnik az újnál pedig létrejön. Az adatjogi logikában az átruházás által új, elsődleges jogosultság jön létre, függetlenül attól, hogy korábban az már fennált egy másik jogalanynál (tehát polgári jogilag származékos, de adatjogilag eredeti jogot eredményez). Fontos, hogy átruházásra csak nem személyes adatok esetén kerülhet sor, és arra is csak akkor, ha az adat-adatforrás kapcsolat nem áll fenn az átruházó vonatkozásában.[1108]

- *Egyetemes jogutódlás*

A római jogtól ismert univeralis successio jogintézménye adatok esetén is alkalmazhatónak mutatkozik, azonban némileg eltérő szabályok mentén. Személyes adatok jogutódlás útján történő (gyakorlatilag öröklése) a jelenlegi logika alapján kizárt, mivel személyes adat elsődleges jogosultja csak azonosított vagy azonosítható természetes személy lehet. Az elhunytra vonatkozó adatok – mivel nem természetes személy – már nem személyes adatok,[1109] amelyekre így eltérő szabályok vonatkoznak. Az Info.tv. 25. § alapján az érintett halálát követő öt éven belül jogszabályban meghatározott, az elhaltat életében megillető egyes adatokkal összefüggő jogokat az érintett által arra ügyintézési rendelkezéssel, illetve közokiratban vagy teljes bizonyító erejű magánokiratban foglalt, az adatkezelőnél tett nyilatkozattal – ha az érintett egy adatkezelőnél több nyilatkozatot tett, a későbbi időpontban tett nyilatkozattal – meghatalmazott személy jogosult érvényesíteni. Ez alapján az elhunytak életükben személyes adatnak minősülő, majd később nem személyes adattá alakuló állománya vonatkozásában a jogokat, a halál bekövetkeztét követő 5 évig örökösük gyakorolja. Az ilyen örökös adatjogi

[1106] Gondolhatunk például a DeepSeek és az OpenAI vitás helyzetére, amiben a relációs jogokkal együttesen az adatjogi felhatalmazások választ adhatnának arra, hogy milyen adatokat, melyik fél és miért kezelhet.
[1107] Lásd: 6.2.2.1. alfejezet
[1108] Az átruházás mellett a megosztás, mint kiemelt jogügylet másodlagos jogot eredményez, így annak végrehajtásához jogalapra és nem jogcímre van szükség, függetlenül attól, hogy személyes vagy nem személyes adatról van szó.
[1109] GDPR (27) preambulumbekezdés

szempontból tekinthető „pszeudo-érintettnek”, mivel jogaiban közel azonos az érintettel, azonban tényszerűen nem minősül annak.[1110] Az „örökölhető” jogok sporadikus jellegéből és az időbeli meghatározottságából azonban arra következtethetünk, hogy az adatjogi jogvédelem és adatforrásvédelem bizonyos szintű továbbélésének a célja az elhunyt személy emberi méltóságának, illetve személyiségének post mortem védelme[1111] és nem az adatjogi jogosulti helyzet rendezése. Összegzően azt mondhatjuk, hogy személyes adatok jogutódlás útján történő megszerzése kizárt, nem személyes adatokká alakult személyes adatok esetén, pedig a nem személyes adatok háramlására vonatkozó szabályokat kell alkalmaznunk. Fontos azonban, hogy az újonnan létrejövő jogosulti pozíciónak a tartalmára jelentős hatással lehet az ideiglenesen jogkezelő (örökös) személy a halált követő 5 évig, aki így az adatkezelési folyamatokat megszüntetheti, az adatokat akár töröltetheti.[1112]

Az egyetemes jogutódlás kérdése sokkal nagyobb relevanciára tehet szert egy jogalany létezésének megszűnésekor nála lévő és elsődleges jogot gyakorló teljes (nem személyes) adatállomány sorsának rendezésekor, ami mind természetes, mind jogi személyek esetén értékelendő. Mivel az adatokat, mint immateriális vagyontárgyakat azonosítottuk ezért az azokkal összefüggő jogoknak és kötelezettségeknek más javakhoz hasonlóan kellene átszállnia valamilyen új jogosultra, így a jogutódlást halál vagy megszűnés esetén bekövetkező átruházási műveletként is felfoghatjuk, azzal, hogy a jogelőd nyilatkozatában erről szabadon is rendelkezhet.[1113] Ez alapján az alábbi eseteteket különíthetjük el:

- ha a jogosult természetes személy, akkor a jogutódlásra az öröklési jog alapján kerülhet sor,
- ha a jogosult jogi személy, akkor a rá vonatkozó szervezeti jog (társasági jog, közigazgatási jog) alapján kerülhet sor a jogutódlásra,
- ha az adatok korlátozó szabály hatálya alatt állnak, az ott meghatározottak irányadók (pl. szerzői jog által meghatározott védelmi idő[1114]),
- az adatvagyon átszállásának akadálya esetén (pl. mert az örökös nem tart rá igényt, arról nem rendelkezik) a másodlagos jogosultak, a fennálló jogaik erejéig elsődleges jogot szerezhetnek (a hézagmentesség érdekében),
- végső esetben egyéb háramlási szabály és jogutód hiányában a nem személyes adatok árva adatnak minősülhetnek és az ezekre vonatkozó szabályok lennének irányadóak.

- *Tercier adatszerzés (a polgári jogi növedék/átalakítás)*

A primer vagy szekunder adatok – jogszerűségi előfeltételeket teljesítő – feldolgozása által létrejövő új adaton a szerzőképes feldolgozó elsődleges jogot szerezhet. Nem személyes adatok

[1110] Ilyen „pseudo-érintettnek” tekinthetjük a cselekvőképtelen vagy korlátozottan cselekvőképes személy képviselőjét, például egy gyermek szülőjét, aki a Ptk. 2:14. § alapján a gyermeke nevében eljár, lévén a cselekvőképtelen kiskorú jognyilatkozata semmis (az érintetti jog gyakorlásához szükséges nyilatkozat, mivel joghatás kiváltására irányul ezért, ebben a kategória esik).

[1111] Görög Márta, „A kegyeleti jog gyakorlásának jogosultjairól és az érvényesíthetőség időbeli korlátairól”, PJK, 2005/2., 15-19. o.

[1112] Jelenleg nem létezik, de elképzelhető lehet ezzel összefüggésben olyan speciális előírás bevezetése, amely meghatározza, hogy személyes adatok mely köre nem alakulhat át nem személyes adattá, ami által erga omnes hatályú törlési kötelezettség lenne létrehozható. Például ez elképzelhető egy olyan jövőbeli technológia esetén, amely az emberi gondolatokat képes kivonatolni és rögzíteni (pl. exocortex, lásd 2.3.1. fejezet). Az ilyen kivonatok magas fokú érzékenységére tekintettel még a legközelebbi hozzátartozók sem biztos, hogy hozzá kell férjenek).

[1113] Vékás Lajos: Magyar polgári jog – Öröklési jog. Budapest, Eötvös József Könyv- és Lapkiadó Bt., 2014. 15-17 o.

[1114] Az Szjt. 31. § (1) bekezdés szerint a szerzői jogok a szerző életében és halálától számított hetven éven át részesülnek védelemben. Az Szjt. 9. § (4) bekezdés szerint a vagyoni jogok örökölhetők, róluk halál esetére rendelkezni lehet, vagyis a védelmi idő alatt az örökös gyakorolja.

esetén ez további magyarázatra nem szorul, hiszen a kapcsolótényezők alapján egyébként is a létrehozóhoz kerül a jogosultság. Személyes adatokon is van lehetőség közvetve a jogszerzésre, de csak abban az esetben, ha az új adatnak az adatalanyhoz való kapcsolata visszaállíthatatlanul megszűnt, ezáltal a személyes adat jellegét elveszítette. Megjegyezhető, hogy az adatok feldolgozása által létrejött adaton az elsődleges jog az újszerűség tényéből ered (amelynek korlátja, hogy nem minősülhet személyes adatnak), azonban magához a feldolgozáshoz – mint adatkezelési művelethez – is már szükség lehetett valamilyen korábbi felhatalmazásra. Ez lehetett olyan egyszerű, mint a tilalom hiánya vagy olyan bonyolult, mint az érintetti hozzájárulás menedzselése.

Személyes adatok esetén a tercier adatszerzés egy kiemelt művelete így az adatok anonimizációja, mivel ezzel a személyes jelleg megszüntethető. Az anonimizálás következtében a forrás és az adat közti kapcsolat végérvényesen megszűnik, függetlenül attól, hogy az egyéb tartalmak megváltoztak-e vagy sem. Itt tehát nem az adat tartalmi újdonsága a mérvadó, hanem az adat-adatforrás közti kapcsolat megszakadása. Ezért személyes adatok esetén, ha a tercier adat még kapcsolatba hozható az eredeti adatalannyal, akkor az elsődleges jogosultság megszerzéséhez az adatok anonimizációjára is szükség van.[1115]

- *Derelinkvált adat megszerzése (a polgári jogi elsajátítás)*

Itt a technikai értelemben – tehát metaadatok által sem azonosítható jogosulttal rendelkező, nem személyes minőségű – elhagyott adatok, vagy a jogosultnak a szerzőképesség hiányában történő kiesése merülhet fel. A derelinkvált adatok megszerzésére a fentebb részletezett árva adatokra irányadó szabályok alkalmazásával mehet a jogszerzés végbe.[1116] Így ha erre alkalmas, akkor az adatforrás szerezhet elsődleges jogot a nem személyes adatokon, függetlenül attól, hogy azokat nem maga hozta létre. Ennek hiányában (ha az adatforrás ezt nem kívánja vagy maga is szerzésképtelen) a közkinccsé vált adaton az állam egy erre kijelölt szervén (pl. NAVÜ) keresztül szerez szükségképpeni elsődleges jogot.

- *Közösen létrehozott uniform vagy diverz adatbázis feletti többes jogosultság szerzése (a polgári jogi egyesítés vagy vegyítés)*

Az új adatbázis elválaszthatatlan részeként, de változatlan formában maradó és tartalommal rendelkező, azonos adatkategóriába tartozó adatok esetén az adatbázis egésze felett többes elsődleges adatjogi jogosultság jöhet létre. Kérdés, hogy milyen személyi kör és milyen alapon lehet részese ennek a jogszerzésnek, amely az adatbázisban szereplő adatok kategóriájától és a részvétel típusától függ. Egyértelmű a kapcsolóelvek alapján, hogy személyes adatok esetén elsődleges jogát megtartja az érintett, nem személyes adatok esetén pedig az adatot létrehozó. Így személyes adatok esetén a természetes személyek, nem személyes adatok esetén az adatokat létrehozók kerülnek többes elsődleges jogosulti pozícióba. Felmerülhet még az adattárgy (nem természetes személy adatforrás) jogszerzése. A jogosultságszerzés itt a kapcsolótényezők alapján alapértelmezetten nem mehetne végbe, ahhoz az adattárgy hozzáférési jogával kell először éljen.[1117] Ebben az esetben viszont már mint elsődleges jogosult szerez jogot, függetlenül az adatbázis lététől. Az adatbázis létrehozója az utolsó érdekelt fél a folyamatban, amely adott esetben elkülönülhet az eddig ismertetett jogosultaktól. Mivel eredeti adatjogi jogosultság új adat létrejötte esetén – a kapcsolótényezőknek megfelelően – valósulhat meg, ezért az adatok egyesítésekor vagy vegyítésekor, tekintve, hogy kompiláció során a beemelt

[1115] Ezért a DGA, a Nah.tv. és az EHDS javaslat adathozzáférést megelőző kötelező anonimizációra, valamint a visszaazonosítás tilalmára vonatkozó előírásai nagyon előnyösen lehetővé tehetik az adathoz hozzáférő számára az elsődleges jog megszerzését. Lásd: 4.3.3.4., 4.3.4.1. és 4.3.5.1. alfejezetek
[1116] Lásd: 6.2.2.2. alfejezet
[1117] Lásd lentebb

adatok változatlan formájúak és tartalmúak, új adatok nem jönnek létre. A kompilált adatbázis alapján létrehozott új (kimeneti) adatok vonatkozásában pedig a tercier adatszerzés jogcíme alapján jön létre elsődleges jog, ha erre egyáltalán sor kerül. Ezek alapján az adatbázis létrehozója az adatbázis létrehozásához szükséges műveletek elvégzéséhez csak másodlagos jogot szerezhet az eredeti jogosultaktól. A létrehozónak egyébként a szerzői jog kompozit előírásai biztosíthatnak védelmet, feltéve, hogy az adatbázis gyűjteményes műnek minősül, vagyis, ha a tartalmának összeválogatása, elrendezése vagy szerkesztése egyéni, eredeti jellegű.[1118]

- *Jogszabályon vagy közhatalmi aktuson alapúló elsődleges jogszerzés*

Az adatjogi relációs jogosultságok jogkérdések és nem ténykérdések. Nem személyes adatok esetén elsődleges adatjogi jogosultság jog által is létrehozható, például egy kötelezően ellátandó feladat hatáskörének jogszabályi címzésével. Ilyenkor az elsődleges jog – hasonlóan a személyes adatokhoz – de iure jön létre. E mellett jogi kötelezettség állhat az adatrögzítés mögött is, ami a folyamatot indukálja és egyúttal legitimálja. Ebben az esetben nem az elsődleges jog kerül kiosztásra, hanem a nem személyes adatot rögzíteni köteles személy/személyi kör, ami által a jogszerzés gyakorlati okokból kell létrejöjjön (a kötelezettség teljesítéséhez szükségszerűen végzett adatkezelési műveletek által).

6.4.2.4. Az adatforrásvédelem alapjainak létrehozási lehetőségéről

Az adatforrásvédelem – jogi személyekre is kiterjedő – minimumkövetelményeit az adatjog hiányterületeként azonosítottuk. Ez a minimum védelem úgy gondolom, hogy ex post jogsérelmes helyzetek rendezésére kellen fókuszáljon, az adatok áramlásának lehető legkisebb mértékű akadályozása mellett. Az 1-3. jogok személyes adatok esetén már ennél erősebb formában léteznek, azonban a 4. pont joga minden adatkategória esetén alkalmazható lehetne.[1119]

- Az adatokhoz való hozzáférés joga, ami az érintetti hozzáférési jogával rokon, tehát egyfajta reaktív tájékoztatásnak is minősül. Az adattárgynak azonban a hozzáférésen keresztül biztosítja a saját adatai feletti elsődleges jog megszerzésének lehetőségét, amely anélkül, hogy elvonná az adatokat a kötelezettség címzettjétől méltányosnak tűnik.[1120]
- A jog arra, hogy amennyiben az adatokon végzett műveleteket sérelmesnek tartja azok megszüntetését kérhesse. Ez a tiltakozási jognak megfelelően a nem személyes adatok kezelésének utólagos jogszerűségi kontrollját adja az adatok forrásának. A jog célja az olyan kirívóan jogsértő helyzetek felszámolása lehetne, amelyek más jogterületek szabályozási köréből kiestek.[1121]
- Az adatok helyesbítésére vonatkozó jog, amelynek tisztán észszerűségi okai lehetnek, mint az elírások kiküszöbölése vagy fals adatok terjedésének megakadályozása. Ez az igény érezhetően nem csak az emberi méltóságot szolgálja, így – az adattárgy részéről megfelelő megalapozottság mellett – nem személyes adatok esetén is érvényesíthető lehetne.
- Egy arra vonatkozó jog, hogy az adatok által elért eredményben az adatforrás részesülhessen. A részesedéshez való jog a jelenlegi jogi környezet és jogtudományi

[1118] Szjt. 60/A. §
[1119] ALI-ELI Alapelvek 122 o.
[1120] Hasonló megoldást alkalmaz a DA 3. és 4. cikkeiben
[1121] Például a jelenleg hatályos Btk. alapján kegyeletsértést csak rágalmazás vagy becsületsértés útján lehet elkövetni a halott vagy emléke sérelmére. Az utólagos kontroll – pl. a hozzátartozók érdekeire tekintettel – megtörténhetne az elhunyt nem személyes adataival való visszaélés esetén is, ha az ténylegesen sérelmes, de nem felel meg a Btk. 226. § és 227. §-ben rögzített tényállási elemeknek.

diskurzus alapján is elrugaszkodottnak tűnhet, hiszen még az adatok monetizációjának lehetősége és az adatok forgalomképessége is a szakirodalom számára megosztó kérdések. A részesedés tekintetében azonban olyan egyszerű megoldás is szóba jöhet, mint a (természetes vagy jogi) adatforrás tájékozódása az eredményről és az adat értékéről.[1122] Ez például pénzben nem kifejezhető eredmény esetén akár az ahhoz való hozzáférést is jelentheti, pl. egy kutatás alapján létrehozott publikációnak díjmentesen történő megszerzésével. Pénzben kifejezhető eredmény esetén az abból való részesedés egy érzékenyebb terület, ráadásul az összegszerűsítés is aggályos lehet. Azonban a szakirodalom az ilyen jog létrehozásától sem zárkózik el.[1123] A részesedést a parttalanság elkerülése érdekében célszerű lehet könnyen értelmezhető feltételekhez kötni:[1124]

- az adat kellően egyedi,
- *és* az eredmény kellően nagy mértékű,
- *feltéve*, hogy az adat létrejöttekor az adatforrásnak nem volt lehetősége jogosultként részt venni a folyamatban.[1125]

6.4.2.5. Az értékegyenlőség vizsgálatáról

Az értékegyenlőségi elvet, mint az adatalapú folyamatokat szabályozó jogot a háttérből mozgató *szabályszerűen érvényesülő tendenciaként* azonosítottuk.[1126] Az értékegyenlőség kimondatlan vizsgálata a személyes adatok esetén a GDPR előírásai által jelenleg is megvalósulnak, mint ex ante előírások. Ezeknek általános megkövetelése egybecseng az uniós jogalkotás arányosságon alapuló megközelítésével,[1127] nem személyes adatok esetén akár ex post számonkérhetőségével. Tehát a szabályozási javaslat lényege az elv intézményesítése, vagyis a létének elismerése és annak megfelelő működés megkövetelése, valamint annak egyedi vizsgálatának legalább utólagos lehetővé tétele és az erre hivatott szerv kijelölése. Az elv vizsgálatának eszközei az adatvédelemből is ismert szükségesség és arányosság vizsgálata, valamint a hatásvizsgálat elvégzése.

