ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

DR. ANTAL TÍMEA

A compliance és a mesterséges intelligencia kölcsönhatásai

Témavezető: Dr. Számadó Róza Zsuzsánna

**BIZTONSÁGTUDOMÁNYI
DOKTORI ISKOLA**

Budapest, 2026. április 20.

Nyilvános védés teljes bizottsága:

Elnök:

Prof. Em. Dr. Berek Lajos

Titkár:

Dr. Szilágyi Győző

Tagok:

Prof. Em. Dr. Makó Csaba

Dr. Szűcs Endre

Dr. habil Szabó Gyula

Bírálók:

Prof. Dr. Rajnai Zoltán

Dr. habil Velencei Jolán

Nyilvános védés időpontja:

2026.

Óbudai Egyetem
Biztonságtudományi Doktori Iskola

D12) Nyilatkozat a munka önállóságáról, irodalmi források megfelelő módon történt idézéséről

NYILATKOZAT

A MUNKA ÖNÁLLÓSÁGÁRÓL, IRODALMI FORRÁSOK

MEGFELELŐ MÓDON TÖRTÉNT IDÉZÉSÉRŐL

Alulírott dr. Antal Tímea kijelentem, hogy a

A compliance és a mesterséges intelligencia kölcsönhatása

című benyújtott doktori értekezést magam készítettem, és abban csak az irodalmi hivatkozások listáján megadott forrásokat használtam fel. Minden olyan részt, amelyet szó szerint, vagy azonos tartalomban, de átfogalmazva más forrásból átvettem, a forrás megadásával egyértelműen megjelöltem.

Budapest, 2026. április 30.

dr. Antal Tímea

TARTALOMJEGYZÉK

BEVEZETÉS

A XXI. században a vállalatok alkalmazkodóképessége és rugalmas működése alapvető feltétele a hosszú távú sikernek. A szervezetek működésük során folyamatosan szembesülnek a kihívások széles körével: az információs és kommunikációs technológiák (IKT) térnyerésétől kezdve, a felhalmozott és folyamatosan bővülő saját adatvagyon kezelésén, továbbá a munkaszervezési, és/vagy a humánerőforrás-képesség fejlesztésén át. A változó környezethez való alkalmazkodás során a kockázatok minimalizálását, a biztonság erősítését szolgálja a compliance (megfelelőség). A mesterséges intelligencia térnyerése új dimenziókat nyit a vállalati működésben: egyrészt jelentős hatékonyságnövelési lehetőségeket kínál, másrészt új versenyhelyzetet és egyben új típusú kockázatokat is teremt. A compliance hiánya biztonsági kockázat a vállalatra nézve a mesterséges intelligencia képességeivel szemben. Az IKT infrastruktúra folyamatos változása nagymértékben megnehezíti a komplex és heterogén informatikai környezet zárt, teljeskörű, folytonos és kockázatarányos védelmét, ami veszélyeztetheti az elvárt szintű biztonsági ellenállóképesség kialakítását és fenntartását. A vállalkozásoknak nyitottnak kell lenni a modern kihívásokra, és lehetőleg a változások tudatos alakítóivá kell válniuk annak érdekében, hogy ne elszenvedői, hanem olyan befolyásolói legyenek a körülményeknek, amelyek előnyükre képesek fordítani a külső behatásokat.

Az európai gazdaság digitalizációjának hajtóereje a mesterséges intelligencia elterjedése. A téma fontosságát jelzi, hogy az Európai Bizottság meghatározta a fő célokat a digitális infrastruktúra, a készségek, az üzleti és kormányzati szolgáltatások területén. Továbbá kijelölte azokat a teljesítménymutatókat is, melyek lehetővé tehetik a 2030-ig kitűzött célok terén elért eredmények mérését a Digitális Évtized Programban [1]. A program 2025. évi jelentése [2] szerint 2025-re a mesterséges intelligencia forradalma további lendületet kap az alapvető technológiák áttörései miatt, mert azok átalakítják az innováció eddigi határait, újraértelmezik a versenyképességet, és gyökeresen megváltoztatják az emberek mindennapi életét. A munkavállalók már jelenleg is mesterséges intelligencia eszközöket használnak a termelékenység növelése érdekében, ezzel egyszerűsítve a munkafeladatokat és egyúttal támogatva a döntéshozatali folyamatokat. Ugyanakkor új potenciális kockázatok, kihívások is megjelentek a mesterséges intelligencia használata során. Ezt támasztja alá, hogy az Európai Unió (EU) Kiberbiztonsági Ügynöksége (ENISA) a 2024. évi márciusi jelentésében kiemelt kockázatnak, azaz a társadalomra potenciálisan leginkább fenyegető tíz tényező közé, a kilencedik helyre rangsorolta a mesterséges intelligenciát [3].

A fenti tendenciák rámutatnak arra, hogy a compliance és a mesterséges intelligencia kapcsolata kulcsfontosságú kérdéssé vált mind a tudományos vizsgálatok, mind a gyakorlati alkalmazás szempontjából. A mesterséges intelligencia alkalmazása egyrészt hozzájárulhat a megfelelési folyamatok hatékonyságának növeléséhez, másrészt azonban új típusú kockázatokat is generálhat, ami indokolttá teszi annak vizsgálatát, hogy a compliance rendszerek miként képesek kezelni ezt a kettősséget, és milyen szerepet játszanak a szervezeti biztonságtudat erősítésében.

A doktori értekezés a compliance és a mesterséges intelligencia kölcsönhatásainak tudományos vizsgálatával és új tudományos eredmények meghatározásával kíván hozzájárulni a tudomány fejlődéséhez úgy, hogy egyúttal segítséget nyújt a kutatási eredmények gyakorlati felhasználásában is.

A tudományos probléma megfogalmazása

A kutatás központjában a compliance és a mesterséges intelligencia kölcsönhatásainak vizsgálata áll. A compliance és a mesterséges intelligencia két új, a tudomány által egyre behatóbban vizsgált terület. Számos kutatás foglalkozik külön-külön ezekkel a témákkal, azonban kapcsolatuk vizsgálata jelenleg nem egységesen kidolgozott. Mind a két téma „hiper-interdiszciplináris" megközelítést igényel a kutatótól (közgazdaságtudomány–jogtudomány–informatika–szervezés–vezetéstudomány), hiszen piaci térnyerésük a mindennapi munkaköri gyakorlatban érhető tetten.

Az alábbi öt szempont mutatja be, hogy miért tartom szükségesnek a compliance és a mesterséges intelligencia összefüggéseinek megteremtését:

- Mind a két jelenség az elmúlt ötven év társadalmi „terméke". A modern kor kihívásainak való megfeleléséhez szükségesek [4]; [5].
- Számos kutatás foglalkozik mindkét fogalom meghatározásával, viszont a szakirodalomban nincs egy egységes, általános érvényű definíció [6]; [7].
- Az egységes jogi szabályozásuk még szintén kiforratlan annak ellenére, hogy alkalmazásukban a szabványok jelentős szerepet töltenek be. Az erkölcsi és etikai szempontok figyelembevétele elengedhetetlen az alkalmazásuk és a szabályozásuk elméleti kialakításában. Továbbá biztonsági, bizalmi szempontok érvényesítése is nélkülözhetetlen a használatuk során [8]; [9].
- A vállalkozások még újdonságként tekintenek mindkettőre. A tanulás és a tudás alkalmazása speciális képességeket igényelnek az egyén és a szervezet részéről egyaránt, ehhez nyitottság és támogatás szükséges a vállalati vezetés irányából is [10].

Rövid távon mindkettő jelentős anyagi befektetést igényel, viszont hosszú távon versenyelőnyt jelenthet az alkalmazásuk a vállalkozások számára. Menedzsmenteszközként hozzájárulhatnak a fenntartható, rugalmas ellenállóképességű vállalati működéshez; hatékonyabb belső működést alakíthatnak ki; növelhetik a szolgáltatási szintet és az eredményközpontúságot [11]. Szükség van a bevált gyakorlatok megismerésére és vizsgálatára.

- A megfelelés és a mesterséges intelligencia több metszetben kapcsolódnak a kockázati tényezőkhöz. A compliance csökkenti a kockázatokat, míg a mesterséges intelligencia kettős kockázati dimenziót jelent a vállalati compliance folyamatokban. Egyrészt csökkentheti a megfelelőségi kockázatokat azáltal, hogy lehetővé teszi a szabályozói követelmények gyorsabb, pontosabb és erőforráshatékonyabb kezelését, másrészt azonban új kockázatokat generálhat – különösen az átláthatóság, az elszámoltathatóság, az algoritmikus torzítás, valamint a jogi felelősség kérdésköreiben.

A fentiek alapján látható, hogy a problémarendszer többrétegű. A definíciós bizonytalanságok, a szabályozási keretek kiforratlansága, valamint a mesterséges intelligencia által generált kettős kockázati hatás együttesen ahhoz vezetnek, hogy a compliance és az MI kapcsolatának értelmezése jelenleg nem egységes sem elméleti, sem gyakorlati szinten. Ennek következtében a vállalkozások számára nem állnak rendelkezésre egységes, megalapozott módszertani iránymutatások a mesterséges intelligencia alapú megoldások megfelelési célú alkalmazására, amely növelheti a hibás bevezetés kockázatát, a rejtett kockázatok és a szabályozási megfelelési hiányosságok valószínűségét.

Álláspontom szerint mind a compliance, mind a mesterséges intelligencia a tudomány és a gyakorlati alkalmazás számára egyaránt kulcsfontosságú. A megfelelés szükséges a mesterséges intelligencia alkalmazásához; a mesterséges intelligenciát lehet használni megfelelési feladatok ellátására is, tehát kétirányú kapcsolatot lehet meghatározni közöttük. A mesterséges intelligencia mint eszköz és mint kockázati tényező is szerepelhet egy magas színvonalú compliance rendszerben.

A fenti tényezők együttesen arra a tudományos problémára mutatnak rá, hogy a compliance és a mesterséges intelligencia kapcsolatának vizsgálata jelenleg széttagolt, és nem áll rendelkezésre olyan egységes elméleti és gyakorlati keret, amely képes kezelni a mesterséges intelligencia által generált kettős kockázati hatást.

Célkitűzések

Kutatási célok

A kutatás fő célja a megfelelőség és a mesterséges intelligencia kölcsönhatásait tudományos igényű elemzéssel vizsgálni. Ennek keretében cél egyrészt a compliance átfogó fogalommagyarázatát meghatározni szakirodalmi, elméleti kutatásra, funkciókra alapozva; másrészt kérdőíves módszerrel és interjú alkalmazásával elemezni a megfelelőség gyakorlati alkalmazását, valamint a mesterséges intelligencián alapuló használatának jellemzőit a magyar vállalkozások esetében; harmadrészt gyakorlati segédleteket készíteni ajánlások és compliance keretrendszer formájában annak érdekében, hogy a biztonsági szempontok előtérbe kerüljenek a mesterséges intelligencia alkalmazásából fakadó kockázatok kezelése során.

A téma kutatási kérdései

A kutatási célrendszer mentén az alábbi kutatási kérdések (KK) fogalmazódtak meg:

KK1. Hogyan határozható meg a compliance fogalma a szakirodalom, az elméleti vizsgálatok, továbbá a gyakorlati működés és a compliance funkciók összevetése alapján?

KK2. Milyen jellemzők és gyakorlati alkalmazási formák figyelhetők meg a megfelelőség és a mesterséges intelligencia gyakorlati alkalmazásában?

KK3. Milyen olyan gyakorlati segédletek alakíthatók ki, amelyek támogatják a mesterséges intelligencia alkalmazását, kezelik a kockázatokat és erősítik a szervezeti biztonságtudatot?

A téma kutatásának hipotézisei

A kutatási célok és kérdések alapján a következő feltételezések, hipotézisek (H) fogalmazódtak meg:

H1. Feltételezem, hogy a compliance fogalmának szakirodalmi, elméleti, gyakorlati és funkcióbeli értelmezései nem alkotnak egységes rendszert, mely alapján indokolt egy átfogó compliance definíció megalkotása.

H2. Feltételezem, hogy a mesterséges intelligencia eszközhasználata összefügg a compliance rendszerek jelenlétével a hazai vállalkozások esetében.

H3. Feltételezem, hogy a mesterséges intelligencia alkalmazása során a compliance nemcsak a biztonságtudatot növeli, hanem hozzájárul a kapcsolódó kockázatok azonosításához és kezeléséhez is.

Kutatási módszerek

Kutatómunkám során törekedtem az elméleti összefüggések és a gyakorlati eljárások komplex vizsgálatára, valamint kvantitatív és kvalitatív kutatási módszereket is alkalmaztam. A szakirodalom és a szabályozási kereteket bemutató dokumentumok elemzésének fő oka a kutatás megalapozása és az eredmények rendszerbe illesztése volt. A nemzetközi és a hazai stratégiai irányt tartalmazó dokumentumokat és tudományos cikkeket dolgoztam fel.

A compliance fogalmának elemzésekor egyrészt a használatban lévő angol nyelvű kifejezéseket vizsgáltam a biztonság fogalmával együtt, majd bibliometriai eszközök (Web of Science és a Magyar Tudományos Művek Tára nevű adatbázisok) alkalmazásával kísérletet tettem a compliance definiálására 2017-2024 időszakra, majd a 2025. évet is vizsgálva. Másrészt azt vizsgáltam az OpenAlex adatbázisban, hogy mely tudományterületek keretein belül született a legtöbb szakmai elemzés a compliance témájában 2017-2024 időszakban, majd a 2025. évben. A műhelyvitát követően a 2025. év elemzésbe történő bevonása indokolttá vált, figyelemmel arra, hogy a vizsgált terület dinamikus fejlődése és gyors változása befolyásolhatja a tézisek tartalmát.

Az elméleti és a szabályozási keretekre építve alkalmaztam a második kutatási módszert, vagyis a kérdőívezést. Adatfelvételt (MS Forms) végeztem online, önkitöltős módszerrel 2024. 11. 07. és 2024. 12. 16. között. A kérdőív 35 kérdést tartalmazott, melyek között szerepeltek nyitott és zárt kérdések egyaránt. A statisztikai elemzéseket az SPSS 30.0 (SPSS Inc.,Chicago, Illions, USA) és MS Excel segítségével készítettem. A kérdőívet 139 fő töltötte ki, nem reprezentatív a kérdőív minta.

A harmadik módszer 10 strukturált szakértői interjú készítése volt, 15 kérdés mentén, 60–80 perc közötti időtartamban. A kérdések sorrendje kötött volt, az interjúvázlatban lévő kérdések jelentős részére kötelezően választ vártam. Az interjúkat Microsoft Teams vagy telefonos hangrögzítés funkcióval rögzítettem, majd Microsoft Wordbe ültettem át a tartalmat.

A doktori értekezésben nem foglalkozom az adatvédelem témakörével, az Environmental (környezeti), Social (társadalmi) és Governance (irányítási) keretrendszerrel – ESG-vel, továbbá a digitális piacokról szóló jogszabállyal, a NIS2 uniós kiberbiztonsági irányelvvel és a hozzá kapcsolódó szabályozással sem. Ennek oka egyrészt az, hogy a fent említettek a kutatás célrendszerével csak közvetett kapcsolatban állnak, másrészt ezen adatok feldolgozása meghaladná az értekezés keretét.

A kutatás 2026. március 14. napján került lezárásra.

1 KUTATÁS KONTEXTUSA

A fejezet ismerteti a kutatás szempontjából releváns környezetet. Először az adatmennyiség jelentőségére hívom fel a figyelmet, majd a mesterséges intelligencia térnyeréséről írok, kiemelve a kockázatok szerepét. Kiemelt jelentőségű a kutatás aktualitásának alátámasztása, ehhez szükséges a mesterséges intelligencia szabályozási kereteinek vizsgálata.

1.1 Adatturbulencia

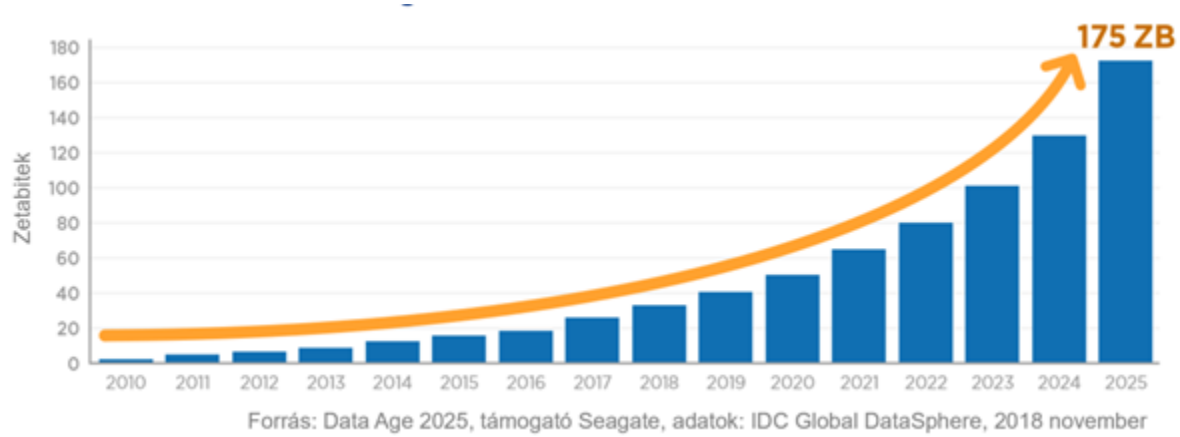
Ebben az alfejezetben az adatforgalom növekedése okán vizsgálom a mesterséges intelligencia trendjeit, elemzem azok kockázatait. Érvelek amellett, hogy miért aktuális és releváns téma a compliance. A Statista [12] adatai szerint egy percnyi adatforgalom az interneten 2021-ben és 2024-ben az alábbi 1. táblázat szerint alakult.

Táblázat 1: Egy percnyi időegység alatt történt adatforgalom az interneten 2021-es és a 2024-es években (Saját szerkesztés)

Adat típusa	**2021**	**2024**
YouTube tartalom feltöltés	500 óra	nincs adat
E-mail küldés	197,6 millió	251,1 millió
Online vásárlás	1,6 millió dollár	nincs adat
Messenger/Whatsapp üzenet, 2021 Reels videók a Facebook és az Instagram oldalain, 2024	69 millió	138,9 millió
TikTok letöltés	5000 letöltés	16000 letöltés
LinkedIn új kapcsolat	9132 új kapcsolat	9000 új kapcsolat

Az adatokból látszik, hogy nőtt az internetforgalom 2021 és 2024 között. Több, mint 25%-kal emelkedett az e-mail küldések száma, háromszorosára nőtt a TikTok letöltés mennyisége. A valóság digitálisan folyamatosan leképeződik, és a fizikai világ mellé fokozatosan egy virtuális valóság kerül. Ebben a folyamatban az előállított és tárolt adatok mennyisége hatványozódik. Az International Data Corporation (IDC) elemzései szerint csak 2018-ban 33

ZB (zetabyte) adat keletkezett, 2025-re ez a mennyiség megközelítheti 175 ZB-ot, ami a 2021-es adat több mint ötszöröse (1 ZB = 10^{21} Byte) [13], melyet az 1. ábra szemléltet.



Ábra 1: A világszerte digitális formában tárolt adatok mennyiségének növekedési üteme [13]

A digitális korszakban az adatok váltak a elsődleges stratégiai erőforrássá, amelyek alapvető szerepet játszanak a gazdasági, társadalmi és szervezeti folyamatok működésében. Számos kutató hangsúlyozza, hogy az adatok a „digitális gazdaság új olajának" tekinthetők, mivel értékük az információalapú döntéshozatalban és az innováció előmozdításában rejlik [14];[15].

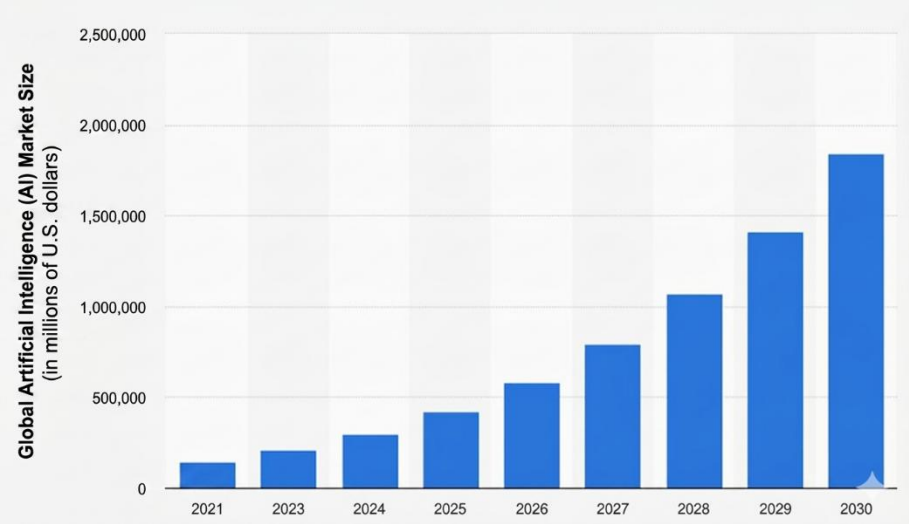
A különböző technológiai trendek számtalan módon fejlesztik az élet minden területét, de az új lehetőségek mellett új hibalehetőségeket, ismeretlen kockázatokat is hordoznak [16]. A biztonsági fenyegetettség erősödik, és egyre kifinomultabb, „egyénre" szabott támadások valósulnak meg. A IKT biztonság és az információbiztonság fenntartása tehát felértékelődött, akárcsak a szabályozások újragondolása. A belső és külső fenyegetések elleni védelem, valamint a jogosulatlan harmadik felek beavatkozásának kizárása elengedhetetlen az adatbiztonsági infrastruktúrák kiépítésében [17].

A szabályozó környezet „természeténél fogva" azonban mindig hátrányban lesz a megjelenő új technológiák gyors fejlődésével szemben, mivel a szabályozóknak először meg kell ismerniük a technológiák gyakorlati működését és kockázatait annak érdekében, hogy megfelelő, de nem túl korlátozó, a gyakorlatban életképes, fenntartható szabályokat alkothassanak. A jogalkotás és szabályozás gyakran később reagál a technológiai változásokra, ezért a szakirodalom javasolja a rugalmas, kockázatalapú megközelítéseket [18].

Mesterséges intelligencia: trendek – kockázatok

Figyelemreméltó kettősség, hogy a mesterséges intelligenciára alapozó ágazatok, szervezetek több tíz milliárdos iparággá nőtték ki magukat az elmúlt évtizedben, azonban a mai napig nem érzékelhető jelentős növekedés a mesterséges intelligenciával kapcsolatos kockázatok mérséklésében. A Statista [19] adatai szerint a mesterséges intelligencia piaci értéke tovább fog

nőni 2030-ig. 2021-ben a közel 100 milliárd dolláros értéke 2030-ra várhatóan hússzorosára, közel 2000 milliárd dollárra nő majd a 2. ábra szerint. Ahogy arra Brynjolfsson és kutatótársai felfigyeltek, a mesterséges intelligencia gazdasági hatásai a robotikai berendezések, eszközök megrendelései volumenének növekedésében, a mesterséges intelligenciával foglalkozó startupok egyre nagyobb számában is tetten érhető [20]; [21]. Empirikus és áttekintő munkák szerint a mesterséges intelligencia beépülése a termelésbe és a vállalati innovációba mérhető vállalkozási és iparági növekedést eredményez majd [20]; [22]. A mesterséges intelligencia gazdasági hatása jelentős: a mesterséges intelligencia alapú eszközök makro- és vállalati szintű hatásait és a növekedési potenciált a közgazdasági irodalom részletesen elemzi [23].



Ábra 2: Mesterséges intelligencia világpiac méret előrejelzés 2021–2030 [19]

A növekvő adatmennyiség kritikus inputként szolgál a mesterséges intelligencia fejlesztéséhez, ami egyben megnöveli az adatkezelési és biztonsági kockázatokat is [15]; [24]. Az adatok minősége értéket képez [25], ezért az adatok estleges sérülése nem csupán működési kockázatot jelent, hanem a bizalom eróziójához is vezethet, amelyek hosszú távon a társadalmi kohéziót is alááshatják [26]; [27]. Eközben a mesterséges intelligencia fogalma, technológiai összetettsége szervesen fejlődik: az etikai iránymutatások, a jogi szabályozások követő üzemmódban, árnyékként kísérik a technológiai pezsgést. Az etikai és jogi irányelvek gyakran utólagos választ adnak a technológiai változásokra; az EU HLEG etikai irányelvei a megbízható mesterséges intelligencia hét követelményét fogalmazták meg [28]. A technológiai fejlődés gyorsasága és a nagy adathalmazok (big data) háttér miatt a modellek komplexitása és működési következményei folyamatosan nőnek [29], [30]. Jelentős felügyeleti, kockázatkezelési/csökkentési tevékenységekre van szükség ahhoz, hogy a megfelelő kontroll érvényesülhessen. A szabványok és kockázatkezelési keretrendszerek szerepe kiemelt: gyakorlati útmutatók (például a NIST AI RMF [31]) a rizikók felmérését és menedzselését

javasolják a fejlesztéstől a telepítésig [31]. A kockázatkezelés ex-ante alkalmazása költséghatékonysági előnyöket biztosít a későbbi incidensekkel szemben [29]; [31]. A biztonság, az adatvédelmi előírásoknak és a jogszabályoknak való megfelelés is kulcsfontosságú kérdések ebben a tekintetben.

A mesterséges intelligencia számos ágazatban van jelen: a pénzügyi szolgáltatások rendszerétől kezdve, az egészségügyi, a közlekedési, a telekommunikáció szektorokon át a mezőgazdaság, a logisztika, és a kereskedelem területéig [32].

A technológia sokszínű iparági penetrációja – pénzügy, egészségügy, logisztika, kiskereskedelem – mind a technikai irodalomban, mind az ipari elemzésekben megfigyelhető [29]; [33]. A cégek körülbelül 30%-a alkalmaz egy vagy több mesterségesintelligencia-technológiát, ezzel szemben a kevésbé digitalizált ágazatok közé tartozik például az utazás és a turizmus, ahol 12% körüli a mesterséges intelligencia térnyerése [34]. Ugyanakkor a rendszerek etikai és társadalmi kockázatai – például igazságosság, átláthatóság és az elszámoltathatóság hiánya – komoly fenyegetést jelentenek [35]; [36]; [37]; [38]; [39]. Kevés vállalat készült fel teljes mértékben a mesterséges intelligencia használatára, vagy azokra a kockázatokra, melyeket az mesterséges intelligencia eszközök jelenthetnek.

A McKinsey 2023-as globális kutatása szerint a válaszadók csupán 21%-a állítja, hogy szervezeteik olyan irányelveket dolgoztak ki, amelyek szabályozzák az alkalmazottak által a mesterséges intelligencia technológiáinak munkájuk során történő használatát [40]. 2019–2023 között a McKinsey többek közt felmérte a mesterséges intelligenciával kapcsolatos kockázatokat. 2023-ban két új kockázati terület is megjelent a leggyakrabban említett rizikófaktorok között: a pontatlanság és a szellemi tulajdon megsértése. A pontatlanságok és IP-kockázatok – különösen generatív modellek esetén – releváns, dokumentált problémák, amelyeket több kutatás is tárgyal [41]. A 2. táblázat bemutatja az öt leggyakoribb kockázati szempontot 2019–2023 között. A 2. táblázat alapján látható, hogy a kiberbiztonság, a szabályozási megfelelőség és a megmagyarázhatóság a legjelentősebb kockázat az adott időszakban.

Táblázat 2: McKinsey kutatásai alapján a mesteréges intelligencia használatának kockázatai (2019–2023) (Saját szerkesztés)

Kockázati szempont	2023	2022	2021	2020	2019
Pontatlanság	56%	nincs adat	nincs adat	nincs adat	nincs adat
Kiberbiztonság	53%	51%	57%	62%	62%
Szellemi tulajdon megsértése	46%	nincs adat	nincs adat	nincs adat	nincs adat
Szabályozási megfelelőség	45%	36%	50%	48%	50%
Megmagyarázhatóság	39 %	22 %	44 %	41 %	39 %

A legnépszerűbb mesterséges intelligencia felhasználási területek több funkcionális tevékenységet is felölelnek a McKinsey 2021-es globális szintű kutatása szerint [42]. Az öt leggyakoribb tevékenység a szolgáltatásműveletek optimalizálása, a mesterséges intelligencia alapú fejlesztések az új termékekben, a contact-center automatizálás, a termékfunkció optimalizálása és a prediktív szolgáltatás és beavatkozás. A kutatás megállapítja, hogy egy vállalat mesterséges intelligencia teljesítményétől függetlenül, a kockázatkezelés szempontjából továbbra is azok a területek a problémásak, ahol számos szempontból szükséges még fejleszteni-fejlődni [42].

Az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) meghatározta a tíz legégetőbb kiberbiztonsági fenyegetést 2030-ig (Ábra 3.). A mesterséges intelligenciával való visszaélés a lista tizedik helyén jelent meg, de trendszerű az erősödése. Véleményem szerint a tizedik hely már most is alacsony ahhoz viszonyítva, hogy húszszorosára emelkedik a mesterséges intelligencia világpiaci részesedése 2030-ra [3].

Ábra 3: Top 10 kiberbiztonsági fenyegetés – 2030 [3]

1 **Szoftverfüggőségek ellátási láncban való kompromittálódása**
2 **Fejlett dezinformációs kampányok**
3 **Digitális megfigyelés autoritarizmusának térnyerése/magánélet elvesztése**
4 **Emberi hibák és kiberfizikai ökoszisztémán belüli örökölt rendszerek kihasználása**
5 **Okoseszköz adatok által okozott célzott támadások**
6 **Űrbe telepített infrastruktúra és objektumok elemzésének és ellenőrzésének hiánya**
7 **Fejlett hibrid fenyegetések terjedése**
8 **Szakemberhiány**
9 **Határokon átnyúló IKT szolgáltatók, mint egyetlen meghibásodási pont**
10 **Mesterséges intelligencia visszaélés**

A fentiek alapján megállapítható, hogy szükség van a mesterséges intelligencia rendszerek elszámoltatható működésének biztosítására, amihez szabályozott folyamatok szükségesek [43]. E folyamatoknak tervezettnek, végrehajthatónak és folyamatosan nyomon követhetőnek kell lenniük annak érdekében, hogy a rendszerek működése átlátható, ellenőrizhető maradjon, és a szükséges beavatkozások megtörténhessenek. A szabályozott folyamatok megfelelő keretet biztosítanak a kockázatok azonosításához és kezeléséhez, ezáltal hozzájárulva a biztonságos és felelős működéshez. Mindezek mellett szükséges, hogy az egyéb szabályozási területek – ideértve az etikai, jogi, biztonsági, felelősségi és átláthatósági aspektusokat – illeszkedjenek a rendszerhez [44]. A compliance-t látom olyan megoldási lehetőségnek, amely hatékony eszköze lehet az elszámoltatható mesterséges intelligencia alkalmazásának, annak képességei, igényei és korlátai kontextusában [45].

Az OECD meghatározta a mesterséges intelligencia felelős kezelésére öt fő alapelvet határozott meg - inkluzív növekedés, fenntartható fejlődés és jólét, emberközpontú értékek és tisztesség, transzparencia és magyarázhatóság, robosztusság és biztonság, elszámoltathatóság [11]. Kiemelendő az utolsó elv, mert hangsúlyozza, hogy szükséges biztosítani a mesterséges intelligencia rendszerek biztonságos, átlátható működését. A mesterséges intelligencia rendszereknek ellenállónak kell lenniük a hibákkal, a visszaélésekkel és az előre nem látható körülményekkel szemben.

A mesterséges intelligencia trendek, a kapcsolódó kockázatok és a szakirodalom alapján a compliance a technológiák folyamatos fejlődésével várhatóan túllép a szervezeti határokon, és valószínűsíthető, hogy komplex üzleti rendszerekben is alkalmazni fogják a megfelelést [46]; [47]; [48]; [49]; [50]; [51].

1.2 Mesterséges intelligencia szabályozási keretek

A compliance és a mesterséges intelligencia kölcsönhatásai tekintetében elengedhetetlen alapvetésnek tartom a mesterséges intelligencia szabályozási kereteinek vizsgálatát.

A mesterséges intelligencia fejlődése új lehetőségeket teremt a gazdasági, társadalmi és tudományos szférában, ugyanakkor kockázatokat hordoz, amelyek indokolttá teszik a szabályozási keretek kialakítását [35]; [52]. A vizsgálathoz először az Európai Unió mesterséges intelligencia térképét rajzolom meg. Az európai uniós vonatkozású mesterséges intelligenciával kapcsolatos, nyilvánosan elérhető dokumentumok (stratégia, ajánlás, irányelv, nyilatkozat, rendelet) elemzései kerülnek középpontba. A vizsgálat módszertana kvalitatív dokumentumelemzés, amely lehetővé teszi a dokumentumok tartalmának rendszerezett feldolgozását, összehasonlítását, és a strukturális mintázatok meghatározását. A

dokumentumok kiválasztásának időbeli kerete 2017–2025. Kizárólag olyan dokumentumokat vizsgálok, melyek a témához közvetlenül kapcsolódnak. A szabályozási térkép kialakításánál az elemzés alapját a célrendszer, az alapelvek meghatározása, a jogi-etikai keretek kidolgozása, a biztonság garantálása képezi. Ezt követően kitekintek az OECD mesterséges intelligencia keretrendszerére, és tanulmányozom az Amerikai Kereskedelmi Minisztérium mesterséges intelligencia kockázatkezelési keretrendszert is.

Az Európai Unió mesterséges intelligencia szabályozási térképe

Az Európai Unió már évek óta foglalkozik a mesterséges intelligencia szabályozás kialakításával. A rendeleti szintű szabályozásnak a hatálybalépéséhez hét évre volt szükség. Az értekezés szempontjából a meghatározó törekvések lényege, hogy az EU érzékeli az mesterséges intelligencia jelentőségét, elsősorban a gazdaság fejlődésével kapcsolja össze. 2017-től számos ajánlás, stratégia, irányelv, továbbá nyilatkozat született, amelyek közül tizenegy dokumentum vizsgálatát végzem el. A szabályozás tartalmának fő iránya az alapelvek meghatározása, a jogi-etikai keretek kidolgozása, a biztonság garantálása a kockázatok minimalizálásával:

- Beruházás az intelligens, innovatív és fenntartható iparba – Az Európai Unió megújított iparpolitikai stratégiája [53],
- Európai Parlament Bizottságnak szóló ajánlása – A robotikára vonatkozó polgári jogi szabályokról [54],
- Európai Tanács EUCO 14/17. számú következtetései [55],
- Mesterséges intelligencia együttműködési nyilatkozat [56],
- Mesterséges intelligencia Európának [57],
- Mesterséges intelligencia magas szintű szakértői csoportja – Megbízható mesterséges intelligenciára vonatkozó etikai iránymutatás, [28],
- Digitális Európa Stratégia [58],
- A mesterséges intelligenciáról szóló összehangolt terv [59],
- Fehér könyv a mesterséges intelligenciáról: A kiválóság és a bizalom európai megközelítése [60],
- Az Európai Parlament és a Tanács Rendelete a Mesterséges Intelligenciára Vonatkozó Harmonizált Szabályok (A Mesterséges Intelligenciáról Szóló Jogszabály) Megállapításáról és Egyes Uniós Jogalkotási Aktusok Módosításáról [61]; [62].

Az EU elsősorban a gazdaság fejlődésével, a technológiai és ipari kapacitásainak erősítésével kapcsolja össze a mesterséges intelligenciát (Digitális Európa Stratégia,

Mesterséges Intelligencia Európának, A mesterséges intelligenciáról szóló összehangolt terv), a digitalizálás az ipar jövőjét fogja meghatározni és a mesterséges intelligenciára eszközként tekint, továbbá, az intelligens technológiák ipari folyamatokba való integrálása hozzájárul a szolgáltatási elemek bővüléséhez (Beruházás az intelligens, innovatív és fenntartható iparba – Az Európai Unió megújított iparpolitikai stratégiája).

Az EU az MI fogalmát az alábbiak szerint határozza meg: a mesterséges intelligencia olyan rendszert jelent, amely intelligens viselkedésre képes, és konkrét célok elérése érdekében vizsgálja a környezetét, továbbá – bizonyos mértékű autonómia birtokában – intézkedést hajt végre (Mesterséges Intelligencia Európának).

Az Unió további általános elveket határozott meg, és kiemelte az etikai és jogi keretek kidolgozásának jelentőségét is (Mesterséges intelligencia együttműködési nyilatkozat, Európai Parlament Bizottságnak szóló ajánlása – A robotikára vonatkozó polgári jogi szabályokról). A nyilatkozat szerint az EU alapvető jogaira és értékeire építve a tagállamok fő célja a folyamatos együttműködés és a közös gondolkodás kialakítása. Kiemelte továbbá a robotikai ágazatban működő, új piaci szegmenseket létrehozó vagy robotokat használó kis- és középvállalkozások és induló innovatív vállalkozások segítését célzó intézkedések fontosságát is. Az etikai elvek kapcsán hangsúlyozta a kockázatok elemzését, javaslatot tett a robotok fejlesztésére, tervezésére, gyártására, használatára és módosítására vonatkozóan egy egyértelmű, szigorú és eredményes, irányadó etikai rendszer kialakításának keretében (Európai Parlament Bizottságnak szóló ajánlása – A robotikára vonatkozó polgári jogi szabályokról). Az álláspontom szerint egy igen jelentős vívmánya ennek a dokumentumnak, hogy egy charta elkészítésére tesz javaslatot, amely a robotikai mérnökök magatartási kódexéből, a robotikai protokollok vizsgálatakor a kutatási-etikai bizottságok által alkalmazandó kódexből, valamint a tervezők és a felhasználók számára alkalmazandó engedélymintákból áll.

Az Európai Tanács rögzíti, hogy ki kell dolgozni a mesterséges intelligencia európai modelljét: a sikeres Digitális Európa kialakításához elengedhetetlen többek közt a jövőorientált szabályozási keretek meghatározása, a kiberbiztonságra vonatkozó egységes szabályozási keret megalkotása, és gyors cselekvés a kialakulóban lévő új trendeknek való megfelelés céljából (Európai Tanács EUCO 14/17. számú következtetései).

Az EU felismerte, hogy fel kell készülni a mesterséges intelligenciából eredő társadalmi-gazdasági változásokra, illetve szükséges a megfelelő etikai és jogi keret biztosítása az Unió értékeire alapozva, valamint az EU alapjogi chartájával összhangban. Rögzítette, hogy szükséges a mesterséges intelligenciára vonatkozó etikai iránymutatás-tervezet kidolgozása, és elemezni kell a biztonságra vonatkozó egyes meglévő szabályok megfelelőségét, továbbá a

felelősségre vonatkozó polgári jogi kérdéseket is, végül a termékfelelősség és az adatvédelem jogi kereteinek fontosságát is hangsúlyozta (Mesterséges Intelligencia Európának Stratégia).

Az EU a megbízhatóságot központi tényezőnek tekinti (Mesterséges intelligencia magas szintű szakértői csoportja – Megbízható mesterséges intelligenciára vonatkozó etikai iránymutatásban), és leszögezi a megbízható mesterséges intelligencia alapelemeit, amelyeknek a rendszer egész életciklusa alatt teljesülniük kell:

- jogszerűség, azaz meg kell felelnie a hatályos jogi szabályozásnak,
- etikusság, vagyis biztosítani szükséges az etikai elveknek való megfelelését,
- műszaki és társadalmi stabilitásnak kell érvényesülnie [28].

Az etikai iránymutatás az alapvető jogokon alapuló etikai elveknek (emberi autonómia tiszteletben tartása, kár megelőzése, méltányosság, megmagyarázhatóság) való megfelelés megközelítését fogalmazta meg. Hét olyan követelményt, amelyeket a mesterséges intelligencia rendszereknek biztosítaniuk kell:

- Emberi cselekvőképesség és felügyelet
- Műszaki stabilitás és biztonság
- Adatvédelem és adatkezelés
- Átláthatóság
- Sokféleség, megkülönböztetésmentesség és méltányosság
- Társadalmi és környezeti jólét
- Elszámoltathatóság

Ezek a követelmények folyamatosan műszaki és nem műszaki tesztelési folyamaton mennek keresztül, és reagálnak a hiányosságokra annak érdekében, hogy a szükségességük és a hatékonyságuk igazolható legyen.

A Digitális Európa Stratégia a mesterséges intelligenciát konkrét, egyedi célkitűzésként határozza meg az 5. cikkben. A mesterséges intelligencia célja a következő működési célkitűzések megvalósítása:

- a mesterséges intelligencia alapvető kapacitásainak, többek között az adatvédelmi jogszabályokkal összhangban lévő adatforrásoknak és algoritmuskönyvtáraknak a kiépítése és megerősítése az Unióban;
- az ilyen kapacitásokhoz hozzáférés biztosítása valamennyi üzleti vállalkozás és közigazgatási szerv számára;
- a tagállamokban meglévő mesterséges intelligenciához kapcsolódó tesztelő és kísérleti létesítmények megerősítése és hálózatba kapcsolása.

A mesterséges intelligenciáról szóló Fehér Könyv [60] rögzíti, hogy az EU célja az innovációt elősegítő jogi környezet kialakítása és a kockázatok csökkentése. A Fehér Könyv az első dokumentum, amely kifejezetten meghatározza a mesterséges intelligencia fejlesztésének és alkalmazásának lehetséges jogi keretrendszerét. Kiemeli, hogy az uniós jogszabályok főszabály szerint az MI bevonásától függetlenül teljes mértékben alkalmazandók maradnak. Figyelemmel kell lenni azonban arra is, hogy a mesterséges intelligenciából eredő kockázatok kezelése miatt szükség lehet akár egyes jogi eszközök kiigazítására. Alapelv, hogy a mesterséges intelligenciára vonatkozó új szabályozási keretnek hatékonynak és biztonságosnak kell lennie, amit kockázatalapú megközelítéssel lehet érvényre juttatni. A Bizottság álláspontja szerint egy MI-alkalmazást főszabály szerint magas kockázatúnak kell tekinteni, ha mind a két alábbi kumulatív feltételnek megfelel:

- Olyan ágazatban használják, ahol – tekintettel a jellemzően végzett tevékenységek természetére – jelentős kockázatok várhatók.
- Az adott ágazatban olyan módon használják a mesterséges intelligencia alkalmazást, ami jelentős kockázatokat okozhat.

A Fehér Könyv meghatározta a nagy kockázatú MI alkalmazásokra vonatkozó követelmények fő elemeit:

- a rendszerek tanításához használt adatok;
- adat- és nyilvántartás-megőrzés;
- tájékoztatás;
- stabilitás és pontosság;
- emberi felügyelet;
- egyes konkrét MI alkalmazásokra vonatkozó egyedi követelmények.

A követelmények ellenőrzéséhez és biztosításához objektív, előzetes megfelelőségértékelésre van szükség, ami tesztelési, ellenőrzési vagy tanúsítási eljárásokat foglalhat magában. A megfelelőségértékelést kötelezővé tenné minden szereplőnek: tehát szükséges a nemzeti hatóságok általi ellenőrzés, továbbá a tényleges bírósági jogorvoslati lehetőségek biztosítása is. Ez a dokumentum alapvetően befolyásolta az Európai Parlament és a Tanács Rendelete a Mesterséges Intelligenciára Vonatkozó Harmonizált Szabályok (A Mesterséges Intelligenciáról Szóló Jogszabály) Megállapításáról és az Egyes Uniós Jogalkotási Aktusok Módosításáról szóló tartalmát. A rendelet tehát jelentős mérföldkő a mesterséges intelligencia szabályozásában. Összetett, kockázatalapú szabályozási környezetet határoz meg, továbbá jelentős, akár a globális árbevétel 6%-át kitevő bírsági tételeket is megenged. A

rendelet nem definiálja a mesterséges intelligencia fogalmát, hanem azt határozza meg, hogy mi a mesterséges intelligencia rendszer, és hogy az ilyen technológián alapuló rendszereknek milyen előírásoknak kell megfelelni. A jogszabály a konkrét célkitűzéseket, a várható eredményeket és a teljesítménymutatókat is meghatározza. A teljesítménymutatókat alkotó adatokat érdemes lenne már előzetesen megvizsgálni annak érdekében, hogy a változások minél pontosabban nyomon követhetők legyenek.

A 9. cikkben meghatározott kockázatkezelési rendszer lényege abban ragadható meg, hogy ötvözi a plan–do–check–act (PDCA; tervezés–cselekvés–ellenőrzés–beavatkozás) logikáját a kockázatmenedzsment módszertanával. A kockázat fogalma egy esemény bekövetkezéséből eredő azon veszélyre utal, amelynek következtében egy tevékenység tényleges eredménye eltér a tervezettől. A kockázatkezelés olyan tudatos és strukturált tevékenységek összessége, amelyek célja, hogy a tényleges eredmény a lehető legjobban megközelítse az elvárt kimenetet. A kockázatmenedzsment magában foglalja a kockázatelemzést, amely során mérik a kockázat bekövetkezésének valószínűségét és lehetséges hatását, továbbá azonosítják a kockázat forrását, a konkrét kockázati tényezőket, az érintett tevékenységeket, a korai figyelmeztető jeleket, valamint kidolgozzák a kezelési akciótervet. A PDCA-ciklus a hatékony feladatvégzés folyamatos fejlesztésére helyezi a hangsúlyt ismétlődő lépéseken keresztül [63] A ciklusban a folyamatok azonosítása, tervezése, végrehajtása, ellenőrzése és folyamatos fejlesztése áll a középpontban annak érdekében, hogy a szervezet hatékonyan és eredményesen teljesítse stratégiai céljait, valamint megfeleljen a külső felek elvárásainak [64]. Ennek keretében a folyamat első lépése a teendők megtervezése, amelyet a feladat végrehajtása követ. Ezután az eredmények ellenőrzése és értékelése, majd szükség esetén beavatkozás történik a folyamat hatékonyabbá tétele érdekében. A ciklus iteratív jellegének köszönhetően a teljes folyamat folyamatosan monitorozható és fejleszthető, ezáltal biztosítva a működés adaptivitását és a kockázatok tudatos kezelését.

A rendelet 53. cikke határozza meg az általános célú MI modellek szolgáltatóira vonatkozó gyakorlati kötelezettségeket. Kiemeli, hogy el kell készíteni és naprakészen kell tartani a modell műszaki dokumentációját, információkat és dokumentációt kell kidolgozni, naprakészen tartani és rendelkezésre bocsátani a mesterséges intelligencia rendszerek azon szolgáltatói részére, amelyek az általános célú MI modellt be kívánják építeni MI rendszereikbe. Szükséges a szerzői és kapcsolódó jogokra vonatkozó uniós jognak való megfelelés bevezetésére irányuló politika, továbbá kellően részletes összefoglaló készítése, valamint elengedhetetlen egy, az általános célú MI modell működésének tanításához használt oktatási anyag közzététele is.

A rendelet 54. cikke szolgálja a biztonságot és az átlátható működést, mert az általános célú MI rendszernek az Unió piacán való forgalomba hozatalát megelőzően a harmadik világ országaiban telepített szolgáltatóknak írásbeli meghatalmazással ki kell nevezniük egy, az Unióban székhellyel rendelkező képviselőt.

Az 55. cikk további kötelezettségeket állapít meg a rendszerszintű kockázatot jelentő általános célú MI modellek szolgáltatóinak. Eszerint modellértékelést kell végezni a technika aktuális állásának megfelelő, szabványosított protokollokkal és eszközökkel összhangban, továbbá értékelni és enyhíteni kell az esetlegesen rendszerszintű kockázatot jelentő általános célú MI modellek fejlesztéséből, forgalomba hozatalából vagy használatából eredő uniós és rendszerszintű kockázatokat. Szükséges nyomon követni és dokumentálni, majd indokolatlan késedelem nélkül jelenteni a mesterséges intelligencia hivatal, és adott esetben az illetékes nemzeti hatóságok részére a súlyos és váratlan eseményeket annak érdekében, hogy az azok kezelését szolgáló korrekciós intézkedésekre vonatkozó információkat az illetékes szervek a megfelelő szintű kiberbiztonsági védelem biztosítása érdekében elemezhessék.

Az uniós rendeleti szabályozás szintjén gyakorlati szabályozást is tartalmaz az 56. cikk, mely szerint gyakorlati kódexek kidolgozása szükséges a rendelet megfelelő gyakorlati alkalmazhatóságához. Ennek nyomán született meg a mesterséges intelligencia általános célú gyakorlati kódexe, amely 2025. augusztus 2. napjától alkalmazandó. A 3. táblázat mutatja be a gyakorlati kódexnek a mesterséges intelligencia rendelettel kapcsolatos összefüggéseit, továbbá tartalmaz egy, a kutatás szempontjából releváns tartalmi összefoglalást is.

Táblázat 3: MI általános célú gyakorlati kódex – MI rendelet összefüggései és tartalmi összefoglalása (Saját szerkesztés)

MI általános célú gyakorlati kódexe	**MI rendelet**	**Tartalom**
Átláthatóság fejezet	53. cikk	Gyakorlati sablont ad a dokumentáció tartalmára vonatkozóan adatok, mérések, módszertanok kidolgozására. Fő elemei: általános információk; modelltulajdonságok; forgalmazási módszerek és licencek; használati paraméterek; képzési folyamat; képzéshez, teszteléshez és validáláshoz használt adatokra vonatkozó információk; számítástechnikai erőforrások (képzés során); energiafogyasztás (képzés és alkalmazás során).

MI általános célú gyakorlati kódexe	MI rendelet	Tartalom
Szerzői jog fejezet	53. cikk	Öt pontból álló intézkedési sorvezetőt határoz meg a szerzői jogok védelme érdekében. Szükséges a szerzői jogi politika kidolgozása, naprakészen tartása és végrehajtása. A világhálón történő keresés során csak törvényesen hozzáférhető, szerzői joggal védett tartalmakat reprodukálhat és használhat fel. A világhálózat feltérképezésekor azonosítani kell és tiszteletben kell tartani a szerzői jogokat. Csökkenteni szükséges a szerzői jogokat sértő eredmények kockázatát. Ki kell jelölni egy kapcsolattartót, és biztosítani szükséges a panaszok benyújtásának lehetőségét.
Biztonságról és védelemről szóló fejezet	55. cikk	Ez a fejezet biztosítja a legpontosabb és legrészletesebb gyakorlati javaslatokat a rendszerszintű kockázatok kezelésére tíz kötelezettségvállalás meghatározásával: • Biztonsági és védelmi keretrendszer kialakítása, alkalmazása, megújítása. • Rendszerszintű kockázatok azonosítása strukturált folyamat keretében, rendszerszintű kockázati forgatókönyvek kidolgozásával. • Rendszerszintű kockázatelemzés kialakítása. • Rendszerszintű kockázat elfogadásának meghatározása. • Biztonsági intézkedések meghatározása. • Védelmi intézkedések meghatározása. • Biztonsági és védelmi modelljelentések kialakítása. • Rendszerszintű kockázati felelősség egyértelmű megosztása. • Súlyos incidensek jelentése. • További dokumentációs feladatok meghatározása és átláthatóság biztosítása.

Nizza megjegyzi továbbá, hogy az egyes modellek szerinti szabályozás a túlzott költségek és bizonytalanság miatt gátolhatják a kutatásokat [65]. Vannak azonban olyan kutatók, akik szerint a hatások fordítottak, és a jogszabály még akár serkentheti is a publikációk számát [28]; [66]; [67]; [68]; [69].

Az OECD MI keretrendszer

Az OECD 2022-ben meghatározta a mesterséges intelligencia rendszerek osztályozási keretrendszerét [70]. Kiindulópontot biztosít a mesterséges intelligencia közös megértésének elősegítéséhez, tekintettel arra, hogy azonosítja a mesterséges intelligencia rendszerek jellemzőit, támogatja a kockázatmenedzsmentet, továbbá biztosítja a minőségmenedzsment szemléletet is.

A keretrendszer a mesterséges intelligencia rendszereit és alkalmazásait a következő dimenziók szerint osztályozza:

- Emberek és bolygó viszonya: amelynek lényege az emberközpontú, megbízható mesterséges intelligencia. Azonosítja azokat az egyéneket és csoportokat, akik kölcsönhatásba lépnek egy alkalmazott MI rendszerrel, de azokat is, akikre csupán hatással van vagy lehet (pl. felhasználók és az érintett stakeholderek). Fontos továbbá a mesterséges intelligencia választhatósága, illetve annak hatása az emberi jogokra, a környezetre, a jólétre, a társadalomra.
- A gazdasági kontextus tekintetében a jellemzők közé tartozik maga az ágazat, amelyben a mesterséges intelligencia rendszert alkalmazzák (pl. egészségügy, pénzügy, gyártás), továbbá az üzleti funkciója és modellje, kritikus (vagy nem kritikus) jellege, hatása és mértéke, valamint a technológiai érettsége.
- Az adatok és input kapcsán a jellemzők közé tartozik azok eredete, a gépi és/vagy emberi gyűjtési módszertan, az adatstruktúra és -formátum, valamint az adatok tulajdonságai is.
- A mesterséges intelligencia modellben az alapvető jellemzők közé tartozik a műszaki típus, a modell felépítésének és a felhasználásának módja.
- A feladat és output dimenziónak a jellemzői közé tartoznak többek közt a rendszerfeladat(ok), a cselekvési autonómia, vagy az alapvető alkalmazási területek, továbbá az értékelési módszerek.

Tehát mindegyiknek megvannak a saját attribútumai vagy aldimenziói, amelyek relevánsak az adott MI rendszerek értékeléséhez. A fenti dimenziókra építve javasolta az OECD a mesterséges intelligencia rendszer kapcsolódó etikai és társadalmi kockázatainak felmérését, amelyek számos ágazatban jelentős gyakorlati jelentőséggel bírhatnak. Függetlenül a kockázati szintek számától vagy attól, hogy melyik szervezet javasolja ezeket, az OECD megállapítása szerint az alábbi három kritérium mindenképp szükséges a mesterséges intelligencia rendszer kockázati szintjének meghatározásához:

- Méret, azaz a káros hatások súlyossága és bekövetkezésük valószínűsége;
- Hatály – célterület, azaz alkalmazási kör, például az érintett személyek száma;
- Opcionalitás, azaz a választás mértékének összehangolása: a mesterséges intelligencia rendszer hatásainak való kitettség. Ez azt jelenti, hogy a felhasználók vagy az érintett érdekelt felek milyen mértékben dönthetnek arról, hogy ki vannak-e téve egy mesterséges intelligencia rendszer hatásainak vagy sem, aktív vagy passzív-e a részvételük. Tehát ez az a mérték, amelyben a felhasználók kivonhatják magukat a mesterséges intelligencia rendszer „hatásai” vagy „befolyásai” alól.

Mesterséges intelligencia kockázatkezelési keretrendszer

2023 januárjában az Amerikai Kereskedelmi Minisztérium megalkotta a Mesterséges intelligencia kockázatkezelési keretrendszert (AI RMF 1.0) [71], aminek egyik lényege, hogy rugalmas alkalmazási lehetőségei ágazatspecifikumoktól függetlenek. A keretrendszer célja, hogy a szervezeteknek és az egyéneknek olyan eszközt biztosítson, amely növelheti a mesterséges intelligencia rendszerek megbízhatóságát, és elősegíti a mesterséges intelligencia rendszerek felelős tervezését, fejlesztését, használatát és fenntartását.

A keretrendszer két fő részből áll: az 1. rész bemutatja, hogy a szervezetek milyen módon képesek meghatározni a mesterséges intelligencia rendszerrel kapcsolatos kockázati tényezőket. Ehhez elemzést készít a mesterséges intelligencia lehetséges kockázatairól, majd meghatározza a megbízható MI rendszerek jellemzőit, úgy, mint érvényesség, megbízhatóság, biztonságos és rugalmas elszámoltathatóság és átláthatóság, magyarázhatóság és értelmezhetőség, fokozott adatvédelem biztosítása és méltányosság a negatív hatások kezelésében. A 2. rész négy olyan fő funkciót mutat be, amelyek segíthetnek a szervezeteknek a mesterséges intelligencia rendszerek kockázatainak gyakorlati kezelésében, és az ehhez szükséges munkamódszerek további alkategóriáinak meghatározásában. A négy funkció és a hozzájuk kapcsolódó elsődleges feladatok az alábbiak:

Az irányítás (govern)

- kockázatkezelési kultúrát alakít ki a mesterséges intelligencia rendszereket tervező, fejlesztő, üzembe helyező, értékelő vagy beszerző szervezetekben;
- olyan folyamatokat, dokumentumokat határoz meg, amelyek előre jelzik, azonosítják és kezelik a rendszer által jelentett kockázatokat, eljárásokat;
- biztosítja a lehetséges hatások felmérését;
- összekapcsolja a mesterséges intelligencia rendszerek tervezésének és fejlesztésének a szempontjait a szervezeti értékekkel, és lehetővé teszi a szervezeti gyakorlatok és kompetenciák kialakítását;
- a termék teljes életciklusával és a kapcsolódó folyamatokkal foglalkozik.

A feltérképezés (map)

- javítja a szervezet kockázatazonosító képességét;
- ellenőrzi a felhasználásra vonatkozó feltételezéseket;
- lehetővé teszi annak felismerését, hogy a rendszerek működése eltávolodott a tervezett keretektől;
- azonosítja az alkalmazásban lévő MI rendszerek előnyös felhasználási módjait;

- azonosítja, érthetővé teszi a mesterséges intelligencia folyamatok korlátait;
- a mesterséges intelligencia rendszerek tervezett használatához kapcsolódó ismert és előre látható negatív hatásokat azonosítja;
- előre jelzi a mesterséges intelligencia rendszerek rendeltetésszerű használaton túli alkalmazásából eredő kockázatokat.

A mérés (measure)

- kvantitatív, kvalitatív vagy vegyes módszerű eszközöket, technikákat és módszereket alkalmaz a mesterséges intelligencia kockázatok és a kapcsolódó hatások elemzésére, értékelésére, összehasonlítására és nyomon követésére;
- felhasználja a feltérképezés funkcióban azonosított mesterséges intelligencia kockázataira vonatkozó ismereteket, és biztosítja azok dokumentálását;
- meghatározza és nyomon követi a folyamatok tesztelését;
- nyomon követhető alapot biztosít a vezetői döntések meghozatalához;
- biztosítja az objektív, megismételhető vagy méretezhető tesztelési, értékelési, ellenőrzési és érvényesítési folyamatokat úgy, hogy a mérési eredményeket a kezelés funkcióban használhatják fel a kockázatfigyelés és a válaszlépések elősegítésére.

A kezelés (manage) lényege, hogy a kockázati erőforrásokat, folyamatokat és a kockázatokat egymás mellé rendeli. A kockázatkezelés olyan terveket jelent, amelyek célja az incidensekre vagy eseményekre való reagálás, az azokból való felépülés, valamint az azokról való kommunikáció.

Az első három funkció megvalósítása biztosítja az átláthatóság és az elszámoltathatóság növelését a kezelés során. Az irányítás az a funkció, ami a mesterséges intelligencia kockázatkezelési folyamatainak és eljárásainak minden szakaszára vonatkozik, míg a másik három funkció kifejezetten MI rendszerspecifikus.

Szabályozási keretek strukturális mintázata

A vizsgált szabályozási és szakpolitikai dokumentumok alapján több visszatérő strukturális mintázat azonosítható. Az első mintázat a gazdasági és innovációs célrendszer megjelenése, amely különösen az európai uniós dokumentumokban hangsúlyos. Az EU a mesterséges intelligenciát nem kizárólag technológiai jelenségként kezeli, hanem a versenyképesség, az iparfejlesztés, a digitális átállás és az innováció eszközeként értelmezi. Ezzel szemben az OECD keretrendszere tágabb társadalmi-gazdasági összefüggésbe helyezi a mesterséges intelligencia rendszereket, míg az AI RMF 1.0 elsősorban szervezeti és kockázatkezelési nézőpontból közelíti meg a kérdést.

A második strukturális mintázat a megbízhatóság és biztonság központi szerepe. Mindhárom rendszer abból indul ki, hogy a mesterséges intelligencia alkalmazása csak akkor tekinthető elfogadhatónak, ha biztosítható a rendszerek jogszerű, biztonságos, átlátható és elszámoltatható működése. Az uniós megközelítés ezt normatív és jogi követelményrendszerként rögzíti, az OECD osztályozási és értékelési dimenziók mentén rendszerezi, míg az AI RMF 1.0 gyakorlati kockázatkezelési funkciókhoz kapcsolja.

A harmadik mintázat a kockázatalapú szabályozási logika térnyerése. Az EU MI rendelete a kockázatok alapján differenciálja a kötelezettségeket, és különös hangsúlyt helyez a magas kockázatú rendszerekre, valamint az általános célú MI modellekre. Az OECD keretrendszere a kockázat meghatározásakor a káros hatások súlyosságát, az érintetti kört és az érintettek választási lehetőségét emeli ki. Az AI RMF 1.0 ezzel szemben nem jogi kategóriákat képez, hanem a kockázatok feltárására, mérésére és kezelésére alkalmas szervezeti folyamatokat határoz meg.

A negyedik strukturális mintázat a folyamatszemlélet és életciklus-alapú megközelítés. A vizsgált dokumentumok nem egyszeri megfelelési követelményként tekintenek a mesterséges intelligencia szabályozására, hanem folyamatos ellenőrzési, értékelési és fejlesztési feladatként. Ez különösen jól látható az EU MI rendelet kockázatkezelési rendszerében, valamint az AI RMF 1.0 irányítás–feltérképezés–mérés–kezelés funkcióiban. A mesterséges intelligencia rendszerek megfelelősége tehát nem statikus állapot, hanem dinamikus, ismétlődő és dokumentált folyamat.

Az ötödik mintázat az irányítási és felelősségi struktúrák erősödése. Az EU szabályozása konkrét jogi kötelezettségeket, dokumentációs előírásokat, megfelelőségértékelési mechanizmusokat és hatósági ellenőrzési lehetőségeket határoz meg. Az OECD keretrendszere az érintettek, felhasználók és társadalmi hatások azonosítására helyezi a hangsúlyt. Az AI RMF 1.0 a szervezeti felelősség, a belső folyamatok, a kockázatkezelési kultúra és a vezetői döntéshozatal szerepét emeli ki. Ennek alapján a compliance nem pusztán jogkövetési kérdésként jelenik meg, hanem irányítási, szervezeti és kockázatkezelési funkcióként is.

Szabályozási keretek összehasonlító elemzése

Megállapítható, hogy az Európai Unió megközelítése normatív és szabályozásközpontú, mivel célja a mesterséges intelligencia rendszerek jogilag kikényszeríthető, harmonizált keretek közé helyezése. Az EU modellje a jogszerűség, az alapjogvédelem, a biztonság, az átláthatóság és az elszámoltathatóság követelményeire épül, és a megfelelést elsősorban kötelezettségek, tilalmak, dokumentációs előírások és ellenőrzési mechanizmusok útján biztosítja.

Az OECD keretrendszere ezzel szemben osztályozó és értelmező jellegű. Nem elsődlegesen jogi kötelezettségeket állapít meg, hanem olyan elemzési dimenziókat kínál, amelyek segítségével a mesterséges intelligencia rendszerek társadalmi, gazdasági, technológiai és etikai hatásai értékelhetők. Erőssége abban áll, hogy a mesterséges intelligenciát nem kizárólag szervezeti vagy technológiai problémaként kezeli, hanem szélesebb társadalmi és gazdasági környezetbe ágyazza.

Az AI RMF 1.0 gyakorlati és működésorientált keretrendszerként értékelhető. Elsősorban azt mutatja meg, hogy a szervezetek miként képesek a mesterséges intelligencia kockázatait azonosítani, mérni, nyomon követni és kezelni. A keretrendszer különös jelentősége abban ragadható meg, hogy a megfeleléshez szükséges szervezeti folyamatokat, döntési pontokat és kockázatkezelési funkciókat rendszerezi. Ezáltal közvetlen kapcsolatot teremt a mesterséges intelligencia kockázatai és a compliance gyakorlati működése között.

A három rendszer összevetése alapján megállapítható, hogy azok eltérő szabályozási logikát követnek, ugyanakkor egymást kiegészítő módon járulnak hozzá a mesterséges intelligencia megfelelési környezetének kialakításához.

1.3 Összefoglalás

A kutatás kontextusba ágyazása elengedhetetlen feladat, ezért több irányból elemeztem a kutatás eredményeire hatást gyakorló tényezőket. A mesterséges intelligencia együtt jár a kockázatok erősödésével, a kockázatokra reagáló eszközök alkalmazásával. A jogi-etikai szabályozás, tehát a kockázatokat csökkentő eszközök mellett szükség van gyorsabban reagáló eszközökre is, ezért a compliance mint biztonsági tényező jelenthet megoldást a problémakezelés nehézségeinek csökkentésére, a megfelelési kérdések megoldására. A különböző iparágakban egyre növekvő szabályozási követelmények miatt az ellenőrzési rendszerek alapvető eszköznek tekinthetők az átfogó ellenőrzés biztosításában, hatékony kezelésében [72]. A compliance szerepe így válik meghatározóvá.

Az uniós MI szabályozások, az OECD standard és az AI RMF 1.0 fókuszában a biztonsági tényezők, az emberközpontúság és természetesen a fenntarthatóság állnak. Az uniós dokumentumok egyelőre leginkább az elméleti kereteket biztosítják, de ezek száma egyúttal mutatja azt is, hogy az EU érzékeli a mesterséges intelligencia jelentőségét. Az OECD keretrendszer és az AI RMF 1.0 már gyakorlati iránymutatásokat tartalmaznak, ezért több hangsúlyt fektetnek a kockázatkezelés alkalmazási módszereire. Míg az AI RMF 1.0 nem ágazatfüggő, és inkább kockázatkezelési szempontból határozza meg a mesterséges intelligencia rendszerek alkalmazását, addig az OECD keretrendszere már figyelembe veszi a

tágabb társadalmi és a gazdasági kockázatokat is. A keretrendszer középpontjában az irányítás funkció áll, amihez a feltérképezés, a mérés és a kezelés főbb folyamatai kapcsolódnak. Az uniós MI szabályozások az OECD standard és az AI RMF 1.0 dokumentumokban az alábbi módokon jelennek meg:

- a gazdasági fejlődés hangsúlyozása;
- az etikai, jogi keretek figyelembevétele;
- a definíciók meghatározása;
- a kockázatok azonosítása, kezelése;
- a folyamatok azonosítása.

A vizsgált szabályozási és szakpolitikai dokumentumok alapján öt visszatérő strukturális mintázatot azonosítottam, mint gazdasági és innovációs célrendszer megjelenése, megbízhatóság és biztonság központi szerepe, a kockázatalapú szabályozási logika térnyerése, folyamatszemlélet és életciklus-alapú megközelítés, végül az irányítási és felelősségi struktúrák erősödése. Elvégeztem a szabályozási keretek összehasonlító elemzését. Az EU a jogi kötelezettségek és az intézményi ellenőrzés oldaláról, az OECD az osztályozás és társadalmi-gazdasági értelmezés oldaláról, míg az AI RMF 1.0 a szervezeti kockázatkezelés és gyakorlati végrehajtás oldaláról közelíti meg a mesterséges intelligencia szabályozását. Ezek az értelmezések egymást kiegészítik és erősítik.

A leírtak alapján megállapítható, hogy az adatok mennyisége egyre növekszik a globális térben, a mesterséges intelligencia rendszerek szabályozásának szerepe felértékelődik, ami együtt jár a megfelelőségi kihívásokra való reagálás szükségességével. A vizsgált dokumentumok alapján a compliance szerepe nem merül ki a szabályoknak való formális megfelelés biztosításában. A compliance és a mesterséges intelligencia kölcsönhatásait ebben az elméleti rendszerben látom relevánsnak. Ez a kutatási kontextus indokolja a compliance fogalmának átfogóbb, többdimenziós vizsgálatát, a megfelelőség gyakorlati alkalmazásának, valamint a mesterséges intelligencián alapuló használatának elemzését a magyar vállalkozások esetében; valamint gyakorlati segédletek készítését.

2 A COMPLIANCE FOGALOM VIZSGÁLATA – FOGALOMALKOTÁS

A kutatási kontextus indokolja a compliance fogalmának többdimenziós, elméletileg megalapozott újragondolását. A compliance napjainkra jelentéstartalmában fragmentált fogalommá vált, amely egyaránt jelen van a különböző tudományterületek diskurzusaiban és a gazdasági gyakorlat eltérő szektoraiban.

Jelen fejezet célja a compliance fogalmának átfogó, több szinten megvalósuló vizsgálata három elemzési perspektívában. Egyrészt a szakirodalomban megjelenő definíciók elméleti összehasonlító elemzésére kerül sor, másrészt bibliometriai elemzések segítségével vizsgálom a compliance tudományos diskurzus szerkezetét, hangsúlyeltolódásait és fejlődési irányait. Harmadrészt a compliance funkció szempontú értelmezését elemzem, különös tekintettel a különböző ágazatokban megjelenő szerepére és beágyazottságára.

A fenti elemzések alapján célom egy elméletileg megalapozott, integratív compliance-definíció megalkotása. Ennek keretében azt a feltételezést vizsgálom, hogy a compliance fogalmának szakirodalmi, elméleti, gyakorlati és funkcióbeli értelmezései nem alkotnak egységes rendszert, mely alapján indokolt egy átfogó compliance definíció megalkotása. (H1)

2.1 A compliance elméleti, bibliometrikus vizsgálata – compliance fogalomalkotás

A modern biztonságtudományi, vállalatirányítási és jogtudományi szakirodalomban a kortárs biztonsági szakértők, stratégák és döntéshozók munkájuk során egyre gyakrabban találkoznak a „compliance” és a „compliance management” (megfelelőségbiztosítás) szakkifejezésekkel. E fogalmak tisztázása, rendszerezése és tudományos igényű egységesítése azonban rendkívül töredezett volt, ami számos, egymással versengő és esetenként ellentmondó elméleti definíció kialakulásához vezetett a hazai és a nemzetközi diskurzusban egyaránt [78]. A hagyományos elméleti megközelítések a compliance-t jellemzően egy szabályozási, statikus és szervezeti fókuszú keretben vizsgálták, amely elsősorban a kötelező jogszabályok betartására, valamint a belső szabályzatoknak és a külső etikai normáknak való megfelelésre szorítkozott. Az akadémiai irodalom a compliance-t a joggal összhangban lévő működés abszolút követelményeként határozta meg [73]. Más definíciók ezt a kört kibővítették, és a compliance-t olyan viselkedési, működési állapotként értelmezték, ahol a szervezet az összes vonatkozó jogi szabálynak, belső iránymutatásnak és külső elvárásnak megfelelően végzi mindennapi tevékenységét [74]. A német jogtudományi megközelítések korábban szigorúan szervezeti szemszögből vizsgálták a fogalmat, olyan gyűjtőfogalomként definiálva azt, amely magában

foglalja a jogkövető magatartás tanúsítását, a belső szabályzatok betartását és az uralkodó piaci ajánlásokhoz való igazodást biztosító megelőző intézkedéseket [75]. Továbbá a vállalatirányítás és a büntetőjog tudósai hagyományosan olyan mechanizmusként tekintettek a compliance-re, amely speciális preventív beavatkozásokat igényel a modern szabályozási környezetek jogszabályi összetettsége miatt [76]. A megfelelőség ezen elméleti kategóriái olyan normakonformitást is magukban foglaltak, amelyek kiterjedtek a nemzetközi standardokra és szabványokra is [77]. Az elméleti megközelítéseket és a megfelelőség tartalmi tényezőit a 4. táblázat foglalja össze:

Táblázat 4: A compliance definíciói (Saját szerkesztés)

Szerző	**A compliance definíciója**	**Tartalmi tényezők**
Georg Gösswein	A joggal összhangban működés követelménye. [73]	Jogszabályi előírásoknak való megfelelés.
Balogh Mónika	„A vonatkozó összes (jogi és egyéb) szabálynak, elvárásnak való megfelelést, azok szerinti működést jelenti.” [74]	Jogszabályoknak, egyéb szabályoknak, elvárásoknak való megfelelés.
Dennis Bock	„A compliance legáltalánosabb értelemben – szervezeti megközelítésből – a jogkövető magatartás tanúsítását, a jogszabályi előírásoknak, belső szabályoknak, illetve egyéb követendő ajánlásoknak megfelelő magatartás elérését szolgáló intézkedések gyűjtőfogalma.” [75]	Jogszabályoknak, belső szabályoknak, ajánlásoknak való megfelelés.
Thomas Rotsch	„A compliance (...) a vállalkozások hatályos jognak megfelelő működését jelenti, amely azokra a területekre jellemző, ahol a komplex és bonyolult szabályozás miatt a jogkövető magatartás tanúsításához szükséges a „szakértők” általi megelőző intézkedések alkalmazása.” [76]	Jogszabályoknak való megfelelés.
Ambrus István, Mezei Kitti, Molnár Erzsébet	„(…) a compliance egyfajta szervezeten belüli normakonformitás, legyen szó akár jogi, akár szervezeti etikai szabályrendszerről.” [77]	Jogszabályoknak, belső szabályoknak etikai normáknak, nemzetközi standardoknak, szabványoknak való megfelelés.