- *A szükségesség és arányosság vizsgálata*

Személyes adatok esetén a GDPR eszmerendszere az adatkezelési cél elérésére való szükségességének és a beavatkozás arányosságának egyenletére alapoz több esetben, így például a GDPR 6. cikk (1) bekezdés e) és f) pont szerinti jogalapok esetén, vagy a 35. cikk (7) bekezdés b) pontjában a hatásvizsgálat tartalmánál. Az adatvédelem vonzáskörén kívül is bőven találhatók hasonló megoldási mechanizmusok, mivel a szükségességi-arányossági vizsgálat gyakorlata alapvetően a második világháború utáni emberi jogvédelem alaptételévé vált.[1128] Adatjogi szempontból a teszt alapelvi szinten jelenhetne meg, a kötelezetti köre pedig minden adattal kapcsolatba kerülő, illetve az adatok kezelésére hatást gyakorlóra kiterjedhetne. A teszt egyfelől az értékegyenlőségi mércén való elhelyezést kellene szolgálja, másfelől egy olyan

[1122] Malgieri, Custers, 2018. 2 o.
[1123] Bergemann et al., 2023. 1064 o.
[1124] A szerzői jog „bestseller-klauzulájához" hasonlóan a részesedés arányossága a cél, így annak pénzbeliségéhez az eredménynek jelentősnek és nem vártnak, az adatforrás adatának pedig kellően egydinek kell lennie. Lásd részletesen: Grad-Gyenge Anikó (Szerk.): Kézikönyv a szerzői jog érvényesítéséhez, ProArt Szövetség a Szerzői Jogokért, 2013. 108-109 o.
[1125] ALI-ELI Alapelvek. 165-167 o.
[1126] Lásd részletesen: 3.4. fejezet
[1127] Gondolhatunk például az alapvetőjogi hatásvizsgálat (FRIA) bevezetésére, ami végső soron szintén az értékegyenlőség fennállásának vizsgálatára irányul, lásd részletesen: Heleen Janssen, „Detecting New Approaches for a Fundamental Rights Impact Assessment to Automated Decision-Making", International Data Privacy Law, Volume 10, Issue 1, February 2020. 76–106 o.
[1128] Székely, Somody, Szabó, 2017. 8. o

generálklauzula szerepét tölthetné be, amely az adatalapú folyamatok rendkívül gyorsan változó közegében egy állandó szempontrendszert jelentene, ezáltal megkönnyítve az értékelésüket.

Gyakorlati szempontból a teszt a – hasonlóan a személyes adatoknál megszokott módszerhez – következőképpen működhetne: magába foglalhatná a kombinált, tényeken alapuló értékelését az adatkezelés hatékonyságának a kitűzött cél tekintetében, valamint annak a vizsgálatát, hogy kevésbé avatkozik-e be a magánszférába (személyes adatok esetén) vagy a fennálló társadalmi rendbe (nem személyes adatok esetén) ugyanazon cél elérésének más lehetőségeivel összehasonlítva. Mivel valamilyen szintű beavatkozást szükségszerűen megvalósít minden adatkezelés ezért tartalmazhatná az adatkezeléshez kapcsolt enyhítő intézkedések és garanciális szabályok értékelését is.[1129]

A szükségességi-arányossági vizsgálatra vonatkozó előírások és módszertanok javarészt jól alkalmazhatóak nem személyes adatok esetén, a lényegi különbség a hatókör meghatározásában húzódhatna. A teszt elsődleges szerepe az értékegyenlőség vizsgálatában rejlik, így ha az adatkezelés kellőképpen szükségesnek és arányosnak mondható – tehát a mögötte álló össztársadalom által méltányolt érdek elég nagyfokú – akkor az adatok felhasználásáról beszélünk. Ha az adatkezelés szükségessége önmagában nem igazolható vagy a vizsgálatok alapján túlzónak vagy aránytalannak bizonyul, de még nem tekinthető jogellenesnek akkor az adatok hasznosításáról lehet szó (ilyenkor az érdek legitimációja össztársadalmi szinten nem egyértelmű, annak alátámasztásához további intézkedésekre van szükség). Amennyiben az adatkezelés kellően nagy mértékben szükségtelen vagy aránytalan akkor az adatkezelés jogellenesnek minősül (az érdek illegitim vagy azt az össztársadalom nem méltányolja). Személyes adatok esetén a jogszabályi környezet jelenleg is ebbe az irányba mutat, nem személyes adatok esetén a helyzet csak bizonyos ágazatok szintjén szabályozott (pl. MI jog). Az új adatjogi paradigmában a szükségesség-arányosság tesztjét tehát minden adatkategóriára érdemes lenne kiterjeszteni azzal a különbséggel, hogy személyes adatok esetén a legmagasabb szükségességet és arányosságot kellene bizonyítani, míg nem személyes adatok esetén ennél enyhébb feltételek teljesítése is elégséges lehetne. Mindazonáltal a teszt kiterjesztése iránymutatást adhatna mindkét adatkategória esetén arra, hogy mely adatokat, milyen feltételekkel lehet felhasználni, valamint mikortól tekinthető egy adatkezelés adathasznosításnak vagy hajlik már át a jogellenességbe.

- *A hatásvizsgálat*

Az adatvédelmi jogban ismert fogalom a hatásvizsgálat. Ezt azokban az esetekben kell lefolytatni, ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. A kötelezettség célja, hogy az adatkezelő az adatkezelést megelőzően a tervezett adatkezelési műveleteket megvizsgálja és értékelje, hogy a személyes adatok védelmét hogyan érintik.[1130] Az adatvédelmi hatásvizsgálat elvégzésének célja az adatkezelés jellegének feltárása, szükségességének és arányosságának vizsgálata, valamint a személyes adatok kezeléséből eredően a természetes személyek jogait és szabadságait érintő kockázatok kezelésének elősegítése, e kockázatok értékelésével és a kezelésükre szolgáló intézkedések meghatározásával.[1131]

[1129] EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data 10-11 o.
[1130] GDPR 35. cikk (1) bekezdés
[1131] GDPR 35. cikk (7) bekezdés

A hatásvizsgálat ellentétben a szükségesség arányosság tesztjével nem tekinthető absztrakt jogi vizsgálatnak, az kifejezetten az alkalmazott technikára és az adatkezelés gyakorlati körülményeire irányul. A pozitív eredménnyel záródó szükségességi-arányossági tesztet követően a hatásvizsgálatnak a megvalósítás részleteire kellene fókuszálnia, és az egyéni vagy a társadalom szélesebb érdekeit – akár csak közvetve – sértő adatkezelési műveletek megelőzésére irányulhatna. Nem személyes adatok esetén a hatásvizsgálat nem csak egy egyén alapjogi védelmét szolgálhatná, hanem a társadalmi rendre veszélyes adatkezeléseket is megelőzhetné. Fontos azonban, hogy például aggregált – nem személyes – adatok felhasználásával is lehetséges olyan üzleti modelleket vagy szolgáltatások létrehozni, amelyek veszélyt jelenthetnek természetes vagy jogi személyek jogaira és szabadságaira, vagy az EU jogpolitikai célkitűzéseire. Az ilyen szolgáltatások létrehozása, mint az adatok felhasználásának vagy hasznosításának a célja így már a fejlesztési szakaszban vizsgálható lehet, még az előtt, hogy valamilyen veszélyeztetési esemény ténylegesen bekövetkezne.[1132]

[1132] Példaként említhető az MI rendelet 9. cikke szerinti kockázatkezelési rendszer bevezetése a nem (csak) személyes adatok esetén nevesített hatásvizsgálati esetről

6.5. A jelen fejezet főbb kutatási eredményei

Az adatok magánjogi megítélése

- Az adat = (immateriális) vagyontárgy mert → emberi szükséglet kielégítésére alkalmas entitás (erőforrás) → tehát jószág → a javak összessége (a fennálló jogok és kötelezettségek által) a vagyon részei
- Az adat ≠ dolog mert → a dolgok (az európai jogrendszerek jelentős részében) testi tárgyak → a numerus clausus és az EUMSz 345. cikk miatt tagállami törvény kell másként rendelkezzen → ez pedig harmonizációs problémát okozhat

Az alkalmazható jog vizsgálata

- Közvetlenül nem alkalmazhatók egyik vizsgált terület (dologi jog, szellemitulajdon, titokvédelem) sem, a hatály hiánya vagy a horizontális/vertikális tagozódásból adódó szabályozási szemlélet különségei miatt
- Kiterjesztve sem megfelelőek, mert bármely területet vesszük alapul, a ténylegesen illeszkedő állapothoz annyi kivételszabályt kellene beépíteni, hogy a végeredmény csak igen távoli rokonságot mutatna az eredeti joggal, ezáltal mindegyik rendszer kereteit aránytalanul szétfeszíthetné

Az adatjogi jogosultság

- A jogosultság pozitív jogi szabályozása szükséges, mert (Malgieri alapján): "amennyiben nem történik meg a jogalkotó általi jogosultság-allokáció, akkor ennek a kiosztása azzal arányban fog megtörténni, amilyen arányban az egyik fél képes kizárni a másikat az (erőforrás) használatából." (Nozick-i ↔ pure force elméletek)

A relációs jogviszony

- A relációs jogosultság részjogosítványok (kvázi-tulajdonhoz hasonló) csokra, amelynek az egyes elemei annak megfelelően aktivizálódnak, ahogy az adatkezelés az értékegyenlőségi elv által felállított görbén halad
- A relációs jogviszony az abszolút és relatív jogviszonyok szerkezeti végpontjai között bármi lehet, az élethelyzettől függően, tehát bizonyos helyzetekben inter alia védelmet biztosíthat, míg más esetekben csak inter partes valósulna meg

A relációs jogosultság tárgya, alanya és létrejötte

- A létrejötte az adat létrejöttéhez igazodik, a jogosultat a kapcsolótényezők jelölik ki:
  - az első kapcsolótényező: a *kire/mire vonatkozik az adat*
  - a második kapcsolótényező: *ki hozta létre az adatot*
- Az elsődleges jogosult: eredeti módon szerző, amely személyes adatok esetén az érintett, nem személyes adatok esetén az adat létrehozója
- A másodlagos jogosult: származékos módon szerző, ilyen személyes adat esetén pl. az adat létrehozója, illetve bármilyen adat esetén pl. felhatalmazással rendelkező adathasználó
- Többes jogosultság lehetséges mindkét alanytípus esetén

A relációs jogosultság tartalma (részjogosítványok)

- Az adat hatalomban tartásának (adattartás) joga
- A használat (felhasználás és hasznosítás) joga
- A hasznok szedésének joga
- A rendelkezési jog
- A jogvédelemhez való jog (elsődleges/másodlagos jogvédelem és adatforrásvédelem)

Az adatjogi szerződések tipizálása

- Az adattovábbítási szerződések (az egyirányú adatmozgáshoz)
  - Átadással járó altípusok
    - Fizikai adatmozgással
    - Online adatmozgással
  - Hozzáférés biztosításával járó altípusok
    - Fizikai jelenléttel / távoli eléréssel
    - Felelősségvállalással / felelősségvállalás nélkül
    - Tárhelyhez / eszközhöz biztosított hozzáféréssel
- Adatfeldolgozói szerződések (kiszervezés önállótlan műveletvégzéssel)
- Adatvegyítési vagy adategyesítési szerződések (közös állományok létrehozása)
- Bizalmi adatkezelési szerződés (kiszervezés önálló műveletvégzéssel)
- Adatközvetítői szerződések (az adatmobilitás biztosítására)
  - A direkt-közvetítő (forprofit működés, egyedi adatokkal és meghatározott felekkel)
  - Az adatpiactérként működő közvetítő (forprofit működés, meghatározatlan adatkörre és felekkel)
  - Adatszövetkezetként működő közvetítők (közös fellépés, saját adatokkal)
  - Adataltruista szervezetként működő közvetítők (nonprofit működés, meghatározatlan adatkörrel és felekkel)

A horizontális minimumszabályok lehetőségei

- Jogi személyek védelmi lehetőségei: magánszféravédelem (mint szociális immunrendszer) és a virtuális személyiségvédelem alapján
- Nem személyes adatok védelme a kimenetek biztonságára tekintettel
- A szabályok módszere: a természetes személyeket az alapjogoknak és az adatvédelmi jognak megfelelően, a jogképes, nem természetes személyeket a korlátozott, de létező személyiségvédelemnek megfelelően, a jogtárgyakat közvetve, az ezeket hatalomban tartók érdekeire tekintettel.

A közös fogalomrendszer

GDPR szerepkörök		*Új (magánjogi) szerepek*
Érintett, adatalany	↔	Elsődleges jogosult, adatforrás
Adattárgy	↔	Adatforrás
Adatkezelő	↔	Elsődleges vagy másodlagos jogosult, adathasználó, de facto adattartó
Adatfeldolgozó	↔	Másodlagos jogosult (adattartó)
Harmadik fél	↔	Relációs kötelezett

Az adatjogi felhatalmazások

- Jogalapok alkalmazása minden adat esetén, mint származékos (másodlagos jog) szerzést lehetővé tevő felhatalmazások
- Új jogcímek létrehozása (főleg nem személyes) adatok eredeti (elsődleges jog) megszerzésére.
  - Az általános jogcímek:
    - Az érintett jogszerzése
    - A tilalom hiánya
  - A különös jogcímek:
    - Az átruházás
    - Egyetemes jogutódlás
    - Tercier adatszerzés
    - Derelinkvált adat megszerzése
    - Közösen létrehozott uniform vagy diverz adatbázis feletti többes jogosultság szerzése
    - Jogszabályon vagy közhatalmi aktuson alapúló elsődleges jogszerzés

Az adatforrásvédelem minimumszabályai

- A hozzáférés joga → elsődleges jogszerzés saját adatokon
- A tiltakozás joga → jogsérelem utólagos kontrollja
- A helyesbítés joga → dezinformáció és fals adatok terjedésével szembeni fellépés
- A részesedés joga → főszabályként természetbeni, de ha az eredmény jelentős és nem várt, az adatforrás adata pedig kellően egydi, akár pénzben kifejezhető formában

Az értékegyenlőség intézményesített vizsgálata

- A szükségesség és arányosság, mint az értékegyenlőség vizsgálat
- A hatásvizsgálat, mint az alkalmazott technika és az adatkezelés alapjogi védelemre és a társadalmi rendre gyakorolt hatásainak vizsgálata

7. Konklúzió

7.1. A kutatási eredmények összegző bemutatása

Jelen dolgozat fókuszába az adatok és az adatalapú életviszonyok kerültek. Ezekkel kapcsolatban a jog által a szabályozásukra tett lépéseket áttekintettük, az elemeket és a közöttük lévő mintázatokat igyekeztük azonosítani. A változásokkal teli világunkban a technológia és a társadalom közti egyensúlynak a jog eszközeivel történő helyreállítására törekedve mérleget vontunk a múlt eredményei és a jövő lehetőségei között, bízva abban, hogy a tárgyilagosságot megőrizve tudtuk megítélni a jelent, egyúttal a modern, adatalapú társadalmak állapotát. Kétségtelen, némely alapvető és akár speciális – ténylegesen konvencióvá alakult – határt kellett megkörnyékezni (és helyenként át is lépni), amelyekkel kapcsolatban jelen dolgozat kutatási célkitűzései és kutatási kérdései kerültek felállításra.

Az első célkitűzés az adatalapú viszonyok egyensúlyi helyzetére irányult, annak érdekében, hogy ahol egyensúlytalanság azonosítható, ott az helyreállítható legyen. Egyfelől globálisan, tehát Európa és a világ más hatalmai között, másfelől közösségi szinten az egyének és kiscsoportok között.

A második célkitűzés az adatjog jelenlegi állapotának feltárása és a területen néhány esetben tapasztalható diszfunkcionalitás kiváltó okának azonosítása és lehetőség szerinti megszüntetése, ezáltal az adatjogi tisztánlátás elérése volt.

A kutatási kérdések alapján vizsgáljuk meg mennyiben sikerült megvalósítani a célkitűzéseket.

1. Az adatok jog általi megragadhatósága érdekében milyen lényeges szempontokat érdemes figyelembe venni?

Az első szempont az adatok absztrakt fogalma, amit a DIKW piramis újragondolásával hoztunk létre. A második az absztrakt fogalmon alapuló, adatok létrejöttének elméleti folyamata, a harmadik az adatok öt ismérve, a negyedik az öt tulajdonságcsoportja, az ötödik pedig az adatfogalmak szemiotikus (szintaktikai és szemantikai rétegződésű) rendszerelmélete.