A modern digitális transzformáció, a mesterséges intelligencia előretörése és a globális, adatvezérelt gazdaság térnyerése azonban rávilágított arra, hogy a szakirodalmi áttekintések és a kizárólag jogelméleti dedukciók már nem elegendőek egy olyan fogalom átfogó megragadásához, amely alapvető technológiai és operatív átalakuláson megy keresztül. A vállalati csalások és adatbiztonsági incidensek statisztikai értékelései rávilágítanak, hogy a

szervezetek átlagosan az árbevételük öt százalékát veszítik el különböző belső és külső visszaélések miatt, ami globálisan több mint 3,6 milliárd dolláros makrogazdasági veszteséget jelent havonta, érintett entitásonként átlagosan 8300 dolláros kárral [47]. Tekintettel arra, hogy átlagosan tizenkét hónap telik el egy vállalati visszaélés felderítéséig, a szigorú, adatalapú compliance-kontrollok bevezetése elengedhetetlen biztonsági követelménnyé vált, ami a megfelelőség fogalmát az adminisztratív jogkövetésből a proaktív biztonságtudomány területére emelte át [47].

A fogalmi tisztázás és az objektív, adatalapú definícióalkotás érdekében elengedhetetlen a bibliometriai vizsgálat és a hálózattérképezés alkalmazása. A hagyományos, leíró jellegű szakirodalmi áttekintésekkel szemben a bibliometriai hálózatelemzés kvantitatív és kvalitatív megközelítést nyújt annak megértéséhez, hogy a tudományos fogalmak hogyan mutálódnak, és a különböző tudományterületek hogyan integrálják azokat az idő múlásával [79]. A bibliometria tudományágának alapjait Pritchard fektette le, aki a korábban használt, meglehetősen többértelmű „statisztikai bibliográfia” kifejezés helyett bevezette a bibliometria fogalmát, amelyet a matematikai és statisztikai módszerek könyvekre és egyéb kommunikációs formátumokra történő alkalmazásaként határozott meg [79]. A terület korai gyökerei az 1930-as évekre, Paul Otlet munkásságára nyúlnak vissza, a bibliometria modern tudományos diszciplínává válása az 1960-as években, a Science Citation Index (SCI) kifejlesztésével vette kezdetét [80]; [81]. A bibliometriai elemzés elsődleges célja, hogy hatalmas mennyiségű bibliográfiai adatból – például a hivatkozások számából, a társszerzőségi mintázatokból és a fogalmi struktúrákból – kvantitatív és objektív következtetéseket vonjon le, feltárva a tudományos hatás, a produktivitás és a kutatási fókuszok rejtett trendjeit [79]. A modern tudományos kutatásban, ahol a publikációk puszta volumene és a tudás exponenciális növekedése meghaladja a manuális feldolgozás korlátait, emiatt a bibliometria elengedhetetlen eszközzé vált a kutatási területek makroszintű feltérképezésében, a kulcsfontosságú publikációk azonosításában és a tudományterületek közötti tudástranszfer vizualizációjában [79].

A jelen alfejezet bibliometriai elemzésének elsődleges analitikai eszköze a VOSviewer szoftver integrált alkalmazása. A van Eck és Waltman által kifejlesztett VOSviewer egy olyan számítógépes program, amely kifejezetten nagyméretű bibliometriai hálózatok (például társszerzőségi, hivatkozási, vagy kulcsszó-együttes előfordulási hálózatok) konstruálására, vizualizálására és klaszterezésére szolgál [82]. A szoftver működésének elméleti alapja a kulcsszavak együttes előfordulásának (co-occurrence) elemzése: amennyiben két szakkifejezés statisztikailag szignifikáns gyakorisággal jelenik meg ugyanabban a tudományos publikációban

– jellemzően a címben, az absztraktban vagy a szerzők által megadott kulcsszavak listájában – , a szoftver algoritmusa azokat szoros koncepcionális kapcsolatban állónak tekinti, feltételezve, hogy közös elméleti vagy gyakorlati problémakört írnak le [82].

A VOSviewer ezeket a mátrixokat egy egységes keretrendszerben (unified framework) kétdimenziós topológiai hálózattérképpé alakítja [82]. A vizualizáció során a hálózat vizuális elemei pontos statisztikai jelentéssel bírnak. A csomópontok (nodes) mérete egyenes arányban áll az adott kulcsszó vizsgált irodalomban való abszolút előfordulási gyakoriságával: minél nagyobb egy fogalom csomópontja, annál dominánsabb szerepet játszik a tudományos diskurzusban [82]. A csomópontokat összekötő élek (edges) vastagsága és száma a kapcsolatok összesített erősségét (total link strength) jelöli, vagyis azt, hogy két adott kifejezést milyen gyakran tárgyalnak együtt a szerzők. A hálózati elrendezésben a fizikai távolság is kulcsfontosságú: a térképen egymáshoz közelebb elhelyezkedő csomópontok erősebb szemantikai rokonságot mutatnak, míg a távolabbiak eltérő, marginalizált kutatási irányokat képviselnek [82].

A szoftver beépített klaszterezési algoritmusa a szorosan összefüggő fogalmakat modularitás alapján azonos színű tematikus klaszterekbe szervezi, amelyek egy-egy koherens elméleti iskolát vagy kutatási paradigmát reprezentálnak [82]. Ezen túlmenően a VOSviewer sűrűségtérképeket (density views) is generál, amelyek a kutatási területek aktuális „forró pontjait” (hot spots) emelik ki a színek intenzitásának változtatásával: a piros színnel jelölt területek magas koncentrációjú, intenzíven kutatott fókuszpontokat jeleznek, míg a kék területek ritkábban vizsgált, elszigetelt fogalmakat [82]. A minimális előfordulási küszöbértékek (thresholds) szisztematikus finomhangolásával a VOSviewer lehetővé teszi a periférikus zaj, a ritka és elszigetelt kifejezések kiszűrését, ezáltal a tudományág uralkodó paradigmájának az izolálását.

A vizsgálat kettő adatbázisra, a Web of Science (WoS), és a Magyar Tudományos Művek Tárra (MTMT) épül és kettő egymásra épülő szakaszra bomlik: a 2017 és 2024 közötti időszak retrospektív feltérképezésére, valamint a 2025. év adatainak összehasonlító értékelésére. A fentieken túl az OpenAlex adatbázist szintén forrásként használtam arra keresve a választ, hogy mely tudományterületek keretein belül született a legtöbb szakirodalmi elemzés compliance témában.

2.1.1 A 2017–2024 közötti időszak szakirodalmi (WoS, MTMT) vizsgálata

A compliance fogalmát a mesterséges intelligencia megjelenése miatt a biztonság kifejezéssel együtt vizsgáltam. A longitudinális vizsgálat a WoS és az MTMT adatbázisából merít. Az elemzés a címekben és a szövegekben történt ahogy ezt az 5. táblázat is mutatja.

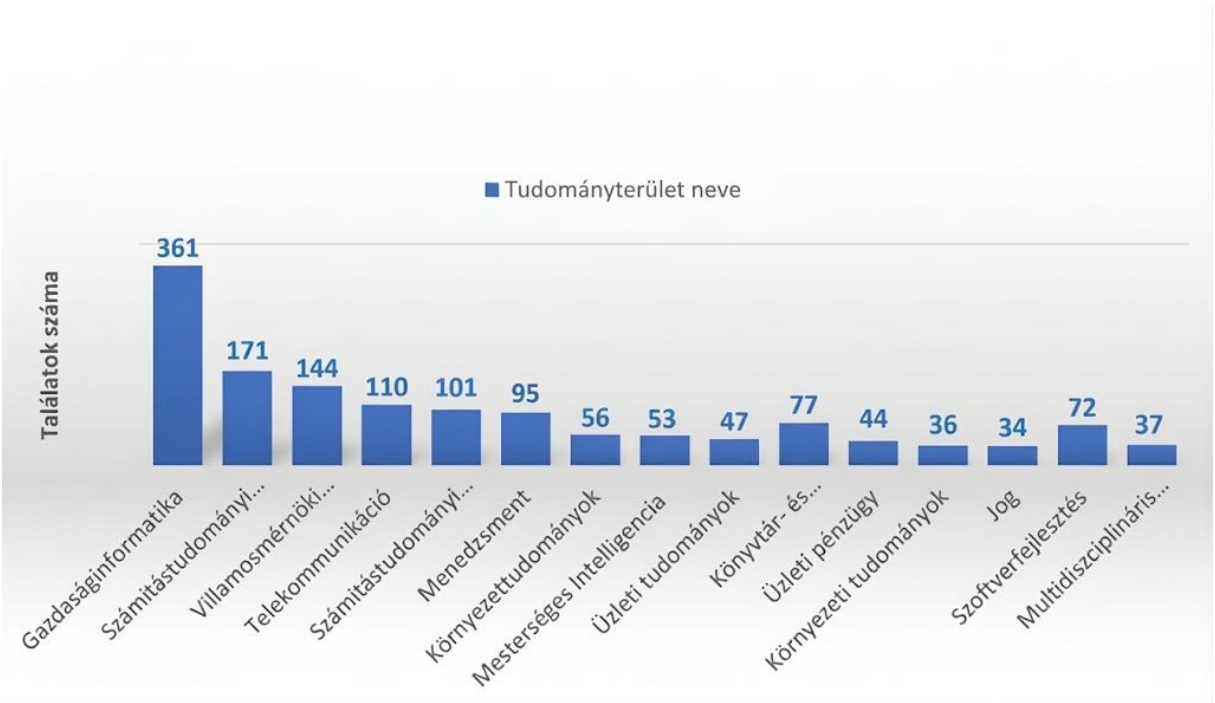
Táblázat 5: A definiálás módszertana (Saját szerkesztés)

Forrásszöveg	A vizsgálat helye	A vizsgálat tárgya
Nemzetközi publikációk a Web of Science alapján	Címek és szöveg	Compliance management és security kulcsszavak
Hazai és nemzetközi publikációk az MTMT alapján	Címek és szöveg	Compliance management és security kulcsszavak

Az adatkinyerési protokoll a „compliance management” és „security” kifejezést alkalmazta a keresőmotorban. Ez a szűrés azért volt indokolt, mert önmagában a „compliance” kifejezésre történő keresés több mint 251 767 találatot eredményezett volna, amely magában foglalt volna teljesen irreleváns tudományágakat is, mint például a farmakológia (több mint 13 000 találat a betegek gyógyszerszedési hajlandóságára vonatkozóan), az onkológia vagy a sebészet. A két fogalom közvetlen összekapcsolásával a lekérdezési szűrés izolálta a szervezeti, vállalati és digitális irányításra vonatkozó releváns szakirodalmat, kizárva az orvosi és biológiai zajt.

A 2017 és 2024 közötti nyolcéves alapidőszakban a keresőmotor összesen 1236 releváns, lektorált tudományos publikációt azonosított. Az adatbázis tudományos beágyazottságát és minőségét a WoS hivatkozáselemzési (citation report) funkciója igazolta: a kinyert 1236 publikációból 890-et (a teljes korpusz 72 százalékát) hivatkoztak legalább egyszer más kutatók, ami magas fokú akadémiai elkötelezettséget és tudományos diskurzust jelez. Ezen felül a hivatkozott cikkek túlnyomó többsége (740 publikáció) kettő vagy annál több független idézést kapott, ami bizonyítja, hogy a vizsgált minta a globális tudományos párbeszéd szerves részét képezte.

A publikációk tudományterületek közötti eloszlása már ebben az időszakban is egyértelmű technológiai beállítottságot mutatott, ugyanakkor kiegyensúlyozott jelenlétet tartott fenn a hagyományos akadémiai és üzleti területeken is. A legnagyobb elemszámot a gazdaságinformatika (361 találat) adta, amelyet a számítástechnikai elmélet (171), a villamosmérnöki tudományok (144), a telekommunikáció (110) és az interdiszciplináris alkalmazott informatika (101) követett [78]. A klasszikus vállalati fókusz relevanciáját mutatja, hogy a hagyományos menedzsment (95 találat), a könyvtár- és információtudomány (47), az üzleti tudományok (44) és a jog (36) szintén a vezető diszciplínák között szerepel. Mindezeket a 4. ábra foglalja össze. Ez az eloszlás egy olyan átmeneti időszakot ír le, ahol az informatikai megoldások már megjelennek, de a megfelelőség menedzselése még erős szervezeti és jogi keretek között zajlik.



Ábra 4: A compliance és a security kifejezések találati aránya a WoS adatbázisában (Saját szerkesztés)

A tudományos érdeklődés dinamikáját egy részletes idősoros elemzés tárta fel. Bár a publikációk abszolút száma folyamatos növekedést mutatott, a növekedés üteme a 2017–2024-es időszakban egy stabil, de egyenletes lineáris trendet követett. A legkisebb négyzetek módszerével számított lineáris regressziós egyenlet alapján ($y=b_0t$) a publikációk száma évente átlagosan 16,01 cikkel nőtt (b_1=16.01, míg az állandó b_0=93,83) [78]. (A 2025. évi adatokkal részletezett táblázat a következő alfejezetben található) Megállapítható volt, hogy 2018 óta minden évben a 2017-es bázisévet (112 publikáció) meghaladva születtek új tudományos írások a témában, ami a társadalomtudományok és a kiberbiztonság fokozatos közeledését jelezte [78]. Ez a növekedési ütem egy olyan diszciplínára utalt, amely még a technológiai adaptáció organikus fejlődési fázisában volt, közvetlenül a generatív mesterséges intelligencia tömeges elterjedése előtt.

Az időszak tudományos prioritásainak és elméleti fókuszainak feltárása érdekében szükséges a legtöbbet hivatkozott szakirodalmak kvalitatív elemzése. Az 6. táblázat a 2017–2024 közötti alapidőszak legbefolyásosabb, legtöbbet idézett publikációit foglalja össze, amelyek a diskurzus irányát meghatározták.

Táblázat 6: A legtöbbet hivatkozott szakirodalmak compliance és security tárgykörben (2017–2024) [78] (Saját szerkesztés)

Szerző(k)	**Cím (Eredeti nyelven)**	Cím (Magyarul)	**Megjelenés éve**	**Hivatkozások száma**

Allam, Z.; Dhunny, Z. A. [83]	On Big Data, Artificial Intelligence and Smart Cities	A Big Data-ról, a mesterséges intelligenciáról és az okosvárosokról	2019	445
Li, J.; Greenwood, D.; Kassem, M. [84]	Blockchain in the Built Environment and Construction Industry: A Systematic Review, Conceptual Models and Practical Use Cases	Blokklánc az épített környezetben és az építőiparban: Szisztematikus áttekintés, koncepcionális modellek és gyakorlati felhasználási esetek	2019	322
Tandon, A.; Dhir, A.; Islam, A. K. M. N.; Mantymaki, M. [85]	Blockchain in Healthcare: A Systematic Literature Review, Synthesizing Framework and Future Research Agenda	Blokklánc az egészségügyben: Szisztematikus szakirodalmi áttekintés, szintetizáló keretrendszer és jövőbeli kutatási ütemterv	2020	189
Cram, W. A.; D'Arcy, J.; Proudfoot, J. G. [86]	Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance	Látni a fától az erdőt: Az információbiztonsági irányelveknek való megfelelés előzményeinek metaanalízise	2019	176
Bernal Bernabe, J.; Luis Canovas, J. et al. [87]	Privacy-Preserving Solutions for Blockchain: Review and Challenges	Adatvédelmet megőrző megoldások a blokklánchoz: Áttekintés és kihívások	2019	166
Majumdar, A.; Shaw, M.; Sinha, S. K. [88]	COVID-19 Debunks the Myth of Socially Sustainable Supply Chain: A Case of	A COVID-19 megdönti a társadalmilag fenntartható ellátási lánc mítoszát: A dél-	2020	161

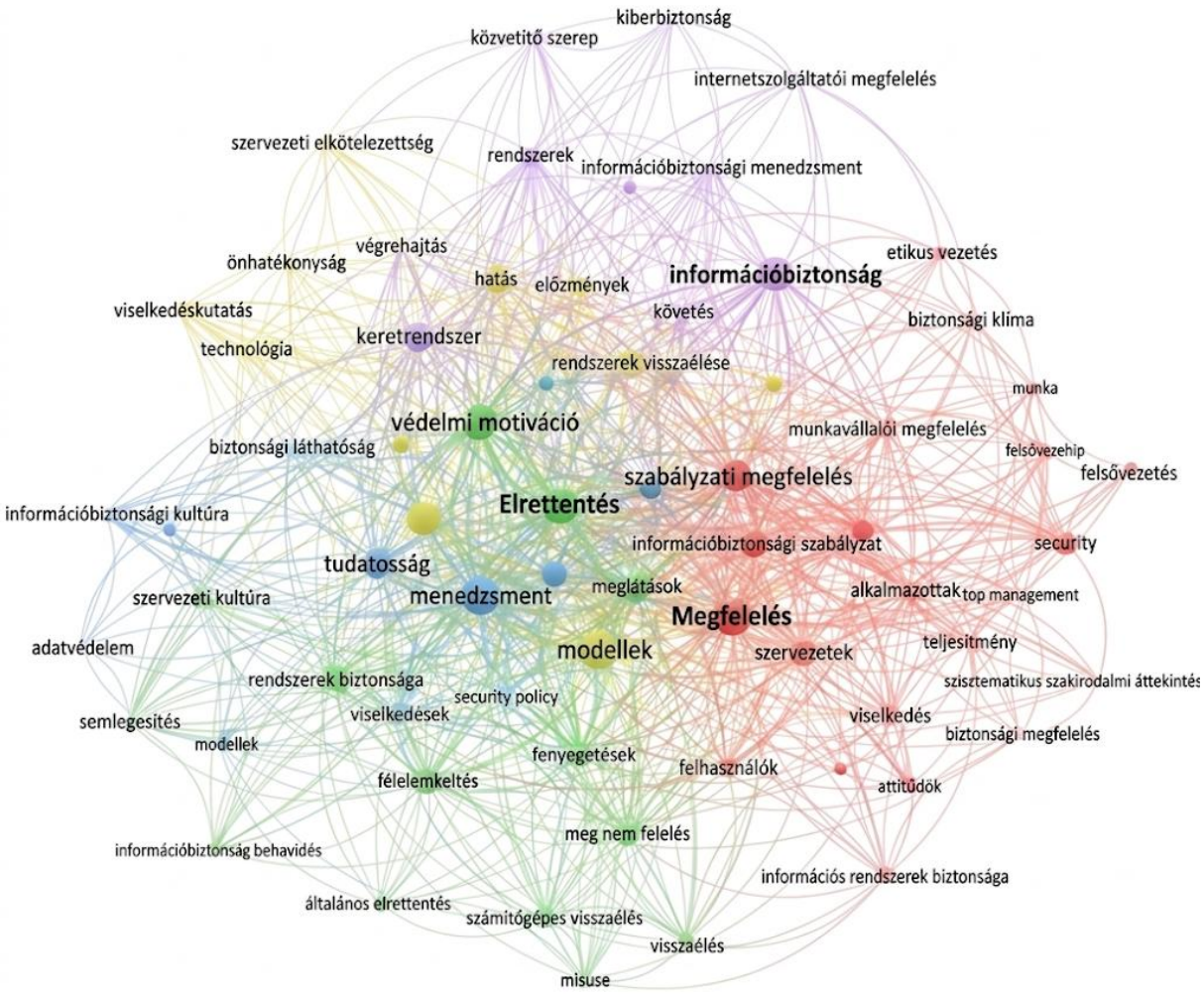
	the Clothing Industry in South Asian Countries	ázsiai országok ruhaiparának esete		
Makhdoom, I.; Zhou, I. et al. [89]	PrivySharing: A Blockchain-Based Framework for Privacy-Preserving and Secure Data Sharing in Smart Cities	PrivySharing: Egy blokklánc-alapú keretrendszer a magánélet védelmét biztosító és biztonságos adatmegosztáshoz az okosvárosokban	2020	151
Mackey, T. K.; Kuo, T. et al. [90]	Fit-for-Purpose? - Challenges and Opportunities for Applications of Blockchain Technology in the Future of Healthcare	Célnak megfelelő? - A blokklánc technológia alkalmazásának kihívásai és lehetőségei a jövő egészségügyében	2019	128
D'Arcy, J.; Lowry, P. B. [91]	Cognitive-Affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study	Az alkalmazottak információbiztonsági irányelveknek való napi megfelelésének kognitív-affektív mozgatórugói: Többszintű, longitudinális vizsgálat	2019	118
Attaran, M. [92]	Blockchain Technology in Healthcare: Challenges and Opportunities	Blokklánc technológia az egészségügyben: Kihívások és lehetőségek	2020	112

A munkák elemzése [83]; [84]; [85] rávilágít arra, hogy a 2017–2024-es időszakban a nemzetközi kutatások két fő paradigma köré csoportosultak [78]. Az első ág az újonnan megjelenő, elosztott főkönyvi technológiák (elsősorban a blokklánc) elméleti integrációjára és a kriptográfiai adatvédelemre fókuszált különböző szektorokban, mint az építőipar vagy az egészségügy [84]; [85]; [87]; [92]. A második, szervezeti irányítás szempontjából sokkal

meghatározóbb ág viszont mélyen gyökerezett az emberi viselkedéstudományban és a hagyományos szervezetpszichológiában. Az olyan kiemelkedő tanulmányok, mint Cram és szerzőtársai metaanalízise, valamint D'Arcy és Lowry longitudinális vizsgálata, elsősorban a munkavállalói magatartásra, az információbiztonsági szabályzatoknak (information security policy) való napi szintű megfelelés kognitív-affektív mozgatórugóira, a biztonságtudatosságra és az elrettentés (deterrence) pszichológiájára összpontosítottak [86]; [91]. Ezen elméleti alapvetések szerint a compliance végső soron egy emberközpontú kihívás: a rendszerek biztonsága azon múlik, hogy a menedzsment milyen pszichológiai és adminisztratív eszközökkel képes rábírni a munkavállalókat a szabályok követésére.

Ennek a hibrid korszaknak a szemantikai és fogalmi elemzését a VOSviewer szoftverrel elvégzett topológiai hálózattérképezés vizualizálta. A Web of Science rendszeréből „Plain Text File" formátumban exportált nyers bibliometriai adatok (absztraktok, kulcsszavak, kutatási területek, hivatkozási hálózatok) betöltését követően a szoftver elemezte a teljes szövegkorpuszban fellelhető 293 egyedi szerzői kulcsszó együttes előfordulását (co-occurrence). Mivel az algoritmus minden olyan szót összeköt, amely ugyanabban a cikkben szerepel, a nyers hálózat átláthatatlan fogalmi zajt generál. A szintetikus definícióalkotás érdekében a kutatás során szisztematikusan emeltem a minimális előfordulási küszöbértéket (threshold), hogy izoláljam a leggyakrabban előforduló, releváns kifejezéseket. [78].

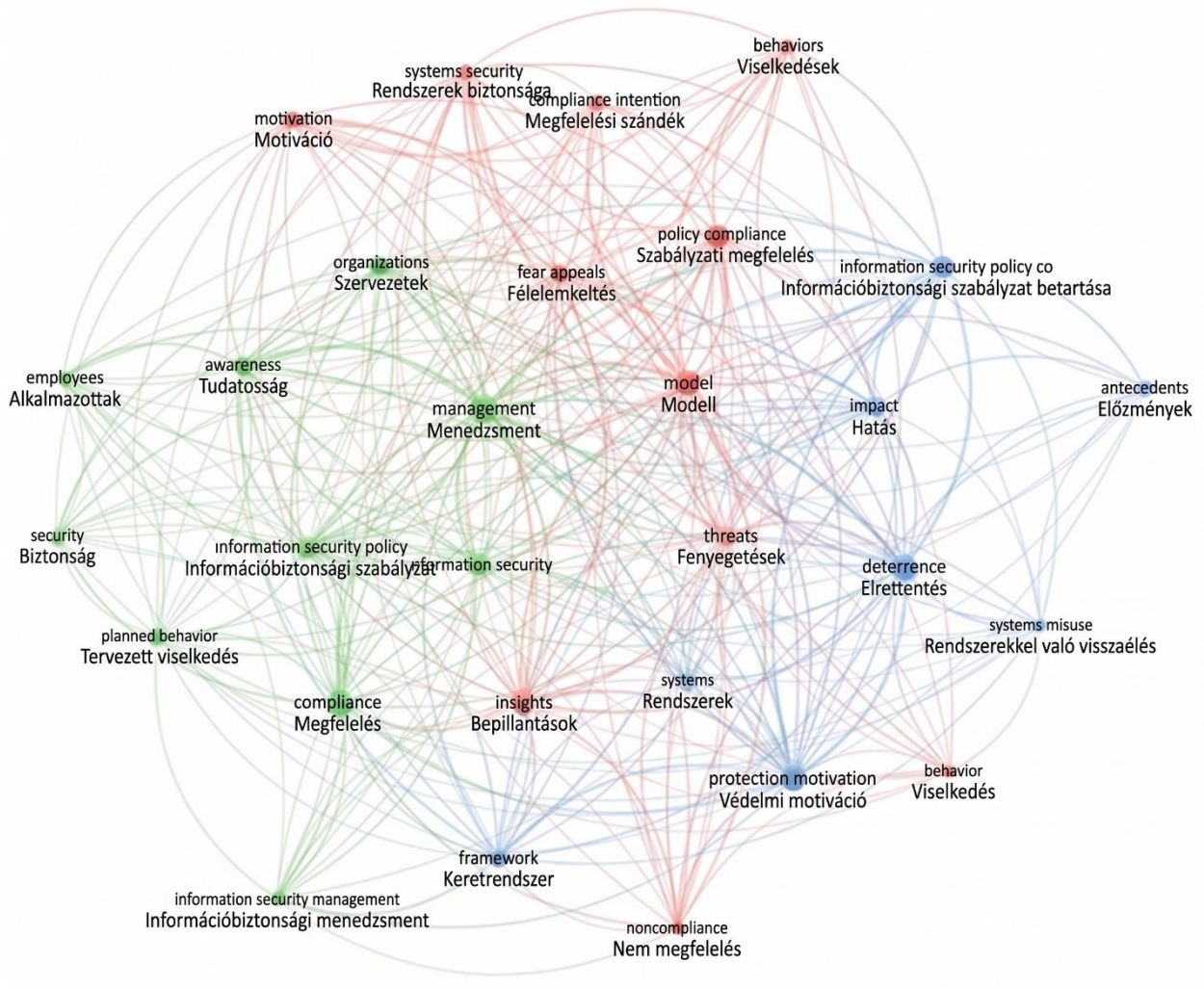
Az első VOSviewer hálózati térképen a minimális előfordulási küszöbértéket 2-re állítottam, ami azt jelentette, hogy egy adott szónak legalább kettő különböző tanulmányban kellett szerepelnie a hálózatba kerüléshez, ezt foglalja össze az 5. ábra.



Ábra 5: Hálózati térkép – kettes küszöbérték (Saját szerkesztés)

Az ábrában a kettes küszöbérték 69 kulcsszót eredményezett a vizualizációban. Ez a hálózat vizuálisan sűrű és „zajos” volt, ugyanakkor jól mutatta a terület elméleti kiterjedtségét. A legnagyobb csomópontok körül olyan fogalmak csoportosultak, mint a vezetés (management), az etikus vezetés (ethical leadership), a szervezeti elkötelezettség (organizational commitment), a motiváció (motivation), valamint az olyan negatív aspektusok, mint a számítógépes visszaélések (computer abuse) és a szabályszegés (noncompliance) [78]. A vizualizáció strukturálisan igazolta, hogy a compliance-t ekkor még dominánsan emberi és vezetési problémaként, pszichológiai attitűdök összességeként kezelték, nem tiszta adatinfrastrukturális vagy algoritmikus kérdésként [78].

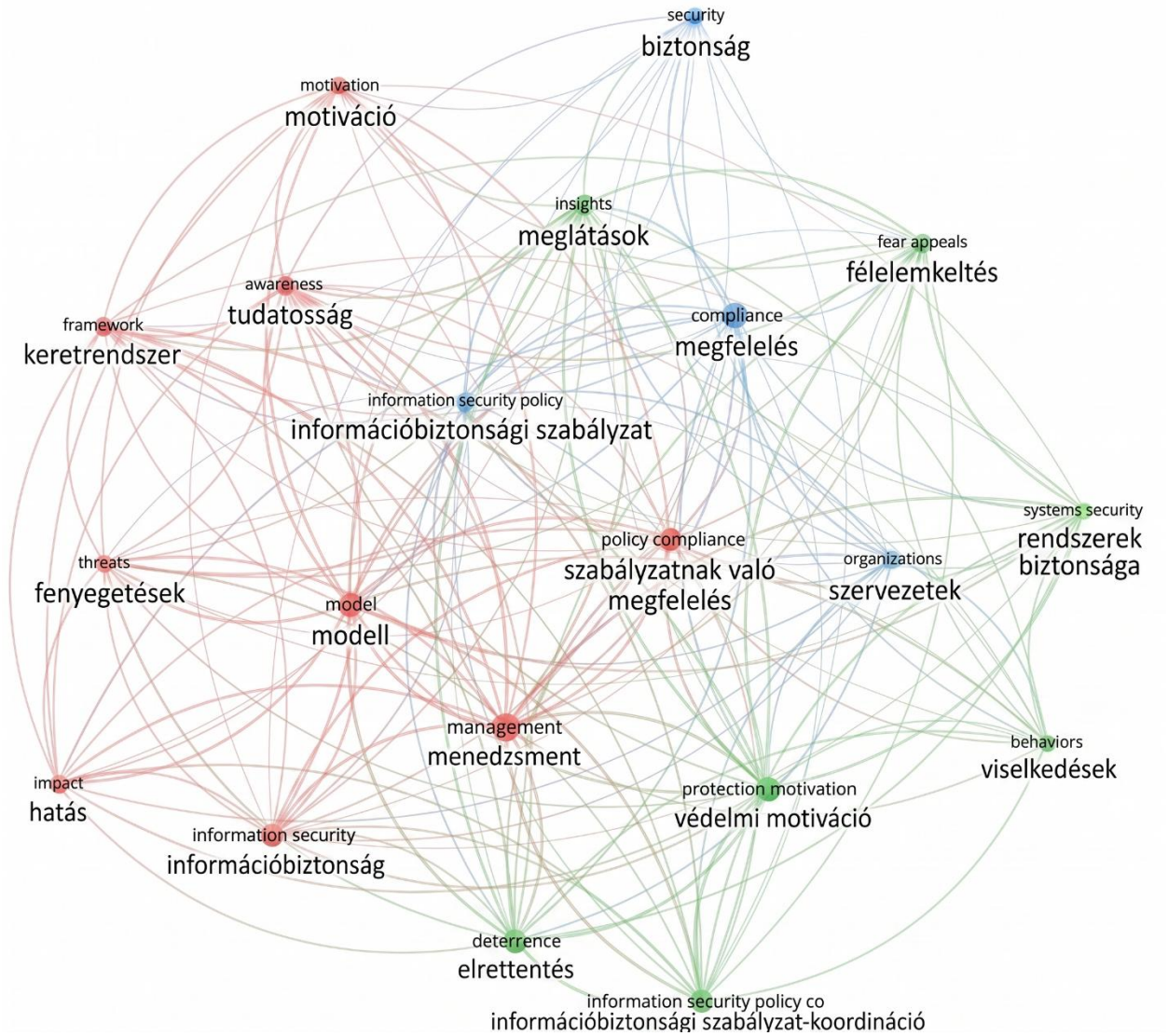
A 6. ábrán a hálózati térképen a minimális előfordulási küszöbértéket 4-re emeltem.



Ábra 6: Hálózati térkép - négyes küszöbérték (Saját szerkesztés)

A szoftver algoritmusa ekkor már csak 29 kulcsszót izolált a 293-ból, kiszűrve a perifériku zajt [78]. A hálózat jelentősen letisztult, és a VOS klaszterezési technika élesen elkülönítette a viselkedési modelleket (planned behavior, protection motivation) az irányítási keretrendszerektől (framework, policy compliance). A csomópontokat összekötő élek (edges) vastagsága és a térbeli elrendezés megmutatta, hogy az információbiztonság (information security) elválaszthatatlanul összefonódott a dolgozói tudatossággal (awareness) és az elrettentés-elmélettel (deterrence theory), rámutatva arra, hogy a kiberbiztonság ezen a ponton az oktatásra és a belső büntetés kilátásba helyezésére épült.

Végül, a 7. ábrán a küszöbérték 6-ra történő emelésével a szoftver kiszűrte az összes harmadlagos és specifikus fogalmat, egy összekapcsolt magot megjelenítve.



Ábra 7: Hálózati térkép – hatos küszöbérték (Saját szerkesztés)

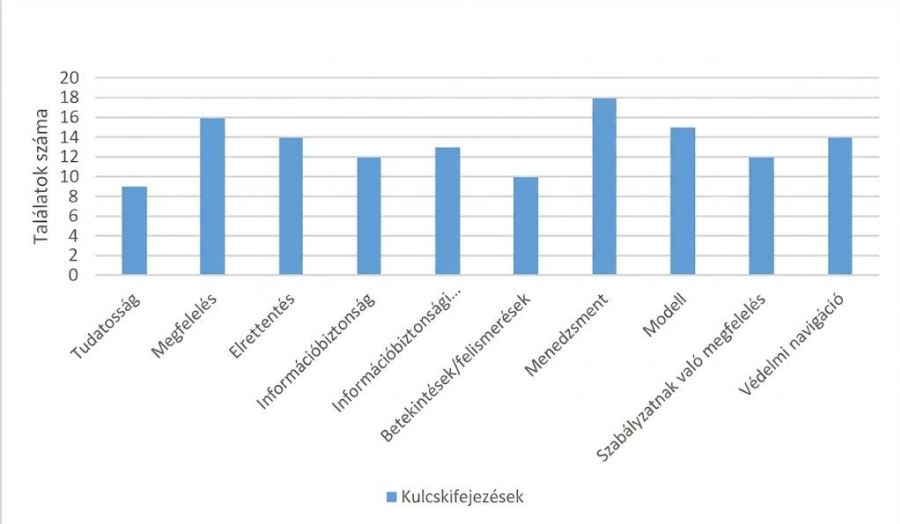
Ez a térkép egyensúlyt teremtett az átláthatóság és a specifikusság között, lecsupaszítva a compliance területét a 2017–2024 közötti időszakra. A hálózat középpontjában, a legnagyobb csomópontokként a management (menedzsment), a model (modell), a deterrence (elrettentés), a protection motivation (védelmi motiváció), a policy compliance (irányelvi megfelelés) és az awareness (tudatosság) álltak [78]. A leggyakrabban előforduló fogalmak statisztikai súlyát a 7. táblázat összegzi:

Táblázat 7: A leggyakrabban előforduló kulcsszavak eloszlási és hálózati adatai (2017–2024) (Saját szerkesztés) [78]

Kulcskifejezés (Eredeti/Magyar)	**Összes megjelenés (Frekvencia)**	**Összes kapcsolat erőssége (Total link strength)**
Management (Menedzsment)	18	107
Compliance (Megfelelés)	16	63
Model (Modell)	15	102

Deterrence (Elrettentés)	14	93
Protection motivation (Védelmi motiváció)	14	91
Information security policy compliance	13	80
Policy compliance (Irányelvi megfelelés)	12	61
Information security (Információbiztonság)	12	61
Awareness (Tudatosság)	9	65

A 7. táblázat alapján vizuálisan is látható a vezető fogalmak dominanciája, amelyet a 8. ábra mutat be.



Ábra 8: A leggyakrabban előforduló kifejezések darabszáma (Saját szerkesztés)

A 2017–2024-es időszak bibliometriai lenyomata és a hálózati statisztikák alapján a compliance fogalmát ebben a korszakban egy olyan preventív, büntetésre és ösztönzésre épülő emberközpontú modellként definiálták, ahol az információbiztonsági irányelvek (information security policy) betartását a vezetés (management) pszichológiai és adminisztratív eszközökkel felügyelte [78]. vizsgálat eredményei alapján körvonalazódik egy olyan értelmezési irány, amely szerint a compliance nem pusztán normakövetési mechanizmusként, hanem emberközpontú, preventív jellegű irányítási megközelítésként is értelmezhető. E felfogás a menedzsment aktív felügyeleti szerepére épít, és a megfelelőség biztosítását nem kizárólag formális kontrolleszközök révén ragadja meg.