A 2. fejezet kutatásai az adatok elemiszintű tulajdonságainak vizsgálatára irányultak, a fogalom-alkotás és a rendszerezés kísérletei által széles látóteret voltunk képesek létrehozni a későbbi kutatások megalapozásához. A kognitív folyamatban betöltött alapvető eszköz és közvetítő közeg szerepe az adatoknak megmutatta azok megkerülhetetlenségét, ezáltal a szabályozás fundamentális szemléletének szükségességét. Az ismérveken és tulajdonságcsoportokon keresztül az egyes területek, mind a jelenlegi szabályok értelmezésében, mind a jövőbeli lehetőségek kereteinek kijelölésében hasznosnak bizonyultak, az adatok magánjogi megítélése például ezek nélkül nem lett volna lehetséges. Az adatok létrejövetelének elméleti folyamata továbbá számos ponton támogatta a jogelméleti okfejtéseket, például e nélkül az adatjogi jogosultságot kijelölő kapcsolótényezők nem lettek volna létrehozhatók. A monetizáció értékeléséhez az adatok értékességi szempontú vizsgálata adott elméleti alapot.

2. Hogyan definiálhatjuk az európai adatjogot, milyen mozgatóelvek és elhatárolási pontok azonosíthatók az egyes elemei között az adatalapú életviszonyok vizsgálatának tükrében?

Az adatjog létének vizsgálatával kapcsolatban arra jutottunk, hogy annak feltételei adottak, a szüksége pedig azonosítható. Dogmatikailag azt, mint új jogterület tudtuk leginkább elképzelni.

Az adatjog kétféle osztályozását végeztük el a 3. fejezetben, amelyeket egymást kiegészítve értelmeztük. Jogdogmatikai szempontból horizontális (ágazatfüggetlen), vertikális (ágazati) és

kompozit (adatjogon kívüli adatjogi) területekre bontottuk, amelyekben természetes széthúzást és azzal szemben ható adatjogi konvergenciát, mint összetartó erőt határoztunk meg. Pragmatikus klasszifikáció által a védelem és használat területeire osztottuk az adatjogot. A védelem az adatokon való műveletvégzés korlátozásokkal történő keretezésére, irányítására (a hogyan jogaként) szolgál, míg a használat az adatokra vonatkozó részletszabályokat (a mit, mikor, miért, meddig stb.) tartalmazza. A használatot felhasználásra és hasznosításra osztottuk tovább. Előbbi esetében az adatok a mindennapi működéssel kapcsolatos eszközként, míg utóbbinál azok az innovációval összefüggő erőforrásokként foghatók fel. Ezekkel kapcsolatban konkrét szerepköröket is azonosítani tudtunk, így az adatok a védelemben, mint elkövetési tárgy, a hasznosításban, mint monetizált erőforrás, a felhasználásban pedig társadalmi csereeszköz jelennek meg.

Az alterületek meghatározásával a jelenlegi jogszabályi környezetet jobban át tudtuk tekinteni, azt jogelméleti és gyakorlati aspektusokból is meg tudtuk közelíteni. A szabályanyag kiterjedtségének ilyen vizsgálatával megteremtődött a lehetőség későbbi elemzésére és ezáltal a hiányosságok azonosítására, illetve korrekciós javaslatok megfogalmazására.

Az adatokhoz való értékrendelés problémakörét (un. adatvalorizációs zavar) is vizsgáltuk, ami során az értékegyenlőségi elvet azonosítottuk, mint egy nem deklarált, háttérben működő szabályszerűen érvényesülő tendenciát (mozgatóelvet). Ezzel tartottuk magyarázhatónak, hogy miért van, hogy egyes esetekben az adatok felett rendelkezni lehet, míg máskor nem, illetve ez adta meg a választ az adatok pénzben kifejezhetőségének ellentmondásaira. Az elv a cél szerinti szükségesség és arányosság vizsgálatán és a megfelelő érdekeltség egyensúlyának igazolásán keresztül működik. A kiindulópontja, hogy a társadalom azokat a folyamatokat favorizálja, amelyek értékegyenlők. Az elv az adatok használatára irányuló területeken érvényesül és mind személyes, mind nem személyes adatok esetén alkalmazható.

Az értékegyenlőségi elv segítségével jobban elhelyezhetők az egyes adatalapú folyamatok az adatjogi spektrumon, valamint a szabályozási igény (helye és ideje) is talán könnyebben megragadható. Az elv mind a jelenlegi rendelkezések értelmezéséhez és értékeléséhez, mind a jövőbeli jogra tett javaslatok megfogalmazásához felhasználásra került.

3.Milyen alterületekre bontható az adatjog és azoknak milyen főbb jellegzetességei vannak?

Az egyes területek 4. fejezetbéli de lege lata elemzésével kapcsolatban az alábbi jellegzetességekre jutottunk:

- A védelem jogának jellegadó elemei alapvetően a személyes adatok védelméből és az információbiztonság szabályanyagából áll. A jelentősége és szabályozási megoldásainak a tekintetében is a GDPR mellett a CRA horizontális szabályai emelhetők ki. Az összes vizsgált joganyag vonatkozásában számos hasonló megközelítés azonosítható, amelyek így az adatjogi összetartás (konvergencia) alkotóelemei lehetnek. Ilyenek például a kockázat-arányos védelem, a kockázatértékelés és -kezelés fontossága, a jelentéstételi kötelezettség és eseménykezelés (pl. incidensek), a by design és by default szemléletek, az egységességre törekvő harmonizált (szinergikus) szabályok, az alkalmazói és felhasználói tudatosság növelésének fontossága, valamint az ex ante jogszerűségi szabályok erősödése.
- Az adat használatának ernyő fogalma alatti adatfelhasználással kapcsolatban azt mondtuk, hogy az bármi lehet, ha kellően magas fokú értékegyenlőséget mutat (ellenkező esetben már hasznosításról vagy végső esetben jogellenességről beszélnénk). A felhasználás joga jellemzően kompozit adatjogi előírásokban testesül meg, amelyek

az adatok kezelésének alapvető paramétereit adják. Ilyen a konkrét adatkezelési cél, adatkör vagy megőrzési idő meghatározása. A felhasználás kevésbé explicit oldalához az ágazati jog által kinyilvánított célok, illetve lehetőségek megvalósítása érdekében végzett adatkezelések tartoznak, amelyeknek azonban a részleteit nem adja meg a joganyag, ezért azt általános adatjogi jogelvek mentén kell az adatkezelőnek meghatároznia. Léteznek a felhasználáshoz tartozó, de felhasználási jog által egyáltalán nem szabályozott területek, amelyeknek egyetlen közös jellemzője, hogy nem létezik rájuk vonatkozóan valamilyen kifejezett tiltás. Ezeknek ilyenformán keretet nem a felhasználás, hanem a védelem összetartó-hatású rendelkezései adnak (pl. alapelvek, jogalapok stb.).

- Az adathasznosítás joga az elmúlt években indult nagyarányú fejlődésnek és bővülésnek. A hasznosítás horizontális tartományában olyan nagy horderejű aktusok találhatók, mint a DGA és a DA. A vertikális terület anyagának a kidolgozása a közös adatterekre vonatkozó jogi aktusokkal még csak most kezdődik, az EHDS és FIDAR javaslatokkal. A hasznosítás jogának közös vonásai az adathordozhatóság fontosságának hangsúlyozása, az átláthatóságot és használhatóságot (adatformátumon keresztül) támogató intézkedések bevezetése, a by design és a by default szemlélet védelemből való átemelése, a díjazásra (monetizációra) vonatkozó előírások alapszintű meghatározása, a célmeghatározás szerepének hasznosításba való átmentése, a hasznosítás korlátozhatóságának kimondása, valamint az anonimizáció és álnevesítés szerepének megjelölése és a hozzáférés engedést megelőző szakaszban való elhelyezése. Fontos továbbá a jogi személyekre és nem személyes adatokra vonatkozó hasznosítási és védelmi szabályok úttörő bevezetése és a szektorális szabályozás előtérbe helyezése.

4. Az adatalapú működés szempontjából milyen általános hiányosságok azonosíthatók a vonatkozó joganyaggal kapcsolatban?

Az 5. fejezetben az adatjog jelenének (sein) és lehetséges jövőjének (sollen) vizsgálata érdekében annak erősségeit, gyengeségeit, lehetőségeit és fenyegetéseit vizsgáltuk. A SWOT analízis alapján azonosítottuk a jelenlegi adatjogi rendszer legfontosabb hiányosságait (diszfunkcionalitásának forrását). Az adatjogi viszonyok egyensúlya érdekében az adatokra vonatkozó joganyag alapjainak befejezésére lenne szükség, ehhez elengedhetetlen első lépés az adatok magánjogi megítélésének tisztázása, valamint az adatjogi szisztéma dogmatikai alapjainak egyértelmű rögzítése. Szükség lenne továbbá egy minden adatkategóriára kiterjedő adatjogi jogosultsági és szerződéses rendszerre azért, hogy az adatok szabad áramlása mellett a jog- és forgalombiztonság is megvalósítható legyen. További horizontális minimum-előírásokra is szükség lehet – különösen a nem személyes magánadatok esetén – az adatjogi tisztánlátás érdekében.

5. A feltárt hiányosságok alapján milyen javaslatok tehetők?

A 6. fejezetben a feltárt hiányosságok vonatkozásában, a gyakorlat által felvetett problémákat esetlegesen orvosolni képes, javaslatokat fogalmaztam meg. Az adatok magánjogi megítélésével kapcsolatban a legjobban alkalmazható megoldásnak az tűnt, ha azokat, mint immateriális vagyontárgyakat kezelnénk. Az EU jog szempontjából az adatok polgári jogi értelemben vett dologként való felfogása nem bizonyult alkalmazhatónak.

A horizontális adatjog teljessé tétele érdekében egy relációs jogosultsági rendszer bevezetésének lehetőségét vázoltam fel, amit mint részjogosítványok (kvázi-tulajdonhoz hasonló) csokraként lehet elképzelni. Ennek az egyes elemei aszerint aktivizálódhatnak, ahogy az adatkezelés az értékegyenlőségi elv által felállított görbén halad. A jogosultat

kapcsolótényezők jelölnék ki. Az első kapcsolótényező, hogy *kire/mire vonatkozik az adat,* a második, hogy *ki hozta létre az adatot.* Az alkalmazhatósághoz kétféle jogosulti típust határoztam meg. Az elsődleges jogosult az, aki eredeti módon szerzett. Ez személyes adatok esetén az érintett, nem személyes adatok esetén az adat létrehozója. A másodlagos jogosult, aki származékos módon szerzett. Ilyen például személyes adat esetén az adat létrehozója, illetve bármilyen adat esetén a felhatalmazással rendelkező adathasználó.

A relációs jogosultság tartalma (részjogosítványai) lehetne az adat hatalomban tartásának (tényleges vagy potenciális műveletvégzés) joga, a használat (célzatos felhasználás és hasznosítás) joga, a hasznok szedésének joga, a rendelkezési jog és a jogvédelemhez való jog (elsődleges/másodlagos jogvédelem és adatforrásvédelem).

Az adatjogi szerződés tipizálására is sor került. Ezek között az adattovábbítási szerződéseket, az adatfeldolgozói szerződéseket, az adatvegyítési vagy adategyesítési szerződéseket, a bizalmi adatkezelési szerződéseket és az adatközvetítői szerződéseket különböztettük meg.

A horizontális minimumszabályok lehetőségei között a közös fogalomrendszert, az adatjogi felhatalmazásokat, az adatforrásvédelem minimumszabályait és az értékegyenlőség vizsgálatára irányuló mechanizmusokat jelöltük, mint szabályozási lehetőségek.

- *A kutatási kérdésekre adott válaszok értékelése*

A kutatási kérdések megválaszolása lehetővé vált jelen dolgozat kutatásai alapján. A jelenleg látható tripoláris elrendezésű, globális adatalapú viszonyok egyensúlyvesztett helyzetén azt gondolom segíthet az erősebb, de az egyének és piaci szereplők autonómiájára fókuszáló jogalkotás. Az értékegyenlőségi elv elismerése, az adat magánjogi megítélésének tisztázása, a relációs jogviszonyok és az adatjogi szerződések tipológiájának rögzítése, valamint a horizontális szabályok minimumelőírásainak bevezetése a célkitűzés eléréséhez hozzájárulhat.

Az adatjog jelenének vizsgálata által azonosított hiányosságokból eredő diszfunkcionalitás orvosolható lehet a fentebb vázolt (vagy ahhoz hasonló módon) teljesebb horizontális adatjogi állapot elérése által. Az adatjogi tisztánlátással kapcsolatban, jelen dolgozat alapján, azt is gondolom, hogy a vertikális jogalkotási irányok (EU adatterek) megfelelőek, azonban a horizontális szabályok egyszerűsítésére és egyúttal lezárására van szükség, ahhoz, hogy ezek a speciálisabb előírások érvényesülni tudjanak. Ezt egy generális, a GDPR párját alkotó jogalkotással lehetne megvalósítani, ami egyúttal az FFNPDR és a DA megoldásait egészíthetné ki (válthatná le). Mivel igyekeztem a gyakorlati kívánalmakat a lehető legjobban figyelembe venni, ezért jogalkotás hiányában a javaslatok részben vagy egészben egy alulról szerveződő, piaci önszabályozás keretében is megvalósulhatnak, bár vélelmezhetően alacsonyabb hatásfok mellett.

7.2. A kutatási eredmények gyakorlati alkalmazhatóságának vizsgálata az egészségügyi adatokon keresztül

A dolgozat zárásaként szeretném a kutatási eredményeket gyakorlati kontextusba helyezni, annak érdekében, hogy a javaslatok érvényesülési lehetőségeit a valós életviszonyokban is el lehessen képzelni. Ehhez egy eddig részben érintetlenül hagyott, de adatjogi szempontból kiemelt jelentőségű területet, az egészségügyi adatok területét választottam. Az EÜ adatok területének vizsgálata indokolt, hiszen a jellemzőnek mondható adatkezelési folyamatok alapértelmezetten magas kockázatúak, a szegmens innovációra hajlamos és kiemelt fontosságú, a működési struktúra összetett, sok szereplős, valamint személyes és különleges adatok nagy mennyiségben keletkeznek és mozognak a rendszeren belül, illetve azt szükségszerűen el is hagyják mind felhasználási, mind hasznosítási célzatokkal.

7.2.1. Az adatkezelési környezet

- *A jogszabályi háttér*

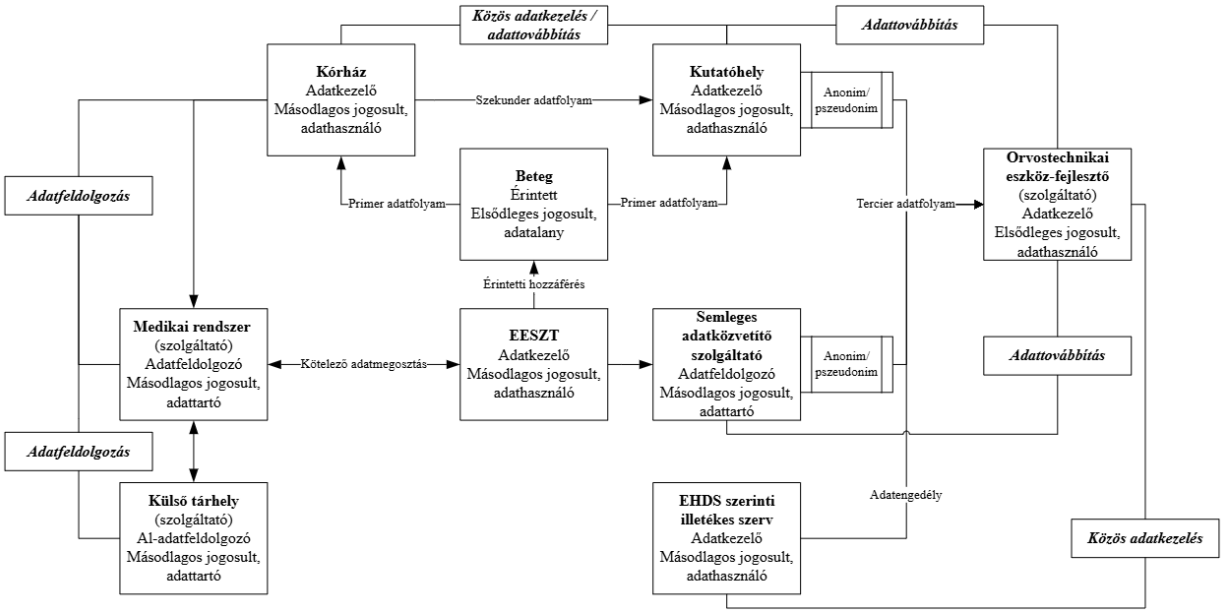
A területre számos jogszabály tartalmaz rendelkezéseket, ezeknek a legjelentősebb elemeit a jogdogmatikai és pragmatikus csoportosításoknak megfelelően az alábbiak szerint sorolhatjuk be:

Jogdogmatikai		*Pragmatikus*	
Horizontális	GDPR, DGA, DA	Védelem	GDPR
Vertikális	Eüaktv., EHDS javaslat	Felhasználás	Eütv., Gent.tv., MDR, IVDR
Kompozit	Eütv.,[1133] Gent.tv.,[1134] MDR,[1135] IVDR[1136]	Hasznosítás	Eüaktv., EHDS javaslat, DGA, DA

- *Az adatkategóriák és típusok*

Az EÜ adatok kezelésének középpontjában a humánegészségügyi ellátásban megjelenők személyes és különleges személyes (egészségügyi, biometrikus, genetikai) adatai állnak. Az adatok megjelenhetnek analóg formában, de a digitalizáció jellemzőnek mondható. Azok egy jelentős része strukturálatlan vagy részben strukturált (pl. lelet, beutaló, képalkotó diagnosztika eredménye). A digitális nyilvántartás részeként létrejövő állományok ezzel szemben strukturáltak lehetnek. A formájukat tekintve vegyesen lehetnek kvalitatívak és kvantitatívak egyaránt, a forrásuk legtöbb esetben az adatalany, de pl. egy szakvélemény kialakításakor származtatott adatok is nagy számban jöhetnek létre. A folyamatok jellemzően összetettek és kiterjedtek, e mellett algoritmizációs fejlesztésekre is nyitottak.