Az elemzett publikációk a compliance fogalma tekintetében arra utalnak, hogy az információbiztonsági irányelveknek való megfelelés elősegítése jelentős mértékben támaszkodhat pszichológiai és adminisztratív eszközökre. Ebben az összefüggésben a szervezeti gyakorlat különös hangsúlyt helyezhet a munkavállalói tudatosság erősítésére, a védelmi motiváció kialakítására, valamint a szabályszegések megelőzését szolgáló mechanizmusokra.

Mindezek alapján a compliance egy olyan összetett, többdimenziós működési keretként ragadható meg, amelynek pontos fogalmi meghatározása további elméleti finomítást igényel.

MTMT-ben megjelenő publikációk

A trendek megfigyelésére a kutatás kiterjedt a hazai és nemzetközi publikációk vizsgálatára is a Magyar Tudományos Művek Tára adatbázisában. Az adatbázis szűrése (a „compliance" és „security" kulcsszavak együttes jelenléte alapján) mindössze 7 lektorált, releváns tudományos publikációt azonosított a vizsgált időszakra. Bár ez a volumen eltörpül a hatalmas nemzetközi WoS adathalmaz mellett, az időbeli eloszlás megerősítette a témakör iránti stabilan növekvő tendenciát: az MTMT adatbázis szerint 2001 és 2017 között egyáltalán nem jelent meg a két kulcsszót együttesen tárgyaló tudományos igényű munka, míg a hét azonosított cikkből hat 2018 után, három kifejezetten a korszak végén, 2023-ban jelent meg [78]. A 8. táblázat mutatja be a szakirodalmakat 2000 és 2024 között.

Táblázat 8: A magyarországi szakirodalom megoszlása (Saját szerkesztés)

Szerzők	Megjelenés éve
Guiditta et al. [93]	2024
Bálint F. [94]	2023
Delpont et al. [95]	2023
Dunay et al. [96]	2020
Bicaku et al. [97]	2019
Barta G. [98]	2018
Dunay P. [99]	2000

Az MTMT-ből szűrt publikációk manuális kvalitatív tartalom-ellenőrzése (például [94]; [95];[96]) igazolta, hogy a szerzők a „compliance" fogalmát konzisztensen a nemzetközi alapdefinícióhoz hasonló, visszamenőleges és audit-fókuszú értelemben használták [78]. Dunay a hagyományos geopolitikai és retrospektív megközelítést példázta, amikor a compliance-t az Európai Biztonsági és Együttműködési Szervezet (EBESZ) égisze alatt kötött fegyverzetellenőrzési kötelezettségek (például a Conventional Armed Forces in Europe (CFE)-szerződés) betartásával, az állami szintű normaszegésekkel és a megállapodások manuális

ellenőrzésével összefüggésben vizsgálta [96]. Bálint a pénzintézeti szektor felől közelített, a pénzmosás elleni küzdelem (AML) és a terrorizmusfinanszírozás megelőzésére fókuszálva, ahol a compliance funkciót a „védelem második vonalaként" írta le, amely a gyanús tranzakciók folyamatos, szakértői monitorozásával biztosítja a jogszabályoknak való megfelelést [94]. Delpont és szerzőtársai a biológiai biztonsági előírások (biosecurity) betartásával és auditálásával összefüggésben vizsgálták a fogalmat, rámutatva, hogy a megfelelőséget különböző emberi szereplők értékelik és rögzítik hagyományos adatbázisokban [95]. A szakirodalom tehát a 2017–2024 közötti időszakban a compliance-re jellemzően mint retrospektív auditálási, jogszabály-követési, emberi erőforrásokra épülő és hagyományos kockázatkezelési folyamatra tekintett, tükrözve a nemzetközi VOSviewer térképeken kirajzolódó „management" és „model" központú paradigmát.

2.1.2 A 2025. év időszak szakirodalmi vizsgálata (WoS, MTMT)

A bibliometriai adatok és a módszertani keretek kiterjesztése a 2025. évre a compliance fogalmi tartalmának változását tárta fel. A 2025. évi bibliometriai adathalmaz nem csupán a korábbi 2017-2024-es trendek szerves, lineáris időbeli folytatása, hanem egy átfogóbb adathalmaz, amely módosíthatja a compliance definiálását. 2025-ben változás történt a szabályozási és a technológiai környezetben is.

A publikációs dinamika és a tudományos termelékenység dinamikusan növekedett 2025-ben. Míg a korábbi, 2017–2024 közötti teljes nyolcéves alapidőszakban összesen 1236 releváns cikket publikáltak, a WoS adatbázisában pusztán a 2025. naptári évre vonatkozóan 458 új, lektorált tudományos publikáció jelent meg a „compliance management'' AND „security'' kulcsszavak metszetében. Ez azt jelenti, hogy az összmennyiség több mint egyharmadát a tudományos közösség egyetlen év alatt termelte ki. Ennek a gyorsulásnak a demonstrálására a korábbi idősoros elemzés és a lineáris növekedési modell ($y=b_0n+b_1t$)) frissítése történt meg. A korábbi időszakban a publikációk száma évente átlagosan 16,01 cikkel nőtt. A 2025. évi magas esetszám integrálásával a regressziós egyenlet meredekségi mutatója évente (b_1) 30,68 publikáció értékre ugrott, közel megduplázva a tudományos kibocsátás ütemét. A számítás az alábbi lineáris egyenletrendszerrel készült, és a 9. táblázat mutatja be a publikációk számának növekedését, ahol az n a vizsgált évek számát (9 évre módosítva), az y a publikációk számát jelöli egy adott évben: $\Sigma y = b_0 \cdot n + b_1 \cdot \Sigma t$ és $\Sigma ty = b_0 \cdot \Sigma t + b_1 \Sigma t^2$.

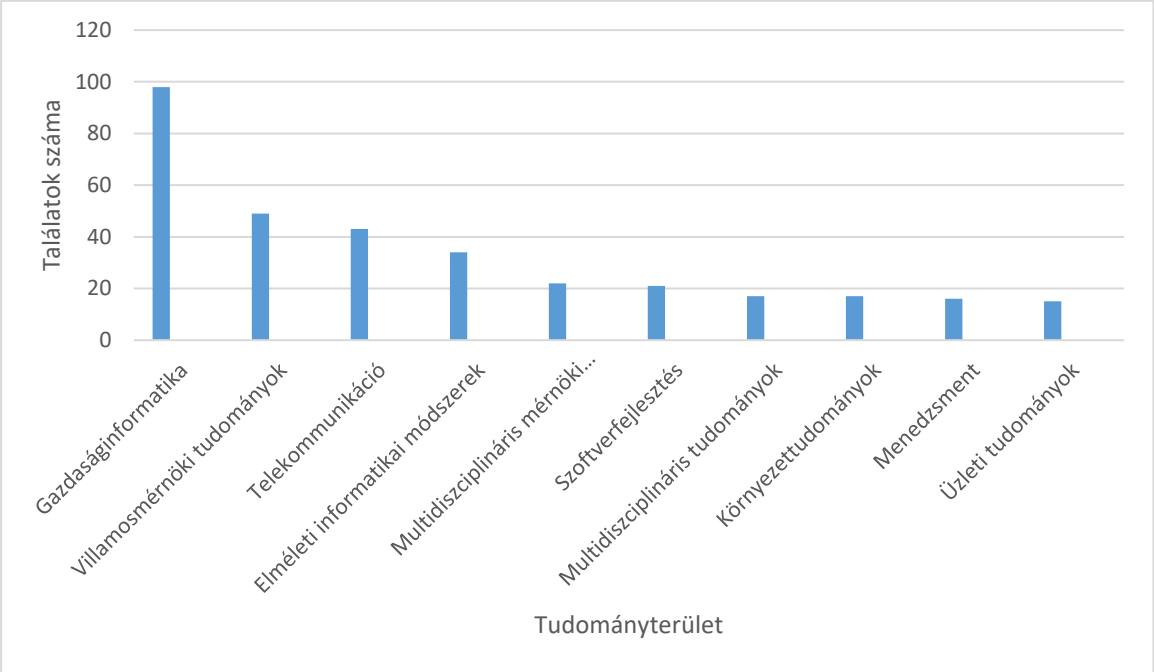
Táblázat 9: A compliance és biztonság témájában megjelent publikációk számának növekedése 2017-2025 (Saját szerkesztés)

Év	Publikációk száma (y)	t	t2	t·y
2017	112	1	1	112
2018	121	2	4	242
2019	165	3	9	495
2020	156	4	16	624
2021	167	5	25	835
2022	171	6	36	1026
2023	170	7	49	1190
2024	265	8	64	2120
2025	458	9	81	4122
Összesen	**1785**	**45**	**285**	**10766**

A statisztika igazolja az „MI-robbanás” (AI explosion) elméletét a compliance szakirodalmában: a terület egy reaktív, jogkövető fázisból a rendszerszintű, proaktív és robbanásszerű növekedés szakaszába lépett, amely a tudományos élet egyik legaktívabb fókuszpontjává vált.

Ez a mennyiségi ugrás nem csupán a cikkek számában mutatkozott meg, hanem együtt járt a tudományágak közötti átrendeződéssel is. 2017-2024 között a tudományos diskurzus egyenletesebben oszlott meg a gazdaságinformatikai és az üzleti területeken, a 2025. évi bibliometriai adatok nagyobb koncentrációt mutatnak a műszaki, és mérnöki fókuszú területeken. A WoS találatainak legnagyobb szelete egyértelműen a Gazdaságinformatika (Computer Science Information Systems) kategóriájába esett, amely 128 önálló publikációval dominálta a mezőnyt. Ezt szorosan követte az Elméleti informatikai módszerek (66), a Villamosmérnöki tudományok (58), a Telekommunikáció (55) és az Interdiszciplináris alkalmazott informatika (50). A kifejezetten a Mesterséges intelligenciának (Computer Science Artificial Intelligence) szentelt kutatások önmagukban 40 publikációt tettek ki, míg a

Szoftverfejlesztés (Software Engineering) 28 publikációval volt jelen. Ezzel ellentétben a hagyományos Menedzsment tanulmányok mindössze 18, a hagyományos Üzleti tudományok (Business) 17 publikációt eredményezett 2025-ben.



Ábra 9: A leghivatkozottabb tudományterületek compliance és a security kifejezések használata alapján a WoS adatbázisában a 2025. évben (Saját szerkesztés)

Ez az átrendeződés ahhoz felismeréshez vezethet, hogy a tudományos közösség a compliance-re már nem dominánsan adminisztratív, jogkövetési vagy klasszikus vállalatirányítási (HR-fókuszú) funkcióként tekint. A számítástechnikai és mérnöki tudományágak dominanciája arra utal, hogy a compliance alapvetően egy komplex adattudományi, rendszermérnöki és szoftverfejlesztési problémává alakult át [100]. Ahogy a szervezetek nem algoritmikus rendszereket és felhőalapú architektúrákat próbálnak irányítani, az üzleti menedzsment hagyományos eszközei – mint például az emberi elrettentésre épülő tréningek, a papíralapú auditok és a visszamenőleges kézi mintavételezés (check-list típusú megfelelés) – teljesen elégtelennek bizonyulnak. Felmerül a gondolat, hogy a compliance súlypontja a vállalati tárgyalóteremből és a HR osztályról a szerverszobába és a fejlesztői környezetekbe helyeződött át.

Ezt a technológiai irányú fogalom változást a legtöbbet hivatkozott 2025. évi szakirodalmak kvalitatív elemzése is kirajzolja. A 2025. évi akadémiai diskurzus elmozdult az elvont, elméleti MI-etikai vitáktól a konkrét, gyakorlati automatizált compliance architektúrák (Automated Compliance Architectures) fejlesztése és implementálása felé. A korábbi pszichológiai fókuszú munkákat felváltották az ipari szintű gépi tanulási modellek. Dhal és Kar a legidézettebb

tanulmányukban az élelmiszerbiztonság területén vizsgálták a mesterséges intelligencia kiaknázását, bizonyítva, hogy a gépi tanulási algoritmusok miként használhatók az automatizált hibafelismerésre és a szennyeződési kockázatok valós idejű csökkentésére [101]. Chen és munkatársai a digitális egészségügyi szenzorok (wearables) terén demonstrálták, hogy a compliance és az adatbiztonság ma már a biometrikus adatok megszakítás nélküli, algoritmikus telemetriai megfigyelésének szinonimája, és a szabályozási akadályok leküzdése csak „metamateriál”- vezérelt biztonsági megoldásokkal lehetséges [102].

Ali, Razzaque, Yousaf és Shan munkája egy olyan automatizált gépi tanulási keretrendszert (Automated Machine Learning Framework) mutatott be, amelyet kifejezetten a kritikus nemzeti infrastruktúrák kiberbiztonsági megfelelésének fokozására terveztek [103]. Ez a kutatás azt igazolta, hogy a fejlett tartalom-alapú szűrő rendszerek és a gépi tanulási osztályozók (classifierek) jelentős pontossággal képesek a lokális szervezeti kontrollokat és biztonsági házirendeket a komplex, globális szabályozási követelményekhez (például az ISO/IEC 27001 szabványhoz) rendelni, megszüntetve a folyamatos emberi felügyelet szükségességét [103].

Ezen tanulmányok együttesen hirdetik a „Folyamatos Automatizált Compliance” (Continuous Automated Compliance) korának beköszöntét, amelynek definiáló technológiai paradigmája a „Policy-as-Code” (Kódként megírt szabályzat). Ebben az új modellben a jogszabályi szövegeket (például a GDPR vagy az EU AI Act paragrafusait), az iparági standardokat és a belső irányelveket nem emberi olvasásra szánt dokumentumokban tárolják, hanem közvetlenül géppel olvasható, végrehajtható algoritmikus kóddá fordítják le. Ez a kód lehetővé teszi a kiterjedt, felhőalapú IT-infrastruktúrák valós idejű, autonóm auditálását, ahol a rendszer minden egyes konfigurációváltozást a másodperc törtrésze alatt összevet a jogszabályi kóddal. A menedzsment szerepe és fókusza ezáltal megváltozik: a retrospektív, és manuális szabályzat-végrehajtásról az algoritmikus irányításra, a gépi modellek stratégiai felügyeletére (model oversight) és az autonóm ágensek finomhangolására helyeződik át.

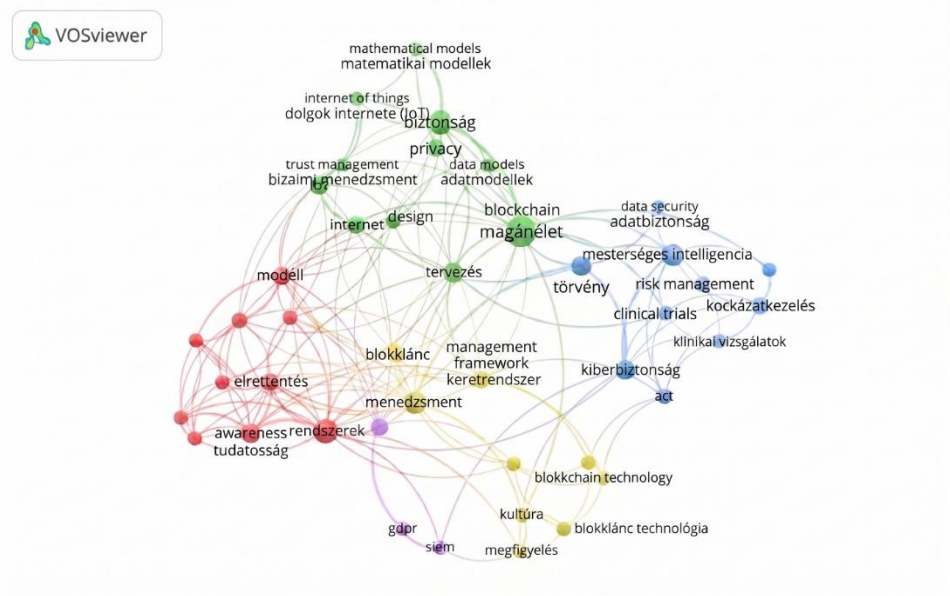
A 10. táblázat három jól elkülöníthető időmetszetben mutatja be a compliance funkciójának és fogalmi keretének változását. Míg a 2020 előtti időszakot a manuális auditok és az alacsony szintű technológiai integráció jellemezte, napjainkra a folyamatos, automatizált compliance, valamint az algoritmikus irányítás vált meghatározóvá. Az áttekintés bemutatja, hogy az egyre komplexebb gépi tanulási modellek és technológiai megoldások térnyerésével párhuzamosan a menedzsment fókusza miként helyeződött át a visszamenőleges, statikus felülvizsgálatokról a proaktív, gyakorlatiasabb validálásra.

Táblázat 10: A compliance fogalmi és operatív keretének változása (Forrás: Saját szerkesztés a bibliometriai adatok alapján).

Fogalmi Korszak	**Domináns Compliance Mechanizmus**	**Elsődleges Menedzsment Fókusz**	**A Technológiai Integráció Szintje**
2020 előtt	Időszakos manuális auditok	Szabályzatírás, visszamenőleges felülvizsgálat és manuális mintavétel.	Alacsony (Táblázatkezelők, alapvető Irányítási és Megfelelőségi szoftverek)
2020–2023	Hibrid auditálás	Felhőbiztonsági eszközök integrálása és automatizált riasztásokra való reagálás.	Közepes (Naplóösszesítés, Biztonsági Információ- és Eseménykezelő rendszerek)
2024–Jelenleg	Folyamatos Automatizált Compliance	Algoritmikus irányítás, modellfelügyelet, autonóm validálás és stratégiai összehangolás.	Magas (Gépi tanulási osztályozók, Policy-as-Code, autonóm ágensek)

A 2025. évi adatok szemantikai megértéséhez, valamint a fogalom változás vizuális demonstrálásához megismételtem a VOSviewer szoftverrel végzett topológiai hálózattérképezést, kizárólag az új, 458 publikációt tartalmazó 2025. évi szövegkorpuszon. A cél annak bemutatása volt, hogy a kulcsszavak szemantikai hálózatai miként alakultak, és mely új elméleti klaszterek uralják a kortárs diskurzust.

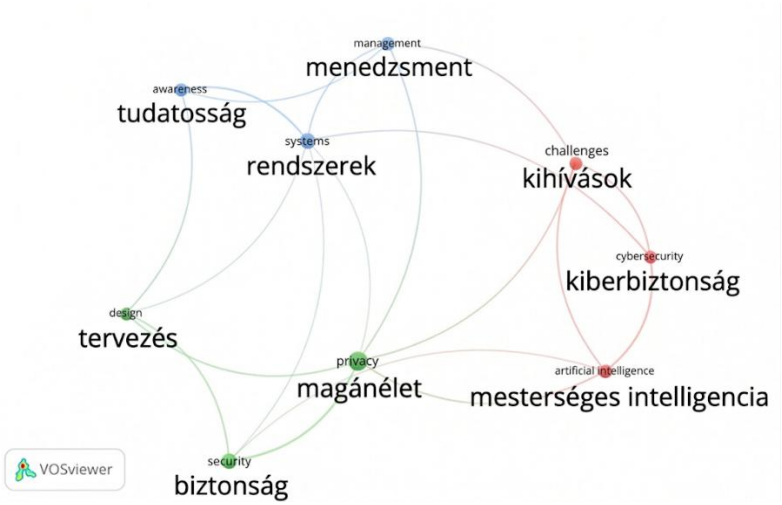
Ahogy a 2017-2024 időszak közötti vizsgálat, a 2025. évi elemzésben is 2-es, 4-es és 6-os küszöbértéket határoztam meg. Amikor a VOSviewer a minimális előfordulási küszöbértéket 2-re állítva dolgozta fel a 2025. évi adatokat, az eredmény 67 egyedi kulcsszóból álló, fragmentált és diaszporikus hálózat volt, ezt foglalja össze a 10. ábra.



Ábra 10: Hálózati térkép - kettes küszöbérték 2025. (Saját szerkesztés)

Bár a „privacy” (adatvédelem) fogalma már ezen a szűretlen térképen is dominált, a vizualizációban erős fogalmi zaj volt megfigyelhető. Olyan specifikus, rétegigényű (niche) fogalmak is megjelentek izolált mikro-klaszterekként, mint a „clinical trials”. Ezek a marginális csomópontok vizuálisan ugyan jól demonstrálták a compliance interdiszciplináris expanzióját, azonban a fókuszált fogalmi szintézishez töredezettek voltak.

A 11. ábrán a küszöbérték 4. A szoftver kiszűrte a harmadlagos koncepciókat, és az algoritmus 9 kulcskifejezésre izolálva megalkotott egy élesen elkülönülő strukturális magot.



Ábra 11: Hálózati térkép - négyes küszöbérték (Saját szerkesztés)

Ebben a finomított modellben a mesterséges intelligencia, biztonság, kiberbiztonság (adatvédelem) egyértelműen dominálta az akadémiai diskurzust, strukturálisan támogatva a kihívások a kiberbiztonság csomópontjai által. Megjelent egy technológiai klaszter

(mesterséges intelligencia, kiberbiztonság), egy szabályozási klaszter (privacy, biztonság, tervezés), valamint feltűnt a „kihívások” (challenges) csomópontja, ami rámutatott az új technológiák implementálásából fakadó súrlódásokra.

A végső fogalmi letisztultság elérése érdekében a VOSviewer algoritmusát a 6-os előfordulási küszöbértékre optimalizáltam, amely a következő vizualizációt eredményezte a 12. ábrán.

Ábra 12: Hálózati térkép - hatos küszöbérték 2025 (Saját szerkesztés)

A hálózati térképen az összes átmeneti kutatási trend és perifériku zaj kiszűrődött, és három, a 2025. évi compliance-identitást és a digitális kort abszolút meghatározó szakkifejezés maradt a topológiai térképen: a privacy, mint adatvédelem, a security, mint biztonság és a rendszerek, mint systems. Azért lehet ennyire kevés csomópont ezen a térképen, mert 2025-ben a korábbi, többéves adathalmazhoz képest sokkal kevesebb adat van, ami miatt az egyre specifikusabb keresési feltételek egyre több tanulmányt szorítanak ki a mintából.

A 2025. évi bibliometriai szintézis alapján egy olyan értelmezési irány rajzolódik ki, amelyben a compliance egyre inkább rendszerszintű összefüggésben vizsgálható, és fókuszában az adatvédelem, valamint a kiberbiztonság kérdéskörei állnak a mesterséges intelligencia alkalmazási környezetében. E megközelítés arra utal, hogy a menedzsment szerepe fokozatosan kiterjed az új technológiák és komplex rendszerek implementációjából fakadó kihívások kezelésére, valamint az adatinfrastruktúrák védelmének biztosítására.

Az elemzések egyben egy lehetséges elmozdulást is jeleznek a compliance értelmezésében: a 2017-2024 közötti időszakra jellemző az emberközpontú, a munkavállalói viselkedés befolyásolására épülő megközelítések mellett egyre hangsúlyosabbá válik egy technológia- és adatvezérelt szemlélet. Míg a korábbi időszakban a belső szabályzatok adminisztratív érvényesítése állt a középpontban, addig a 2025-re kirajzolódó tendenciák arra utalnak, hogy a mesterséges intelligencia integrációjából eredő kihívások, valamint a kiberbiztonság és az adatvédelem technológiai menedzselése növekvő jelentőséggel bír.

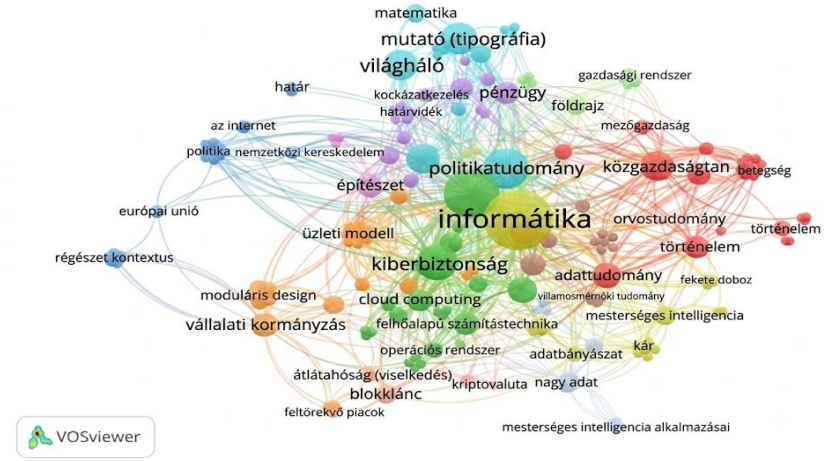
Mindezek alapján a compliance fogalma ebben a kontextusban egy átalakulóban lévő, többdimenziós jelenségként ragadható meg, amelynek elméleti körülhatárolása további vizsgálatot igényel.

MTMT-ben megjelenő publikációk

A nemzetközi trendek magyarországi összevetése céljából a Magyar Tudományos Művek Tára adatbázisának 2025. évi frissített adatait is feldolgoztam. Bár a publikációk abszolút volumene a magyar tudományos adatbázisban alacsonyabb maradt, a kvantitatív keresőalgoritmus (amely a „compliance” és „security” kulcsszavak együttes jelenlétét vizsgálta) olyan publikációkat azonosított, amelyek minőségi tartalma és mérnöki fókusza lekövette a globális eltolódást.

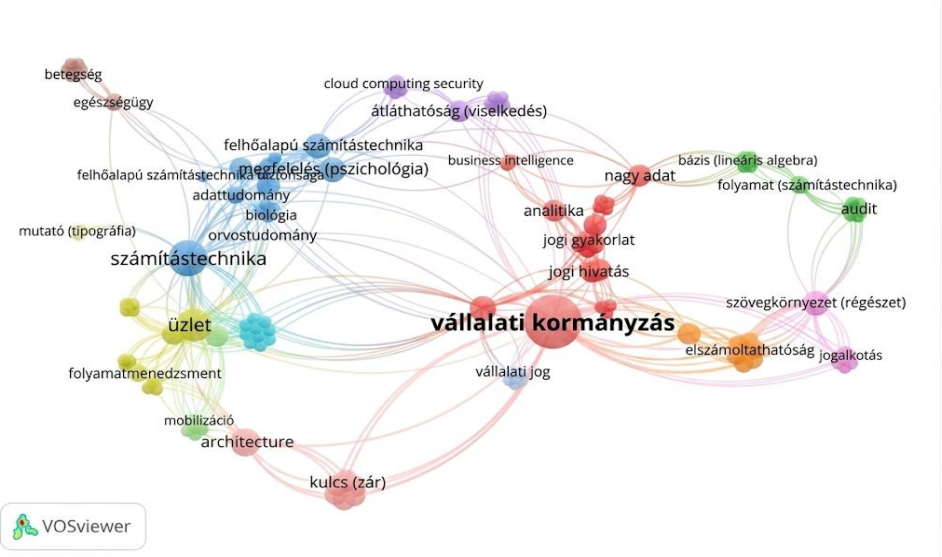
Filipović és munkatársai a Cybersecurity Act keretében az SSL/TLS tanúsítványok és a hálózati kommunikációbiztonság automatizált elemzését vizsgálták. Publikációjukban a „compliance” szó 22, a „security” szó 42 alkalommal szerepel, ami a célkoncepciók iránti mély elkötelezettséget mutatja. Kutatásuk célja egy olyan autonóm eszköz fejlesztése volt, amely emberi beavatkozás nélkül nyújt a vállalatirányítási compliance számára „gyakorlatba ültethető felismeréseket”, támogatva a szervezeteket a félrekonfigurált hálózati elemek azonnali technikai azonosításában [104]. Hasonlóképpen, Isazade és munkatársai az Ipari IoT (IIoT) rendszerekben a GDPR-megfelelés okosszerződésekkel (smart contracts) történő automatizált betartatását kutatták [105]. Ezek az MTMT-eredmények megerősítik, hogy az akadémiai fókusz a fejlett mérnöki tudományok, a hálózatbiztonság, az automatizálás és a Policy-as-Code megoldások felé tolódott el, maga mögött hagyva a kézi auditálás retrospektív megközelítését [100].

Az adatbázis alapján készült részletes kulcsszó-hálózati elemzést követően, a kapott eredmények validálása és a téma legfrissebb trendjeinek feltárása érdekében, egy összehasonlító elemzést végeztem az OpenAlex adatbázis felhasználásával is. Az elemzés célja az volt, hogy összevessem a compliance témakörének történeti fókuszpontjait (2010–2024) a legaktuálisabb, 2025. évre vonatkozó kutatási irányokkal. A vizualizáció a VOSviewer szoftver segítségével készült el, feltárva a leggyakrabban előforduló fogalmakat és azok kapcsolati rendszerét. A keresett kifejezések a következők voltak: compliance; security; management; business; artificial intelligence; law. A történeti időszakot (2010–2024) vizsgáló hálózat, 13. ábra, egy sűrű térkép, amely összesen 189 releváns kulcsszót tartalmaz.



Ábra 13: OpenAlex adatbázis eredményei 2010-2024 között a megadott kifejezések alapján (Sajét szerkesztés)

A 14. ábrán a térkép központi, legmeghatározóbb csomópontjai – amelyek a gyakorisági listák élén is szerepelnek – a klasszikus vállalati működéshez kapcsolódnak: „informatika”, „kiberbiztonság”, „adattudomány”, és „közgazdaságtan”. A klaszterek szoros kapcsolatot mutatnak a belső ellenőrzéssel, a vállalatirányítással és a cégmérettel. Ez a struktúra tükrözi, hogy az elmúlt másfél évtizedben a compliance kutatások elsősorban a szabályozási környezetnek való megfelelés pénzügyi hatásaira, a közzétételi kötelezettségekre (pl. non-financial reporting) és az ezekhez kapcsolódó adminisztratív költségekre fókuszáltak.



Ábra 14: OpenAlex adatbázis eredményei a megadott kifejezések alapján 2025-ben (Saját szerkesztés)

Ezzel szemben a 2025. évet vizsgáló kulcsszó-hálózat eltolódást mutat. A releváns kulcsszók száma 189-ről mindössze 43-ra csökkent, ami egy sokkal koncentráltabb, célzottabb kutatási fókuszt jelez. A hálózat ritkább, de új, domináns témák köré szerveződik. A leggyakrabban

előforduló kifejezések mára a „vállalati kormányzás”, a „számítástechnika”, a „üzlet” és „nagy adathalmazok” (big data) lettek. A vizualizáció azt mutatja, hogy a compliance kutatások súlypontja a klasszikus számviteli-jogi ellenőrzésről áthelyeződött a technológiai implementációra és az adatbiztonságra.

Az OpenAlex-ben végzett összehasonlító elemzés eredményei arra utalnak, hogy a compliance-hez kapcsolódó kutatási fókuszok 2025-re átrendeződésen mentek keresztül. Míg a 2010–2024 közötti időszakban a vizsgálatok elsősorban a szabályozásnak való megfelelés költségvonzataira és szervezeti kereteire – különösen az audit- és belső kontrollmechanizmusokra – koncentráltak, addig 2025-ben a hangsúly egyre inkább a megfelelőség megvalósításának technológiai eszközeire (pl. mesterséges intelligencia, deep learning), valamint az új típusú kockázati területekre (adatvédelem, kiberbiztonság, fenntarthatósági jelentéstétel) helyeződött át.

Ez az elmozdulás összhangban áll az adatbázison végzett elemzés eredményeivel, és egy olyan átfogó tendenciát jelez, amelyben a compliance vizsgálata egyre szorosabban kapcsolódik a digitális transzformáció és az adatvagyon-gazdálkodás kérdésköreihez.

Összegzés

A 2.1. alfejezet eredményei alapján megállapítható, hogy a compliance fogalma nem tekinthető egységes, lezárt kategóriának. A szakirodalom a fogalmat hagyományosan jogkövetési, normakonformitási és szervezeti kontrollfunkcióként értelmezte, azonban a digitális transzformáció, a mesterséges intelligencia, valamint az adat- és kiberbiztonsági kockázatok megjelenése ennek a keretnek tágítását teszi szükségessé.

A 2017–2024 közötti bibliometriai elemzés alapján a compliance értelmezése elsősorban emberközpontú és szervezetirányítási jellegű volt. A domináns kulcsfogalmak — így a menedzsment, a tudatosság, az elrettentés, a védelmi motiváció és az információbiztonsági irányelveknek való megfelelés — arra utalnak, hogy a megfelelőség biztosítása ebben az időszakban főként a munkavállalói magatartás és a vezetői kontroll összefüggésében jelent meg.

A 2025. évi adatok ugyanakkor érdemi hangsúlyeltolódást jeleznek. A publikációs volumen növekedése, valamint a mesterséges intelligencia, a kiberbiztonság, az adatvédelem és a rendszerszintű technológiai megoldások előtérbe kerülése azt mutatja, hogy a compliance vizsgálata egyre inkább technológia- és adatvezérelt irányba mozdul el.

A szakirodalmi eredmények összevetése alapján ez az átrendeződés Magyarországon is érzékelhető, bár kisebb publikációs volumen mellett. Az OpenAlex- és adatbázis-alapú elemzések megerősítik, hogy a compliance kutatási fókusza a klasszikus audit- és jogkövetési

megközelítéstől fokozatosan a digitális transzformáció, az adatvagyon-gazdálkodás és az automatizált kontrollmechanizmusok felé tolódik.

Mindezek alapján a fejezet alátámasztja, hogy a compliance szakirodalmi, gyakorlati és funkcionális értelmezései jelenleg nem alkotnak teljesen egységes rendszert. Ez indokolttá teszi egy átfogóbb, elméletileg megalapozott compliance-értelmezés kidolgozását, amely képes összekapcsolni a hagyományos normatív megközelítéseket a digitális korszak technológiai és biztonsági kihívásaival.

2.2 Compliance funkciók vizsgálata

A compliance fogalmának átfogó, több szinten megvalósuló vizsgálatának harmadik szintje a compliance funkciók szempontjából történő felülvizsgálata. Ebben az értelmezési keretben a compliance nem pusztán normatív kategóriaként, hanem szervezeti működésben megjelenő, konkrét irányítási és kontrollmechanizmusok összességeként vizsgálható. A compliance funkciók elemzése három perspektívában történik. Egyrészt a védelmi vonalak rendszerén keresztül, amely a szervezeti kontrollstruktúrák intézményi beágyazottságát ragadja meg. Másrészt a gyakorlati működés során jelentkező kihívások és előnyök feltárásával, amelyek a megfelelőség operatív dimenzióit tükrözik. Harmadrészt a compliance szempontból kritikus területek vizsgálatával.

Az elemzés célja, hogy a compliance fogalmát funkcionális oldalról tovább árnyalja, és hozzájáruljon annak pontosabb elméleti körülhatárolásához.

A compliance a védelmi vonalak metszetében

A compliance funkció egyik meghatározó értelmezési kerete a védelmi vonalak modellje, amely a megfelelőség szervezeti beágyazottságát és működési logikáját rendszerszinten ragadja meg. Ebben a megközelítésben a compliance nem önálló kontrolleszközként jelenik meg, hanem egy komplex, több szintű kockázatkezelési és irányítási rendszer integráns elemeként, amely a különböző védelmi szintek metszéspontjában fejti ki hatását.

A megfelelőségi funkció alapvető célja a compliance kockázatok azonosítása, mérséklése és kezelése. Jacsó csoportosításával összhangban e kockázatok közé tartozik a jogi és felügyeleti szankciók kockázata, a pénzügyi veszteségek, a hírnévromlás, valamint a bizalomvesztés [106]. Ezek a kockázati dimenziók együttesen jelzik, hogy a compliance nem pusztán normatív megfelelési kérdés, hanem a szervezeti működési stabilitás kulcstényezője.

Az Institute of Internal Auditors által kidolgozott három védelmi vonal modellje [107] alapján az első védelmi szint az operatív működéshez kapcsolódó szervezeti egységeket foglalja magában, amelyek a napi üzleti folyamatok során közvetlenül kezelik a kockázatokat. A

második védelmi vonal – amelybe a compliance funkció is tartozik – strukturált módon támogatja a kockázatkezelést, proaktívan monitorozza a kockázati tényezőket, valamint módszertani és kontrolltámogatást nyújt az első vonal számára. A harmadik védelmi vonal ezzel szemben független ellenőrzési szerepet tölt be, amely a teljes rendszer hatékonyságát és megfelelőségét értékeli.

A Financial Markets Standard Board további pontosításokat fogalmaz meg a három védelmi vonal működésével kapcsolatban [108], ugyanakkor a modell alkalmazhatósága nem tekinthető problémamentesnek. Egyes kutatók – például Eulerich [109] – rámutatnak arra, hogy a modell implementációja komplex szervezeti és technológiai környezetben korlátokba ütközhet. Ennek ellenére a modell gyakorlati elterjedtsége arra utal, hogy továbbra is meghatározó referenciakeretként szolgál a compliance funkció strukturálásában.

A védelmi vonalak hatékony működésének előfeltétele, hogy az első és a második vonal egyaránt kockázatalapú megközelítésre építse működését. Ebben a rendszerben a szervezet irányító testülete biztosítja a jogi, szabályozási és etikai elvárások felügyeletét, míg a menedzsment felel azok operatív megvalósításáért. A szervezeti működést emellett külső bizonyosságot nyújtó szereplők – például a könyvvizsgálók – is támogatják, tovább erősítve a kontrollkörnyezet integritását.

A compliance kontroll funkciója tartalma nem merül ki egyes kontrolltevékenységek felsorolásában, hanem egy integrált irányítási mechanizmusként értelmezhető, amely több területet fog át. Ide tartozik különösen a kockázatok és érdekkonfliktusok azonosítása és kezelése, a szabályszerű működés támogatása, a korrupció és piaci visszaélések megelőzése, a pénzmosás és terrorizmus finanszírozása elleni fellépés, valamint az adatvédelem és információbiztonság biztosítása. Emellett a compliance funkció hozzájárul a szervezeti transzparencia erősítéséhez, az ügyfelekkel való tisztességes bánásmód kialakításához, valamint a panaszkezelési mechanizmusok működtetéséhez.

A compliance támogató szerepköre szintén többdimenziós: magában foglalja a hiányosságok feltárását és a korrekciós intézkedések kezdeményezését, a szervezeti tudatosság fejlesztését, a felsővezetés irányába történő rendszeres riportálást, valamint a reputáció és a jó hírnév fenntartását. Ezen túlmenően a compliance funkció aktívan részt vesz az ellenőrzési folyamatok tervezésében és végrehajtásában, továbbá kulcsszerepet tölt be a hatóságokkal való kapcsolattartásban. Mindezek alapján a compliance a védelmi vonalak rendszerében nem csupán végrehajtó vagy ellenőrző funkcióként jelenik meg, hanem olyan közvetítő mechanizmusként, amely összekapcsolja a szervezeti működés operatív, irányítási és ellenőrzési dimenzióit.

A compliance működése a gyakorlatban: főbb kihívások és előnyök

A compliance működésének gyakorlati megvalósítása alapvetően kockázatalapú megközelítésre épül, amelynek célja a megfelelőségi kockázatok bekövetkezési valószínűségének és hatásának egyidejű mérséklése a szervezeten belül. E cél elérése nem egységes módon történik, hanem jelentős mértékben függ az adott ágazat sajátosságaitól, a szervezet méretétől, valamint a működési és szabályozási környezettől. Ennek megfelelően a compliance gyakorlati alkalmazása kontextusfüggő, adaptív jellegű.

A compliance működése nem tekinthető statikus folyamatnak, hanem egy iteratív, folyamatos fejlesztésen alapuló rendszerként írható le. A működési logika jól értelmezhető a PDCA-ciklus mentén, amely a tervezés, a megvalósítás, az ellenőrzés és a visszacsatolás egymásra épülő fázisain keresztül biztosítja a szervezeti tanulást és az alkalmazkodóképességet. A compliance rendszerek hatékonysága így nem egy adott állapothoz, hanem a folyamatos korrekció és fejlesztés képességéhez köthető.

A hatékony compliance működés egyik alapfeltétele a felsővezetés elkötelezettsége, amely a szervezeti kultúra és etikai normák kialakításán keresztül fejti ki hatását (tone at the top). A vezetői magatartás meghatározó szerepet játszik az elszámoltathatóság, az integritás és az átláthatóság érvényesülésében. Ezzel összefüggésben a compliance funkció szervezeti beágyazottsága is kulcsfontosságú, amely jellemzően dedikált felelősi szerepkör (compliance officer) vagy szervezeti egység formájában jelenik meg. A funkcionális függetlenség biztosítása mellett e szerepkör egyaránt igényel jogi, technológiai és üzleti kompetenciákat.

A compliance funkció gyakorlati működésében egyszerre jelenik meg a kontroll- és a támogató jelleg. Egyrészt hozzájárul a szabályozási megfelelés biztosításához, a kockázatok és érdekkonfliktusok azonosításához, valamint a jogsértések és visszaélések megelőzéséhez. Másrészt támogatja a szervezeti működés szabályozottságát, a belső folyamatok fejlesztését, valamint a tudatosság növelését a munkavállalók és a partnerek körében. E kettős szerep révén a compliance egyfajta koordinációs mechanizmusként is értelmezhető, amely összekapcsolja a jogi, informatikai és üzleti dimenziókat.

A compliance működés során alkalmazott kontrollmechanizmusok jelentős része a folyamatokba integrált módon jelenik meg. Ez lehetővé teszi a megfelelőségi hiányosságok korai azonosítását, valamint a szervezeti, technológiai és adatbiztonsági keretrendszerek folyamatos újraértékelését. A compliance ilyen értelemben nem csupán ellenőrzési funkció, hanem a szervezeti reziliencia kialakításának egyik kulcseleme is.

A gyakorlati megvalósítás ugyanakkor számos kihívással jár. A compliance rendszerek működtetése jelentős erőforrásigénnyel rendelkezik, mind pénzügyi, mind időbeli és szervezeti

értelemben. A menedzsment számára ezért folyamatos egyensúlykeresést jelent a szabályozási megfelelés, a működési hatékonyság, a kockázatkezelés és a gazdasági célok összehangolása. Ebből következően a compliance struktúrák kialakítása szükségszerűen az adott szervezet kockázati profiljához és működési sajátosságaihoz igazodik.

A compliance működés előnyei jellemzően nem rövid távon jelentkeznek, hanem a szervezeti stabilitás, a bizalom és a reputáció hosszabb távú erősödésében ragadhatók meg. A megfelelően kialakított compliance kultúra hozzájárul a szervezet ellenállóképességének növeléséhez, valamint versenyelőnyt biztosíthat a szabályozási és piaci környezetben.

A fentiek alapján megállapítható, hogy a compliance funkció súlypontja fokozatosan elmozdul az ellenőrző jellegtől a preventív és támogató működés irányába. Ez az elmozdulás arra utal, hogy a compliance egyre inkább a szervezeti működés integrált, stratégiai jelentőségű elemévé válik.

Compliance érzékeny ágazatok

A compliance szempontjából érzékeny ágazatok olyan gazdasági területek, amelyek működését magas szintű szabályozottság, jelentős kockázati expozíció, valamint kiemelt reputációs és társadalmi következmények jellemzik. E szektorokban a megfelelőség nem pusztán jogszabályi kötelezettségként jelenik meg, hanem a működési stabilitás, a bizalom fenntartása és a szervezeti fenntarthatóság alapvető feltételeként értelmezhető.

A compliance-érzékenység három fő dimenzió mentén ragadható meg: a szabályozási intenzitás, a kockázatok komplexitása és súlyossága, valamint a reputációs és társadalmi hatások mértéke. Ezen dimenziók mentén a pénz- és tőkepiaci szektor, a gyógyszeripar, valamint a telekommunikáció olyan kiemelt ágazatokként azonosíthatók, amelyekben a compliance funkció stratégiai jelentőséggel bír. A WoS-alapú bibliometriai vizsgálatban a műszaki szektorokból származott a legtöbb compliance-szel kapcsolatos tudományos publikáció.

A compliance a pénz- és tőkepiaci szektorban

A pénzügyi terület compliance-érzékenysége elsősorban a magas szabályozási intenzitásból és a rendszerszintű kockázatokból fakad. Működését kiterjedt jogszabályi környezet, nemzetközi standardok és felügyeleti elvárások határozzák meg, amelyek betartása közvetlen hatással van a pénzügyi rendszer stabilitására. A Magyar Nemzeti Bank követelményei [110] is ezt a szigorú kontrollkörnyezetet tükrözik.

A compliance funkció ebben az ágazatban olyan kulcsterületekre fókuszál, mint a pénzmosás és a terrorizmus finanszírozása elleni fellépés, a korrupció megelőzése, az összeférhetetlenségi helyzetek kezelése, valamint a piaci visszaélések (pl. bennfentes

kereskedelem) kiszűrése. Ezen túlmenően kiemelt szerepet kap az adatvédelem, a fogyasztóvédelem és a reputáció megőrzése, amelyek együttesen biztosítják a pénzügyi intézmények iránti bizalom fenntartását [111]; [112].

A szabályozási környezet folyamatos fejlődését jelzi a Magyar Nemzeti Bank 12/2022. (VIII.11.) számú ajánlása, amely a belső védelmi vonalak működésére és a kontrollfunkciók erősítésére vonatkozó követelményeket határoz meg [113]. Az ajánlás külön hangsúlyt helyez a csalásmegelőzési kultúra kialakítására, az ellenőrzési nyomvonalak fejlesztésére, valamint a pénzmosás elleni megfelelőségi felelősség szervezeti szintű megerősítésére.

A compliance a gyógyszeriparban

A gyógyszeripar compliance-érzékenysége elsősorban a betegbiztonság, az etikai megfelelés és a hatósági kontrollok szigorúsága mentén értelmezhető. Ebben az ágazatban a megfelelőség közvetlen kapcsolatban áll az emberi élet és egészség védelmével, ami a compliance funkciót kiemelt jelentőségűvé teszi. A szabályozási környezet mellett az iparági önszabályozás is meghatározó szerepet játszik, különösen az orvosokkal és egészségügyi szereplőkkel való együttműködés, a gyógyszerpromóció és a tájékoztatás területén. A compliance kockázatok közé tartozik a tisztességtelen befolyásolás, a nem megfelelő kommunikáció, valamint az egészségügyi adatok védelmének hiányosságai.

A szakirodalom [114]; [115] rámutat arra, hogy a gyógyszeripari compliance egyszerre jogi és etikai dimenzióval rendelkezik, amelynek célja a transzparens működés és a tisztességes piaci magatartás biztosítása. Ennek következtében a compliance ebben az ágazatban nem csupán kontrollmechanizmus, hanem bizalomépítő eszköz is.

A compliance a telekommunikációban

A telekommunikációs ágazat compliance-érzékenysége elsősorban az adatvédelem, az információbiztonság és a digitális infrastruktúrák működéséből fakadó kockázatokhoz kapcsolódik. A szektor sajátossága, hogy a compliance funkció gyakran integrált irányítási rendszerek részeként jelenik meg, szoros együttműködésben a jogi és kockázatkezelési területekkel. A compliance fókuszában a korrupció elleni fellépés, az etikai normák érvényesítése, valamint a belső és külső kommunikáció szabályozása áll. A digitális környezetből fakadóan különös jelentőséggel bír az adatvédelem és a felhasználói adatok biztonságos kezelése.

Grant és Agoro megállapítása szerint a szervezeteknek proaktívan kell alkalmazkodniuk az adatvédelmi és technológiai kihívásokhoz annak érdekében, hogy elkerüljék a reputációs és pénzügyi következményeket [116]. Ez a megközelítés jól illusztrálja, hogy a compliance ebben

az ágazatban egyre inkább a technológiai kockázatok kezelésének eszközévé válik [117], [118], [119].

Az alfejezet végén megjegyzendő, hogy a közszférában szintén egyre jelentőssebbé válik a compliance alkalmazása, viszont ennek részletezését a doktori értekezés keretei nem teszik sem szükségessé sem lehetővé. A compliance érzékeny ágazatokban a compliance funkciók jelen vannak, azok védelmi-biztonsági és problémamegelőző szerepe egyaránt jelentős hatással az ágazatok működésére.

Összegzés

Az elemzés alapján megállapítható, hogy a compliance-érzékeny ágazatok eltérő működési sajátosságokkal rendelkeznek, ugyanakkor azonosítható közös mintázat a magas szabályozottság, a komplex kockázati környezet és a jelentős reputációs kitettség. Ezek a tényezők együttesen arra utalnak, hogy a compliance funkció e szektorokban nem pusztán operatív, hanem stratégiai jelentőségű szerepet tölt be [120].

A compliance fogalmának felülvizsgálatából kiindulva a 2.2 alfejezet célja a fogalom funkcionális aspektusainak értelmezése és újragondolása volt. A compliance funkcióit mint a fogalom gyakorlati megnyilvánulásait és szervezeti hatásait vizsgálta három dimenzió mentén. A védelmi vonalak rendszerének összefüggéseit, majd a compliance gyakorlati kihívásait és előnyeit tárgyalta. Végül a compliance szempontból érzékeny szervezeti gyakorlatok bemutatására került sor, amelyek értelmezése további alapot nyújtott a fogalom pontosításához:

Az eredmények alapján kirajzolódik egy olyan értelmezési keret, amelyben a compliance nem statikus megfelelési kategóriaként, hanem dinamikus, szervezeti működésben megjelenő folyamatként vizsgálható. E folyamat különböző szabályozási, szervezeti és etikai dimenziók összehangolásán keresztül fejti ki hatását [121].

2.3 Összefoglalás

A fejezet célja a compliance fogalmának többdimenziós, elméletileg megalapozott vizsgálata volt, amely három egymásra épülő elemzési perspektívában valósult meg: az elméleti definíciók összehasonlító elemzésén, a bibliometriai vizsgálaton, valamint a funkcionális megközelítésen keresztül. A kiinduló kutatási kontextus rámutatott arra, hogy a compliance napjainkra fragmentált jelentéstartalmú fogalommá vált, amely különböző tudományterületek és gyakorlati szektorok eltérő értelmezési kereteiben jelenik meg.

A szakirodalmi elemzés eredményei alapján megállapítható, hogy a compliance hagyományos megközelítése elsősorban jogkövetési és normakonformitási keretben mozgott, amely a szervezeti működés szabályozottságára és kontrolljára helyezte a hangsúlyt.

Ugyanakkor a bibliometriai vizsgálatok rámutattak arra, hogy a fogalom tartalma időben dinamikusan változik. A 2017–2024 közötti időszakban a compliance értelmezése dominánsan emberközpontú és szervezetirányítási jellegű volt, amely a munkavállalói magatartás, a vezetői kontroll és a szervezeti tudatosság szerepét hangsúlyozta. Ezzel szemben a 2025. évi adatok egyértelmű hangsúlyeltolódást jeleznek a technológiai és adatvezérelt megközelítések irányába, ahol a mesterséges intelligencia, a kiberbiztonság és az adatvédelem kerülnek a vizsgálatok középpontjába. A hazai és a nemzetközi adatbázisok publikációinak számából kitűnik, hogy az utóbbi években megnőtt iránta a tudományos érdeklődés. A nemzetközi szakirodalomban leggyakrabban előforduló kifejezések, valamint a releváns kulcsszavak közötti kapcsolatrendszerek elemzésével létrehozott hálózati térképek lehetővé tették a compliance diskurzus strukturális mintázatainak feltárását. A bibliometriai eredmények hozzájárultak egy olyan szintetizáló értelmezési keret kialakításához, amely a kutatás empirikus megállapításaira építve alapot teremt a fogalom további elméleti pontosításához.

A nemzetközi és a hazai adatbázis eredmények összevetése megerősítette, hogy ez az átrendeződés általános jelenség, amely a hazai adatbázis alapján is megjelenik, bár eltérő intenzitással. A compliance kutatási fókusza a klasszikus audit- és jogkövetési megközelítésektől egyre inkább a digitális transzformáció, az automatizált kontrollmechanizmusok és az adatvagyon-gazdálkodás irányába mozdul el. Ez a tendencia alátámasztja azt a feltételezést (H1), hogy a compliance fogalmának különböző értelmezései nem alkotnak egységes rendszert.

A compliance funkciók szempontjából történő megközelítés tovább árnyalta a compliance értelmezési kereteit. A védelmi vonalak modelljén keresztül feltárhatóvá vált a compliance szervezeti beágyazottsága és kontrollmechanizmusa, míg a gyakorlati működés vizsgálata rámutatott a megfelelőség dinamikus, folyamatorientált jellegére. A compliance működése a egyszerre jelenik meg kontroll- és támogató funkcióként, amely a kockázatok kezelésén túl hozzájárul a szervezeti működés koordinációjához is.

A compliance-érzékeny ágazatok elemzése további empirikus alapot nyújtott a fogalom értelmezéséhez. Az eltérő szektorok összehasonlítása alapján azonosíthatóvá vált egy közös strukturális mintázat, amelyet a magas szabályozottság, a komplex kockázati környezet és a jelentős reputációs kitettség jellemez. Ez arra utal, hogy a compliance szerepe ezekben az ágazatokban túlmutat az operatív működésen, és egyre inkább stratégiai jelentőséggel bír.

A funkciók elemzése és az empirikus vizsgálatok együttesen arra utalnak, hogy a compliance szerepe túlmutat az operatív kontrollmechanizmusokon, és egyre inkább a szervezeti működés stratégiai jelentőségű elemévé válik. A gyakorlati alkalmazás rámutat arra, hogy a compliance

nem egyetlen funkcionális területhez köthető, hanem a jogi, információbiztonsági, menedzsment és pénzügyi dimenziók metszetében jelenik meg, amely tovább rétegzi a fogalom tartalmát.

A második fejezet eredményei összességében egy olyan értelmezési keretet rajzolnak ki, amelyben a compliance nem statikus fogalomként jelenik meg, hanem dinamikusan változó, több dimenzióban értelmezhető jelenségként. A fogalom tartalma a jogi, szervezeti, technológiai és etikai szempontok metszetében alakul. A második fejezet megalapozott egy olyan integratív compliance-értelmezés kidolgozását, amely képes összekapcsolni a hagyományos normatív megközelítéseket a digitális korszak új típusú kihívásaival.

3 A COMPLIANCE – A MESTERSÉGES INTELLIGENCIA MEGJELENÉSÉNEK VIZSGÁLATA A HAZAI VÁLLALKOZÁSOK MŰKÖDÉSÉBEN – KÉRDŐÍVES ÉS INTERJÚELEMZŐ MÓDSZEREKKEL

A kérdőívet és az interjú kérdéssot az elméleti vizsgálatok eredményeinek értelmezése és gyakorlatban való leképezésének céljából készítettem. E fejezetben először a kérdőíves, majd az interjús kutatási módszerekre alapozva vizsgálom a mesterséges intelligencia megjelenését a hazai vállalkozások működési gyakorlatában. A kérdőíves kutatási módszer ismertetését követően az egyes feltételezéseket vetem össze a kérdőívre adott válaszokkal. Ezt követően interjús kutatási módszerrel vizsgálom meg a feltételezések egyes állításait.

Ahhoz, hogy a mesterséges intelligencia és a compliance kapcsolatát a hazai vállalati gyakorlatban megfelelően értékeljem, a kutatás a szocio-technikai rendszerek (STS) elméletére támaszkodik [122]. Ebből a mérnöki-menedzsment perspektívából a compliance nem csupán statikus szabályok halmaza, hanem egy dinamikus szocio-technikai kontrollrendszer. Az MI rendszerek olyan szervezeti kontextusokba ágyazódnak be, amelyek magukban foglalják az emberi döntéshozatalt, a munkafolyamatokat és az irányítási struktúrákat [122]. A hatékony MI-kormányzás (governance) tehát megköveteli a technikai kontrollok és a szervezeti gyakorlatok – különösen a munkavállalói biztonságtudatosság – szoros összehangolását [123], [124]; [125], [126], [127].

3.1 A kérdőíves kutatási módszer

Az adatfelvétel (MS Forms) kérdőívvel történt 2024. 11. 07. és 2024. 12. 16. között online, önkitöltős módszerrel. A kérdőív 35 kérdést tartalmazott, melyek között szerepeltek nyitott és zárt kérdések egyaránt. A zárt kérdések esetén a „Nem tudom”, „Nincs válasz”, „Nem vagyok érintett” válaszlehetőségeket elemzés során eltávolítottam; adatbevitel nem történt. Az elemszámokat minden vizsgálat esetén jelöltem.

A válaszadók, azaz a mintavételi egységek magyarországi cégek képviselői voltak. A 140 válaszadóból 27 fő (19,3%) a cég vezetője, 39 fő (27,9%) a cég tulajdonosa és 74 fő (52,9%) egyéb munkatárs volt; e dolgozók közül 47 fő (33,6%) a könyvelés, 42 fő (30,0%) a menedzsment, 27 fő (19,3%) egyéb, 13 fő (9,3%) az IT, 5 fő (3,6%) a marketing, 4 fő (2,9%) az adminisztráció és 2 fő (1,4%) a HR területen dolgozott.

Az elemzés egységei a vizsgálat egy részében maguk a válaszadók voltak (rájuk vonatkoztak a K6, K7, K9, K13–K26, K29, K30, K32, K37 kérdőívkérdések), míg bizonyos esetekben

maguk a cégek (rájuk vonatkoztak a K3–K5, K8, K10–K12, K27, K29, K31, K33–K36 kérdőívkérdések). Minden adatfeldolgozás során jelölésre került, hogy az adott elemzés a válaszadókra vagy a cégekre irányult-e.

A cégek 79,3%-a (111 cég) mikro-, vagy kisvállalkozás, 9,3%-a (13 cég) középvállalkozás és 11,4%-a (16 cég) nagyvállalat volt. A minta viszont nem tekinthető reprezentatívnak a magyarországi aktív, működő vállalkozások méretmegoszlása szempontjából. A statisztikai elemzéseket az SPSS 30.0 (SPSS Inc., Chicago, Illions, USA) és MS Excel segítségével végeztem.

3.2 A H1 hipotézis kérdőíves vizsgálata – a compliance fogalom

Kutatási kérdésként került megfogalmazásra, hogy hogyan határozható meg a compliance fogalma a szakirodalom, az elméleti vizsgálatok, továbbá a gyakorlati működés és a compliance funkciók összevetése alapján. A terület átalakulása és fejlődése következtében feltételezhető, hogy a compliance vállalati szintű alkalmazásában változások vannak a mesterséges intelligencia előretörése miatt. Ennek a kérdésnek a megválaszolásához felülvizsgáltam a compliance fogalmát.

A válaszadókra irányuló alábbi nyitott kérdés feldolgozása utólagos kódolással történt: „K9: Mi az a három dolog, ami a compliance (megfelelőség) és a mesterséges intelligencia kifejezések hallatán először eszébe jut?” Utóbb kiderült, hogy a válaszadók – a nem megfelelő kérdésfeltevés miatt – nem különítették el a compliance-re, valamint a mesterséges intelligenciára vonatkozó válaszaikat, emiatt a kódolás, valamint a statisztikai elemzés a két fogalomra együttesen történt meg. A válaszok rendszerezése során az összefüggő kifejezésekből, a szinonimákból alkottam összefoglaló kategóriákat. A kérdésre 139 értékelhető válasz érkezett; ezek mindegyike besorolható volt a 18 kategória közül valamelyikbe, esetleg többe is. A kategóriák részletezését, valamint a gyakorisági mutatókat a 11. táblázat mutatja be.

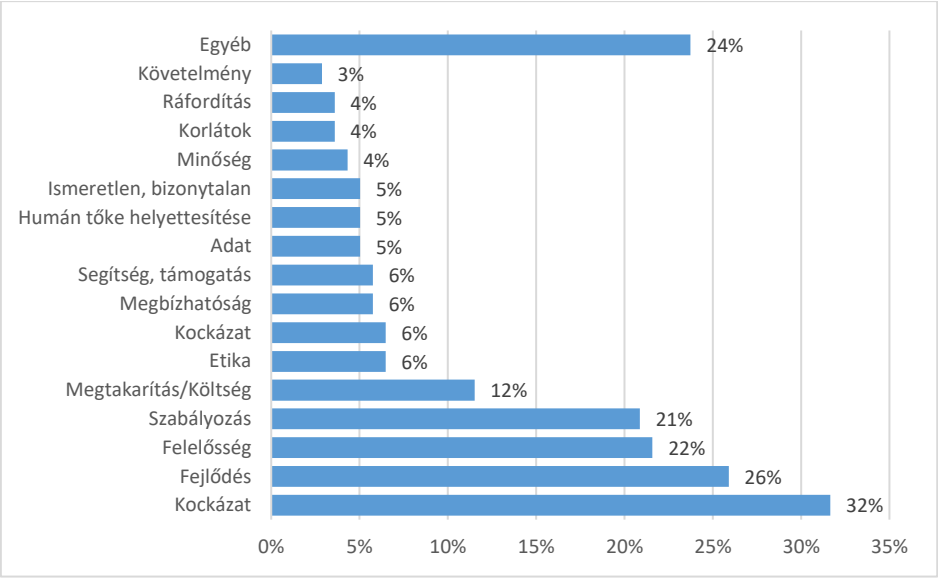
Táblázat 11: A compliance, illetve a mesterséges intelligencia meghatározása (Az érvényes válaszokra – 139-re – vetítve, saját szerkesztés)*

Kategória		**Említés gyakorisága**	
Megnevezése	**Részletezése, példák**	**fő**	**%***
Biztonság	biztonság, adatvédelem, adatbiztonság	59	42%
Kockázatkezelés	kockázat/kockázatkezelés	44	32%
Fejlődés	innováció, fejlődés, fejlesztés, jövő, lehetőség	36	26%
Felelősség	felelősség	30	22%
Szabályozás	jogszerű, jogszabályi megfelelés, törvény, szabályozás/szabályozatlan, átláthatóság, standard	29	21%
Megtakarítás/Költség	idő, pénz, adminisztráció, megkönnyítés, gyorsaság, kényelem, hatékonyság	16	12%
Etika	etikusság, etikai megfelelés, morális kérdések	9	6%
Kockázat	veszély, félrevezető információk, hibák	9	6%

Megbízhatóság	ellenőrzés/ellenőrizhetetlen, garancia, megbízhatóság	8	6%
Segítség, támogatás	segítség, támogatás, elégedettség	8	6%
Adat	információbázis, segíti az információ elérését, információtömeg, információkereskedelem, adathalászat	7	5%
Humán tőke helyettesítése	automatizáció, robotika, szakmák megszűnése, munkanélküliség	7	5%
Ismeretlen, bizonytalan	ismeretlen, idegen, kiforratlan, bizonytalanság, bizalmatlanság, óvatosság	7	5%
Minőség	szakmai minőség, precizitás, pontosság	6	4%
Korlátok	korlátok, határok, büntetés, szigor	5	4%
Ráfordítás	tanulás, tanítás, képzés, felkészítés, beállítás	5	4%
Követelmény	kötelező, elengedhetetlen, kényszer	4	3%
Egyéb	konkrét tevékenységek (pl. fordítás, képgenerálás), szoftverek (chat GPT), irányelvek, szabványok (NIS2, ISO) megnevezése (ide tartoznak a 2% alatti gyakoriságú említések is)	33	24%

Az ismertetett adatok alapján kimutatható, hogy öt kategória 20% fölötti gyakorisággal szerepelt a válaszokban. A biztonság kategóriájának gyakorisága kiemelkedően magas (42%), ezt követi a kockázatkezelés (32%), majd a fejlődés (26%), végül a felelősség és a szabályozás is közel azonos gyakorisággal volt említve. 3–6 % közötti gyakorisággal használták az etika, a kockázat, a megbízhatóság, a segítség, a támogatás, az adat, a humán tőke helyettesítése, az ismeretlen, a bizonytalan, a minőség, a korlátok, a ráfordítás és a követelmény kategóriákat. Azon válaszok között, amelyek minősítést tartalmaztak, szinte fele-fele arányban oszlottak meg a pozitív és a negatív reakciók, vagyis az inkább pozitív minősítések száma 53, az inkább negatívaké 51. Leggyakrabban a biztonság, a kockázat, a joggal kapcsolatos megjegyzések, a felelősség, az adatokkal való kapcsolat került fókuszba, valamint a jövő és innováció tárgyköre volt hangsúlyos. Továbbá megállapítható az is, hogy a válaszadók értékítélete inkább volt pozitív kicsengésű.

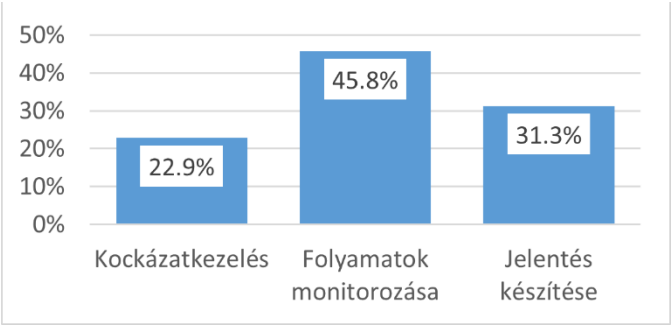
A válaszok megoszlását mutatja be a 15. ábra is.



Ábra 15: A compliance, illetve a mesterséges intelligencia meghatározása (N=139) (Saját szerkesztés)

A válaszadókhoz intézett következő kérdésre reagálva („Milyen compliance területen használná a mesterséges intelligenciát?”) mindössze 48 válaszadó (34,3%) volt képes szakmai területet megjelölni. A fennmaradó 92 fő (65,5%) a „Nem használ ilyet a szervezetem” választ húzta be. A legnagyobb arányban a folyamatok monitorozását és a jelentések készítését jelölték meg. Ugyanakkor a válaszokból az is kitűnik, hogy a területen a jövőben jelentős előrelépést lehet majd prognosztizálni, aminek következtében a használathoz, a szabályozáshoz kapcsolódó kérdéskörök felértékelődése várható.

A megjelölt területek megoszlását a 16. ábra mutatja:



Ábra 16: Milyen compliance területen használná a mesterséges intelligenciát? (N=48) (Saját szerkesztés)

A kérdőíves kutatás eredményei további empirikus szempontokkal egészítik ki a második fejezetben kialakított compliance-értelmezési keretet. A válaszok alapján különösen a biztonság dimenziója válik hangsúlyosabbá, amely a fogalom további értelmezését és finomítását indokolja.

Összegzés

A kutatás arra kereste a választ, hogy miként értelmezhető a compliance fogalma a szakirodalmi, elméleti és gyakorlati megközelítések összevetésével, különös tekintettel a mesterséges intelligencia hatására. A kérdőíves vizsgálat eredményei ezt az értelmezési keretet empirikus szempontból egészítették ki.

A válaszok alapján a compliance és a mesterséges intelligencia a válaszadók gondolkodásában szorosan összekapcsolódik, amelyet elsősorban a biztonság, a kockázatkezelés, a szabályozás és a felelősség dimenziói határoznak meg. Kiemelkedő a biztonság hangsúlya, ami a compliance és az adatvédelmi, valamint kiberbiztonsági kérdések közötti erős kapcsolatot jelzi. A gyakorlati alkalmazás tekintetében a mesterséges intelligencia használata még korlátozott, azonban elsősorban a folyamatok monitorozásában és a jelentéskészítésben jelenik meg, ami a jövőbeni bővülés lehetőségére utal. Az alfejezet alapján a compliance a gyakorlatban is egy komplex, dinamikusan alakuló jelenségként jelenik meg, amelynek értelmezésében a biztonsági és technológiai dimenziók egyre hangsúlyosabbá válnak.

3.3 A H2 hipotézis kérdőíves vizsgálata – az MI eszközhasználat és a compliance megoldások

Feltételezem, hogy a mesterséges intelligencia eszközhasználata összefügg a compliance rendszerek jelenlétével a hazai vállalkozások esetében.

A következő vizsgálat cégekre, mint elemzési egységekre vonatkozik. A cégek MI eszközhasználatát a következő kérdőívkérdésekkel vizsgáltam:

- K10: Használ az Ön cége bármilyen mesterséges intelligencián alapuló eszközt? (Igen/Nem)
- K11: Amennyiben az előző kérdésre „Igen” volt a válasza, melyek ezek? (Több választ is megjelölhet egyszerre: Dall-E / ChatGPT / DeepL / Brickabrack AI / Gemini / Claude / Midjourney / Character.AI / QuillBot / Microsoft Copilot / TensorFlow / SAP /Bard / Novel AI / CapCut / Janitor AI / Civitai)
- K12: Mely területeken tapasztalta, hogy vállalkozása mesterséges intelligencián alapuló alkalmazást/eszközt használ? (Egyszerre több válaszlehetőséget is megjelölhet: Nem használ ilyet a szervezetem / Könyvelés, számvitel / HR / Ügyfélszolgálat, támogatás / Adminisztráció / Marketing / Menedzsment / Értékesítés)

Ezek közül a K10 kérdés az eszközhasználat tényét, míg a K12 kérdésből létrehozott K12_K változó (amely a megjelölt területek számát összegezi) az eszközhasználat kiterjedtségét méri.

A megfelelőség biztosításának vizsgálata az alábbi kérdések nyomán létrehozott változókkal történt:

- K33: Van compliance (megfelelőség) előírása, szabályzata a vállalkozásnak? (Van/Nincs)
- K34: A vállalkozása milyen gyakran vizsgálja felül a compliance (megfelelőség) szabályrendszerét? (3: Évente. / 2: Időszakosan. / 1: Akkor, amikor valami új kockázati tényező felmerül. / 0: Soha)
- K35: Mire használja jelenleg az Ön szervezete a megfelelőségi (compliance) szabályokat? (Több választ is megjelölhet: Jogszabályok változásainak nyomon követésére. / Képzési és tanúsítási követelmények kezelésére. / Reputáció céljából. / Előírások és jóváhagyások nyomon követésére és kezelésére.)
- K36: Hogyan tájékoztatják szervezeténél a munkavállalókat, a szerződött feleket és más felelős személyeket a vállalkozás megfelelőségi (compliance) mechanizmusairól? (Több választ is megjelölhet: Képzésekkel. / Belső szabályozókkal (pl.: Etikai kódex vagy Mesterséges intelligencia eszköz felhasználási útmutató). / Belső kommunikációval. / Belső, céges weboldal használatával. / Tudatosságnövelő események szervezésével.)

E kérdések közül a megfelelőség biztosításának tényét a K33 változóval mértem, míg ennek hangsúlyosságát a K34_2 változóval, mely a K34 kérdőívkérdés 1–3 válaszlehetőségeinek az összevonásával jött létre a következők szerint: 0: Soha. / 1: Időszakosan.

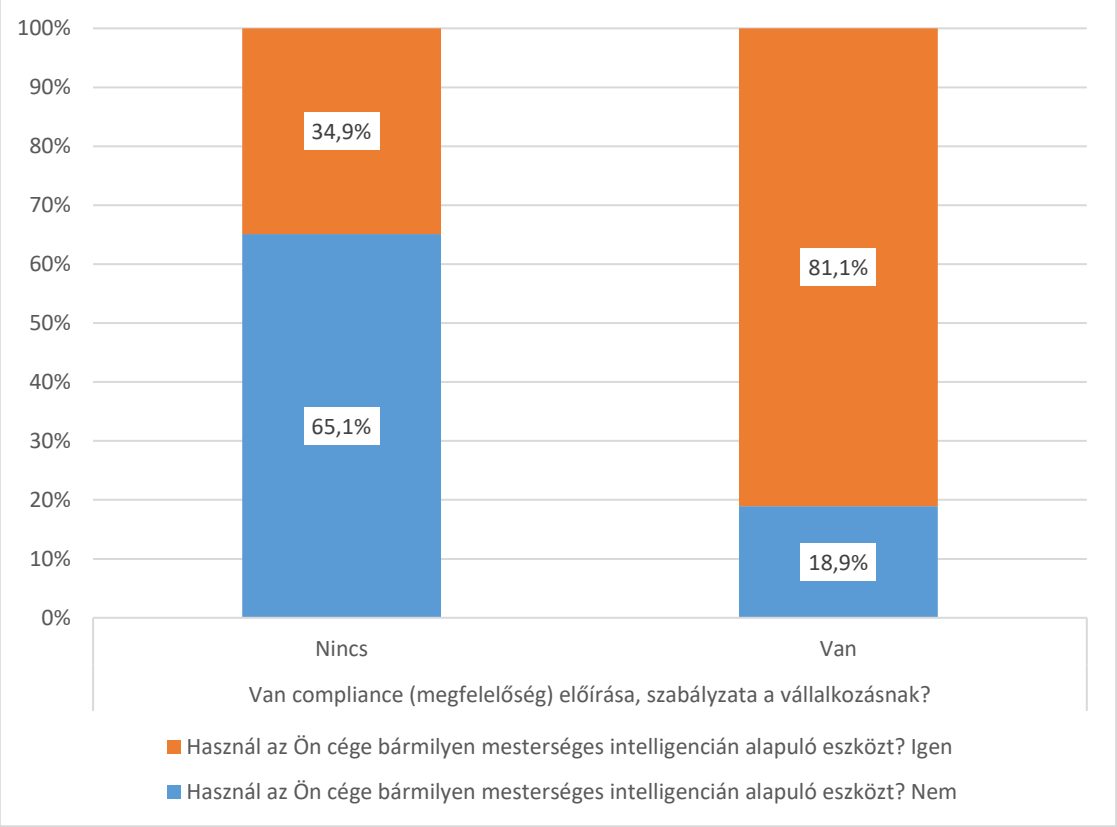
Az eszközhasználat és a megfelelőség biztosítása tényének együttesét kereszttábla-elemzéssel vizsgáltam. A K10 és K33 változóból létrehozott kereszttábla a 12. táblázat.