- *Példa a résztvevőkre és az adatfolyamok irányaira*



21. ábra: lehetséges résztvevők az egészségügyi adatfolyamban

[1133] Az egészségügyről szóló 1997. évi CLIV. törvény

[1134] A humángenetikai adatok védelméről, a humángenetikai vizsgálatok és kutatások, valamint a biobankok működésének szabályairól szóló 2008. évi XXI. törvény

[1135] Az Európai Parlament és a Tanács 2017/745/EU rendelete az orvostechnikai eszközökről

[1136] Az Európai Parlament és a Tanács 2017/746/EU rendelete az az in vitro diagnosztikai orvostechnikai eszközökről

Az adatok forrásai jellemzően az érintettek, akikről elmondható, hogy nagyszámban vesznek részt a folyamatokban, sok esetben kiskorúak és/vagy kiszolgáltatott helyzetben lévők. Az érintett, mint természetes személy ipso iure elsődleges jogosultként jelenik meg a saját adatai tekintetében, a GDPR 9. cikk alapján a különleges adatokra pedig megkülönböztetett (közel abszolút) védelem valósul meg. Az elsődleges ellátást biztosító intézmény (kórház), az érintettel közvetlen kapcsolatban lévő kutatóhely, mind adatkezelők, másodlagos jogosult adathasználók. Előbbi a gyógykezelés primer folyamatában, utóbbi akár primer (un. prospektív kutatás: közvetlenül az érintettől történő új adat gyűjtése esetén), akár szekunder (un. retrospektív kutatás: a kórháztól történő, már létező adat gyűjtése esetén) tevékenységet is végezhet. A kórház jellemzően adatfelhasználás, míg az értékegyenlőség függvényében a kutatóhely adatfelhasználási vagy akár adathasznosítási tevékenységet is végezhet. A kórház és a kutatóhely a megállapodásuknak megfelelően közös adatkezelői kategóriába tartozhat vagy nagyobb függetlenség esetén egymásközt adattovábbítást valósíthat meg. A kórház a működésébe, más önállótlan feleket is bevonhat, így pl. a saját medikai (nyilvántartó) rendszerének üzemeltetésébe. Ez a szolgáltató (az ő általa alkalmazott külső tárhelyszolgáltatóval együtt) adatfeldolgozónak, másodlagos jogosult adattartónak minősülnének, mivel nem rendelkeznek saját céllal a folyamatban. A medikai rendszer elképzelhető,[1137] hogy köteles csatlakozást létrehozni az egészségügyi szolgáltató és az EESZT között. Az EESZT működtetője a Belügyminisztérium, amely, mint adatkezelő, másodlagos jogosult adathasználó jelenik meg, magas fokú önállósága miatt.[1138] Az EESZT egyfelől oda-vissza kommunikációt valósít meg az ellátóval, valamint hozzáférési lehetőséget biztosít az érintett számára. Másfelől az EHDS javaslat alkalmazandóvá válása esetén az adathasznosításban is részt vállalhat. Egy semleges adatközvetítő szolgáltatón keresztül, az EHDS szerinti illetékes szerv irányítása mellett az EÜ adatok harmadik felek számára hozzáférhetővé tehetők, anonimizált vagy álnevesített formában. Az EHDS javaslattól függetlenül, a hasznosítás pl. a kutatóhely irányából is megindulhat, ahol szintén adattovábbítás valósulhat meg harmadik felek irányába. A harmadik fél (pl. egy orvostechnikai eszköz fejlesztője) az anonimizált adatokon a megállapodásnak megfelelő műveleteket végezhet, a maga által létrehozott (tercier) nem személyes adatokon elsődleges jogot is szerezhet.

7.2.2. Az új szabályok alkalmazhatóságának egyes kérdései

A fenti folyamatban látható, hogy számos résztvevővel és érdekelt féllel lehet és kell is számolni. Az érintett elsődleges érdeke az ellátás igénybe vétele, itt az értékek egyenlősége erősnek tekinthető. Az ehhez szorosan kapcsolódó kutatási célú adatkezelések még felhasználásnak minősülhetnek, de az érintett érdekeitől távolodva (pl. új, hatékonyabb gyógyszer nem jelent egyet az új, hatékonyabb gyógyszerfejlesztési módszerrel) az adatkezelés hasznosítási folyamattá alakulhat át és felmerülhet az ellentételezés kérdése. Hogy ez közvetlen pénzteljesítéssel, egy új gyógykezelési programban való részvétel lehetőségével vagy egyéb módon valósul meg, azt speciális szabályoknak vagy ágazati gyakorlatoknak (pl. orvosetikai előírások) kell megítélnie. A védelem előírásait ettől függetlenül mindvégig figyelembe kell venni, így jogszerű céllal és érvényes felhatalmazással kell a folyamatnak rendelkeznie (amely a másodlagos jogosultság megszerzését egyáltalán lehetővé teszi), miközben az olyan előírásokat is be kell tartani, mint a kockázat-arányosság (amit az érintettre jelentett

[1137] Eüak. 35/B. §

[1138] Belügyminisztérium, Egészségügyi Szolgáltató és Fejlesztési Központ, EESZT lakossági adatkezelési tájékoztató, Hatályállapot: 2023.06.01-től visszavonásig. Elérhető: https://www.eeszt.gov.hu/documents/20182/36430/EESZT_Lakossagi_adatkezelesi_tajekoztato_20230828.pdf/a105eae6-951f-b82a-b707-f06dd441dc17

kockázatokra tekintettel kell meghatározni, így pl. a náthára és a meddőségre vonatkozó adatokat differenciáltan kell kezelni).

Az ábrán látható az adatok egészségügyi ellátórendszerből való kilépésének két lehetősége. Fontos azt látni, hogy a harmadik fél elsődleges jogszerzésének a feltétele, hogy az adat ne minősüljön személyes adatnak, ezért az anonimizáció/álnevesítés mindkét esetben szükségesek. Ez az érinett érdekeit védő természete mellett, az adatgazdasági hasznosulás kiszámíthatóságát is szolgálja, hiszen a tercier adatszerzés jogcímével csak így kerülhet elsődleges jogosulti pozícióba a szerző fél (a nemo plus iuris elve miatt pedig az ellátórendszer nem tud több részjogosítványt megosztani, mint amennyivel maga is rendelkezik). Az ellátórendszer anonimizációs műveletre való felhatalmazása az információs önrendelkezési jogot leginkább védő módon történhet hozzájárulás megadásával, vagy amennyiben a társadalmi legitimáló erő kellően erős a fennálló érdekeltség igazolásával is (pl. az EHDS javaslatnak megfelelő eljárás esetén). A folyamatban látható a relációs jogosultságok „vetélkedése", az érintett és az adatkezelő(k) részjogosítványai úgy aktivizálódnak, ahogy azt az aktuális folyamat értékegyenlőségi szintje megköveteli (így tehát hozzájárulás esetén az adatkezelést az érintett megakaszthatja a hozzájárulás visszavonásával, vagy a törlési jog gyakorlásával, más jogalap esetén azonban legfeljebb tiltakozási jogával élhet, amit az adatkezelő akár el is utasíthat).

A jelen dolgozatban vázolt adatjogi rendszer szerint az érintett (pl. adathordozhatósághoz való jogának gyakorlása keretében) a saját adatait, saját elhatározása alapján is hasznosításba adhatja, közvetlenül az adatot átvevő harmadik féllel kapcsolatot létesítve. Ebben az esetben az adatok anonimizációja az érintettől nem feltétlenül várható el, a megállapodás alapján (a privátautonómiának megfelelően) arról rendelkezhetnek, hogy milyen feltételekkel és módon szerez (másodlagos joga keretében) részjogosítványokat az átvevő fél. Így az anonimizáció mellett (ami szintén megtörténhet erre irányuló szolgáltatás igénybe vételével) ebben az esetben a részjogosítványokon keresztül megvalósuló műveleti korlátozásokkal szabhat az érintett kereteket a folyamatnak. A kapcsolat létrehozatalában semleges adatközvetítő vagy bizalmi adatkezelő is támogathatja az érintettet.

Érdekes kérdés az anonimizálás következtében létrejövő nem személyes adatok kezelése. Ezeken már elsődleges jog szerezhető az azt létrehozó által, továbbá a jogosultság a létrehozatalt követően át is ruházható. A jogcímes szerzéssel a nem személyes adatok feletti részjogosítványok a személyes adatokéhoz hasonlóan gyakorolhatók vagy akár meg is oszthatók, azonban az elsődleges (uralkodó) jogosult mindvégig azonosítható maradhat. A tipizált szerződések lehetővé tehetik más szereplőknek a folyamatba való bevonását, illetve a felek közötti tranzakciók lebonyolítását. Az értékegyenlőségi elv szerinti vizsgálatok (SZAT, hatásvizsgálat) támogathatják a résztvevőket a folyamat elfogadhatóságának megítélésében, a káros kimenetek pedig hatóság által ex post vizsgálhatók és szankcionálhatók lehetnek.

Az adatok anonimizációjának gyakorlatilag az ellentétét jelenti azoknak (adatszett vagy adatbázis szintjén történő) *visszaállíthatatlan egyedivé tétele*, például valamilyen blokklánc-alapú technológia alkalmazásával (pl. NFT[1139]). Ebben az esetben az adatok tartalma és jogosultja kétséget kizáróan hitelesíthető, az adott eredeti vagy másolt állományon szerzett részjogosítványok és azok alanya (metaadatok formájában) rögzíthetők lehetnek. Ezzel a későbbi adatmozgások könnyebben nyomonkövethetők és – bár a közhiteles nyilvántartásban (lakcímnyilvántartáshoz hasonlóan) való elhelyezés nem tűnik arányos ráfordítással

[1139] Non-fungible token. Blokklánc-alapú technológia, ami egyedi digitális jogosultság igazolására képes. Jelenleg például művészeti alkotások, játékok, zenék, kriptovaluták esetében kerül alkalmazásra. Lásd: IBM, „The rising NFT tide lifts all tokens: So what is an NFT?", 2021. Elérhető: https://www.ibm.com/think/topics/nft

megvalósíthatónak – egy relációs jogviszony esetében a korábbi és jelenlegi felek, illetve jogaik és kötelezettségeik „naplózhatók" és így a későbbi jogvédelem és igényérvényesítés könnyebbé tehető, valamint az egyedszintű kizárólagosság is megvalósítható. Ez akár személyes adatok esetén is alkalmazható lehetne, amennyiben a kiindulópontban (un. „genezis-blokkban) az adatvédelem által megkövetelt jogszerűségi feltételek fennállnak,[1140] és ha az adatkezelési folyamat természete a visszaállíthatatlan egyedivé tételt egyáltalán szükségessé/lehetségessé teszi (pl. az érintett vagyoni érdekei védelme érdekében). A jogosult rögzítése az adatok forrásának azonosíthatatlanná tételét kizárhatja, ha azok egybeesnek egymással (ami bizonyos esetekben aggályosnak bizonyulhat). Azonban egy „pszeudo-érintett" is megjelölhető lehet a valódi helyett, így pl. egy közös jogkezelést megvalósító adatközvetítő vagy bizalmi adatkezelő betöltheti ezt a szerepet. Így még akkor is, ha az adatok objektíve nem anonimak, az átvevő oldaláról csak a közös jogkezelő lenne látható, a mögötte álló tényleges adatalanyok nem. Az adatok technológiailag visszaállíthatatlan egyedivé tételére elsődlegesen a hasznosításba kerülő adatok esetén lenne szükség, ahol ez az előállítás költségei között megtéríttethető lehet az átvevővel mind köz, mind magánszervezetek esetén. Az adatok ilyen formátumtípusára uniós standardok lehetnek alkalmazhatók az interoperabilitás megkönnyítése érdekében. A folyamat az okos szerződések rendszeréhez illeszkedően önvégrehajtóan is működhet, az egyediesítés megítélése (ellentétben az anonimitással) objektív paraméterek alapján megtehető. Az interoperabilitás megkövetelése és az okos-szerződések alkalmazhatósága az uniós adatjog által már elismerésre és szabályozásra került a DA keretében.[1141]

Végezetül a részesedéshez való jog kérdése merülhet fel, mint adatforrásvédelmi jogosítvány gyakorolhatósága. Fontos, hogy amennyiben a folyamat felhasználásnak minősül ez nem jön számításba. A részesedéshez a jogosult és az adattartalom valamilyen formában történő rögzítésére (pl. a fentebb látható, akár pszeudo-érintettel való egyediesítésre) van szükség. Egy egészségügyi folyamat esetén a nem pénzbeli részesedés az ellátórendszeren belül is rendezhető (pl. programban való részvétellel). Pénzügyi eredmény esetében az anonimizáció miatt a visszakövethetőség meg kell szakadjon, így a kifizetés kalkulálása és teljesítése nehézkes lehet. Egy lehetséges módszer szerint a jogosultak részesedését a költségek között lehetne feltüntetni, az így befolyt pénzt pedig egységes és arányos szempontok szerint lehetne visszaosztani. Ennek módszertanát a korábban szerzői jogi értelemben vett fájlcserélés megoldásaiból lehetne meríteni. Így pl. Lessig a kérdésben egyfajta statikus (adójellegű) jogdíjszerű megoldást javasolt.[1142] Ezt az adatokra vonatkoztatva egy a szolgáltató által időszakosan meghatározott, a hasznosításban lévő és így hozzáférhetővé tehető adatok mennyiségének és minőségének megfelelően felszámított, előfizetés-jellegű díjként képzelhetnénk el, amit a potenciális adatátvevők fizetnek meg. Az időszakban beérkező, az összes előfizető adatátvevőtől érkező teljes összeg kerülhetne felosztásra az összes jogosult között anélkül, hogy azoknak a kilétét fel kellene fedni az átvevő előtt. A megosztás aránya igazodhat az adatok bármely paraméteréhez, így akár a jogosultankénti mennyiséghez vagy az adatok egyedi minőségéhez. A szükséges szerződéses viszonyokban egy pszeudo-érintett, akár maga az ellátórendszer is megjelenhet az adatalany helyett.

A dolgozat zárásaképpen azt mondhatjuk, hogy az adatjog nagyon is létező területének megerősödése zajlik, az európai megoldások pedig számottevő hatással lehetnek a globális adatalapú folyamatokra és egyfajta ellensúlyként is működhetnek a másik két pólus (USA és Kína) megközelítéseivel szemben. A horizontális adatjog teljessé tételének egy módja lehet a jelen dolgozatban vázolt megközelítés és az így esetlegesen hozzájárulhat az EU

[1140] Eszteri Dániel, „A blokklánc mint személyes adatkezelési technológia GDPR-megfelelőségéről", ÁJT, 2020/4. 24-51. o.
[1141] DA VIII. fejezet
[1142] Mezei, 2012. 260-261 o.

adatszuverenitásának és az európai adatalapú folyamatok egyensúlyának eléréséhez, valamint az uniós érdekelt feleket szolgáló adatjogi tisztánlátás kialakításához.

7.3. Angol nyelvű összefoglaló / English language summary

- Research objectives and research questions

The overarching goal of my work is to identify data law solutions to balance data-based relationships, and in the absence of such solutions, to define them.

The first main objective is therefore to rebalance data-based relationships so that where imbalances can be identified, they can be corrected. On the one hand, at the global level, i.e. between Europe and other world powers, and on the other hand, at the community level, between individuals and small groups. My second objective is to explore the current state of data law and to identify and, where possible, eliminate the root cause of dysfunctionality, thereby achieving clarity on data law.

To achieve the above two research objectives, the following research questions can be addressed.

1. To ensure that data can be more accurately captured by the law, what are the essential aspects to consider?
2. How can we define European data law, what are the driving forces and demarcation points between its different elements in the light of the analysis of data-driven situations?
3. What sub-areas can data law be divided into and what are their main characteristics?
4. From a data-driven perspective, what general shortcomings can be identified in the relevant legislation?
5. Based on the shortcomings identified, what proposals can be made?

- Assessment of the fulfilment of the research objectives

The research results will be used to assess the extent to which the objectives have been achieved.

1. To ensure that data can be more accurately captured by the law, what are the essential aspects to consider?

The first aspect is the abstract notion of data, created by rethinking the DIKW pyramid. The second is the theoretical process of data creation based on the abstract concept, the third is the five characteristics of data, the fourth is the five sets of attributes of data, and the fifth is the semiotic (syntactic and semantic layering) systems theory of data concepts.

The research in Chapter 2 focused on the element-level properties of data, and through the attempts at conceptualisation and systematisation we were able to create a broad horizon to underpin future research. The role of data as a fundamental tool and mediating medium in the cognitive process has shown the inescapability of data and thus the need for a fundamental approach to regulation. Through the criteria and sets of attributes, each area has proved useful both in interpreting current rules and in setting the framework for future possibilities; for example, the private law treatment of data would not be possible without them. Moreover, the

theoretical process of data creation has supported the legal theoretical reasoning at several points, for example, without it, the linking factors that determine data entitlement could not have been created. The value analysis of data has provided a theoretical basis for assessing monetisation.

2. How can we define European data law, what are the driving forces and demarcation points between its different elements in the light of the analysis of data-driven situations?