Táblázat 12: Az eszközhasználat és a megfelelőség biztosításának összefüggése kereszttábla-elemzéssel (Saját szerkesztés)

		K10: Használ az Ön cége bármilyen mesterséges intelligencián alapuló eszközt?		Összesen
		Nem	Igen	
K33: Van compliance (megfelelőség) előírása, szabályzata a vállalkozásnak?	Nincs	56	30	86
	Van	7	30	37
Összesen		63	60	123

A végrehajtott khí-négyzet próba igazolta az eszközhasználat ténye és a megfelelőség biztosításának ténye közötti összefüggést (chi2=22,098, df=1, p<,001). A kapcsolat a Cramer V együttható alapján közepes erősségű (V=0,424, p<,001).

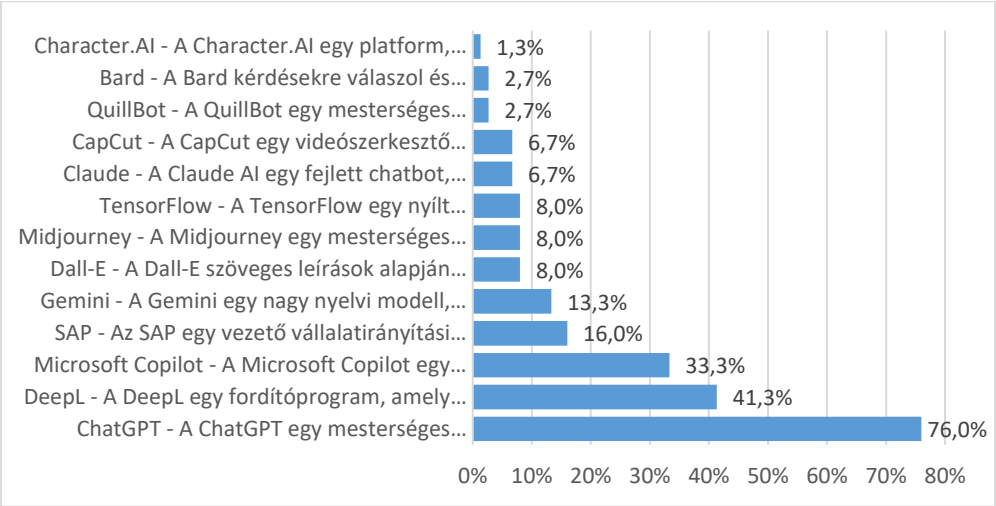
Az alábbi, 17. ábra mutatja be, hogy azon cégek között, amelyek nem biztosítják a megfelelőséget, alacsonyabb a mesterséges intelligencián alapuló eszközhasználat aránya (34,9%), míg a megfelelőséget biztosítók között jelentősen magasabb ez az arány (81,1%).



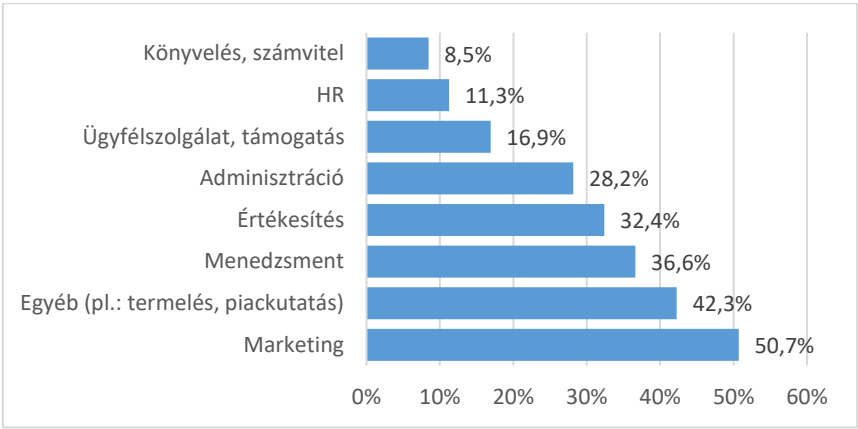
Ábra 17: A mesterséges intelligencia eszközhasználat és a compliance szabályzat összefüggései (N=123) (Saját szerkesztés)

Megállapítható tehát, hogy a mesterséges intelligencia eszközhasználat szignifikánsan együtt jár a megfelelőség biztosításával, tehát azoknak a vállalkozásoknak, amelyek használnak MI eszközt nagyobb valószínűséggel van compliance előírása, mint azoknak, amelyek nem használnak MI-t [128].

A következőkben a mesterséges intelligencia eszközt használó cégek körében vizsgáltam meg a használt eszközök megoszlását (K11) (18. ábra), valamint az alkalmazás területeit (K12) (19. ábra). Valamilyen mesterséges intelligencián alapuló eszközt a válaszadók több, mint fele használ: legnépszerűbbek a ChatGPT, a DeepL és a Microsoft Copilot. A szervezet működése során a mesterséges intelligencián alapuló eszközök alkalmazásának preferált területei: a marketing, a termelés, a piackuatatás és a menedzsment.

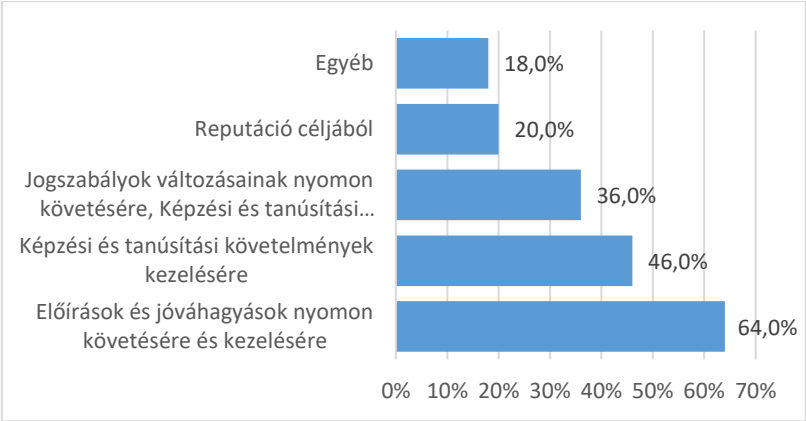


Ábra 18: A mesterséges intelligencia alapú eszközök használati megoszlása (N=75) (Saját szerkesztés)



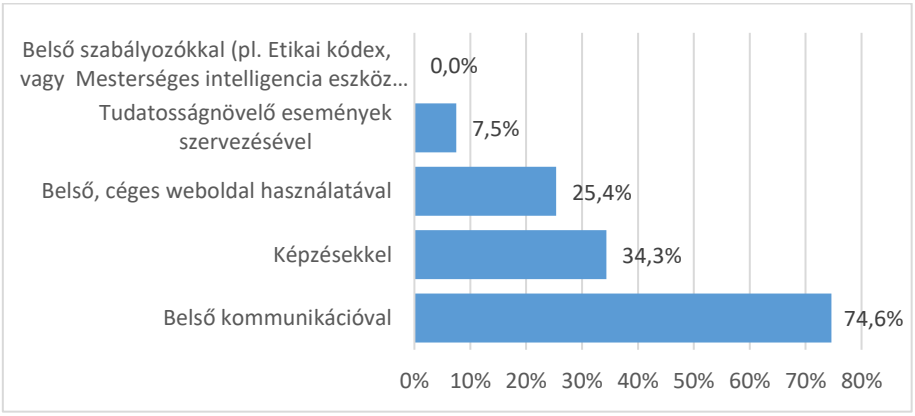
Ábra 19: A mesterséges intelligencia eszközök használatának területei megoszlása (N=75) (Saját szerkesztés)

Azon cégek körében, amelyek biztosítják a megfelelőséget azt is megvizsgáltam, hogy miként alkalmazzák a megfelelőségi (compliance) szabályokat (K35) (19. ábra), valamint a tájékoztatás módjait (K36) (20. ábra). Egyértelműen kiderült a válaszokból, hogy leginkább a szervezeti munkafolyamatok monitorozására használják a compliance szabályokat:



Ábra 20: A compliance szabályok használati területei (N=50) (Saját szerkesztés)

A tájékoztatás módjai közül a belső kommunikáció magasan a leggyakoribb volt, de kiemelték a képzéseket és a weboldal használatát is, melyet a 21. ábra mutat be.



Ábra 21: A compliance tájékoztatási módok (N=67) (Saját szerkesztés)

Végül a mesterséges intelligencia eszközt alkalmazó és a megfelelőséget is biztosító (N=37) cégek körében az eszközhasználat kiterjedtségének és a megfelelőség hangsúlyosságának együttjárását korrelációelemzéssel vizsgáltam. A K12_K változó (0 értékeinek eltávolítása) és a K34 változó korrelációelemzése a Spearman-féle rangkorrelációs együtthatóval és annak szignifikancia tesztelésével történt. Az eredmények azt mutatják, hogy bár a mintában pozitív együttjárás figyelhető meg (rhó=0,318) az eszközhasználat kiterjedtsége és a megfelelőség hangsúlyossága között, addig az összefüggés nem szignifikáns (p=0,059). Tehát az eszközhasználat kiterjedtségének és a megfelelőség hangsúlyosságának együttjárása nem igazolható, vagyis a mesterséges intelligencia eszközök alkalmazási területeinek száma nem befolyásolja a compliance (megfelelőség) szabályrendszer felülvizsgálati gyakoriságát.

Összegzés

Az eredmények alapján megállapítható, hogy az MI-eszközök alkalmazása és a megfelelőségi szabályozás megléte között szignifikáns, közepes erősségű kapcsolat áll fenn. Azok a vállalkozások, amelyek mesterséges intelligencián alapuló eszközöket használnak, nagyobb

valószínűséggel rendelkeznek formalizált compliance szabályzattal, mint azok, amelyek nem alkalmaznak ilyen technológiákat. Az MI-eszközhasználat a vizsgált mintában elsősorban a marketing, a menedzsment, az adminisztráció és az ügyféltámogatás területén jelenik meg, ami arra utal, hogy a technológia integrációja jelenleg főként támogató és operatív funkciókhoz kötődik. A leggyakrabban alkalmazott eszközök szintén azt jelzik, hogy a vállalatok elsősorban általános, széles körben elérhető MI-megoldásokat használnak. A compliance rendszerekkel rendelkező szervezetek esetében a megfelelőségi szabályok alkalmazása leginkább a szervezeti működés és folyamatok monitorozására irányul, ami a kontrollfunkció hangsúlyosságát mutatja. A compliance mechanizmusok kommunikációja elsősorban belső kommunikációs csatornákon, képzéseken és szervezeti szabályozókon keresztül valósul meg, ami a tudatosság és a szervezeti beágyazottság fontosságát emeli ki.

Ugyanakkor a részletesebb elemzés rámutat arra is, hogy az MI-eszközhasználat kiterjedtsége és a compliance hangsúlyossága között nem áll fenn statisztikailag szignifikáns kapcsolat. Bár gyenge pozitív együttjárás megfigyelhető, az eredmények alapján nem igazolható, hogy az MI alkalmazási területeinek bővülése automatikusan együtt járna a megfelelőségi rendszerek intenzívebb működtetésével vagy gyakoribb felülvizsgálatával. Az eredmények arra utalnak, hogy a mesterséges intelligencia alkalmazása és a compliance rendszerek jelenléte között létezik kapcsolat, azonban ez elsősorban a megfelelőség meglétének szintjén ragadható meg.

3.4 A H3 hipotézis kérdőíves vizsgálata – a compliance és a biztonságtudat

Feltételezem, hogy a mesterséges intelligencia alkalmazása során a compliance nemcsak a biztonságtudatot növeli, hanem hozzájárul a kapcsolódó kockázatok azonosításához és kezeléséhez is.

A feltételezés vizsgálata során a mesterséges intelligencia eszközhasználat, valamint a megfelelőség biztosítása a cégekre, míg a mesterséges intelligencia előnyeinek, kockázatainak érzékelése és a biztonságosság/bizonytalanság érzése a válaszadókra mint elemzési egységekre vonatkozik.

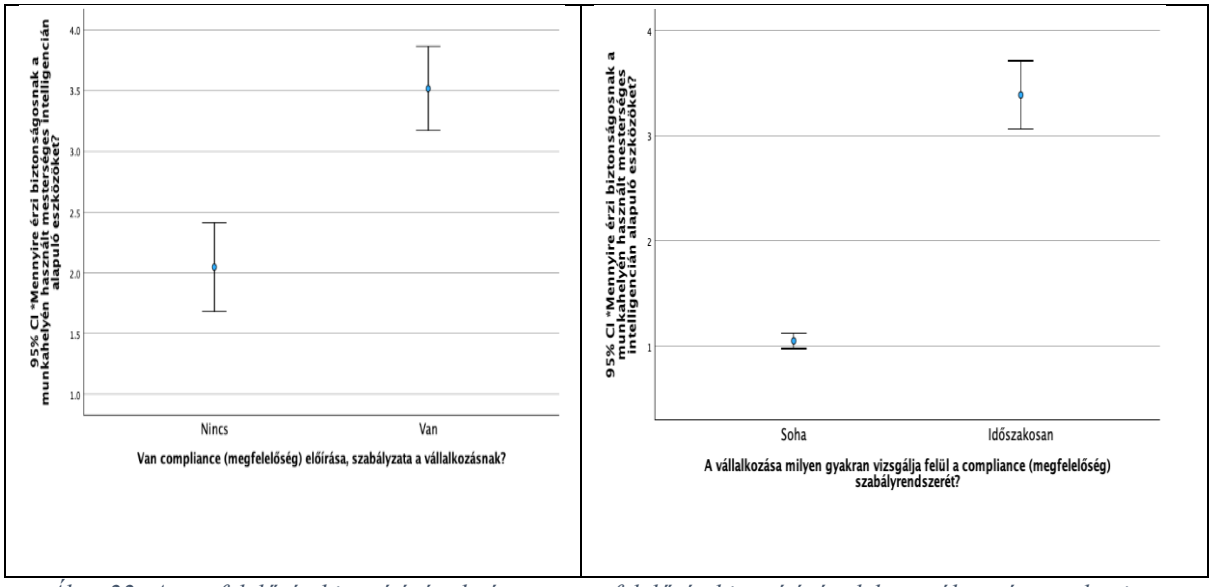
A mesterséges intelligencia eszközök használata kapcsán a megfelelőség biztosításának tényét (K33) és a megfelelőség biztosításának hangsúlyosságát (K34), valamint a biztonságtudat (K30) összefüggését Spearman-féle rangkorrelációs együtthatóval (rhó) és szignifikancia tesztelésével vizsgáltam. Az eredményeket mutatja be a 13. táblázat. Mind a megfelelőség biztosításának ténye (rhó=,482; p<,001) és megfelelőség biztosításának

hangsúlyossága (rhó=,902; p<,001) szignifikáns pozitív hatással van a dolgozók biztonságtudatára.

Táblázat 13: Összefüggések a biztonságtudat és a megfelelőség biztosításának ténye, valamint a megfelelőség biztosításának hangsúlyossága között (Spearman-rhó) (Saját szerkesztés)

		K30: *Mennyire érzi biztonságosnak a munkahelyén használt mesterséges intelligencián alapuló eszközöket?
K30: *Mennyire érzi biztonságosnak a munkahelyén használt mesterséges intelligencián alapuló eszközöket?	Spearman-rhó	1,000
	Sig.	.
	N	99
K33: Van compliance (megfelelőség) előírása, szabályzata a vállalkozásnak?	Spearman-rhó	,482**
	Sig.	<,001
	N	92
K34: A vállalkozása milyen gyakran vizsgálja felül a compliance (megfelelőség) szabályrendszerét?	Spearman-rhó	,932**
	Sig.	<,001
	N	70

Megállapítható, hogy a compliance (megfelelőség) előírás-szabályzat biztosításával és annak rendszeres felülvizsgálatával növelhető a dolgozók biztonságtudata (22. ábra).



Ábra 22: A megfelelőség biztosításának ténye, a megfelelőség biztosításának hangsúlyossága, valamint a biztonságtudat összefüggései (átlag és 95% CI) (Saját szerkesztés)

Végül azt vizsgáltam, hogy a cégek képesek-e befolyásolni a dolgozók biztonságtudatát informatikai biztonsággal kapcsolatos tréningekkel. Annak érdekében, hogy az előbb kimutatott – megfelelőség biztosításának ténye és a megfelelőség biztosításának hangsúlyossága – hatásokat kiszűrve tudjam mérni a tréningek hatását, lineáris regressziós modellt építettem, melyben a biztonságtudat (K30) mint függő változó szerepel, a tréningek gyakorisága, hasznossága, valamint a megfelelőség biztosításának ténye és a megfelelőség biztosításának hangsúlyossága pedig dichotóm (dummy) változóként. A dummy változók

kialakítása a megfelelő eredeti változókból történt, kategória-összevonással. A regressziós modellben alkalmazott dummy változók a következők voltak:

- K31_2: „Évente hányszor tartanak a munkahelyén informatikai biztonsággal kapcsolatos tréninget, avagy bármilyen ebbe a témakörbe tartozó oktatást?" (0: nem tartanak / 1: tartanak.)
- K32_2: „Ezek az oktatások mennyire aktuálisak, hasznosak?" (0: inkább nem hasznos / 1: inkább hasznos). A vágópontot a minta átlagaként határoztam meg. A medián egyenlő hárommal (Me=3). Az 1-es és 2-es válaszlehetőség az „inkább nem hasznos" kategóriába, míg a 3., 4., 5. válaszok a „legalább semleges, vagy inkább hasznos" kategóriába került.
- K34_2: „A vállalkozása milyen gyakran vizsgálja felül a compliance (megfelelőség) szabályrendszerét?" (0: soha. / 1: időszakosan.)
- A K33: „Van compliance (megfelelőség) előírása, szabályzata a vállalkozásnak?" Változó eredetileg eltérő dummy kódolású volt, így annak átkódolására nem volt szükség. (0: nincs. / 1: van.)

Két modell került tehát felépítésre, mivel a K33 és K34_2 együttjárása meglehetősen erősnek bizonyult (VIF_{K33}=5,878, VIF_{K34_2}=8,824), ez bizonytalanná tehette volna a paraméterbecsléseket. A K33 és K34_2 változókat ezért külön modellekben szerepeltettem.

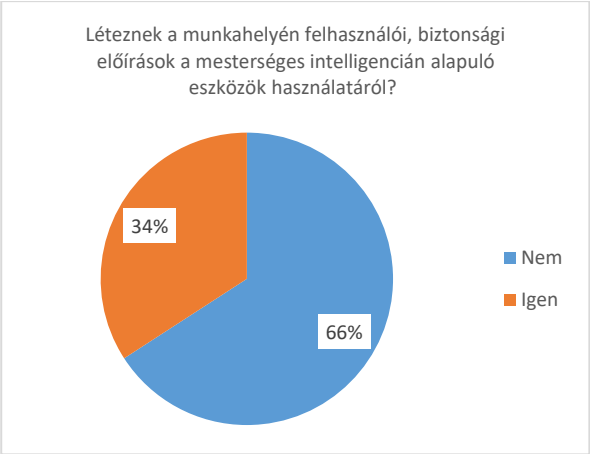
A regressziók eredményeit bemutató 14. táblázatból látszik, hogy a dolgozók biztonságtudatára a megfelelőség biztosításának ténye és a megfelelőség biztosításának hangsúlyossága mellett szignifikáns hatással van a tréningek hasznossága is, ennek ellenére a tréningek gyakorisága mégsem bizonyult szignifikáns prediktornak. A dolgozók biztonságtudatát a cég befolyásolni képes compliance (megfelelőség) előírás-szabályzat által, annak időszakos felülvizsgálatával, valamint olyan tréningek-oktatások biztosításával, amelyek aktuálisak, hasznosak a munkavállalók számára. Ezek közül a legerősebb prediktor a standardizált béták alapján az oktatások hasznossága, azonban nem befolyásoló tényező a tréningek gyakorisága.

Táblázat 14: A biztonságtudat összefüggése a tréningek gyakoriságával, hasznosságával, valamint a megfelelőség biztosításának tényével és a megfelelőség biztosításának hangsúlyosságával (lineáris regresszió) (Saját szerkesztés)

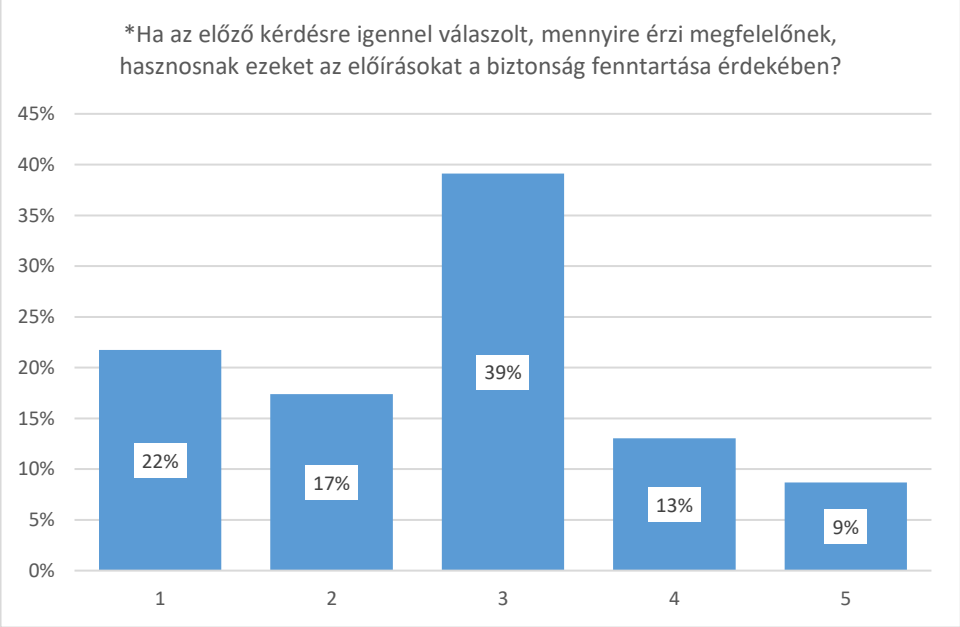
Modell		**Standardizálatlan Együtthatók**		**Standardizált Együtthatók**	**t**	**Sig.**
		B	**Std. Hiba**	**Béta**		
1	(Constans)	1,276	,151		8,464	<,001
	K33: Van compliance (megfelelőség) előírása, szabályzata a vállalkozásnak?	,721	,289	,236	2,491	,015
	K31_2: Évente hányszor tartanak a munkahelyén informatikai biztonsággal kapcsolatos tréninget, avagy bármilyen ebbe a témakörbe tartozó oktatást?	,039	,261	,012	,148	,883
	K32_2: *Ezek az oktatások mennyire aktuálisak, hasznosak?	1,715	,262	,599	6,545	<,001
2	(Constant)	1,054	,110		9,591	<,001
	K34_2: A vállalkozása milyen gyakran vizsgálja felül a compliance (megfelelőség) szabályrendszerét?	,415	,097	,406	4,274	<,001
	K31_2: Évente hányszor tartanak a munkahelyén informatikai biztonsággal kapcsolatos tréninget, avagy bármilyen ebbe a témakörbe tartozó oktatást?	,202	,201	,072	1,004	,319
	K32_2: *Ezek az oktatások mennyire aktuálisak, hasznosak?	1,279	,252	,484	5,072	<,001
Függő Változó: K30: *Mennyire érzi biztonságosnak a munkahelyén használt mesterséges intelligencián alapuló eszközöket?						

A biztonságtudat további vizsgálatához az alábbi kérdésekre adott válaszokat elemeztem:

- K28: „Léteznek a munkahelyén felhasználói, biztonsági előírások a mesterséges intelligencián alapuló eszközök használatáról?” (0: nem. / 1: igen.) A 23. ábra szerint.
- K29*: „Ha az előző kérdésre igennel válaszolt, mennyire érzi megfelelőnek, hasznosnak ezeket az előírásokat a biztonság fenntartása érdekében?” (1: Egyáltalán nem érzem biztonságosnak. / […] 5: Teljesen biztonságosnak érzem.) A 24. ábra szerint.



Ábra 23: A mesterséges intelligencia eszközhasználathoz tartozó felhasználói, biztonsági előírások rendelkezésre állása (N=41) (Saját szerkesztés)



Ábra 24: A mesterséges intelligencia eszközhasználathoz tartozó felhasználói, biztonsági előírások megfelelősége (N=23) (Saját szerkesztés)

Összegzés

Az alfejezet eredményei alapján megállapítható, hogy az MI-eszközök alkalmazása és a megfelelőségi szabályozás megléte között szignifikáns, közepes erősségű kapcsolat áll fenn. Ez arra utal, hogy a mesterséges intelligenciát alkalmazó szervezetek nagyobb valószínűséggel rendelkeznek formalizált compliance keretrendszerrel, amely képes kezelni az új típusú kockázatokat és szabályozási kihívásokat.

Az elemzés ugyanakkor rámutat arra is, hogy az MI-eszközhasználat és a compliance közötti kapcsolat differenciált módon értelmezhető. Míg a compliance jelenléte és az MI alkalmazása

között szorosabb összefüggés mutatható ki, addig az eszközhasználat kiterjedtsége és a megfelelőségi rendszerek működési intenzitása között nem azonosítható statisztikailag szignifikáns kapcsolat. Ez arra enged következtetni, hogy a mesterséges intelligencia integrációja önmagában nem eredményezi a compliance rendszerek mélyebb intézményesülését vagy fejlettebb működését.

A vizsgálat további fontos eredménye, hogy az MI alkalmazása elsősorban operatív és támogató funkciókhoz kapcsolódik, különösen a marketing, a menedzsment és az adminisztratív folyamatok területén. Ezzel párhuzamosan a compliance funkciók dominánsan a szervezeti működés monitorozására és a szabályozási megfelelés biztosítására irányulnak, ami a kontrolljelleg fennmaradását jelzi. A compliance mechanizmusok kommunikációja elsősorban belső csatornákon keresztül történik, ami a szervezeti tudatosság és a belső beágyazottság jelentőségét hangsúlyozza.

Az interjúk alapján megállapítható, hogy a mesterséges intelligencia és a compliance rendszerek kapcsolata nem lineáris, hanem többszintű és kontextusfüggő. A compliance jelenléte inkább előfeltétele vagy kísérőjelensége az MI alkalmazásának, mintsem annak közvetlen következménye. Ez a megállapítás alátámasztja azt a tágabb elméleti értelmezést is, miszerint a compliance a digitális transzformáció kontextusában egyre inkább adaptív, kockázatérzékeny és technológiai szempontok által formált működési keretként jelenik meg. A kutatás rámutat a technológiai innováció és a megfelelőségi rendszerek közötti kapcsolat strukturális sajátosságaira, ugyanakkor további vizsgálatok szükségességét is jelzi a kapcsolat oksági és fejlődési dinamikájának mélyebb feltárása érdekében.

3.5 Kérdőív – Összefoglalás

A kérdőívre adott válaszok elemzése alátámasztja a feltételezéseket hipotéziseket, ugyanakkor rámutat arra is, hogy a két terület integrációja a hazai vállalkozások körében még kialakulóban lévő jelenség. A válaszok alapján a compliance és a mesterséges intelligencia értelmezése ambivalens képet mutat: a pozitív és negatív megítélések közel azonos arányban jelennek meg. A leggyakoribb asszociációk a biztonság, a kockázatkezelés, a szabályozás, a felelősség és az adatok köré szerveződnek, ami arra utal, hogy a compliance funkcióját a válaszadók elsősorban biztonsági és kockázatkezelési dimenzióban értelmezik. Kiemelendő, hogy a biztonság mint központi kategória meghatározó szerepet tölt be.

A vizsgálat eredményei továbbá azt mutatják, hogy a mesterséges intelligencia eszközhasználata és a compliance rendszerek jelenléte között szignifikáns kapcsolat áll fenn. Az MI-t alkalmazó vállalkozások nagyobb valószínűséggel rendelkeznek formalizált

megfelelőségi szabályozással, ami arra utal, hogy a technológiai innováció és a szabályozási tudatosság bizonyos mértékig együtt jár. Ugyanakkor az eszközhasználat kiterjedtsége és a compliance működés intenzitása között nem mutatható ki egyértelmű összefüggés, ami azt jelzi, hogy a technológiai alkalmazás mélysége nem feltétlenül eredményezi a megfelelőségi rendszerek fejlettebb működését.

A mesterséges intelligencia alkalmazása a gyakorlatban jelenleg elsősorban támogató jellegű funkciókhoz kapcsolódik, különösen a marketing, a menedzsment, az adminisztráció és a piackutatás területén. Ezzel párhuzamosan a compliance szabályok használata leginkább a szervezeti folyamatok monitorozására és a képzési, illetve tanúsítási követelmények kezelésére irányul. A megfelelőségi mechanizmusok kommunikációja döntően belső kommunikációs csatornákon és képzéseken keresztül valósul meg, ami a szervezeti tudatosság fejlesztésének kiemelt szerepére utal.

Az eredmények alapján megállapítható, hogy a mesterséges intelligencia eszközök használata kapcsán a megfelelőség biztosításának ténye és hangsúlyossága összefügg a biztonságtudattal. A megfelelőségi szabályzatok megléte és azok rendszeres felülvizsgálata hozzájárul a szervezeti szintű biztonsági szemlélet erősítéséhez, ami a digitális környezetben egyre nagyobb jelentőséggel bír.

A hazai eredmények összhangban állnak a nemzetközi kutatások megállapításaival, amelyek szerint Magyarország a mesterséges intelligencia alkalmazása terén az EU-n belül inkább a felzárkózó országok közé sorolható [129]; [130]. Ugyanakkor a vizsgálat azt is jelzi, hogy a compliance és az MI fokozatosan teret nyer a vállalati gyakorlatban, még ha alkalmazásuk jelenleg számos bizonytalansággal is terhelt. Ezt a tendenciát az Európai Bizottság vonatkozó jelentései is megerősítik, külön kiemelve a további fejlesztési irányok szükségességét [131].

A kérdőív kutatás eredményei arra utalnak, hogy a compliance és a mesterséges intelligencia integrációja egy dinamikusan fejlődő, de még nem teljesen kiforrott terület, amelyben a biztonság, a tudatosság és a szabályozási keretek erősítése kulcsszerepet játszik. A jövőbeni fejlődés szempontjából kiemelt jelentőségű az információmegosztás, a szervezeti szintű tudatosítás, valamint a gyakorlati útmutatók és képzési rendszerek kialakítása, amelyek képesek támogatni a technológiai és megfelelőségi szempontok összehangolt érvényesülését.

3.6 Az interjú, mint kutatási módszer

Az interjúkat szintén az elméleti vizsgálatok eredményeinek értelmezése és a gyakorlatban való leképezése céljából készítettem. Először a kutatási módszert ismertetem, majd az egyes feltételezéseket vizsgálom.

A kutatás során 10 strukturált szakértői interjú készült 15 kérdés mentén, körülbelül 60–80 perc időtartamban. A kérdések sorrendje kötött volt, és az interjúvázlatban lévő kérdések jelentős részére kötelezően választ vártam. Az interjúkat Microsoft Teams vagy telefonos hangrögzítés funkcióval rögzítettem, majd Microsoft Wordbe ültettem át a tartalmat, és így végeztem el az elemzést.

Az életkor szempontjából az interjúalanyok fele 40–50 év, 3 fő 30–40 év és 2 fő 50–60 év közötti volt. A nemek megoszlása szerint 9 férfi és 1 nő vett részt a kutatásban. Mindenki felsőfokú végzettséggel rendelkezik, és szakterületükön vezető pozíciót töltenek vagy töltöttek be. A képviselt szervezetek fő tevékenységi területei a pénzügy, a biztonság, az informatika, az egészségügy, a jog, az oktatás és a kutatás.

3.7 A H1 hipotézis interjús vizsgálata – a compliance fogalom

Az interjúk kvalitatív feldolgozása során világossá vált, hogy a compliance fogalmának értelmezése a mesterséges intelligencia megjelenésével új keretbe helyeződik. A megkérdezettek válaszaiban egyaránt megjelentek a jogi és etikai kihívások, a kockázatkezelési és felelősségi kérdések, valamint a compliance definíciójára vonatkozó új értelmezések.

Az interjúk alapján érzékelhető volt – ami az első feltételezést egyrészt tágabb kontextusba helyezte, másrészt alá is támasztotta –, hogy mind a compliance, mind a jogrendszer és ezáltal a nagyobb társadalmi környezet, amelyben a vállalkozások a működésüket végzik, egy gyökeres változás folyamatában van [132]. Ez a változás anómikus [133] helyzetbe ágyazódik be: az anómia olyan átmeneti helyzet, amikor valamilyen gyors változás következtében a társadalmat szabályozó korábbi normák, szabályok az érvényüket veszítik, de még nem alakult ennek a helyére új szociális norma, ezért a társadalom időlegesen elveszíti szabályozó mechanizmusait. Az anómia tehát egy olyan állapot, amikor a társadalom szereplőinek viselkedését nem szabályozzák megfelelő normák, keretek. A rend akkor áll vissza, amikor az új helyzet kezelésére kialakulnak és stabilizálódnak az új legitim szabályok [134]. Erre a bizonytalan helyzetre szemléletesen mutattak rá az interjúalanyoknak a munkakörülményekkel, általában a társadalom és a gazdaság kihívásaival összefüggésben adott válaszaik. Az álláspontom szerint a jogi, illetve a strukturális kérdésekre, valamint a mesterséges intelligencia megjelenésével kapcsolatos aggályokra megoldást adhat a compliance, mint kockázatcsökkentő tényező. A jogi és strukturális kihívások, valamint a mesterséges intelligencia alkalmazásával kapcsolatos etikai és szabályozási aggályok kezelése olyan komplex megoldásokat igényelnek, amelyek a szervezeti működés jogszerűségét, biztonságát és fenntarthatóságát egyaránt biztosítják. Az interjú alapú empirikus vizsgálat eredményei arra utalnak, hogy a compliance

keretrendszer bevezetése és működtetése releváns válaszként értelmezhető, mivel kockázatcsökkentő tényezőként hozzájárul a szabályozási megfelelés előmozdításához, a szervezeti biztonság növeléséhez, valamint az átlátható működés fenntartásához.

A compliance és a mesterséges intelligencia gyakorlati értelmezése

Az interjúalanyok egyöntetűen hangsúlyozták, hogy mind a compliance, mind a mesterséges intelligencia a gyakorlatban „új fogalomként" van jelen életükben, amelyet még nem sikerült a hagyományos szabályozási eszköztárral megragadni. Az interjúalanyok tisztában vannak a mesterséges intelligencia alkalmazásából fakadó biztonsági kockázatokkal, azonban a hatékonyságnövelés és az innovációs lehetőségek miatt továbbra is ellenőrizetlenül alkalmazzák ezeket a technológiákat. A digitális fejlődés gyorsasága és a jogi-szabályozási környezet lassú reakcióideje közötti aszinkronitás kifejezetten jelent volt válaszaikban.

Az interjúalanyok megerősítették, hogy a gyakorlatban is érzékelik az etikai elvárások egyre nyomasztóbb szükségességét. Bár a gyorsan változó társadalmi környezet miatt szükség van ezekre az új technológiákra, mégsem képesek releváns választ adni azok gyakorlati alkalmazására az eddig használatos fogalmi keretek között, tehát érzékelik, hogy a korábbi gyakorlattól eltérő megközelítést igényel a probléma (7. interjú).

A digitális technológiára szükség van; hasznosságát nem is kérdőjelezték meg, ugyanakkor az újdonsága miatt nincsenek sem bevett gyakorlatok, sem jogszabályi kapaszkodók, annak ellenére sem, hogy a mesterséges intelligencia szabályozás európai uniós szinten elérhető (lásd első fejezet). A hétköznapokban a compliance-t nem tudják a gyakorlatban alkalmazni. (6. interjú).

Az élet minden területén jelen lévő mesterséges intelligencia és a különböző algoritmusok a jogi szabályozásnál nagyobb hatással befolyásolják és határozzák meg az életet. (7. interjú).

A megkérdezettek hangsúlyozták, hogy azért van nehéz helyzetben az, aki érvényre akarja juttatni a compliance-t, mert a mesterséges intelligencia leginkább a háttérbe húzódva, illetve rendszerekbe beépülve végzi a munkát (7. interjú). Egyes vélemények szerint az etikai elvek jövője is kérdéses, mert a technológia alkalmazásával kapcsolatban is szükség van új erkölcsi normákra (6. interjú). Az interjúk alapján egyértelmű, hogy számtalan megválaszolatlan társadalmi-etikai-jogi kérdés merül fel a mesterséges intelligencia előretörésével párhuzamosan. Tehát érezhető a bizonytalanságérzet, ami miatt az adatközlők többsége nyitott a biztonsági megoldások irányába.