In examining the existence of the right to data, it is concluded that its conditions are given and its needs can be identified. Dogmatically, we could best conceive of it as a new area of law.

Two classifications of data law were made in Chapter 3, which were interpreted as mutually complementary. From a legal-dogmatic point of view, we have divided it into horizontal (sector-independent), vertical (sectoral) and composite (data law outside data law) areas, in which we have identified natural discord and data law convergence acting against it as a cohesive force. By pragmatic classification, we divided data law into the domains of protection and use. Protection is the law to frame and control (as the law of *how*) the operations on the data, while use is the right to regulate the details of the data (what, when, why, for how long, etc.). Usage is further divided into application and utilization. For the former, data can be understood as a tool for day-to-day operations, while for the latter it can be understood as a resource for innovation. We were also able to identify specific roles in relation to these, with data appearing in protection as the instrument of commission, in utilization as a monetised resource and in application as a social exchange tool.

By defining the sub-areas, we were able to take a better look at the current legal environment and approach it from both a theoretical and practical perspective. Such an examination of the scope of the body of rules and regulations provided the opportunity for further analysis and thus for identifying gaps and proposing corrective measures.

The problem of attributing value to data (so-called “data valorization”) is a key issue. This was considered to explain why in some cases data can be disposed of while in other cases it cannot, and to provide an answer to the contradictions in the monetisation of data. The principle works through a test of necessity and proportionality to the purpose and a justification of the balance of interests. Its starting point is that society favours those processes that are value-equal. The principle applies to areas where data are used and can be applied to both personal and non-personal data.

The value-equivalence principle helps to better place each data-based process on the data rights spectrum and may also help to better capture the regulatory need (place and time). The principle has been used both to interpret and evaluate current provisions and to formulate proposals for future law.

3. What sub-areas can data law be divided into and what are their main characteristics?

The analysis of each area in Chapter 4 has led to the following characteristics:

- The main characteristics of data protection law are basically the protection of personal data and the rules on information security. In terms of its relevance and regulatory solutions, the horizontal rules of the CRA stand out alongside the GDPR. A number of similar approaches can be identified for all the legal instruments examined, which can thus be considered as components of data law convergence. These include, for example, risk-proportional protection, the importance of risk assessment and management, reporting obligations and incident management (e.g. incidents), by design and by default approaches, harmonised (synergistic) rules aiming at consistency, the importance of raising awareness among users and adopters, and the strengthening of ex ante legality rules.
- In relation to the umbrella concept of data use, we have said that it can be anything if it has a sufficiently high degree of value equivalence (otherwise we would be talking about utilization or, ultimately, unlawfulness). The right of use is typically embodied in composite data law provisions that provide the basic parameters for the treatment of data. These include the definition of a specific purpose, scope or retention period. On the less explicit side of use, data processing is carried out in pursuit of purposes or opportunities expressed in sectoral law, but the details of which are not specified in the legislation and therefore have to be defined by the controller along general data law principles. There are areas of use which are not covered by a right of use at all, but which have one common characteristic: they are not subject to any explicit prohibition. They are thus framed not by the use, but by the coherent provisions of protection (e.g. principles, legal bases, etc.).
- The law concerning the utilization of data has developed and expanded rapidly in recent years. In the horizontal area of utilization, there are high-profile acts such as the DGA and the DA. In the vertical area, the development of the law on common data spaces is only just beginning, with the EHDS and FIDAR proposals. Common features of the utilization law are the emphasis on the importance of data portability, the introduction of measures to support transparency and usability (through data format), the shift from a by design and by default approach to a protectionist approach, the basic definition of provisions on monetisation, the shift from the role of purpose limitation to utilization, the statement that utilization can be limited, and the indication of the role of anonymisation and pseudonymisation and their placement in the pre-accession phase. It is also important to pioneer rules on the use and protection of legal persons and non-personal data and to prioritise sectoral regulation.

4. From a data-driven perspective, what general shortcomings can be identified in the relevant legislation?

In Chapter 5, we looked at the strengths, weaknesses, opportunities and threats of data law in order to examine its present and possible future. Based on the SWOT analysis, the main weaknesses (sources of dysfunctionality) of the current data regime have been identified. In order to balance the data-based relationships, the foundations of the data law need to be completed, and a first step to this end is to clarify the private law status of data and to clearly establish the doctrinal basis of the data law regime. A system of data rights and contracts

covering all categories of data is also needed to ensure the free flow of data. Further horizontal minimum standards are also needed, in particular for non-personal private data, to ensure clarity of data law.

5. Based on the shortcomings identified, what proposals can be made?

In Chapter 6, I set out proposals to address the problems raised previously in the light of the shortcomings identified. As regards the private law status of data, the most applicable solution seemed to be to treat them as intangible assets. From the perspective of EU law, the concept of data as a legal thing did not seem to be applicable.

In order to complete the horizontal data law, I outlined the possibility of introducing a relational entitlement system, which could be conceived as a bundle of rights (quasi-property-like). The individual elements of this could be activated as data processes progresses along the curve set by the principle of value equivalence. The entitled would be identified by contact principles. The first is to whom/to what the data relates, the second is who created the data. For applicability, I have defined two types of authorizer. The primary holder is the one who originally acquired it. This is the data subject in the case of personal data and the data creator in the case of non-personal data. The secondary right holder is the one who acquired the data by derivative means. This is for example the data creator in the case of personal data or the authorized data user in the case of any data.

The content (sub-entitlements) of the relational right could be the right to hold the data (actual or potential operation), the right of use (purposeful data application and utilization), the right to obtain benefits, the right of disposal and the right to legal protection (primary/secondary legal protection and data source protection).

The data contracts have also been typified. Among these, a distinction was made between data transfer contracts, data processor contracts, data merging or data aggregation contracts, data fiduciary contracts and data broker contracts.

Among the options for horizontal minimum standards, I have identified common definitions, data mandates, minimum standards for data protection and mechanisms for assessing equality of value as regulatory options.

- Summary of results

Answering the research questions was made possible by the research in this thesis. I believe that the imbalanced situation of global data-based relationships, with the current tripartite arrangement we see, can be helped by stronger legislation focused on the autonomy of individuals and market actors. Recognising the principle of equality of value, clarifying the private law status of data, establishing a typology of relational legal mechanisms and data contracts, and introducing minimum standards for horizontal rules could contribute to achieving this objective.

The dysfunctionality resulting from the shortcomings identified by the present data law analysis can be remedied by achieving a horizontal data law status as outlined above (or similar). In relation to data law clarity, based on this thesis, I also believe that the vertical legislative

directions (EU data laws) are adequate, but that the horizontal rules need to be simplified and at the same time completed in order to allow these more specific provisions to take effect. This could be achieved by a general legislation, similar to the GDPR, which could complement (replace) the FFNPDR and DA solutions. As I have tried to take into account practical needs as much as possible, in the absence of legislation, the proposals could be partly or fully implemented through a bottom-up market self-regulation, although presumably with a lower degree of effectiveness.

7.4. Irodalomjegyzék

Folyóiratkcikkek

- Abas Mirzaei, Dean Charles, Hugh Wilkie, Amelie Jay Burgess, „Does human value-expressive brand anthropomorphism on social media lead to greater brand competitiveness?", Journal of Retailing and Consumer Services, Volume 81, 2024.
- Alessandro Mantelero, Giuseppe Vaciago, Maria Samantha Esposito and Nicole Monte, „The common EU approach to personal data and cybersecurity regulation", International Journal of Law and Information Technology, 2020, 28, 2021.
- Alexandra Anghel, Elena Novacescu, Madalina Cuc, „Big Data and Its Secrets: Types of Big Data" Romanian Intelligence Studies Review 27. 2022.
- Amy Affelt, "Big Data, Big Opportunity" Australian Law Librarian, vol. 21, no. 2, 2013.
- Andreas Wiebe, „Protection of industrial data – a new property right for the digital economy?", Journal of Intellectual Property Law & Practice, 2017, Vol. 12, No. 1.
- Andreas Wiebe, „Protection of industrial data – a new property right for the digital economy?" Journal of Intellectual Property Law & Practice, 2017, Vol. 12, No. 1.
- Anya Bernstein, „What Counts as Data?", Brooklyn Law Review, 86(2),
- Balogh Zsolt György, „Közterületi térfigyelés és adatvédelem", Vezetéstudomány XLII. ÉVF. 2011. 3. szám.
- Bankó Zoltán, „A munkáltatói hatalom korlátai a munkaviszony megszüntetése során – a felmondási tilalmak és korlátozások a magyar munkajogban", JURA 2015/2.
- Barcsi Tamás, „Erkölcsi és emberi méltóság a középkori keresztény filozófiában", DÍKÉ. 6.
- Bart Custers and Helena Ursic, „Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection", International Data Privacy Law, vol. 6, no. 1. 2016.
- Bart Custers, Daniel Bachlechner, „Advancing the EU Data Economy - Conditions for Realizing the Full of Potential of Data Reuse", Information Polity, 22(4). 2017.
- Bart Custers, Gianclaudio Malgieri, „Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data", computer law & security review 45., 2022.
- Bart Custers, Helena U Vrabec and Michael Friedewald, „Assessing the Legal and Ethical Impact of Data Reuse: Developing a Tool for Data Reuse Impact Assessments (DRIA)", European Data Protection Law Review (EDPL), 5(3), 2019.

- Bart Custers, Helena U. Vrabec, Michael Friedewald, „Assessing the Legal and Ethical Impact of Data Reuse: Developing a Tool for Data Reuse Impact Assessments (DRIA), European Data Protection Law Review (EDPL), vol. 5, no. 3. 2019.
- Bernard Stiegler: The age of Disruption: Technology and Madness in Computational capitalism. Campbridge, Polity, 2019.
- Blutman László, Görög Márta, „Alapvető alanyi jogi pozíciók a Polgári Törvénykönyvben (2013)”, JK, 2013/6.
- Carlos Eduardo Lourenco, Juliana Correa Ferreira, Vanessa Martins dos Santos, „Humanizing brands in social media: The impact of anthropomorphism on brand identification, engagement, and advocacy”, Journal of Marketing Communications, 1–22.
- Carlos Saura García, „Datafeudalism: The Domination of Modern Societies by Big Tech Companies”, Philosophy & Technology (2024) 37:90, 2024.
- Chander, Anupam „The Racist Algorithm?” Michigan Law review, Volume 115, Issue 6. (2017)
- Charles I. Jones, Christopher Tonetti, „Nonrivalry and the Economics of Data”, American Economic Review, 110(9), 2020. 2819–2858 o.
- Claudio Bonvino, Marco Giorgino, „A valorization framework to strategically manage data for creating competitive value”, Int. J. Production Economics 269., 2024.
- Computer Science Laboratory, SRI International
- Corwin D. Edward, „The Meaning Of Quality”, Quality Progress, Volume 1 Issue 10. 1968.
- Czapári Dóra, Szőke Gergely László, „Az adatvédelem és az adathasznosítás egyik kulcskérdése: a személyes adatok anonimizálása”, JURA, 2022/4.
- Daniel J. Solove, „Introduction: Privacy Self-Management and the Consent Dilemma”, 126 Harv. L. Rev. 1880, 2013.
- Daniel J. Steinbock, „Data Matching, Data Mining, and Due Process”, Georgia Law Review 40, no. 1., 2005.
- Darin K. Fox, "What Is Web 2.0", AALL Spectrum, vol. 13, no. 9. 2009.
- Dirk Bergemann , Jacques Cremer , David Dinielli , Carl-Christian Groh , Paul Heidhues , Maximilian Schafer , Monika Schnitzer , Fiona M. Scott Morton, Katja Seim, Michael Sullivan, „Market Design for Personal Data”, Yale Journal on Regulation, 40(3).
- Douglas M. Kochelek, „Data Mining and Antitrust”, Harvard Journal of Law & Technology 22, no. 2, 2009.
- Edwards, Lilian „Enslaving the Algorithm: From a “Right to an Explanation” to a “Right to Better Decisions”?” IEEE Security & Privacy (2018) 16(3),
- Emily R. D. Murphy, Jesse Rissman, 'Evidence of Memory from Brain Data' 7(1) Journal of Law and the Biosciences 1., 2020.
- Eszteri Dániel, „A blokklánc mint személyes adatkezelési technológia GDPR-megfelelőségéről”, ÁJT, 2020/4.

- Eszteri Dániel, „Az Európai Uniós adatvédelem mindenhová elérő keze: a GDPR alkalmazásának kiterjesztése harmadik országokra, különös tekintettel az amerikai egyesült államokra”, Állam- és Jogtudomány, 65 (2).
- Eszteri Dániel, „Elosztott adatbázisok, okoseszközök, automatikus döntések és a GDPR: adatvédelmi kapcsolódási pontok néhány új technológia vizsgálata kapcsán”, MJ, 2022/9.
- F. Kawohl, (2008) ‘Commentary on Josef Kohler's *The Author's Right* (1880)', in *Primary Sources on Copyright (1450-1900)*, eds L. Bently & M. Kretschmer. www.copyrighthistory.org
- Frances G. Burwell, Kenneth Propp „The European Union and the Search for Digital Sovereignty:: Building “Fortress Europe” or Preparing for a New World?”, Atlantic Council. 2020.
- Francesco Banterle, „Data ownership in the data economy: a European dilemma”, SSRN Electronic Journal, 2018.
- Fred H. Cate, Viktor Mayer-Schönberger, „Notice and consent in a world of Big Data”, International Data Privacy Law, 2013, Vol. 3, No. 2.
- Frits W. Hondius, „Data Law in Europe.” Stanford Journal of International Law, 16., 1980.
- Füzes Barnabás, Szőke Gergely László, „A technológiai változások hatása a munkavégzésre, különösen a munka-magánélet elhatárolására és annak jogi megítélésére”, Pécsi Munkajogi Közlemények 17 : 1. online különszám, 2024.
- Gál István László, „The Protection of the State Secret in the Legal History of Europe”, Zbornik Radova: Pravni Fakultet u Novom Sadu Vol. 56, no. 2, 2022.
- Gianclaudio Malgieri, „’Ownership’ of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?”, Journal of Internet Law, Vol. 20, n.5, 2016.
- Gianclaudio Malgieri, Bart Custers, „Pricing Privacy the Right to Know the Value of Your Personal Data” Computer Law & Security Review Volume 34, Issue 2., 2018.
- Giulia Finocchiaro, Antonio Landi, Gianluca Polifrone,Davide Ruffo, Francesco Torlontano, „The Regulatory Future Of Synthetic Data, Data synthesis as a resource for scientific research, innovation, and public policy in the European legal landscape”, Italian Institute for Privacy and Data Protection, Data Intermediaries Alliance, 2024.
- Görög Márta, „"Valami mocorog a felszín alatt" - Tézis, antitézis és szintézis a személyiségi jog területén”, GJ, 2023/1-2.
- Görög Márta, „A jogi személy személyi értéke”, JK, 2011/11.
- Görög Márta, „A kegyeleti jog gyakorlásának jogosultjairól és az érvényesíthetőség időbeli korlátairól”, PJK, 2005/2.
- Görög Márta, „Az általános személyiségi jog posthumus védelme a német joggyakorlatban”, EJ, 2002/4.
- Görög Márta, „Gondolatok a személyiségi jog egyes összetevőinek kereskedelmi értékéhez”, Corvinus Law Papers CLP – 1/2018.
- Győrffyné Holló Krisztina, „Az információbiztonság jelentősége és története”, Gradus Vol 8, No 2 (2021) 102-112.

- Heleen Janssen, „Detecting New Approaches for a Fundamental Rights Impact Assessment to Automated Decision-Making”, International Data Privacy Law, Volume 10, Issue 1, February 2020.
- Herbert Zech, „A legal framework for a data economy in the European Digital Single Market: rights to use data”, Journal of Intellectual Property Law & Practice, 2016, Vol. 00, No. 0.
- Herbert Zech, „Information as property”, 6 JIPITEC 192, para 1., 2015.
- Hohmann Balázs, „Interpretation the Concept of Transparency in the Strategic and Legislative Documents of Major Intergovernmental Organizations”, Közigazgatási és Infokommunikációs Jogi PhD Tanulmányok 2(1), 2021.
- Hohmann Balázs, „Szempontok munkáltatói teljesítmény-értékelési rendszerek adatkezelési folyamatainak megalapozásához”, Pécsi Munkajogi Közlemények 17 : 1. online különszám, 2024.
- Inge Graef, Raphaël Gellert, Martin Husovec, „Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation”, TILEC Discussion Paper, Tilburg University, 2018.
- James Boyle, „The Second Enclosure Movement and the Construction of the Public Domain” Duke Law School Public Law and Legal Theory Research Paper Series, Research Paper No. 53., 2003.
- Jingran Wang, Yi Liu, Peigong Li, Zhenxing Lin, Stavros Sindakis, Sakshi Aggarwal, „Examining the Dimensions, Antecedents, and Impacts of Data Quality”, J Knowl Econ, 2023.
- John D. Trimmer, „The Present Situation in Quantum Mechanics: a Translation of Schrödinger's "Cat Paradox Paper"”, Proceedings of the American Philosophical Society, 124.
- Jóri András, „Adatvédelem: az alapjogvédelmi teszttől az érdekmérlegelésig”, ABSz, 2018/1.
- Josef Drexl, „Designing competitive markets for industrial data – between propertisation and access”, Max Planck Institute for Innovation and Competition Research Paper No. 16-13, 2016.
- Juan Ortiz Freuler, "Datafication, Identity, and the Reorganization of the Category Individual", Temple Law Review, vol. 95, no. 4. 2023.
- Juhász Csilla: Teljesítményértékelés a gyakorlatban. Jelenkori Társadalmi és Gazdasági Folyamatok. 3, 1 (2008).
- Kimberly A. Houser, John W. Bagby, „The Data Trust Solution to Data Sharing Problems”, Vanderbilt Journal of Entertainment & Technology Law, 25(1), 2023.
- Kirstie Ball: Workplace surveillance: an overview. Labor History, 51:1, 2021.
- Kis Kelemen Bence, Hohmann Balázs, „a Schrems ítélet hatásai az európai uniós és magyar adattovábbítási gyakorlatokra”, Infokommunikáció és Jog, 2016/2-3.
- Kyu Yub Lee, Hyun Park, „Data, Privacy, and Artificial Intelligence”, SSRN Electronic Journal 2022.