A mesterséges intelligencia megjelenése kihívásokat teremtő helyzetet alakított ki: az interjúk során megállapításra került, hogy egy olyan változásnak vagyunk a részesei, amiben a társadalmat alakító szabályozó rendszer nem mindig alkalmas arra, hogy a változásra

rugalmasan reagáljon. A jogszabályok tehát nem tudják lekövetni a változást, megelőzni a változásból eredő problémákat. Mintha annak a jognak, amit eddig ismertünk a lehetőségei ezen a ponton bezárulnának, a biztonságra azonban szükség van, és kellenek a stabilitást nyújtó keretek is. Ebben nyújthat támpontot a compliance alkalmazása, ami a biztonságérzetet is megerősítheti.

Kockázatok és felelősségi dilemmák

Az interjúalanyok ambivalens viszonyban vannak a mesterséges intelligenciával: egyszerre tekintették lehetőségnek és kockázatnak is. Az innováció, a munkaerő-kiváltás és a gyorsaság a lehetőségek oldalán jelentek meg, ugyanakkor az átláthatóság, a felelősség és a megbízhatóság hiánya a kockázati dimenziókat erősítették. A kockázat érzete szinte minden interjúban hangsúlyosan jelent meg. Több interjúalany szerint a mesterséges intelligencia „*fekete dobozként*" működik, amelynek algoritmikus logikája átláthatatlan, így a kiberbiztonsági és integritási problémák kezelése nehézkes.

A mesterséges intelligencia alkalmazásával szemben egységesen az egyik kiemelt aggály, hogy az interjúalanyok többsége pillanatnyilag nagyobb volumenű problémának tartja a használatával járó kockázatokat, mint az azzal járó előnyöket. Tehát jobban félnek tőle, minthogy az előnyeire fókuszálnának. A félelmek gyökere, hogy megszűnik a vertikális bizalom, vagyis a joggyakorlatba vetett bizalom a digitális tér esetében jelentős mértékben csökken. A szereplők bizonytalanságérzete azért is adekvát, mert a vertikális bizalomhiány mellett úgy érzik, hogy egyelőre nem bízhatnak a digitális kihívások megoldására létrehozott társadalmi intézményekben sem, hiszen azok még újak, és kevés a gyakorlati tapasztalatuk, a változás egyre gyorsabb, amivel alig tudnak lépést tartani. A kockázatok hangsúlyozása azért is van jelen a válaszokban, így a piaci környezetben, mert az emberek tudatosítása, edukációja is gyerekcipőben jár. A jelenlegi felhasználói környezetben és a jelenlegi biztonságtechnikai fejlettségi szint mellett a mesterséges intelligencia sokkal inkább kockázat, mint lehetőség, tehát ezzel még nem tudnak élni, vagy nem ott tartanak még a használat tekintetében, hogy kiaknázhatnák annak összes lehetőségét (2., 3., 10. interjú).

A felelősség kérdéskörét is említették az interjúalanyok. Egyesek szerint a felelősség a legmegfoghatatlanabb elem a digitális tértől befolyásolt közegben. Lényegesnek tartják azt tisztázni, hogy a felelősség kit terhel (8., 9. interjú).

A jogi szabályozás diszfunkciója miatt nem átlátható a mesterséges intelligencia kapcsán az azt alkalmazó személyek felelőssége sem. A hagyományos értelemben vett jogi szabályozás – ami tények, szabályok alapján dönt egyes helyzetekben – ez esetben nem alkalmazható, mert a fennálló helyzet nem írható le a hagyományos jogi fogalmakkal.

Bizonytalanság és bizalomhiány

Az interjúkban visszatérő motívum a bizonytalanságérzet és a vertikális bizalom megingása. Az interjúalanyok többsége szerint a jogba vetett bizalom jelentősen csökken, mivel a jogrendszer lassúsága és diszfunkciói miatt nem képes kezelni a mesterséges intelligencia által generált helyzeteket. A társadalmi intézményekbe vetett bizalom hiánya tovább erősíti ezt a bizonytalanságot. Ennek következtében a résztvevők fokozott nyitottságot mutatnak a compliance alapú biztonsági megoldások iránt.

Compliance mint lehetséges megoldás – fogalom

Az interjúk alapján a compliance a résztvevők szemében nem pusztán jogi kategóriaként, hanem holisztikus, multidiszciplináris megközelítésként értelmeződik. A jogi anomáliák megoldására a klasszikus szankcionálási eszközök diszfunkcionálisak, nem biztosítják a hatékonyságot. Mindezek miatt a compliance-nek egészen új problémakezelési eszközökhöz kell nyúlnia. A compliance szerepe sokkal nagyobb a kockázatok bekövetkezésének minimalizálásában és a biztonság növelésében. Vagyis az interjúalanyok alapvetően nem jogi, hanem valamilyen strukturális, szervezeti, folyamat szintű megoldást vázolnak fel.

A definíciós kísérletekben rendre előkerültek a kockázatkezelés, a biztonság, az auditfunkciók és az etikai működés elemei. Egyes interjúalanyok szerint a compliance olyan keretrendszer, amely képes strukturálni és standardizálni a szervezeti folyamatokat, valamint ajánlásokat nyújt a diszfunkciók kezelésére (1. interjú). Mások inkább filozófiaként, szemléletmódként tekintenek rá, amely a stratégiai tervezést is segíti

A megkérdezettek számára a compliance elsősorban auditfolyamatként értelmeződik. E folyamat kiindulópontját a vállalkozás céljainak, funkcióinak és feladatainak feltárása képezi, kiegészülve a felhasználói elégedettség, valamint a munkavállalói jólét szerepének vizsgálatával. A compliance audit feladata ezen tényezők rendszerezése és standardizált gyakorlatokba való integrálása. Az audit során a compliance nem csupán azonosítja az esetleges anomáliákat, diszfunkciókat vagy hibákat, hanem azok tudásdeficitre visszavezethető okait is feltárja. Ennek eredményeképpen a compliance képes rámutatni a szervezeti működés azon pontjaira, ahol változtatás szükséges, továbbá ajánlásrendszert biztosít arra vonatkozóan, hogy a folyamatok milyen módosításai járulhatnak hozzá a hatékonyabb és biztonságosabb működéshez (1. interjú). A compliance egy lehetőség, ami a környezeti kockázatot azonosítja, és a mesterséges intelligencia használatában rejlő kockázatokat is csökkenti (2., 3., 4. interjú). A compliance egy szabályozás, amit egy megfelelőségi rendszerként azonosított az 5. interjú alanya. Hangsúlyozta, hogy a compliance egy megfelelőségi nyilatkozat, egy deklarátum, ami rögzíti az összes releváns üzleti folyamatot, amely komplexen magában foglalja a szervezeti

háttérfolyamatokat is (döntéshozatal, adatkezelés). Gyakorlatilag iránymutatást tud adni, és keretek között tudja tartani a céges működést. A 6. interjúban a jogszerűség és etikus működés került előtérbe, az adatközlő a szemléletmódot emelte ki a compliance fogalma kapcsán: „*soft skill-ek gyülekezete*" – szólt a meghatározás (6. interjú). A compliance egy összetett fogalom, amely azért szükséges, mert a szabályozás önmagában már kevés. Egy képesség, amely a másokkal való együttműködést jelenti (7., 8. interjú). A megfelelőség egy keretrendszer, több dimenzió mentén történő együttműködés (9. interjú). A szabályok betartása, a korlátok szabása, a korlátozás, a közös értékek megfogalmazása, tiszteletben tartása a compliance lényege a 10. interjú alanya szerint.

Összegzés

Az interjúalanyok egyhangúan kiemelték, hogy a mesterséges intelligencia megjelenésével a jogi kihívások és a kockázatok nőttek. A beszélgetések során visszaköszöntek az elméleti kutatásban leírtak, illetve a kérdőívben adott válaszok a compliance fogalmával kapcsolatban. Egyértelművé vált, hogy a felelősség problémája nehezebben kezelhető, mert nincsen a rendelkezésre álló fogalmak szerint alanya a felelősségre vonásnak és a szankcionálásnak. Az interjúk eredményei rámutattak arra is, hogy a compliance fogalma a mesterséges intelligencia kontextusában nem redukálható a hagyományos jogi-szabályozási megfelelésre. Ehelyett egy dinamikus, kockázatalapú és etikai dimenziókat is integráló fogalomként értelmeződik, amelynek fő funkciója a kockázatok minimalizálása, a biztonság erősítése, valamint a szervezeti működés átláthatóbbá tétele.

Az interjúkészítés eredményei kiegészítik és tovább árnyalják az elméleti, valamint a kérdőíves kutatások alapján kirajzolódó compliance fogalmat.

3.8 A H2 hipotézis interjús vizsgálata – a mesterséges intelligencia eszközhasználat és a compliance megoldások

Feltételezem, hogy a mesterséges intelligencia eszközhasználata összefügg a compliance rendszerek jelenlétével a hazai vállalkozások esetében.

A feltételezés vizsgálatát az alábbi szempontokra építem: a compliance funkcióinak átalakulása a mesterséges intelligencia hatására; a check list alapú megközelítés elégtelensége; a kontroll, a felelősség és az új kompetenciák megjelenése; a proaktív és reaktív compliance feladatok jellege; a compliance és a szervezeti kultúra összefüggése; továbbá a mesterséges intelligencia, mint compliance támogató eszköz.

A compliance funkcióinak átalakulása a mesterséges intelligencia hatására

A compliance több funkciót lát el: kontroll-, támogató- és tanácsadói szerepkörrel egyaránt rendelkezik. Az interjúalanyok szerint a mesterséges intelligencia megjelenésével e funkciók hangsúlyossága átrendeződik. Rövid távon az ellenőrző és tanácsadói funkciók erősítése válik kulcsfontosságúvá, míg az edukatív jellegű szerep akkor kerülhet előtérbe, amikor a felhasználók már megfelelő gyakorlattal rendelkeznek a mesterséges intelligencia alkalmazásában (10. interjú).

A szabályozás kapcsán a legnagyobb dilemmát az jelenti, miként lehet olyan keretrendszert kialakítani, amely egyfelől biztosítja a normák és előírások betartását, másfelől nem okoz versenyhátrányt, és képes megelőzni a reputációs vagy szervezeti károk kialakulását. Az interjúk tanúsága szerint a compliance és a mesterséges intelligencia kapcsolatában jelenleg a megértési fázis dominál: a szervezetek a fogalmi keretek tisztázására, a kockázatok feltárására és a szabályozási lehetőségek feltérképezésére helyezik a hangsúlyt. Ez a hangsúly összefügghet azzal, hogy a biztonságérzet alacsony szintű a mesterséges intelligencia eszközhasználat esetén. (2. interjú). A mesterséges intelligencia eszközök megfelelőség biztosítása során sokkal nagyobb a hangsúly a kockázatok feltárásán, azok szervezetbe építetten történő kezelésén, tekintettel arra, hogy sok esetben nem belátható a potenciális kár mértéke. A kockázatok bekövetkezésének a valószínűségét és/vagy a hatását csökkenti a compliance, kiemelten a mesterséges intelligencia eszközhasználat megjelenésével.

A check list alapú megközelítés elégtelensége

Az interjúk egyik központi témája a compliance hagyományos, check list alapú működésének korlátossága volt. A válaszadók szerint a mesterséges intelligenciához kapcsolódó megfelelőség biztosításához a statikus ellenőrző listák nem elegendőek. Ehelyett dinamikus, kockázati mátrixokra épülő értékelési rendszerek szükségesek, amelyek képesek figyelembe venni a kockázatok bekövetkezési valószínűségét és hatását (3. interjú). A check list ugyan megfelelő kiindulópont lehet jól ismert folyamatok esetében, de a mesterséges intelligencia által generált bizonytalanságok kezeléséhez komplexebb megközelítések szükségesek (10. interjú). Az interjúk megerősítették, hogy egy holisztikus szemlélet szükséges, és nem elegendő a check list központú compliance működés a mesterséges intelligencia támasztotta kihívásokra. Az adatközlők a következő válaszokat fogalmazták meg ezzel kapcsolatban:

„*Ezt már nem lehet check list alapján, ehhez mátrixokat kell fölrántani, és akkor a valamit a valaminek, tehát különböző változóknak, mint egy kockázati mátrix, tehát a valamit a valaminek a függvényében nézek, és akkor annak néznem kell a bekövetkezési valószínűségét is, meg a hatását is, és akkor abból fog következni az én beavatkozásomnak a sürgőssége, meg*

a mélysége. Ezt én ugyanígy gondolom a compliance-ről is, tehát hogy az egyre összetettebb, meg egyre kevésbé belátható, hogy akkor most mit nézek, a folyamatot nézem, az alap, tehát a meghúzódó elvárt dolgot, vagy annak a digitális megjelenését, vagy annak a lefutását." (3. interjú).

A check list statikus ellenőrzésre alkalmas, az alapvizsgálatokra elegendő, azonban a mesterséges intelligencia eszközhasználat kockázatos dolog, ezért önmagában, a teljeskörű kontrollra kevés az ellenőrző lista. A felgyorsult technológiai környezetben dinamikus compliance működtetés szükséges. A hagyományosnak tekintett, évente egyszer végzett szabályzatmódosítás, amiben a változtatások átvezetésre kerültek nem elegendő, nem hatékony. (2 interjú). A check listet egy nagyon jól ismert és nagyon jól körülhatárolt folyamatnál érdemes használni. „*Megfelelő kiindulási alap, ha van egy check list, mert azzal el lehet indulni, azonban ahhoz ragaszkodni olyan folyamat esetén, amit még nem jól ismer az ember, ott nem elegendő.*" (10. interjú). A check list alapú ellenőrzéssel a megfelelést bizonyos szintig lehet csupán ellenőrizni. A mesterséges intelligencia világában a megfelelőség megvalósításához ismerni kell magát a mesterséges intelligencia eszközt és annak működését is.

Kontroll, felelősség és új kompetenciák

Az interjúalanyok kiemelték, hogy a compliance-nek reagálnia kell a mesterséges intelligencia által előidézett változásokra, ugyanakkor megoszlanak a vélemények arról, hogy szükséges-e teljesen új funkciók bevezetése. Egyes nézőpontok szerint elegendő a meglévő compliance eszköztár kiterjesztése a mesterséges intelligenciára, mások viszont új kompetenciák kialakítását sürgetik. Abban egyetértés mutatkozott, hogy a kontrollfunkciót ki kell terjeszteni a mesterséges intelligencia által meghozott döntések magyarázhatóságára, minőségére és a felelősség kérdésére is (2. interjú). Ennek megvalósítása megköveteli a compliance szakemberektől, hogy közelebb kerüljenek a digitális világhoz, megértsék a mesterséges intelligencia működését, és képesek legyenek kockázatainak kezelésére is (10. interjú).

Az interjúk alapján az rajzolódik ki, hogy compliance szakterületnek meg kell érteni, hogy mi az a folyamat, amit szabályoz. Ha a compliance túlszabályoz, és emiatt versenypiaci hátrányt okoz a cégnek, akkor a munkája nem hatékony. Ha a compliance alulszabályoz, és ennek bírság, vagy rossz hangulat, akár negatív reputáció lesz az eredménye, akkor a compliance nem tölti be kontrollszerepét, ezért kell tehát megérteni, hogy a compliance mivel kapcsolatban hoz intézkedéseket. A compliance-nek mindenképpen válaszolnia, reagálnia kell a mesterséges intelligencia megjelenésével és a digitális fejlődéssel együtt járó változásokra. Abban azonban nem minden interjúalany ért egyet, hogy a compliance, mint szakterület új feladatokat, új funkciókat integráljon a működésébe. Azt emelték ki, hogy a compliance-szel foglalkozó

embernek kell megértenie az új helyzetet, és a hagyományos compliance eszközökkel megoldani a mesterséges intelligencia megjelenésével járó problémákat. Tehát nem a rendszer változtatása, hanem egyrészt a mesterséges intelligencia működésének megértése szükséges, másrészt a kontroll és támogató funkciók kell, hogy a középpontba kerüljenek, illetve a funkciók közötti hangsúlyok változnak meg (10. interjú). A compliance-esnek közelebb kell mennie a digitális világhoz, a mesterséges intelligenciához, meg kell értenie, hogy mi a mesterséges intelligencia, és milyen munkajogi, adatvédelmi, etikai, versenyjogi kockázatokat hordoz. „*A compliance-es mindset mindenhol ugyanaz kell legyen, de a termék vagy a produktum, amivel kapcsolatban ő a compliance programot futtatja, az különböző. ... Érteni kell. ..... Csak közel kell menni ehhez is. Ez egy némi idő*.” (10 interjú).

Az egyik interjúalany szerint lényeges lehatárolni a compliance és az egyéb területek határait is: „*... a compliance az legyen compliance. Tehát a megfeleléseknek a gyűjteménye vagy a különböző akár külső, akár belső, akár törvényi előírások. Az egy intakt valami, meg az egy fajta megközelítés. Én ebben nem keverném bele például a kiberbiztonságot, még ha ott is van ugye megfelelési kérdés. Mert az már egy csomószor technológiát is érint, nemcsak szabályozást*” (2. interjú). Tehát koordinálni szükséges a compliance és a többi szakterület együttműködését, ami a menedzsment feladata.

A compliance teljes megújulását azonban nem tartja indokoltnak a 6. interjúalany. „*Én ebből most így nem érzem, hogy a mesterséges intelligencia most kidöntené a compliance dogmatikát a helyéről. Hanem inkább úgy képzelném el, hogy a mesterséges intelligencia mondjuk az olyan, mint amikor van egy szoba, aminek tiszta a levegője, és akkor valahonnan belefújunk egy vanília illatot, és akkor ugye az egész illat szétterjed a szoba egész levegőjébe. A mesterséges intelligencia szerintem most így fog átforgatni mindent, de nem külön-külön csinál valamit a jogrendszerrel, vagy külön csinál valamit a compliance-nél.*” (6 interjú). Azzal együtt, hogy a mesterséges intelligencia eszközhasználatot szabályozni kell, további biztonsági kérdés, hogy a compliance hogyan reagál erre az eszközre. Egyes adatközlők úgy ítélik meg, hogy a compliance megújulása mindig az adott szervezeti körülményektől, környezettől, szervezeti működéstől és a személyi állománytól is függ (2. interjú). Ugyanakkor a legtöbb interjúalany úgy gondolja, hogy a compliance feladatrendszeren belül több területnek meg kell újulni, és új feladatokat kell kapniuk. Megoszlanak a tekintetben a vélemények, hogy a compliance reaktív vagy proaktív szerepet kapjon-e a vállalkozások életében. A compliance reaktív és proaktív aspektusai megítélése tekintetében igen nagy különbségek érzékelhetők. Ez döntően az anómikus helyzetre való megfelelő reagálás hiányából ered, mert a nem hatékony megelőzés miatt a kialakult problémák után futva próbálnak megoldást találni.

Proaktív és reaktív szerepek

Az interjúk rávilágítottak arra, hogy a compliance szerepe egyszerre lehet reaktív és proaktív. Egyes adatközlők szerint a compliance jellemzően reaktív módon működik, és csak komoly bírságok vagy incidensek után reagál (2. interjú). Mások hangsúlyozták a megelőző, proaktív kontroll szerepének jelentőségét, különösen olyan területeken, mint a kiberbiztonság vagy a pénzmosás megelőzése (1., 10. interjú). A két megközelítés közötti egyensúly megteremtése a jövő egyik kulcskérdése. Egyesek szerint proaktív és reaktív szerepe is van a compliance-nek a mesterséges intelligencia megjelenésével összefüggésben. „*Részben reaktív, mert azért vannak olyan területek, ahol meg szerintem igenis muszáj előre lépni. Kiberbiztonság tekintetében, meg a pénzmosást, csalás megelőzés tekintetében biztos, hogy lépni kell. Tehát látjuk, hogy muszáj előre lépni, előre menni. ... Tehát hogy vannak a prioritások, a kockázatoknak megfelelően alakulnak, és először azokat veszed elő, ami jobban fáj*." (1. interjú). A compliance összetett tevékenység, és a helyzettől függően jelen kell lennie a proaktív és a reaktív szerepkörének is (2 interjú). Egy másik interjúalany a reaktív üzemmódot találta hasznosnak: „*Ez olyan, mint a csalás meg a csalásmegelőzés. Tehát, hogy szerintem mindig jellemzően inkább reaktívak vagyunk. Tehát itt is így lesz, majd jön egy-két komoly eset, jön egy-két komoly bírság, és akkor szépen arra reagálunk. ... Ahogy haladsz előre benne, úgy majd reagálsz azokra mind a kockázatokra, mind a jogi problémákra, az olyan dolgokra, amik meg közben jöttek*." (2. interjú). Az aktív, tehát a preventív szerepkört is azonosította az egyik dolgozó: „*Igen, a compliance megelőz. ... az egy preventív kontrol. Tehát teljesen összeférhetetlen szerintem a jog alatt. Csak ennyire gyerekcipőben van még a corporate compliance, hogy még ezt se látják*." (10. interjú). Az interjúalanyok egy jelentős része úgy nyilatkozott, hogy a compliance szakmának megújuláson kell átesnie, és új feladatokat kell magára vállalnia. Ezekről a következőképpen nyilatkoztak:

A mesterséges intelligencia eszközhasználat nem működhet humán kontroll nélkül, melyben szerepe van a compliance-nek is. „*Azt mondanám, hogy az adott egységtől függően csinálnék egy kockázatelemzést, hogy mennyire kell változtatnom a compliance-emet. Megnézném, hogy mennyire oké is az, hogy én reaktív vagyok, mennyire jó a PreDeCo elv alapján, hol lépjen be a compliance, hol, milyen mértékben léphet be a compliance, és ezt hol, milyen mértékben lehet esetleg kiváltani ilyen miatt. Lehet, hogy nem fontos, hogy nekem ott legyen, mert egyszerűen nincs mögötte akkora kockázatom, olyan tevékenységet végzek, olyan szervezet vagyok, olyan munkában. Viszont, ha meg igenis fontos, akkor már legyen ott az elejétől*" (1. interjú). A compliance akkor tudja betölteni a mesterséges intelligenciával szemben a kontrol funkcióját, ha alaposan ki van dolgozva a mesterséges intelligencia használatának folyamata. Ezt a

compliance-nek meg kell érteni. „*Mindenféleképpen kell, hogy a compliance haladjon a korral*.” (1. interjú). A compliance kontrollnak ki kell terjedni a mesterséges intelligencia eszközök használatával meghozott döntések magyarázhatóságára, a döntések helyességére, illetve a felelősség vizsgálatára. Olyan rendszert kell kialakítani, ami képes egy valós idejű compliance funkció működtetésére. „*Kellenek új funkciók is ... például az AI logikájának az ellenőrzése. De ehhez speciális tudás is kell. Tehát önmagában a compliance, az biztos, hogy nem fogja, ezt tudni kiszolgálni. De ha azt mondtuk, hogy ezeket a fogalmakat kell vizsgálni, akkor ezeknek a fogalmaknak a vizsgálatára kell kompetenciát biztosítani*.” (2. interjú). Tehát a nehézséget az adja, hogy bár folyamatos ellenőrzésre lenne szükség, maguk a kontrolleszközök és a környezet is dinamikus változásban vannak, amit nehéz lekövetni. „*Az MI eszköz használata nem kezelhető egyszerűen szabályozási kérdésként, hanem compliance kérdésként alkalmazható, ... ahol igazából az a kérdés, hogy kinek mi az alkuértéke. Van három irány, ... társadalmi, üzleti, és jogi, tehát a törvények.*” (7. interjú). A transzparencia a legfontosabb: a szolgáltatást kell compliance szempontból megközelíteni, nem magát a mesterséges intelligenciát (7. interjú). A mesterséges intelligencia eszközhasználatot minőségellenőrizni szükséges, azaz vizsgálni kell, hogy rendben volt-e az adott helyzetben meghozott döntés (10. interjú).

Az interjúk során a mesterséges intelligencia eszközhasználat és a megfelelőség biztosítása, továbbá a compliance feladatok, funkciók felülvizsgálata kapcsán kiemelt kérdéssé vált a szervezeti keretek tudatos működtetése.

A compliance és a szervezeti kultúra

Az interjúk alapján a compliance akkor lehet hatékony, ha szervesen beépül a szervezeti kultúrába, annak minden szintjébe és a vállalati etika részévé válik. Ez a folyamat elsősorban a vezetők felelőssége, akiknek példamutató magatartással, képzésekkel és folyamatos tudatosítással kell támogatniuk a megfelelőségi szemlélet megerősítését (1., 7., 8., 10. interjú). A compliance hosszú távon etikus szervezeti kultúrát alapozhat meg, amely nemcsak a szabályok betartásáról, hanem a felelősségvállalásról és a belső motivációról is szól (7. interjú). A compliance tehát több, mint egy vállalkozás szabályrendszere. Ennek megfelelően az interjúk mindegyike egyértelműen a vállalkozás vezetőjét tette felelőssé azért, hogy a szervezeti kultúrába mennyire épül bele a compliance szemlélet. A munkavállalók edukációja egyértelműen a szervezeti kultúra kérdéseként merült föl. (1. interjú).

A vállalati kultúrában az első számú vezetőn múlik, hogy milyen elvárásokat támaszt a körülötte lévő menedzsmenttel szemben. A tulajdonosnak, a menedzsmentnek van általában gondos gazda szemlélete (2. interjú). A vezetőnek komoly elköteleződést kell mutatni a

compliance funkció működtetése szempontjából, és energiát kell arra szánnia, hogy megértesse a szervezettel annak szükségességét akár oktatás, vagy tájékoztató, esetleg különböző programok keretében. A compliance-szel kapcsolatban még számos érzékenyítő programra lesz szükség addig, míg tudatossá válik az alkalmazása (3., 7. interjú). Ezt a gondolatot vitte tovább a 6. interjúalany is amikor hangsúlyozva, hogy akkor jó a check list, ha a végén van edukáció is, tehát a vezetői példamutatás. A vezetőnek egyértelmű feladata, hogy ellenőrizze a szabályok betartatását (8. interjú), meg kell határoznia, hogy mi helyes, és mi nem; példát kell mutatnia, továbbá az oktatásra, edukációra kell fókuszálnia, és együttműködéseket kell kialakítania a munkatársakkal (10. interjú).

A biztonságra épülő működésre az interjúk által említett alkalmas megoldás a compliance szemléletből eredő hosszú távú működésen alapuló szervezeti kultúra kialakítása. Az egyik interjú például rávilágít arra, hogy nemcsak a jogrendszerben, hanem a vállalati gondolkozásban, a munkáltatói és munkavállalói attitűdökben is változásra van szükség. Eszerint tehát nem a rövid távú, hanem a hosszú távú elköteleződés a vállalati működés záloga. Következésképpen, át kell alakítani a munkáltató-munkavállaló viszonyát úgy, hogy a munkavállaló érdekeit közelítenie kell a vállalati értékekhez. Lényeges stratégia szempont továbbá, hogy a compliance-nek a mesterséges intelligencia kihívásokra akkor van módja reagálni, ha a compliance kompetenciák be vannak építve a szervezeti struktúrába. Ezt úgy lehet modellezni, hogy a mesterséges intelligencia a compliance-szel egy tudásszövetet alkot a vállalkozás vázán. A szervezeti MI és compliance elköteleződés együttműködését csakis egy támogató szervezeti kultúrában lehet elérni. A megfelelést a szervezetben úgy kell elhelyezni, hogy kapcsolódások szükségesek a kompetenciák tekintetében, mert eltérő probléma megoldására különböző képességekre van szükség. A mesterséges intelligencia eszközhasználat esetén ennek megszervezése egyrészt innovációs kihívás, másrészt eszköz is a csoportkohézió szilárdítására (9. interjú).

A compliance összetett, és hosszú távú működtetéséhez munkaerőre is szükség van. Az egyéni felelősség köre akkor bővíthető, ha a munkavállaló érti, hogy mi mért történik. (7. interjú). A compliance akár lehet egy olyan működési keretrendszer, amitől a cég más, mint a többi cég, ez hozzáadott értéket jelenthet a felelősség növelésében.

A compliance-re épülő szervezeti kultúra is megjelent az egyik interjúalany válaszaiban. Természetesen vannak olyan esetek is, amikor a szervezeti kultúra részét azért alkotja evidens módon a compliance és a mesterséges intelligencia biztonság, mert a vállalatra szigorú jogszabályok, nemzetközi standardok vonatkoznak, vagy/és régi bevált gyakorlatokkal rendelkezik (3., 4. interjú). Mindezekkel összefüggésben a jövőben a reputáció egyik

legfontosabb pillére a hosszú távon való gondolkozás és a stabilitás lesz; ezek megvalósításának alapja a megbízhatóság, a transzparencia és a megfelelő mesterséges intelligencia és compliance stratégia.

A mesterséges intelligencia, mint compliance támogató eszköz

Az interjúalanyok többsége szerint a mesterséges intelligencia nemcsak kockázati tényező, hanem a compliance támogatására is alkalmas eszköz lehet. Az azonosított felhasználási lehetőségek közé tartozik a jogszabályváltozások nyomon követése, a dokumentum-összefoglalás, a képzési anyagok készítése, a kockázatelemzés, a csalásmegelőzés és a prediktív monitoring (1., 2., 3., 4., 10. interjú). A mesterséges intelligencia így képes lehet az emberi kontroll mellett részfeladatok automatizálására és a döntés-előkészítés támogatására is. „*Arra is lehet használni, hogy a kockázatokat AI segítségével értékeljem, egy módszertan segítségével. Mindenféle kockázat, pénzügyi, működési, informatikai, bármi. ... mert ez megint feladattól függ. ... Az AI bevezetését, akár a compliance-re, akár a szervezet egyéb folyamataira, azzal könnyíted meg igazából a saját dolgodat, mert akkor ugye minden ágensére figyelsz, a tervezéstől egészen a végrehajtásig, mindenhova*." (1. interjú). A compliance akkor tudja hatékonyan és eredményesen betölteni funkcióját, ha az adott folyamatok a kiindulóponttól a végpontig ki vannak dolgozva – felelősökkel, határidőkkel, elemi, atomi feladatrészekkel, és az átadási pontok jól látszanak, tehát folyamatszabályozás szükséges a működtetéséhez (1. interjú) [135]. A mesterséges intelligencia lehet a megfelelést segítő eszköz jogszabályváltozás követésére, a szövegírásban, a képzési anyagok készítésében, az események elemzésében, a tesztek előállításában, a végrehajtásában és a kiértékelésében (2. interjú). A mesterséges intelligencia egy szabályrendszer keretében alkalmas lehet a compliance feladatainak támogatására: részfeladatok elvégzésére, elemzési feladatok végrehajtására, döntéselőkészítésre, adatellenőrzésre. Például „*az egészségügyben be akarok vezetni leletek értékelésére egy MI megoldást, akkor az compliance oldalról nagyon durván le akarom ellenőrizni, hogy az valóban elvárt módon elemzi az adatokat, és a várható legnagyobb gondossággal jár el, és nem fog félrenézni olyan leleteket, amik várhatóan betegséghez vezetnének*." (3. interjú) [136], [137].

Compliance tevékenységet megkönnyítheti a csalásmegelőzés, a csalásfigyelés, a prediktív ügyek intézése a mesterséges intelligencia által (4. interjú). Ezt a logikát követte a 10. interjú adatközlője is. „*Például én azt egy jó gyakorlatnak tartom, hogyha a visszaélés-megelőzés annak bármely fajtajával kapcsolatban használják a mesterséges intelligenciát, mert egy csomó olyan feladatot el tud végezni, ami ilyen nagyon iteratív és nagyon előre meghatározott szabályok szerinti. Tehát mondjuk egy pénzmosás-megelőzésnél, mondjuk a fals pozitív*

találatoknak a kezelésére abszolút alkalmas, vagy ugye ott abban ilyen szcenáriók vannak, a szcenárióknak az átnézegetésére is adott esetben…. Lehet az egy csalás is. Tehát arra is alkalmas az AI, hogy védekezzünk általa az újonnan megjelent, vagy akár nem újonnan megjelent régóta fennálló veszélyek ellen." (10. interjú). A mesterséges intelligencia eszközhasználat jelent meg továbbá a dokumentumok tartalmának összefoglalására, a szakmai anyagok feltárására, vagy azok előkészítésére is [138].

Összegzés

Az interjúk elemzése alapján a mesterséges intelligencia eszközhasználata és a compliance kapcsolatában a résztvevők leginkább a működési kockázatok csökkentését emelték ki. A compliance funkcióinak felülvizsgálata azt mutatja, hogy a kontroll funkció megerősítése elengedhetetlen, ugyanakkor a hatékony működéshez megfelelő szervezeti keretekre is szükség van. Az interjúk rávilágítottak továbbá arra, hogy számos compliance funkció támogatására már most is alkalmasak lehetnek MI eszközök.

Az interjúk azt mutatják, hogy a compliance és a mesterséges intelligencia kapcsolatában jelenleg a bizonytalanság és a kísérletezés időszaka zajlik. A compliance-nek reagálnia kell a digitális fejlődésre, és a kontroll valamint tanácsadói funkciók megerősítésével képes lehet a mesterséges intelligencia eszközhasználatból fakadó kockázatok mérséklésére. A hosszú távon sikeres működés záloga a compliance beágyazódása a szervezeti kultúrába, a vezetői példamutatás, valamint a mesterséges intelligencia, mint támogató eszköz integrálása a megfelelőségi folyamatokba.

3.9 A H3 hipotézis interjús vizsgálata – a compliance és a biztonságtudat

Feltételezem, hogy a mesterséges intelligencia alkalmazása során a compliance nemcsak a biztonságtudatot növeli, hanem hozzájárul a kapcsolódó kockázatok azonosításához és kezeléséhez is [139], [140].

Az interjúk a mesterséges intelligencia eszközök használata tekintetében a kockázat aspektusából értelmezték a compliance biztonságtudatot növelő szerepét. Az interjúalanyok három meghatározó kockázati típust azonosítottak a mesterséges intelligencia eszközhasználat kapcsán.

1. Az adatok hitelességének és tisztaságának kockázata

Több vezető kiemelte, hogy az ellenőrizhetetlen vagy mesterségesen generált adatokra épülő MI eszközök komoly reputációs és jogi kockázatot hordoznak. Ennek kezelésére a zárt, saját fejlesztésű MI rendszerek alkalmazását tartják elengedhetetlennek, amelyek lehetővé teszik az adatforrások kontrollját. Ugyanakkor e megoldás piaci egyenlőtlenséget teremt, mivel a

szükséges kompetenciák és erőforrások elsősorban a tőkeerős vállalkozások számára hozzáférhetők.

A szervezeti hatékonysághoz elengedhetetlen, hogy a vállalatok saját adatbázisból saját adatokon alapulva építsenek maguknak MI eszközöket. Ezt az interjúk azzal indokolják, hogy a mesterséges intelligencia legnagyobb kockázata a hamis, nem megfelelő forrású, érvényességű, pontos, hiteles adatok használata. Emiatt a vállalatoknak nem konzerv – megbízhatatlan forrásokból kialakított – MI eszközöket kell vásárolniuk, hanem zárt, saját rendszereket kell fejleszteniük. Ezzel tudják csökkenteni a téves információk alkalmazásának kockázatát. Ilyen mérnöki, fejlesztői kompetencia csak a tőkeerős, általában nagyobb vállalkozások számára áll rendelkezésre, míg a kisebb cégek ezt a tudást nem tudják megfizetni, az számukra egyáltalán nem hozzáférhető [141]. „… *a compliance szempontjából az adatkihívás szerintem a nagyobb dolog. Mert hogyha ott gubanc van, akkor megvan a jogszerűtlen működés. ... És ugye a mesterséges intelligencia kapcsán hát onnan indítunk, hogy nem tudjuk azt sem sokszor, hogy milyen legális adattal tanították azt az eszközt, de amivel utána én akár legálisan, akár ilyen szoft módon az otthoni íróasztalomnál, mint a vállalat dolgozója titokban használom. De végül az eredményt meg beviszem a főnöknek, csak nem árulom el neki, hogy mondjuk ezt használtam, és lehet, hogy már a vállalati adatot bevittem a ChatGPT-be, vagy a másik alkalmazásba, miközben mondjuk a vállalat lehet, hogy még le se szabályozta, hogy ezt hogyan kellene, vagy lehet- e egyáltalán használni*.” (6. interjú). Ha a mesterséges intelligencia fejlesztése történik, akkor már a tervezésnél működnie kell a biztonságalapú tervezési módszernek, a compliance, az adatvédelem, és információbiztonság érvényesítésével (1. interjú) [142], [143]. Kontrollpontokat kell elhelyezni nemcsak az adatok, hanem a folyamatok tekintetében is, és így a saját MI eszköz fejlesztése növelheti a biztonságot (9. interjú). Ezt a gondolatmenetet vitte tovább a 3. interjú alanya is. A mesterséges intelligencia eszközt leválasztották a nagy modellről, áttették annak a kódrendszerét a saját gépeikre, majd azt fejlesztették és ellenőrizték. Végül csak nagyon alacsony hibaszázalékú működés után kezdték el élesben használni, és engedték rá az adatokat [144], [145]. „… *annyi adat van már az MI által fönn a neten, hogy amikor tanítja valaki egy új feladatra a mesterséges intelligenciáját, az input oldalról, fogalmunk sincs, hogy az normális adat, vagy egy MI által darabolt adat. Az ilyen MI a hibákat exponenciálisan hordozza magában problémaként. Ha MI-ból tanítunk egy másik MI-t, sokkal rosszabb lesz egyébként a hatásfok az MI-oknál. Ezért van például, hogy mindenkinek el kéne kezdeni saját magának tiszta adatokat gyűjtögetni, hogy tudjon, min tanítani*” (4. interjú).