- Larisa-Antonia Capisizu, „Legal Perspectives on the Internet of Things," Conferinta Internationala de Drept, Studii Europene si Relatii Internationale 2018.
- Lenkovics Barnabás, „A tulajdonszerzés-módok eredeti, illetve származékos jellege", PJK, 2003/3.
- Luciano Floridi, „Is Semantic Information Meaningful Data?" Philosophy and Phenomenological Research, 2005.
- Maria Nikolova, „The Approach of the European Union to the Information Society" Working Paper, European Parliamen, INDU 101 EN, 2003.
- Maryam Farboodi, Laura Veldkamp, „A Model of the Data Economy", NBER Working Paper No. 28427, 2021.
- Menyhárd Attila, „Az egészségügyi adatok forgalomképessége", Információs Társadalom XXII, 3. szám, 2022.
- Menyhárd Attila, „Köztulajdon - közdolgok – forgalomképesség", PJK, 2005/2.
- Nadezhda Purtova, „Do property rights in personal data make sense after the Big Data turn? Individual control and transparency", 10(2) Journal of Law and Economic Regulation, 2017.
- Nestor Duch-Brown, Bertin Martens, Frank Mueller-Langer, „The economics of ownership, access and trade in digital data", JRC Digital Economy Working Paper 2017-01.
- Nine Riis, „Shaping the Field of EU Data Law", Journal of Intellectual Property, Information Technology and Electronic Commerce Law 14, no. 1, 2023.
- Omri Ben-Shahar, „Data Pollution", 11 J. Legal Analysis 104., 2019.
- Oswald, Marion, Jamie Grace, Sheena Urwin, and Geoffrey C. Barnes. 2018. "Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality." *Information & Communications Technology Law* 27 (2). 223–250 o.
- Paul de Hert, Michael Friedewald, Dara Hallinan, Philip Schütz, „Neurodata and Neuroprivacy: Data Protection Outdated?", *Surveillance & Society* 12(1), 2014.
- Paul De Hert: Identity management of e-ID, privacy and security in Europe. A human rights view,. Information Security Technical Report, 13 sz.
- Paul M. Schwartz, „Property, Privacy, and Personal Data." Harvard Law Review 117 (2004): 2056.
- Pierangela Samarati, Latanya Sweeney, „Protecting Privacy when Disclosing Information k Anonymity and Its Enforcement through Generalization and Suppression" Technical Report SRI-CSL-98-04.
- Polyák Gábor, Szőke Gergely László, „Technológiai determinizmus és jogi szabályozás, különös tekintettel az adatvédelmi jog fejlődésére", In: E-közszolgálatfejlesztés. Nemzeti Közszolgálati Egyetem, Budapest, 2014.
- Purtova, „The Illusion of Personal Data as No One's Property", 7 Law, Innovation and Technology 83, 2015. 28 o.
- Purtova, Nadezhda, Do Property Rights in Personal Data Make Sense after the Big Data Turn?: Individual Control and Transparency (November 13, 2017). N Purtova 'Do

property rights in personal data make sense after the Big Data turn? Individual control and transparency', 10(2) Journal of Law and Economic Regulation November 2017, Tilburg Law School Research Paper No. 2017/21.

- Robert D. McIntosh, Elizabeth A. Fowler, Tianjiao Lyu, Sergio Della Sala, „Wise up: Clarifying the role of metacognition in the Dunning-Kruger effect", Journal of Experimental Psychology: General, vol. 148, no. 11., 2019.
- Samuel D. Warren, Louis D. Brandeis, „The Right to Privacy", Harvard Law Review, Vol. 4, No. 5. 1890.
- Sascha D. Meinrath, James Losey, Victor Pickard, „Digital Feudalism", Advances in Computers, vol. 81. 2011.
- Schultz Márton, „A vagyoni értéku személyiségi javak szabályozási problematikájának egyes kérdései. A tárgyiasulás alapú vagyoni személyiségvédelem" IJ, 2020/2. (75.).
- Shoshana Zuboff, „Big other: surveillance capitalism and the prospects of an information civilization", Journal of Information Technology (2015) 30, 2015.
- Sophie Van Meyel, Maximilian Körner, Joël Meunier, „Social immunity: why we should study its nature, evolution and functions across all social systems", Current Opinion in Insect Science, Volume 28, 2018
- Susan Ariel Aaronson, „Private Firms Want to Control the Data They Collect and Prefer Not toShare It", Centre for International Governance Innovation, 2023.
- Susan Ariel Aaronson, „What Do We Mean by Data Sovereignty and How Might It Impede Data Sharing?", Centre for International Governance Innovation, 2023.
- Susan Ariel Aaronson, „Why Are We Talking about Data as a Public Good?", Centre for International Governance Innovation, 2023.
- Székely Iván, Somody Bernadette, Szabó Máté Dániel, „Biztonság és magánélet: az alku-modell megkérdőjelezése és meghaladása, II. rész" Információs társadalom, 17. évf. 1. sz. 2017.
- Szilágyi Ferenc, „Kié a digitális adat? Az allokatív adatjog létjogosultsága a magánjogi (dologi jogi) megközelítés margóján. I. rész", Polgári Jog 2022/9-10.
- Szilágyi Ferenc, „Kié a digitális adat? Az allokatív adatjog létjogosultsága a magánjogi (dologi jogi) megközelítés margóján. II. rész", Polgári Jog 2022/11-12.
- Szőke Gergely László, „A közadat-újrahasznosítás új európai szabályozása - egy újabb lépés előre", MJSZ, 2021/1., 1. Különszám
- Szőke Gergely László, „Az adatvédelem szabályozásának történeti áttekintése", Infokommunikáció és Jog, 2013/3. (56.)
- Szőke Gergely László, „Recent and Future Developments of PSI Re-use in Europe", Studia Iuridica, 155, Essays of Faculty of Law, University of Pécs, Yearbook of 2017-2018.
- Szőke Gergely László: Gondolatok a hazai titokvédelmi szabályozás rendszeréről, JURA, 2018/2.
- T. Bonaci, J. Herron, C. Matlack and H. J. Chizeck, "Securing the exocortex: A twenty-first century cybernetics challenge," 2014 IEEE Conference on Norbert Wiener in the 21st Century (21CW), Boston, MA, USA, 2014.

- Tóth András, „A tisztességes adatkereskedelmet biztosító szabályozás szükségességéről”, ÁJT, 2021/3.
- Tóth András, „Az Európai Unió (szabályozási) útja a szuverenitás felé az adatalapú gazdaságban”, Európai Tükör, Évf. 24 szám 2., 2021.
- Tóth András, Szabó Endre Győző, Németh Szabolcs, Rudics Regina, Rideg Gergely, „A GDPR és a Digital Markets Act viszonyának tisztázása” IN MEDIAS RES 2023/2., 3, 2023.
- Tóth András: A digitális állam információbiztonsági kihívásai. Budapest, Nemzeti Közszolgálati Egyetem Ludovika Egyetemi Kiadó, 2022.
- Tóth András: a digitális átalakulás szabályozása az Európai Unióban. Budapest, ORAC Kiadó Kft., 2024.
- Ulises A. Mejias, Nick Couldry, „Datafication”, Internet Policy Review Journal On Internet Regulation Volume 8 | Issue 4. 2019.
- Václav Janeček, „Ownership of personal data in the Internet of Things”, Computer Law & Security Review Volume 34, Issue 5, 2018.
- Wolfgang Kerber, „A new (intellectual) property right for non-personal data? An economic analysis, MAGKS Joint Discussion Paper Series in Economics, No. 37-2016, Philipps-University Marburg, School of Business and Economics, Marburg.
- Yann Padova, „Data Ownership versus Data Sharing: And What about Privacy?”, Lex Electronica, 26(1), 2021.

Könyvek és könyvfejezetek

- Albert János, „Az iderendszer korai evolúciójának számítógépes modellezése”, In: Pléh Csaba (Szerk.): A megismeréstudomány és a mesterséges intelligencia filozófiai problémái. Budapest, Akadémia Kiadó, 1998.
- Arany-Tóth Mariann: A munkavállalók személyes adatainak védelme a magyar munkajogban. Szeged, Bába Kiadó, 2008.
- Arany-Tóth Mariann: Személyes adatok kezelése a munkaviszonyban. Budapest, Wolters Kluwer, 2016.
- Balogh Zsolt György: Jogi Informatika. Budapest-Pécs, Dialóg campus Kiadó, 1998.
- Bankó Zoltán, Berke Gyula, Kiss György, Szőke Gergely László: Nagykommentár a munka törvénykönyvéhez. Budapest, Wolters Kluwer Hungary, 2019.
- Bankó Zoltán, Szőke Gergely László: Az információtechnológia hatása a munkavégzésre. Pécs, Utilitates Bt., 2015.
- Bíró György, Lenkovics Barnabás, Barzó Tímea, Pusztahelyi Réka, Juhász Ágnes: Általános tanok és személyek joga. Novotni Kiadó, Miskolc, 2014.
- Bölcskei Krisztián: GDPR kézikönyv, Új Európai Uniós Adatvédelmi Szabályozás. Budapest, Vezinfó Kiadó és Tanácsadó Kft., 2018.
- Charu C. Aggarwal, Philip S. Yu, General Survey of Privacy-Preserving Data Mining Models and Algorithms, in Privacy-Preserving Data Mining: Models and Algorithms, Springer, 2008.

- Clare Southerton, „Datafication”, Laurie Schintler, Connie McNeely, (Szerk.): Encyclopedia of Big Data. Springer, 2020.
- David B. Grigg: A világ mezőgazdasági rendszerei. Mezőgazdasági Könyvkiadó, 1980.
- David Boddy, Albert Boonstra, Graham Kennedy: Managing Information Systems: Strategy and Organisation. Pearson Education, 2008.
- David Lyon: Surveillance Society: Monitoring Everyday Life. McGraw-Hill Education (UK), 2001.
- Dermot Groome, „Chapter 1: Overview of Human Rights Law”, Handbook of Human Rights Investigation, 2nd edition 2011.
- Eszteri Dániel, „A deepfake-technológia adatvédelmi értékelése a GDPR tükrében” In: Aczél Petra, Veszelszki Ágnes (szerk.): Deepfake: a valótlan valóság. Budapest, Médiatudományi Könyvek, 2023.
- Eszteri Dániel, „Az új technológiák megjelenésének hatása a személyes adatok védelmére: gépi tanulás, blokklánc, internet-of-things, agyhullám-olvasás.”, Szemelvények az információs jogokról - a rendszerváltástól napjainkig. Budapest, Patrocinium Kiadó, 2021.
- Florent Thouvenin, Aurelia Tamò-Larrieux, „Data Ownership and Data Access Rights Meaningful Tools for Promoting the European Digital Single Market?”, In: Mira Burri: Big Data and Global Trade Law. Cambridge University Press; 2021.
- Fodor Klaudia Franciska, Gubicz Flóra Anna, „Szerzői jogi felhasználási szerződés”, in Jakab András – Könczöl Miklós – Menyhárd Attila – Sulyok Gábor (szerk.): Internetes Jogtudományi Enciklopédia (Szerzői jog és iparjogvédelem rovat, rovatszerkesztő: Grad-Gyenge Anikó, Pogácsás Anett), 2024.
- Gárdos Péter, Vékás Lajos (szerk.): Nagykommentár a Polgári Törvénykönyvről szóló 2013. évi V. törvényhez
- Gellért György (Szerk.): Nagykommentár a Polgári Törvénykönyvről szóló 1959. évi IV. törvényhez, Budapest, Complex, 2009.
- Gosztonyi Gergely: Cenzúra - Arisztotelésztől a Facebookig. Budapest, Gondolat Kiadó, 2022.
- Görög Márta, „A képmáshoz és hangfelvételhez való jog védelmének fejlődéstörténete és a jogosultat megillető „rendelkezési jog” gyökere”, In: Görög Márta, Menyhárd Attila, Koltay András: A személyiség és védelme - Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül. Budapest, ELTE Állam- és Jogtudományi Kar dékánja, 2017.
- Görög Márta, „A technológia-, tudástranszfer jogi eszközei”, In: Bajmócy Zoltán – Elekes Zoltán (szerk.): Innováció: a vállalati stratégiától a társadalmi stratégiáig. Szeged, JATEPress, 2013.
- Görög Márta, „Gondolatok a személyiség magánjogi védelme körében”, In: Menyhárd Attila, Gárdos-Orosz Fruzsina (Szerk.): Személy és személyiség a jogban. Budapest, Wolters Kluwer, 2016.
- Grad-Gyenge Anikó (Szerk.): Kézikönyv a szerzői jog érvényesítéséhez, ProArt Szövetség a Szerzői Jogokért, 2013.

- Grad-Gyenge Anikó: Egy modern szerzői jog. Budapest, Wolters Kluwer Hungary, 2019.
- Gyenge Anikó: Szerzői jogi korlátozások és a szerzői jog emberi jogi háttere. Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2010.
- Gyertyánfy Péter, Legeza Dénes (szerk.): Nagykommentár a szerzői jogról szóló 1999. évi LXXVI. törvényhez
- Herbert Zech, „Data as a Tradeable Commodity – Implications for Contract Law", Josef Drexl (ed.), Proceedings of the 18th EIPIN Congress: The New Data Economy between Data Ownership, Privacy and Safeguarding Competition, Edward Elgar Publishing, Forthcoming, 2017.
- Hohmann Balázs: Az átláthatóság értelmezése és követelményrendszere a közigazgatási hatósági eljárások tükrében. Pécs, Novissima Kiadó, 2022.
- Hornyák Szabolcs: Az emberi méltóság és egy alapvető jogok elleni bűncselekmények. In: Tóth Mihály, Nagy Zoltán (Szerk.): Magyar Büntetőjog, Budapest, Osiris Kiadó, 2014.
- Jóri András, Soós Andrea Klára, Bártfai Zsolt, Hári Anita: A GDPR magyarázata. Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2018.
- Jóri András: Adatvédelmi Kézikönyv, Elmélet, Történet, Kommentár. Budapest, Osiris Kiadó, 2005.
- Kajtár István: Egyetemes állam- és jogtörténet. Budapest-Pécs, Dialóg Campus Kiadó, 2005.
- Karoliny Eszter, Komanovics Adrienne, Mohay Ágoston, Pánovics Attila, Szalayné Sándor Erzsébet: Az Európai Unió joga. Budapest-Pécs, Dialóg Campus Kiadó, 2015.
- Keleti Arthur, „Nem minden az, aminek látszódni akar - a deepfake és a hitelesség jelene és jövője" In: Aczél Petra, Veszelszki Ágnes (szerk.): Deepfake: a valótlan valóság. Budapest, Médiatudományi Könyvek, 2023.
- Kengyel Miklós: Magyar Polgári Eljárásjog. Budapest, Osiris Kiadó, 2014.
- Kerekné Jakó Nóra, Mikes Lili, Szabó Zsolt: Alkotmányjog. Budapest, Patrocinium Kft., 2021.
- Kovács János: Egyetemes és magyar agrárfejlődés. Budapest, Agroinform Kiadó és Nyomda, 2005.
- Lábady Tamás: A magyar magánjog (polgári jog) általános része. Budapest-Pécs, Dialóg Campus Kiadó, 2012.
- Laura Beth Nielsen, „Relational rights: a vision for law and society scholarship", Cambridge University Press, 2024.
- Lenkovics Barnabás: Dologi jog. Eötvös József Könyvkiadó, 2014.
- Leonard M. Jessup, Joseph S. Valacich: Information systems today: managing in the digital world. Upper Saddle River, N.J.: Pearson Prentice Hall, 2008.
- Lontai Endre, Faludi Gábor, Gyertyánfi Péter, Vékás Gusztáv: Szerzői jog és iparjogvédelem. Budapest, Eötvös József Könyvkiadó Kft., 2015.

- Lontai Endre, Faludi Gábor, Gyertyánfy Péter, Vékás Gusztáv: Magyar polgári jog, szerői jog és iparjogvédelmi jog. Budapest, Eötvös József Könyv- és Lapkiadó Bt., 2015.
- M.A. Nielsen, I.L. Chuang: Quantum Computation and Quantum Information, 2000, Cambridge University Press; első kiadás.
- M.J. Adler: A Guidebook to Learning: For a Lifelong Pursuit of Wisdom. London, Macmillan, 1986.
- Menyhárd Attila, „Forgalomképes személyiség?", In: Menyhárd Attila, Gárdos-Orosz Fruzsina (Szerk.): Személy és személyiség a jogban. Budapest, Wolters Kluwer, 2016.
- Mezei Péter, Harkai István: A platformgazdaság szerzői jogi kihívásai. Budapest, ORAC Kiadó Kft, 2024.
- Mezei Péter: A fájlcsere dilemma – A perek lassúak, az internet gyors. Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2012.
- Mohay Ágoston, „A mesterséges intelligencia szabályozási perspektívái az Európai Unióban", Kis Kelemen Bence – Mohay Ágoston (Szerk.): A technológiai fejlődés jogi kihívásai: Kézikönyv a jogalkotás és jogalkalmazás számára (Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2021)
- Moritz Hennemann, Gordian Konstantin Ebner, Benedikt Karsten, Gregor Lienemann, Marie Wienroeder: Data Act – An introduction. Baden-Baden, Nomos Verlagsgesellschaft mbH & Co. KG, 2024.
- Murray Milgate: Goods and Commodities. In: The New Palgrave Dictionary of Economics. Palgrave Macmillan, London, 2008.
- Parti Tamás: digitális adatok tulajdoni adaptációja a digitális javak vagyonjogi kölcsönhatásainak tükrében. Budapest, Wolters Kluwer Hungary Kft., 2024.
- Pataki Gábor, Szőke Gergely László „Az online személyiségprofilok jelentősége". In: Polyák Gábor (Szerk.): Algoritmusok, keresők, közösségi oldalak és a jog – a forgalomirányító szolgáltatások szabályozása. Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2020.
- Paul Adrien Maurice Dirac: The Principles of Quantum Mechanics. Clarendon Press, 1981.
- Péterfalvi Attila, Révész Balázs, Buzás Péter: Magyarázat a GDPR-ról. Budapest, Wolters Kluwer Hungary, 2018.
- Petrétei József: Az alkotmányos demokrácia alapintézményei. Budapest-Pécs, Dialóg Campus, 2009, 2011.
- Petrétei József: Magyar alkotmányjog I. Budapest-Pécs, Dialóg Campus Kiadó, 2002.
- Pintér Róbert, „Úton az információs társadalom megismerése felé", In: Pintér Róbert (Szerk.): Az információs társadalom - Az elmélettől a politikai gyakorlatig. Budapest, Gondolat Kiadó, Új Mandátum, 2007.
- Pléh Csaba: A megismeréstudomány alapjai. Typotex Kiadó, 2012.
- Polyák Gábor, Pataki Gábor, „A személyes adatok értéke a Facebook–WhatsApp összefonódás versenyjogi értékelésében", In: Polyák Gábor (Szerk.): Algoritmusok,

keresők, közösségi oldalak és a jog – a forgalomirányító szolgáltatások szabályozása. Budapest, HVG-ORAC Lap- és Könyvkiadó Kft., 2020.
- R.B. Seeley és W. Burnside: Twenty Essays on the Practical Improvement of God's Providential Dispensations, as Means of Moral Discipline to the Christian. Oxfordi Egyetem, 1838. 53-54 o. Elérhető: https://books.google.hu/books/about/Twenty_essays_on_the_practical_improveme.html?id=lFwEAAAAQAAJ&redir_esc=y
- Rácz Lilla, „A jogi személyek személyiségvédelme – képzelet vagy valóság?", In: Görög Márta, Menyhárd Attila, Koltay András (Szerk.): A személyiség és védelme. Budapest, Felelős kiadó az ELTE Állam- és Jogtudományi Kar dékánja, 2017.
- Rob Kitchin: The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences. SAGE Publications Ltd, 2014.
- Robert Nozick: Anarchy State And Utopia. Basic Books, 1974.
- Ryan Holiday: Az egyensúly a kulcs. Budapest, 21. Század Kiadó, 2020.
- Sárközy Tamás, „Személy és személyiségvédelem", In: Menyhárd Attila, Gárdos-Orosz Fruzsina (Szerk.): Személy és személyiség a jogban. Budapest, Wolters Kluwer, 2016.
- Sepsi Tibor: GDPR útikalauz adatkezelőknek. Budapest, Wolters Kluwer Hungary, 2019.
- Sir Frederick Pollock: A First Book of Jurisprudence. London, Macmillan and Co., 1918.
- Sólyom László: A személyiségi jogok elmélete. Budapest, Közigazgatási és Jogi Könyvkiadó, 1983.
- Szabó Máté Dániel: Az információs hatalom alkotmányos korlátai. Miskolc, Miskolci Egyetem, 2012.
- Szalai Ákos, „A szervezetek jogi személyiségének mennyiségi elmélete", In: Menyhárd Attila, Gárdos-Orosz Fruzsina (Szerk.): Személy és személyiség a jogban. Budapest, Wolters Kluwer, 2016.
- Szántó György Tibor: Anglia története. Budapest, Maecenas, 1992.
- Szénay László, Villányi László: Agrárgazdaságtan. Budapest, Mezőgazdasági Szaktudás Kiadó, 2000.
- Szőke Gergely László, „A közadatok újrahasznosítása – a szabályozás alapjai", In: Czékmann Zsolt (Szerk.): Infokommunikációs Jog. Budapest, Dialóg Campus, 2019.
- Szőke Gergely László, „A közösségi oldalak működése az európai adatvédelmi szabályozás tükrében", In: Barzó Tímea, Czékmann Zsolt, Csák Csilla: „Gondolatok köztere" A közösségi média személyiségvédelemmel összefüggő kihívásai és szabályozása az egyes államokban. Miskolc, Miskolci Egyetemi Kiadó, 2021.
- Tamás András: Legistica, A jogalkotástan vázlata. Nemzeti Közszolgálati Egyetem, 2013.
- Tattay Szilárd, „Az emberi személy, mint „önmaga tulajdonosa": a donimium siu fogalmától a self-ownerhip eszméjéig, In: Menyhárd Attila, Gárdos-Orosz Fruzsina (Szerk.): Személy és személyiség a jogban. Budapest, Wolters Kluwer, 2016.

- Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein: Introduction to Algorithms. Third Edition. Cambridge, Massachusetts, London, England, The MIT Press, 2009.
- Thomas Hoeren, Stefan Pinelli: European Data Law. Berlin, De Gruyter, 2025.
- Thomas Streinz, „The Evolution of European Data Law" In: Paul Craig, Gráinne de Búrca (Szerk.): The Evolution of EU Law, 3rd edn. Oxford, 2021.
- Todd Groff, Thomas Jones: Introduction to Knowledge Management. London, Routledge, 2003.
- Tolcsvai Nagy Gábor: Szöveg és típus - Szövegtipológiai tanulmányok. Budapest, Tintakönyvkiadó, 2006.
- Tóth András, „A technológia szabályozásának jogi kihívásai", in: Tóth András (szerk.): Technológia jog – Új globális technológiák jogi kihívásai. Budapest, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 2016.
- Tóth András, Koltay András, Lapsánszky András: Nagykommentár a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról szóló, az Európai Parlament és a Tanács 2022. szeptember 14-i (EU) 2022/1925 rendelethez (digitális piacokról szóló jogszabály). Budapest, Wolters Kluwer, 2024.
- Vékás Lajos: Magyar polgári jog – Öröklési jog. Budapest, Eötvös József Könyv- és Lapkiadó Bt., 2014.
- Viktor Mayer-Schönberger, Kenneth Cukier: Big Data. Budapest, HVG Kiadó Zrt., 2014.
- Visegrády Antal: Jogi alaptan. Pécs, Janus Pannonius Tudományegyetem Állam- és Jogtudományi Kar, 1996.
- W.K. Jenkins: Signal Processing, Analog. Encyclopedia of Physical Science and Technology (Third Edition) 2003.
- Yuval Noah Harari: Homo Deus: A holnap rövid története. Magyar kiadás, Animus Kiadó, 2016.
- Z. Karvalics László: Információ, társadalom, történelem. Válogatott írások. Budapest, Typotex Kiadó, 2003.
- Ződi Zsolt, „Elvek és valóság Európában: a PSI-irányelv érvényesülésének problémái (miért nem szereti az európai közszféra megosztani az adatait a magán-vállalkozásokkal?) In: Sáry Pál (Szerk.): Decem anni in Europaea Unione I. - Jogtörténeti és jogelméleti tanulmányok. Miskolci Jogtudományi Műhely 6., Miskolci Egyetemi Kiadó, 2015.
- Ződi Zsolt: Platformok, robotok és a jog. Budapest, Gondolat Kiadó, 2018.

Európai uniós jogszabályok

- Az Európai Parlament és a Tanács 2016/1148/EU irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről
- Az Európai Parlament és a Tanács 2019/1024/EU irányelve a nyílt hozzáférésű adatokról és a közszféra információinak további felhasználásáról (PSI irányelv)

- Az Európai Parlament és a Tanács (EU) 2018/1807 rendelete a nem személyes adatok Európai Unióban való szabad áramlásának keretéről (FFNPDR)
- Az Európai Parlament és a Tanács (EU) 2023/2854 rendelete a méltányos adathozzáférésre és -felhasználásra vonatkozó harmonizált szabályokról (adatrendelet, DA)
- Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról (MI rendelet)
- Az Európai Parlament és a Tanács 2002/14/EK irányelve az Európai Közösség munkavállalóinak tájékoztatása és a velük folytatott konzultáció általános keretének létrehozásáról
- Az Európai Parlament és a Tanács 2002/58/EK irányelve az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (e-Privacy irányelv)
- Az Európai Parlament és a Tanács 2014/65/EU irányelve a pénzügyi eszközök piacairól, valamint a 2002/92/EK irányelv és a 2011/61/EU irányelv módosításáról.
- Az Európai Parlament és a Tanács 2016/680 irányelve a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról (bűnügyi irányelv)
- Az Európai Parlament és a Tanács 2017/745/EU rendelete az orvostechnikai eszközökről
- Az Európai Parlament és a Tanács 2017/746/EU rendelete az az in vitro diagnosztikai orvostechnikai eszközökről
- Az Európai Parlament és a Tanács 2019/1150 rendelete az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról (P2B rendelet)
- Az Európai Parlament és a Tanács 2019/770 irányelve a digitális tartalom szolgáltatására és digitális szolgáltatások nyújtására irányuló szerződések egyes vonatkozásairól
- Az Európai Parlament és a Tanács (EU) 2022/1925 rendelete a digitális ágazat vonatkozásában a versengő és tisztességes piacokról, valamint az (EU) 2019/1937 és az (EU) 2020/1828 irányelv módosításáról (Digitális Piacokról szóló rendelet vagy DMA)
- Az Európai Parlament és a Tanács 2022/2065 rendelete a digitális szolgáltatások egységes piacáról (DSA)
- Az Európai Parlament és a Tanács 2022/2554 rendelete a pénzügyi ágazat digitális működési rezilienciájáról (DORA)
- Az Európai Parlament és a Tanács 2022/2555 irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS2)
- Az Európai Parlament és a Tanács 2022/868 rendelete az európai adatkormányzásról (adatkormányzási rendelet, vagy DGA) által alkotott általános jogi adatfogalom szerint az adatok az aktusok, tények vagy információk digitális megjelenítései

- az Európai Parlament és a Tanács 2024/1183/EU rendelete a 910/2014/EU rendeletnek az európai digitális személyazonossági keret létrehozása tekintetében történő módosításáról
- Az Európai Parlament és a Tanács 2024/2847 rendelete a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről (kiberrezilienciáról szóló rendelet vagy CRA)
- Az Európai Parlament és a Tanács 2025/38 rendelete kiberfenyegetések és -események észlelése, valamint az azokra való felkészülés és reagálás érdekében az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról (kiberszolidaritási rendelet vagy CSA)
- Az Európai Parlament és a Tanács 852/2004/EK rendelete az élelmiszer-higiéniáról
- Az Európai Parlament és a Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról
- Az Európai Parlament és a Tanács 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (adatvédelmi irányelv)
- Az Európai Parlament és a Tanácsnak a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló 2016/679 sz. rendelete (általános adatvédelmi rendelet vagy GDPR)
- Az Európai Unió Alapjogi Charta
- Az Európai Unió működéséről szóló szerződés (EUMSz)
- Digitális tartalom szolgáltatására és digitális szolgáltatások nyújtására irányuló szerződések egyes vonatkozásairól szóló 2019/770 irányelv

Magyar jogszabályok

- A cégnyilvánosságról, a bírósági cégeljárásról és a végelszámolásról szóló 2006. évi V. törvény
- A foglalkozás-egészségügyi szolgáltatásról és a munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről szóló 33/1998. (VI. 24.) NM rendelet
- A foglalkozási betegségek és fokozott expozíciós esetek bejelentéséről és kivizsgálásáról szóló 27/1996. (VIII. 28.) NM rendelet
- A humángenetikai adatok védelméről, a humángenetikai vizsgálatok és kutatások, valamint a biobankok működésének szabályairól szóló 2008. évi XXI. törvény
- A kisajátításról szóló 2007. évi CXXIII. törvény
- A kormányzati igazgatásról szóló 2018. évi CXXV. törvény
- A kötelező egészségbiztosítás ellátásairól szóló 1997. évi LXXXIII. törvény (Ebtv.)
- A közadatok újrahasznosításáról szóló 2012. évi LXIII. törvény
- A közterület-felügyeletről szóló 1999. évi LXIII. törvény (Ktftv.)
- A közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény

- A magasabb összegű családi pótlékra jogosító betegségekről és fogyatékosságokról szóló 5/2003. (II. 19.) ESzCsM rendelet
- A minősített adat védelméről szóló 2009. évi CLV. törvény (Mavtv.)
- A munka törvénykönyvéről szóló 2012. évi I. törvény (Mt.)
- A munkaügyi ellenőrzésről szóló 1996. évi LXXV. törvény
- A munkavédelemről szóló 1993. évi XCIII. törvény (Mvtv)
- A munkavédelemről szóló 1993. évi XCIII. törvény egyes rendelkezéseinek végrehajtásáról szóló 5/1993. (XII. 26.) MüM rendelet
- A nemzeti adatvagyon hasznosításának rendszeréről és az egyes szolgáltatásokról szóló 2023. évi CI. törvény (Nah.tv.)
- A nemzeti köznevelésről szóló 2011. évi CXC. törvény
- A nevelési-oktatási intézmények működéséről és a köznevelési intézmények névhasználatáról szóló 20/2012. (VIII. 31.) EMMI rendelet
- A Polgári Törvénykönyvről szóló 2013. évi V. törvény
- A Rendőrségről szóló 1994. évi XXXIV. törvény (Rtv.)
- A számvitelről szóló 2000. évi C. törvény
- A személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.)
- A szerzői jogok és a szerzői joghoz kapcsolódó jogok közös kezeléséről szóló 2016. évi XCIII. törvény
- A szerzői jogról szóló 1999. évi LXXVI. törvény (Szjt.)
- A szociális hozzájárulásról szóló 2018. évi LII. törvény
- A társadalombiztosítás ellátásaira jogosultakról, valamint ezen ellátások fedezetéről szóló 2019. évi CXXII. törvény (Tbj.)
- A társadalombiztosítási nyugellátásról szóló 1997. évi LXXXI. törvény (Tny.)
- Az adózás rendjéről szóló 2017. évi CL. törvény (Art.)
- Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.)
- Az általános forgalmi adóról szóló 2007. évi CXXVII. törvény
- Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény
- Az egészségügyről szóló 1997. évi CLIV. törvény
- Az egyenlő bánásmódról és az esélyegyenlőség előmozdításáról szóló 2003. évi CXXV. törvény (Ebktv.)
- Az elektronikus hírközlésről szóló 2003. évi C. törvény
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Info.tv.)
- Az önkormányzati hivatalok egységes irattári tervének kiadásáról szóló 78/2012. (XII. 28.) BM rendelet
- Az üzleti titok védelméről szóló 2018. évi LIV. törvény
- Magyarország Alaptörvénye
- Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (Kib.tv.)

Nemzetközi jogi dokumentumok

- Az Európa Tanács 108. Egyezménye
- Emberi Jogok Egyetemes Nyilatkozata
- Emberi Jogok Európai Egyezménye

Esetjogi dokumentumok

- 1/1994. (I. 7.) AB határozat
- 15/1991. (IV. 13.) AB Határozat
- 3110/2013. (VI. 4.) AB határozat
- 4/2017. (XI. 28.) KMK vélemény
- 8/1990. (IV. 23.) AB határozat
- ABI-19532/2011/P
- BH1998. 195.
- BH1999. 331.
- BVerfG65.1. (69.f.)
- C342/12. sz. „Worten" ügy
- C-434/16 sz. „Nowak" ügy
- Dean Spielmann főtanácsnok indítványa, Európai adatvédelmi biztos kontra Egységes Szanálási Testület ügyében (C-413/23. P.)
- Kúria Mfv. 10.636/2015/8.
- MK 154. számú állásfoglalás
- MK 95. számú állásfoglalás
- NAIH/2019/2076/11
- NAIH-1006-3/2022.
- NAIH-963-10/2022

Internetes források

- "The Writing Telegraph", Scientific American. 40 (13): 196. March 1879. Elérhető: https://sciam-cms.s3.amazonaws.com/sciam/cache/file/9AFDF555-B4F7-4FEB-8867941F917A1005.pdf
- „The Technology Landscape Of Data Spaces" Sitra Working Paper
- 2011. évi CXII. törvény indokolása az információs önrendelkezési jogról és az információszabadságról
- 2023. évi CI. törvény végső előterjesztői indokolása a nemzeti adatvagyon hasznosításának rendszeréről és az egyes szolgáltatásokról
- A 29. cikk szerinti munkacsoport 02/2017. számú véleménye a munkahelyi adatkezelésről (WP249)
- A 29. cikk szerinti munkacsoport iránymutatása az (EU) 2016/679 rendelet szerinti hozzájárulásról (WP259 rev.01.)
- A 29. cikk szerinti munkacsoport iránymutatása az adathordozhatóságról (WP 242 rev.01)

- A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Úton a prosperáló adatközpontú gazdaság felé (COM(2014) 442 final)
- A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Európai digitális egységes piaci stratégia (COM(2015) 192 final)
- A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Az Európai Adatgazdaság kiépítése (COM(2017) 9 final)
- A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, A digitális egységes piaci stratégia végrehajtásának félidős értékelése (COM(2017) 228 final)
- A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, A közös európai adattér kialakítása felé (COM(2018) 232 final)
- A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Digitális iránytű 2030-ig: a digitális évtized megvalósításának európai módja (COM(2021) 118 final)
- A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az Európa digitális jövőjének megtervezéséről (COM(2020) 67 final)
- A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Európai adatstratégia (COM/2020/66 final)
- A Mesterséges Intelligencia közös európai megközelítéséről szóló dokumentuma (COM(2021) 205 final)
- A NAIH tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről (2016)
- A pénzügyi adatokhoz való hozzáférésre vonatkozó keretről szóló EU bizottsági javaslat (COM(2023) 360 final)
- Adó Online, „KoKaIn-nal és RADAR-ral veszi fel a harcot az adócsalókkal az APEH” https://ado.hu/ado/kokain-nal-es-radar-ral-veszi-fel-a-harcot-az-adocsalokkal-az-apeh/
- Adrienne Wilmoth Lerner, „Espionage and Intelligence, Early Historical Foundations” Encyclopedia of Espionage, Intelligence, and Security. Elérhető: https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/espionage-and-intelligence-early-historical-foundations
- Agencia Española Protección Datos (AEPD): Technologies and Data Protection in Public Administrations (2020)
- Alexander S. Gillis, „web crawler definition”, TechTarget. Elérhető: https://www.techtarget.com/whatis/definition/crawler
- ALI-ELI Principles for a Data Economy - Data Rights and Transactions - ELI Final Council Draft. 2021. (ALI-ELI Alapelvek)
- Allgemeines Bürgerliches Gesetzbuch (ABGB)

- Aoife Walsh, „TikTok stops working as US ban comes into force” BBC News. Elérhető: https://www.bbc.com/news/articles/cz6p1g54q85o
- Artificial intelligence: Algorithms face scrutiny over potential bias” BBC NEWS (2019) https://www.bbc.com/news/technology-47638916
- Az európai egészségügyi adattérről szóló EU bizottsági javaslat (COM/2022/197 final)
- Belügyminisztérium, Egészségügyi Szolgáltató és Fejlesztési Központ, EESZT lakossági adatkezelési tájékoztató, Hatályállapot: 2023.06.01-től visszavonásig. Elérhető: https://www.eeszt.gov.hu/documents/20182/36430/EESZT_Lakossagi_adatkezelesi_tajekoztato_20230828.pdf/a105eae6-951f-b82a-b707-f06dd441dc17
- Caitlin Andrews, „European Commission withdraws AI Liability Directive from consideration”, IAPP, 2025. Elérhető: https://iapp.org/news/a/european-commission-withdraws-ai-liability-directive-from-consideration
- Cameron Hashemi-Pour, „What is the CIA triad?”, TechTarget. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA
- Carole Cadwalladr, ‘Capitalism is dead. Now we have something much worse’: Yanis Varoufakis on extremism, Starmer, and the tyranny of big tech”, The Guardian. Elérhető: https://www.theguardian.com/world/2023/sep/24/yanis-varoufakis-technofeudalism-capitalism-ukraine-interview
- Chase Bibby, Jonathan Gordon, Gustavo Schuler, Eli Stein, „The big reset: Data-driven marketing in the next normal”, McKinsey & Company, 2021. Elérhető. https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-big-reset-data-driven-marketing-in-the-next-normal
- CORDIS, „Bangemann report: Europe and the global information society”. Elérhető: https://cordis.europa.eu/article/id/2730-bangemann-report-europe-and-the-global-information-society
- Corti Inc. Elérhető: https://www.corti.ai/
- Cuemat, „Data Handling”. Elérhető: https://www.cuemath.com/data/data-handling/
- David McCandless, The beauty of data visualization. 2010. TEDGlobal
- David Weinberger, „The Problem with the Data-Information-Knowledge-Wisdom Hierarchy”, Harvard Business Review. Elérhető: https://hbr.org/2010/02/data-is-to-info-as-info-is-not
- DORDA Rechtsanwälte GmbH; Arthur Cox LLP; Ramón y Cajal Abogados SLP, „Preliminary Assessment Reports on SWIPO IaaS and SaaS Codes of Conduct”, 2020.
- EDPB Opinion 08/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms
- EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR
- EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data
- EDPS, „Opinion on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content” Opinion 4/2017.

- EDPS, „Data Protection” Elérhető: https://www.edps.europa.eu/data-protection/data-protection_en
- EDPS, „Opinion on coherent enforcement of fundamental rights ont he age of big data” Opinion 8/2016.
- Eduardo Baptista, „What is DeepSeek and why is it disrupting the AI sector?”, Reuters, 2025. Elérhető: https://www.reuters.com/technology/artificial-intelligence/what-is-deepseek-why-is-it-disrupting-ai-sector-2025-01-27/

Egyéb források

- Eszteri Dániel, „Adatmonopólium és buboréklét”, Országút (Magyar Szemle Alapítvány). Elérhető: https://orszagut.com/tudomany/adatmonopolium-es-buborekleteszteri-daniel-4438
- Eszteri Dániel, „Neurális adatok és az emberi elme sértetlensége: Az agy-számítógép interfész technológia adatvédelmi problémái Chile legfelsőbb bíróságának ítéletén keresztül”, Társadalomtudományi Kutatóközpont, jtiblog. Elérhető: https://jog.tk.hu/blog/2024/10/neuralis-adatok-emberi-elme-sertetlensege
- EU Bizottság, „EU Compass to regain competitiveness and secure sustainable prosperity”, 2025. Elérhető: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_339
- EU Quantum Technology Strategy, „Supporting Quantum Technologies beyond H2020” Elérhető: https://qt.eu/app/uploads/2020/04/Strategic_Research-_Agenda_d_FINAL.pdf
- EURLEX, „A méltányos adathozzáférésre és -felhasználásra vonatkozó szabályok (adatrendelet)” Elérhető: https://eur-lex.europa.eu/legal-content/HU/LSU/?uri=CELEX:32023R2854&qid=1729329473643
- EURLEX, „A nem személyes adatok Európai Unióban való szabad áramlása” https://eur-lex.europa.eu/legal-content/HU/LSU/?uri=CELEX:32018R1807
- EURLEX, „A rendőri és büntető igazságszolgáltatási szervek által használt személyes adatok védelme” elnevezésű dokumentum összefoglaló. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:310401_3
- EURLEX, „Európai adatkormányzás” Elérhető: https://eur-lex.europa.eu/legal-content/HU/LSU/?uri=CELEX:32022R0868
- Európai Bizottság, „Javaslat az elektronikus hírközlési adatvédelmi rendeletre”. Elérhető: https://digital-strategy.ec.europa.eu/hu/policies/eprivacy-regulation
- Európai Tanács sajtóközleménye a „Budapesti nyilatkozat az új európai versenyképességi megállapodásról”, 2024. Elérhető: https://www.consilium.europa.eu/hu/press/press-releases/2024/11/08/the-budapest-declaration/
- European Data Market Study 2021–2023, D2.5 Second Report On Policy Conclusions. The Lisbon Council (2023).
- European Parliament, „EU AI Act: first regulation on artificial intelligence” Elérhető: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

- European Parliamentary Research Service, Scientific Foresight Unit (STOA): The impact of the General Data Protection Regulation (GDPR) on artificial intelligence PE 641.530. 2020.
- Fehér Könyv a nemzeti adatpolitikáról, Fehér Könyv a nemzeti adatpolitikáról, Budapest, Nemzeti Hírközlési és Informatikai Tanács Szakértői Tanácsadó Testülete, Budapest, 2016. Elérhető: https://www.magyary.hu/wp-content/uploads/2019/09/Adatpolitikai_feher_konyv_201608.pdf
- Gianluca Misuraca, Colin van Noordt, „Overview of the use and impact of AI in public services in the EU", Publications Office of the European Union, Luxembourg, EUR 30255 EN, 2020.
- Hal R. Varian, „Markets for Information Goods", Institute for Monetary and Economic Studies, Bank of Japan, 1999. Elérhető: https://people.ischool.berkeley.edu/%7Ehal/Papers/japan/
- IBM, „The rising NFT tide lifts all tokens: So what is an NFT?", 2021. Elérhető: https://www.ibm.com/think/topics/nft
- IBM, „What is strong AI?". Elérhető: https://www.ibm.com/topics/strong-ai
- Inception Impact Assessment - European free flow of data initiative within the Digital Single Market, Európai Unió Bizottsága (CONNECT.E2), 2016.
- Information Commissioner's Office, „International data transfer agreement and guidance" Elérhető: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/
- Jean-Jacques Rousseau: A társadalmi szerződés. Fordította és a bevezetést írta: Radványi Zsigmond. Budapest, Phönix-Oravetz-Kiadás, 1947.
- Jessica Groopman, „7 common file sharing security risks", TechTarget, 2022. Elérhető: https://www.techtarget.com/searchcontentmanagement/tip/7-common-file-sharing-security-risks
- John Herrman, „TikTok Is Shaping Politics. But How?" The New York Times Elérhető: https://www.nytimes.com/2020/06/28/style/tiktok-teen-politics-gen-z.html
- Julia Carrie Wong, „The Cambridge Analytica scandal changed the world – but it didn't change Facebook", The Guardian, 2019. Elérhető: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook
- Jyoti Narayan, Krystal Hu, Martin Coulter, Supantha Mukherjee, „Elon Musk and others urge AI pause, citing 'risks to society'", Reuters, 2023. Elérhető. https://www.reuters.com/technology/musk-experts-urge-pause-training-ai-systems-that-can-outperform-gpt-4-2023-03-29/
- Kinza Yasar, What is blockchain? Definition, examples and how it works, TechTarget. Elérhető: https://www.techtarget.com/searchcio/definition/blockchain
- land-der-ideen.de, PRECOBS – software for predicting crimes. Elérhető. https://Land-Der-Ideen.De/En/Project/Precobs-Software-For-Predicting-Crimes-355
- Magyarország Mesterséges Intelligencia Stratégiája (2020-2030)
- Magyarország Nemzeti Digitalizációs Stratégiája (2022-2030)

- Marcus Aurelius: Elmélkedések. Fordította: Huszti József. A fordítás alapjául szolgáló kiadás: I. H. Leopold: M. Antoninus imperator ad se ipsum. Oxonii, 1908. Elérhető: https://mek.oszk.hu/00600/00606/ 3 o. (továbbiakban: Elmélkedések)
- Mark Sweney, Dan Milmo, „OpenAI 'reviewing' allegations that its AI models were used to make DeepSeek", The Guardian, 2025. Elérhető: https://www.theguardian.com/technology/2025/jan/29/openai-chatgpt-deepseek-china-us-ai-models
- Martin Keen, „What are GANs?", IBM Technology. Elérhető: https://www.youtube.com/watch?v=TpMIssRdhco&t=1s
- Massimo Pigliucci (City University of New York) „Stoicism", Internet Encyclopedia of Philosophy. Elérhető: https://iep.utm.edu/stoicism/#H4
- Matt Burgess, Reece Rogers, „How to Stop Your Data From Being Used to Train AI", Wired, 2024. Elérhető: https://www.wired.com/story/how-to-stop-your-data-from-being-used-to-train-ai/
- McKinsey & Company, „What is Web3?". Elérhető: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-web3#/
- Michelle Knight, „What Is Data-Driven?", Dataversity, 2021. Elérhető: https://www.dataversity.net/what-is-data-driven/
- Midjourney. Elérhető: https://www.midjourney.com/home
- Misuraca, Gianluca – van Noordt, Colin: Overview of the use and impact of AI in public services in the EU, (Publications Office of the European Union, Luxembourg, 2020)
- Mohammed bin Rashid Center for Government Innovation, Artificial Intelligence to Ensure Compliance with Estonia's Land Use Laws. Elérhető: https://ibtekr.org/en/cases/artificial-intelligence-to-ensure-compliance-with-estonias-land-use-laws/
- Nemzeti infokommunikációs stratégia 2014-2020
- NOYB, „US Cloud soon illegal? Trump punches first hole in EU-US Data Deal" Elérhető: https://noyb.eu/en/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal
- OECD, „Data-Driven Innovation: Big Data for Growth and Well-Being", Paris, OECD Publishing, 2015
- OpenAI, DALL·E 3. Elérhető:https://openai.com/index/dall-e-3/
- OpenAI. Elérhető: https://openai.com/chatgpt/overview/
- Petroc Taylor, „Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2023, with forecasts from 2024 to 2028" STATISTA, 2024. Elérhető: https://www.statista.com/statistics/871513/worldwide-data-created/#:~:text=Over%20the%20next%20five%20years%20up%20to%202028%2C,data%20created%20and%20replicated%20reached%20a%20new%20high.
- Politico, „Trump's in. Here's what it means for Europe." Elérhető: https://www.politico.eu/article/donald-trump-washington-us-elections-win-2024-kamala-harris-europe-russia/

- Prokopios Drogkaris, Javier Gomez Prieto (Szerk.), „Engineering Personal Data Protection in EU Data Spaces”, Version 1.0, ENISA, 2024.
- Proofed, „What Is AI-Generated Content?”. Elérhető: https://proofed.com/knowledge-hub/what-is-ai-generated-content/
- Rahul Rao, „What happens if AI grows smarter than humans? The answer worries scientists.”, Popular Science, Elérhető: https://www.popsci.com/science/ai-singularity/
- Ralf Leszinski, Michael V. Marn, „Setting value, not price”, The Mckinsey Quarterly 1997 Number 1.
- SARTORIUS, „How Manufacturers Are Using Big Data Analytics to Improve Processes”, 2019. Elérhető: https://www.sartorius.com/en/knowledge/science-snippets/how-manufacturers-are-using-big-data-analytics-to-improve-processes-507146
- Sastry Chilukuri, „The role of big data in medicine”, McKinsey & Company, 2015. Elérhető: https://www.mckinsey.com/industries/life-sciences/our-insights/the-role-of-big-data-in-medicine#/
- Second Report on the application of the General Data Protection Regulation (COM(2024) 357 final)
- Soham Jethani, Pankhuri Malhotra, Hena Ayisha és Tanvi Nimje, „The Closing Act of 2024: South Korea’s AI Basic Act”, TLP Advisors. Elérhető: https://techlawpolicy.com/2025/01/the-closing-act-of-2024-south-koreas-ai-basic-act/#:~:text=South%20Korea%20passed%20its%20AI%20Act%2C%20a%20comprehensive,EU%20AI%20Act%2C%20adopting%20a%20similar%20risk-based%20approach
- Sophia Bernazzani Barron, „A Basic Definition of First Party, Second Party, & Third Party Data”, HubSpot.com Elérhető. https://www.bing.com/search?q=first+party+data&qs=UT&pq=first+party&sc=10-11&cvid=398B6C979C8644D8B811AF3980A74637&FORM=QBRE&sp=1&ghc=1&lq=0&ntref=1
- Steve Lohr, The Age of Big Data, N.Y. TIMES (2012) Elérhető: https://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html
- StudyCorgi, „Locke and Berkeley: If a Tree Falls in a Forest.” 2021. https://studycorgi.com/berkeley-and-locke-if-a-tree-falls-in-a-forest/
- Sziklay Júlia: Az információs jogok kialakulása, fejlődése és társadalmi hatása. Doktori értekezés, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskolája, 2011.
- Szőke Gergely László: Mikor tűnik el az ember a személyes adatok mögül? - Avagy az anonimizálás kihívásai. Konferencia-előadás „Az ember a legújabb technológiák között” c. konferencia, Budapest, Nemzeti Közszolgálati Egyetem, 2023.05.31.
- SZTNH, „Árva művek” tájékoztató anyaga, 2023. Elérhető: https://www.sztnh.gov.hu/sites/default/files/10_arva_muvek_2023.pdf#:~:text=%C3%81rva%20m%C5%B1veknek%20nevezz%C3%BCk%20az%20ismeretlen%20vagy%

20ismeretlen%20helyen,%28Szjt.%29%2041%2FB.%20%C2%A7-41%2FE.%20%C2%A7-ai%2C%20a%20138%2F2014.%20%28IV.%2030.%29

- Techopedia: What Does internet of Thnigs (IoT) Mean? https://www.techopedia.com/definition/28247/internet-of-things-iot
- The Lisbon Council, „European DATA Market Study 2021–2023", D2.5 Second Report On Policy Conclusions.
- The New York Times, Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html
- Thomas Margoni, „Public Sector Information Open Data Directive", Technical Report.
- Tim O'Keefe (Georgia State University) „Epicuros", Internet Encyclopedia of Philosophy. Elérhető: https://iep.utm.edu/epicur/
- Tőzsér János, „Metafizika. 4. fejezet: A fizikai tárgyak létezése az időben. 4.4 Thészeusz hajója", ELTE Szabadbölcsészet. Elérhető: https://mmi.elte.hu/szabadbolcseszet/mmi.elte.hu/szabadbolcseszet/index7649.html?option=com_tanelem&id_tanelem=1069&tip=0
- Trevor Haynes, „Dopamine, Smartphones & You: A battle for your time" Harvard University, Science in the News. Elérhető: https://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time/
- University of Cambridge, „Helping police make custody decisions using artificial intelligence", Elérhető: https://www.cam.ac.uk/research/features/helping-police-make-custody-decisions-using-artificial-intelligence
- Vidyut Jha, „DeepSeek vs OpenAI (2025): A Comparative Analysis", AItectonic. Elérhető: https://aitechtonic.com/deepseek-vs-openai/