A mesterséges intelligencia eszköz használatakor az első negatív tapasztalatokat a compliance és a biztonság kérdésének felmerülése okozza. Ekkor lehet az a megoldás – ha a cég beruház erre a fejlesztésre –, hogy saját szerverparkokon működtetik a mesterséges intelligenciát, és a cégen belül tartják annak hatáskörét. Ezzel a zárt megoldással nagyobb biztonságot lehet fenntartani (5. interjú). A 6. interjúalany is úgy fogalmazott, hogy a mesterséges intelligencia használata esetén a megfelelőség ténye és annak hangsúlyossága abból is látszik, hogy az eszközt saját IT rendszeren, saját biztonsági rendszeren belül, a saját céges szabályzatokhoz igazítva használják. A saját rendszerek fejlesztését még az is indokolttá teszi, hogy ezáltal a szervezet meg tudja tartani a saját szervezeti folyamatait. Ez egy megfelelő biztonságot szavatol, hiszen nem a szervezeti működést alakítják egy programhoz, hanem a programot alakítják a saját, egyedi szervezeti igényeikhez (7. interjú).

2. A döntéshozatal kockázata

Az interjúk egyöntetűen rámutattak arra, hogy a mesterséges intelligencia által generált kimenetek becslésen alapulnak, és nem tekinthetők megbízható döntéseknek. Ez indokolja a humán kontroll beépítését a folyamatokba, amely biztosítja a döntés-előkészítés és a döntéshozatal szétválasztását. Az emberi tényező tehát továbbra is kulcsszerepet játszik az üzleti folyamatokban, különösen akkor, ha a döntések szubjektív, jogi vagy stratégiai tényezőket is érintenek.

Az interjúalanyok egy másik kockázattal összefüggő általános tapasztalata, hogy a mesterséges intelligenciát nem lehet döntésekre használni, csak döntések előkészítésre. Ennek az az oka, hogy a kimenetel, az output alapvetően egy becslést és nem egy konkrét megbízható adatot tartalmaz. Az egyik interjúalany ezt a következőképpen magyarázta el: „*Két szoftver között az a különbség, hogy akinek jobb szoftvere van, abban több tapasztalat van leprogramozva. És bele vannak programozva a lépések, a hogyanok. ... Az AI az nem ilyen. Az AI, amikor elérsz egy ponthoz, akkor egymillió fele mehetsz tovább, nem csak három fele. Ugyanis az AI-ban nincs beleprogramozva a hogyan. Pont ezért, mert gyakorlatilag mintázatokból képes a promptok alapján keresni, ... nagyon nagy adatbázisban, és ezekből a mintázatokból próbál egy végkimenetet megjósolni. De az a lényeg, hogy nem végeredményt számol. Tehát nem tudod számon kérni azt, hogy kettő meg kettő meg négy, mert nem számológép, mert hogy becsléssel dolgozik... Ezáltal nagyon nehéz szabályoznod igazából gyakorlatilag, hogy mi az elvárt kimenet, és akkor mi számít jónak, vagy mi nem. ... Egy csődközeli pénzügyi helyzetre adott jó válasz az egy mintázat.*” (5. interjú).

Szükséges a döntéshozatal, az adatokból való következtetés, tehát az előkészítésből a következtetés levonása, ezek továbbra is abszolút emberi beavatkozást igényelnek. Egészen

addig van szükség humán kontrollra, amíg valami nem elemi szintű (3. interjú). Üzleti döntéseket mesterséges intelligenciák önmagukban, most még nem hozhatnak, a jogi keret sem biztosított ehhez. Megfelelő szintű döntés akkor hozható, ha azt jóvá hagyja egy felelős személy is (4. interjú). A 8. interjú válaszadója is kiemelte, hogy mindaddig, amíg egy ugyanolyan parancsra teljesen más válasz is generálható, és saját adatbázisból dolgozik a mesterséges intelligencia, addig szükséges a humán validáció, mert az a személy „*a mögöttes tartalmat hozzá tudja tenni*" (8. interjú).

Az interjúalanyok egy kivételével mind azt hangsúlyozták, hogy az üzleti életben a folyamatokból nem hiányozhat az emberi tényező. Ennek oka, hogy a folyamatokba jelenleg nem programozható be minden olyan paraméter, amely alapján egy optimális döntést lehet meghozni. Ilyenek a szubjektív egyedi tényezők, a jogi vagy politikai szempontok (például a diverzitás elvei), de lehet ennek oka az is, hogy míg a gép statisztikai szinten hoz döntéseket, addig egy cégvezetés a kvalitások – egyéb, a gép által nem értelmezhető minőségi tényezők – alapján is optimalizálhatja a döntéseit [146], [147]. Mindezekre adnak példát a következő interjúrészletek:

„*… ha csak azt vizsgáljuk, hogy milyen kritériumoknak kell megfelelnie, akkor a hiba vagy a túlfutás ott van, amikor ezeknek az operációknak túlzottan sok részét bízzuk a gépi oldalra, és nem marad elég humánkontroll a folyamatban… ahol ugye a gépi adatfeldolgozásnak van egy kimenete, a bemenete valami másnak, ahol meg kell dolgoknak történnie, és a kimenet meg a bemenet között nincs emberi értelem, ami megnézné, hogy az, amit a gép kiköpött, mit jelent a bemenet számára a következő oldalon*." Ha egy folyamatot rosszul alkottak meg, akkor hiányoztak belőle bizonyos paraméterek, amelyeket nem vizsgáltak felül, nem ellenőriztek, és emiatt hiányos adatok alapján szükségszerűen rossz következtetésekre juthat, tehát nem lehet kihagyni az embereket (1. interjú). A mesterséges intelligencia eszköz alkalmazása akkor lehet hatékony, ha többszintű és folyamatos ellenőrzésen megy át (8. interjú). Ezt a véleményt erősíti a 10. interjúalany is, mert a tapasztalata szerint a mesterséges intelligencia nem működhet megfelelően emberi felügyelet nélkül. A döntések során csak korlátos számban tud bizonyos szempontokat figyelembe venni, így a döntése nem optimális a vállalati folyamatokban. A legtipikusabb hiányossága a szervezeti szükségletek fel nem ismerése és az adatokban való eligazodás problémája – számolt be erről egybehangzóan számos adatközlő is. E tekintetben az a kihívás, hogy a szervezetek nem tudják a mesterséges intelligencia segítségével begyűjthető, elemezhető óriási adatmennyiségből kihámozni azt, hogy valójában mi az adatok közötti összefüggés, és az adatokat mire is használják fel, hogyan építhetnék be a cég hatékonyságnövelése céljából a vállalat működésébe. Ez a probléma valójában már a társadalmi

intézményeket, az oktatási és képzési rendszert is érinti. Az interjúk rávilágítanak arra, hogy a mesterséges intelligencia használata által kialakuló új lehetőségek kiaknázásához egyelőre nincsen rendelkezésre álló megfelelő kompetencia és tudás. A képzési rendszer még volt képes elég hatékonyan és gyorsan alkalmazkodni ehhez a változáshoz.

3. A kompetenciahiány kockázata

A válaszadók hangsúlyozták, hogy a mesterséges intelligencia eszközök hatékony és biztonságos használatához multidiszciplináris tudás szükséges, amely magában foglalja az informatikai, jogi, közgazdasági és szervezeti szakértelmet is. A hiányzó kompetenciák következtében a szervezetek gyakran nem képesek megfelelően kiaknázni a mesterséges intelligenciában rejlő lehetőségeket, ez a tudásmenedzsment és tudáskormányzás hiányos, problémás működésére is rámutat.

Az interjúk alapján a harmadik kockázat az, hogy hiányzik az a szaktudással rendelkező személy vagy csoport is, ami ismeri a mesterséges intelligenciát, valamint azokat a folyamatokat is, amelyek segítenek összehangolni a használatát a szervezet működésével. „*Egy régi probléma, gyakorlatilag ez mind-mind szervezeti probléma, amiről beszélek, mindig tudásmenedzsment probléma, vagy, amit szívesebben használok újabban, tudáskormányzás, (knowledge governance) probléma. És az új és új és új technológiai környezetben mindig reprodukálják magukat ezek a problémák, szervezeti problémaként, döntési problémaként. Csak attól függően, hogy mi az új technológia, mi érkezik, attól függően a problémáknak a természete mindig kicsit más lesz… A tudáskormányzás mögött meg egy józan észnek kell állnia.*” (1. interjú). Olyan szakértő munkavállaló lenne az ideális, aki egy személyben informatikus, jogász, közgazdász, és az adott szervezethez kapcsolódó speciális szaktudással is rendelkezik (2. interjú).

Az interjúalanyok kitértek arra is, hogy a mesterséges intelligencia önmagában keveset ér akkor, ha nem rendelnek hozzá megfelelő emberi kompetenciát, elemzői tudást. Az egyik interjúalany például a matematikai tudást tartja olyan kulcskompetenciának, amivel egy szervezetnek rendelkeznie kell ahhoz, hogy az eszközt jól és biztonságosan tudja használni. A mesterséges intelligencia sikere azon múlik tehát, hogy vele „*szakértői döntéstámogatást lehetett végezni algoritmizált módon*.” (4. interjú). Egy algoritmus nem működik megfelelő adatok és üzleti folyamatszakértők nélkül. „*Úgy veszem észre, hogy nem az ember kontra AI már a kérdés egy ideje, hanem az a kérdés, hogy ember kontra AI-t jól kezelő ember*.” (8. interjú).

Annak szemléltetésére, hogy a kvalitatív bizonyítékok miként magyarázzák és egészítik ki a kvantitatív mintázatokat, a kutatási eredményeket egy kevert módszertani táblázat segítségével integráltam, és a 15. táblázatban foglaltam össze.

Táblázat 15: A kvantitatív és kvalitatív eredmények összevetése és értelmezése a compliance keretrendszer tükrében (Saját szerkesztés)

Kvantitatív eredmény (Kérdőív)	Kvalitatív téma és reprezentatív idézet (Interjúk)	Értelmezés	Hatás a compliance keretrendszer területeire (lásd. 1. számú függelék)
MI alkalmazás és „árnyék IT”: A válaszadók több mint 50%-a (n=75) használ valamilyen MI eszközt, elsősorban a marketing (50,7%), a termelés (42,3%) és a menedzsment (36,6%) területén.	Szabályozatlan használat és láthatóság: „A munkavállalók saját eszközeiken használnak generatív eszközöket anélkül, hogy tájékoztatnák az IT-t. A vezetés legnagyobb kihívása a láthatóság és annak meghatározása, hogy valójában hová kerülnek az adataink.”	Az MI alkalmazása gyorsabban történik, mint a formális irányítási struktúrák kialakítása.	I és V. terület: Szükség van egy hivatalos biztonsági megfelelési irányelvre és az üzleti folyamatok egyértelmű leképezésére a rendszer határainak egyértelmű meghatározása érdekében.
Compliance motiváció: Az MI-t használó szervezetek esetében statisztikailag szignifikánsan nagyobb a valószínűsége a formális megfelelőségi szabályzatok meglétének (81,1%) a nem használókhoz képest.	Kockázatcsökkentés a folyamatok formalizálásán keresztül: „Amikor az MI megjelenik, új megfelelőségi problémákat generál. Ezt a szabályok intézményesítésével és a mindennapi munkafolyamatba épített ellenőrző pontokkal kezeljük.”	Az MI kényszerítő erőként hat a szervezeti érettségre, megkövetelve az ad-hoc menedzsmentről a formalizált rendszermérnöki kontrollokra való áttérést.	II. és III. terület: Szükséges a compliance megvalósításáért felelős személy kijelölése és egy mérföldkövekkel ellátott, strukturált intézkedési terv kidolgozása.
Kockázatérzékelés: A jogi bizonytalanságok (21%), az adatvédelem (42%) és a pontatlan döntéshozatal (32%) a válaszadók által	Adathitelesség és algoritmikus hallucinációk: „Az adatok hitelességének kockázata óriási. Ha a pénzügyi előrejelzéseket egy hallucinált kimenetre	Az MI technikai kockázatai közvetlenül üzleti és jogi felelősséggé válnak, ami proaktív fenyegetésmodellezést és folyamatos nyomon	IV. terület: Átfogó kockázatkezelési stratégia, amely az algoritmikus átláthatóságra, az adatok eredetére és a folyamatos

leginkább érzékelt kockázatok.	alapozzuk, a felelősség teljes mértékben minket terhel. Specifikus kontrollokra van szükség az MI kimenetek ellenőrzéséhez.”	követést tesz szükségessé.	visszacsatolási hurokra összpontosít.
Biztonságtudat: A biztonságérzetben nagy szórás mutatkozik; ugyanakkor a rendszeres oktatás pozitív korrelációt mutat a magasabb biztonságtudatossági pontszámokkal.	Kompetenciahiány és „human-in-the-loop”: „A rossz döntés kockázata nem csak az algoritmusban rejlik; a kimenetek ellenőrzéséhez szükséges emberi kompetencia hiánya a gond. Az oktatás nem lehet csak egy kipipálandó feladat; valódi képességeket kell építenie.”	A biztonságtudat a folyamatos, releváns oktatás és az aktív szocio-technikai szerepvállalás eredménye, nem a szabályzatok statikus terjesztéséé.	VI. terület: Biztonságtudat: A biztonságérzetben nagy szórás mutatkozik; ugyanakkor a rendszeres oktatás pozitív korrelációt mutat a magasabb biztonságtudatossági pontszámokkal.

Összegzés

Az interjúk elemzése alapján megállapítható, hogy a mesterséges intelligencia eszközeinek alkalmazása szorosan összefügg a megfelelőség biztosításával, amely közvetlen hatással bír a szervezetek biztonságtudatosságára. A válaszok többsége arra utal, hogy a mesterséges intelligencia megjelenése új megfelelőségi kérdéseket generál, amelyek megoldása elsősorban új folyamatok, intézményesített szabályok és kontrollmechanizmusok kialakításán keresztül valósítható meg. E megoldások következményeként a biztonságtudat növekszik, és a compliance szerepe a szervezetek működésében hangsúlyosabbá válik [148], [149].

A vizsgálat rávilágított arra is, hogy a compliance szerepe a mesterséges intelligenciához kapcsolódó kockázatok kezelésében háromdimenziós: egyrészt adatvédelmi és információbiztonsági garanciákat nyújt, másrészt folyamatszabályozási kereteket biztosít, harmadrészt kompetenciafejlesztési feladatokat foglal magában. A biztonságalapú tervezés, a kontrollpontok kialakítása és a szervezeti folyamatokhoz igazított rendszerek fejlesztése együttesen képesek mérsékelni a mesterséges intelligencia alkalmazásából fakadó kockázatokat, és ezáltal növelik a szervezeti biztonságtudatot. Az interjúk tanúsága szerint a mesterséges intelligencia és a compliance kapcsolata dinamikus, egymást erősítő tényezőként értelmezhető: a mesterséges intelligencia alkalmazása új megfelelőségi kihívásokat generál,

amelyek megoldása ugyanakkor hozzájárul a szervezeti biztonság és a jogszerű működés szintjének emeléséhez is [150].

3.10 Interjú – Összefoglalás

Az interjúk eredményei összhangban vannak a kérdőíves kutatás eredményeivel, továbbá a kutatás elméleti eredményeivel is. A compliance és a mesterséges intelligencia fogalma kapcsán a jogi-etikai kihívások, a kockázat, és annak csökkentése, valamint a biztonság voltak hangsúlyos kérdések. Ezek új, szabályozatlan, nem megszokott tényezők a szervezetek életében. Az interjús kutatás egyik következtetése, hogy a mesterséges intelligencia által okozott társadalmi, biztonsági, jogi stb. kockázatok szabályozhatósága, kontroll alatt tarthatósága új szabályozási, megfelelőségi, biztonsági folyamatok szükségességét kívánja meg [151], [152].

A mesterséges intelligencia eszközhasználat és a compliance összefüggése tekintetében az interjúalanyok egyértelműen a kockázatok csökkentését hangsúlyozták. A compliance funkcióinak felülvizsgálata rámutatott arra is, hogy a kontroll funkció további erősítése elengedhetetlen. A funkciók működtetéséhez szükség van innovatív szervezeti keretekre. Kiemelésre kerültek olyan compliance funkciók is, amelyek mesterséges intelligencia eszközökkel támogathatók. Az ilyen jellegű eszközök használata kapcsán a megfelelőség biztosítása növeli a biztonságtudatot. A compliance megoldásokat az jellemzi, hogy a szervezet a felmerült új kérdéseket, helyzeteket új folyamatok, új eszközök intézményesítésével, beillesztésével oldja meg. Ha a mesterséges intelligencia eszköz használatba kerül, akkor a szervezetben a megfelelőség is nagyobb valószínűséggel mutatkozik meg, és sokkal hangsúlyosabbá válik a szerepe a biztonságtudat növelése által [153], [154].

Az interjúk során három olyan típusú kockázat azonosítható a mesterséges intelligencia eszközhasználat kapcsán, amelyekkel kapcsolatban az adatközlők meghatároztak biztonságtudatot növelő megfelelési megoldásokat: 1. az adat hitelességének, tisztaságának kockázatára a saját MI eszköz fejlesztése a megoldás, 2. a rossz/megbízhatatlan döntések kockázatára a mesterséges intelligencia humán kontrollfolyamatokba integrálása lehet a válasz, 3. a mesterséges intelligencia ismeretének hiányára a megfelelő kompetencia szervezeti működésbe való beépítését emelték ki megoldásként.

A compliance megújuló feladatainak, új kihívásainak az implementációja nem evidencia. Az interjúalanyok mégis kevés akadályt neveztek meg ezzel összefüggésben. Az egyik akadály a pénz; a másik a tudatosság hiánya; a harmadik a kulturális problémák; a negyedik egy szervezet felkészültsége a mesterséges intelligencia integrálására. A mesterséges intelligencia

használatból eredő lehetőségek kiaknázásához megfelelő szervezeti és ágazati feltételek szükségesek. A digitális eszközök intenzívebb használata és a compliance alkalmazása ugyanakkor versenyelőnyt biztosíthatnak szigorúbb felügyeleti feladatok megvalósításával, kiemelt dokumentációs fegyelemmel, átláthatósági követelmények alkalmazásával és folyamatos kockázat alapú megfelelés működtetésével. Több interjúalany kiemelte, hogy ha compliance értékek alapján lennének képesek gondolkozni a vállalkozások, akkor sokkal jobb együttműködési lehetőségeik lennének. A compliance, vagy egy ahhoz közelítő értékrend és gondolkodási mód lehet a fejlődés az egyik kulcstényezője.

ÖSSZEGZETT KÖVETKEZTETÉSEK

A kitűzött kutatási célrendszer teljesítése érdekében széleskörű kutatást végeztem. A vizsgálat és az eredmények elemzése alapján a hipotéziseket bizonyítottam, továbbá új tudományos eredményeket fogalmaztam meg, és gyakorlati segédleteket készítettem.

A kutatómunka összefoglalása

Értekezésemben célul tűztem ki a compliance és a mesterséges intelligencia kölcsönhatásainak tudományos igényű, komplex vizsgálatát a gyakorlati alkalmazhatósági szempontok figyelembevételével.

Az első fejezetben a kutatás aktualitását támasztottam alá. Bemutattam a mesterséges intelligencia térnyerését kiemelve a kockázatok szerepét. Részletesen bemutattam és elemeztem az Európai Unió, az OECD és az Amerikai Kereskedelmi Minisztérium mesterséges intelligencia szabályozásával. A második fejezetben compliance fogalmát átfogó, több szinten megvalósuló vizsgálat alá vetettem három elemzési perspektívában. Egyrészt a szakirodalomban megjelenő definíciók elméleti összehasonlító elemzésére került sor, másrészt bibliometriai elemzések segítségével vizsgáltam a compliance tudományos diskurzus szerkezetét 2017-2024 közötti időszakban, továbbá 2025. évre vonatkozóan a WoS és az MTMT tudományos adatbázisokban. Harmadrészt a compliance funkciók szempontjából történő fogalom felülvizsgálatot végeztem el. Elemeztem a compliance funkciókat három szempontból megközelítve: a védelmi vonalak, a főbb kihívások és előnyök, illetve a megfelelésérzékeny ágazatok felől. Tárgyaltam a compliance megjelenését különböző tudományterületeken az OpenAlex adatbázis alkalmazásával. A többi tudományterület compliance vizsgálata alkalmas tárgya lehet a jövőben további tanulmányoknak; hiánypótló lenne a jelen kutatás alapján azt megvizsgálni, hogy létezik-e olyan tudományterület, specializáció, ahol a szintetikus definíció esetleg nem használható. A harmadik fejezet pillanatfelvételt mutat be a compliance és a mesterséges intelligencia megjelenéséről a hazai vállalkozások esetében, továbbá szakértői interjúk alapján.

A compliance és a mesterséges intelligencia témakörében még nem került sor ennyire összetett felmérésre. A kutatás keretében felmértem a hazai vállalkozások compliance és a mesterséges intelligencia témájával kapcsolatos véleményét, felkészültségét, képességeit és működési gyakorlatát. Erre online kérdőíves formában került sor, aminek eredményeit leíró és matematikai-statisztikai módszerekkel vizsgáltam. A fejezet gerincét az online felmérés eredményeinek elemzése és bemutatása teszi ki, továbbá a fejezet tárgyalja az interjúkat az elméleti vizsgálatok eredményeinek értelmezése és a mindennapi gyakorlatba történő

leképezése céljából. Az elméleti kutatás, a bibliometriai elemzés, a gyakorlati funkciók vizsgálata, a kérdőív és az interjúk eredményei alapján végeztem el a hipotézisek vizsgálatát, és alkottam meg a téziseket, a kutatási eredményeket és az ajánlásokat.

Tudományos eredmények

A disszertáció tudományos értéke abban áll, hogy új elméleti keretrendszert alkot a compliance és a mesterséges intelligencia összekapcsolására, továbbá gyakorlati segédleteket kínál a vállalkozások számára a megfelelési rendszer működtetéséhez. A kutatás nemcsak a tudományos diskurzushoz járul hozzá, hanem közvetlen gyakorlati haszonnal is bír: segíti a szervezeteket abban, hogy ne csupán reagáljanak a külső környezet változásaira, hanem proaktívan alakítsák azokat, versenyelőnyt kovácsolva így a compliance és a mesterséges intelligencia szinergiáiból.

Összességében az értekezés rávilágít arra, hogy a digitális korban a megfelelés nem tekinthető statikus kötelezettségnek: olyan dinamikus és adaptív keretrendszerre van szükség, amely képes lépést tartani a technológiai fejlődés ütemével. A gyakorlati segédletek és a tudatos szervezeti kultúra biztosítják, hogy a compliance ne csupán formai megfelelést jelentsen, hanem a hosszú távú biztonság, a bizalom és a fenntartható működés alapja legyen. A kutatás konkrét eredményei:

Elméleti eredmények

1. Kidolgoztam és javaslatot tettem a compliance fogalmára, amely jelentős fejlődésen ment keresztül, tartalmában kiszélesedett és összekapcsolódik a biztonsági tényező funkcióval. Ezt támasztotta alá a szakirodalmi kutatás is, továbbá a kérdőíves vizsgálatban, az interjúkban is egyértelműen a biztonság fogalmával kötötték össze a megkérdezettek.

   A compliance fogalma:

   A compliance a szervezeti működés dinamikus, integratív és kockázatérzékeny irányítási rendszere, amely a normatív, szervezeti és technológiai dimenziók összehangolásán keresztül biztosítja a működés szabályozottságát és a kockázatok proaktív kezelését a digitális, adatvezérelt környezetben.
2. Bizonyítottam egyrészt, hogy szükséges a compliance funkciók felülvizsgálata, másrészt, hogy a compliance szolgáltató és megelőzést biztosító funkciója vált hangsúlyosabbá.

Empirikus eredmények

1. Bizonyítottam, hogy a mesterséges intelligencia eszközhasználat együtt jár a megfelelőség biztosításával a hazai vállalkozások esetében. Hipotézisemet kereszttábla-elemzéssel igazoltam, alátámasztottam. Kimutattam, hogy azoknak a vállalkozásoknak, amelyek használnak MI eszközt, nagyobb valószínűséggel van compliance (megfelelőség) előírása, mint azoknak, melyek nem használnak MI-t.
2. Bizonyítottam, hogy a mesterséges intelligencia eszközök használata kapcsán a megfelelőség növeli a biztonságtudatot. A mesterséges intelligencia eszközök használata kapcsán a megfelelőség alkalmazásának ténye és hangsúlyossága összefügg a biztonságtudattal. Megállapítható, hogy a compliance (megfelelőség) előírás és szabályzat biztosításával, valamint annak rendszeres felülvizsgálatával növelhető a dolgozók biztonságtudata.
3. Megállapítottam, hogy a dolgozók biztonságtudatát a cég befolyásolni képes compliance előírás és szabályzat biztosításával, annak időszakos felülvizsgálatával, valamint olyan tréningek, oktatások szervezésével, melyek aktuálisak, gyakorlatorientáltak, hasznosak a munkavállalók számára.
4. Három olyan típusú kockázat azonosítható a mesterséges intelligencia eszközhasználat kapcsán, amelyekkel kapcsolatban a biztonságtudatot növelő megfelelési megoldások is felmerültek: 1. az adat hitelességének, tisztaságának kockázatára a saját MI eszköz fejlesztése, 2. a rossz/megbízhatatlan döntések kockázatára a humán kontrollfolyamatokba integrálása, 3. a mesterséges intelligencia ismeretének hiányára a megfelelő kompetencia szervezeti működésbe való beépítése jelenthet megoldást.
5. Megállapítottam, hogy a compliance-nek be kell ágyazódnia a szervezeti kultúrába a vállalkozás minden szintjén. Ettől válik hitelessé, ettől válik a vállalati működés és etika szerves részévé. A compliance több, mint egy vállalat szabályrendszere.

Gyakorlati eredmények

1. A kutatás lényeges eredménye, hogy gyakorlati segédletei közvetlenül hasznosíthatóak a gyakorlatban. További kutatásokra ösztönző megállapítások születtek a munka során, hiszen ajánlásokat fogalmaz meg arra vonatkozóan, hogy a mesterséges intelligencia alkalmazása esetén milyen compliance módszertani kérdések vizsgálata szükséges; compliance javaslatokat ad a mesterséges intelligencia használatára vonatkozóan; továbbá compliance feladatok ellátásához ajánlja a mesterséges intelligencia eszköz alkalmazását.
2. A kutatás leglényegesebb eredménye a compliance ajánlások és keretrendszer katalógus.

A kutatási kérdéseket, a feltevéseket, az eredményeket és a téziseket foglalja össze a 16. táblázat.

Táblázat 16: A kutatási eredmények összefoglalása (Saját szerkesztés)

Kutatási kérdések	Feltételezések	Eredmények	Tézisek
KK1. Hogyan határozható meg a compliance fogalma a szakirodalom, az elméleti vizsgálatok, továbbá a gyakorlati működés és a compliance funkciók összevetése alapján?	H1. Feltételezem, hogy a compliance fogalmának szakirodalmi, elméleti, gyakorlati és funkcióbeli értelmezései nem alkotnak egységes rendszert, mely alapján indokolt egy átfogó compliance definíció megalkotása.	Igazoltam elméleti eredményekel.	1. tézis Igazoltam, hogy a compliance fogalma fejlődésen ment keresztül az szakirodalmi, elméleti, gyakorlati felülvizsgálat és a funkciók vizsgálata alapján, ennek során tartalmában kiszélesedett, és indokolt egy átfogó compliance definíció megalkotása. A compliance a szervezeti működés dinamikus, integratív és kockázatérzékeny irányítási rendszere, amely a normatív, szervezeti és technológiai dimenziók összehangolásán keresztül biztosítja a működés szabályozottságát és a kockázatok proaktív kezelését a digitális, adatvezérelt környezetben.
KK2. Milyen jellemzők és gyakorlati alkalmazási formák figyelhetők meg a megfelelőség és a mesterséges intelligencia gyakorlati alkalmazásában?	H2. Feltételezem, hogy a mesterséges intelligencia eszközhasználata összefügg a compliance rendszerek jelenlétével a hazai vállalkozások esetében.	Igazoltam empirikus eredményekkel.	2. tézis Igazoltam, hogy a mesterséges intelligencia eszközhasználat összefügg a megfelelőség biztosításával a hazai vállalkozások esetében, azzal a kitétellel, hogy nem reprezentatív a kérdőív minta.
KK3. Milyen olyan gyakorlati segédletek alakíthatók ki, amelyek támogatják a mesterséges intelligencia alkalmazását, kezelik a kockázatokat és erősítik a szervezeti biztonságtudatot?	H3. Feltételezem, hogy a mesterséges intelligencia alkalmazása során a compliance nemcsak a biztonságtudatot növeli, hanem hozzájárul a kapcsolódó kockázatok azonosításához és kezeléséhez is.	Igazoltam gyakorlati eredményekkel.	3. tézis Igazoltam, hogy a mesterséges intelligencia eszközök használata kapcsán a megfelelőség biztosításának növeli a biztonságtudatot.

A compliance rendszerek hatékonysága végső soron azon múlik, hogy a normatív keretek miként fordíthatók le a szervezeti gyakorlat nyelvére. A gyakorlati segédletek alkalmazása biztosítja, hogy a megfelelés ne formális követelmény maradjon, hanem a szervezeti működés integrált, élő és fenntartható elemévé váljon.

A disszertáció eredményei azt mutatják, hogy a compliance működésének fenntarthatósága azon múlik, mennyire sikerül a szabályozási követelményeket érthető, alkalmazható és a

szervezeti célokhoz illeszkedő formába önteni. Ebben kulcsszerepe van a gyakorlati útmutatóknak, belső képzési anyagoknak, folyamatleírásoknak és esettanulmányoknak, amelyek segíthetnek a megfelelés mindennapi megélésében.

A kutatás eredményei gyakorlati szempontból is hasznosíthatók. Gyakorlati segédleteket állítottam össze, melynek részleteit a függelék tartalmazza. A kutatási eredmények hasznosítását támogató, a kutatás eredményeire támaszkodó gyakorlati segédletek tételesen az alábbiak:

1. Ajánlások

- Ajánlás vállalkozások részére, a mesterséges intelligencia alkalmazása esetén vizsgálandó módszertani kérdésekre.
- A mesterséges intelligencia használatára vonatkozó compliance ajánlások.
- A mesterséges intelligencia alkalmazásának lehetősége a compliance feladatok ellátásában.

2. Compliance keretrendszer

A kutatási eredményekre alapozott és részletes követelményeket tartalmazó compliance keretrendszer került összeállításra, annak érdekében, hogy jogszerűen biztosítsa a vállalati adaptációt a dinamikusan fejlődő digitális környezethez. Indokolt a kutatás alapján az alábbi compliance szempontú működési elvek érvényesítése szervezetre szabva, azaz a vállalkozás üzleti működésének, méretének, tevékenységének, jogi és szabályozási adottságainak, céljainak, folyamatainak, egyéb sajátosságainak figyelembevételével. A keretrendszerben meghatározott követelmények szükségességét a kutatás alátámasztja.

A keretrendszer célja, hogy jogszerűen biztosítsa a vállalati adaptációt a dinamikusan fejlődő digitális környezethez. A compliance menedzsment rendszer kialakítása, alkalmazása, fenntartása, folyamatos fejlesztése a menedzsment feladata. A compliance kötelezettségek a szervezet tevékenységeiből, termékeiből, szolgáltatásaiból erednek, és hatással vannak a működésre.

A compliance szempontú biztonsági folyamatok PDCA logika szerinti bevezetése és folyamatos fejlesztése garantálja a biztonságot. Kockázatmenedzsment szempontból a kockázatok bekövetkezésének a valószínűségét és/vagy a hatását csökkenti a szervezetben. Amennyiben a dokumentált folyamatok egyértelműen meghatározzák a szereplők feladatait és felelősségi köreit, valamint a hozzájuk rendelt folyamatlépéseket, a szervezet képes hatékonyabban reagálni a biztonsági kockázatok bekövetkezésére, gyorsabban kezelni a biztonsági incidenseket, és ezáltal minimalizálni azok hatásait.

A kontroll és a támogató funkciók finomhangolása szükséges, melyhez a compliance megelőzést szolgáló feladata került előtérbe. Ez azt jelenti, hogy egy compliance kockázati értékelés kialakítása szükséges, így a híd szerepét leginkább a szolgáltató funkcióval képes biztosítani. A vezetők és a szervezet compliance iránti stratégiai elköteleződése, a folyamatos információcsere, a hasonló ágazatok együttműködése, tapasztalata szükségesek a hatékony és eredményes compliance érdekében. A megfelelőség iránti elköteleződés magasabb szintjét biztosítja az, ha compliance kultúra kerül kialakításra és működtetésre a topmenedzsment részéről.

A compliance működtetése a szervezeti működési modell átfogó felülvizsgálatára és folyamatos fejlesztésére épül, amely magában foglalja a stratégia, a folyamatok, a feladatok és a kontrollmechanizmusok újragondolását, a plan–do–check–act ciklus következetes alkalmazásával. Ennek keretében elengedhetetlen a kockázatok szisztematikus azonosítása, értékelése, mérséklése és folyamatos nyomon követése, valamint az eredmények visszamérése annak érdekében, hogy a beavatkozások hatékonysága biztosítható legyen. A működés alapját olyan, a szervezet sajátosságaihoz illeszkedő compliance célok és indikátorok képezik, amelyek mérhetőek, dokumentáltak és nyomon követhetőek.

A hatékony működés érdekében komplex üzleti és működési monitoring rendszer kialakítása szükséges, amelyet részletesen kidolgozott belső szabályzatok és folyamatleírások támasztanak alá. Ezek egyértelműen rögzítik a működés kereteit, a folyamatlépéseket, a felelősségi viszonyokat, valamint a döntési hatásköröket és az alkalmazandó szankciókat. A compliance rendszernek egyúttal reagálnia kell a folyamatosan változó jogi és szabályozási környezetre, amelynek nyomon követése és beépítése a működésbe alapvető követelmény.

Kiemelt szerepet kap az emberi tényező fejlesztése is: a munkatársak folyamatos képzése, a szakmai kompetenciák erősítése és a proaktív szemlélet kialakítása hozzájárul a megfelelőség fenntarthatóságához. Ezt támogatja a belső tudásmegosztás és a segítői hálózatok – például compliance mentorok és szakmai közösségek – kiépítése, valamint a compliance funkció folyamatos támogató jelenléte a szervezetben.

A működés adatvezérelt megalapozása érdekében biztosítani kell az adatokhoz való hozzáférést, az adatminőség fenntartását, valamint a különböző rendszerek közötti integrációt. Ezzel párhuzamosan a megfelelőség ellenőrzése ad hoc és rendszeres vizsgálatok révén valósul meg, amely lehetővé teszi a valós idejű beavatkozást is. A dokumentáltság, a nyomon követhetőség és a rendszeres jelentéskészítés kulcsszerepet játszik, mivel ezek biztosítják az ellenőrzési tevékenységek visszakövethetőségét és az eredmények értékelését. A compliance működés hatékonyságát rendszeres – legalább éves – elemzések keretében szükséges

felülvizsgálni, amely során a feltárt jó gyakorlatok azonosítása és szervezeti szintű megosztása is hozzájárul a folyamatos fejlesztéshez.

A keretrendszerben compliance követelményeket részleteiben határoztam meg, - mindegyikhez külön-külön megállapítva a célkitűzést, a szerepköröket, a bemeneteket, a folyamatlépéseket, a kimeneteket, az ellenőrzési pontokat, a mérőszámokat, a felülvizsgálati ciklust - az alábbi hat intézkedési területen:

1. A szervezeti működés és üzleti folyamatok meghatározása
2. Compliance-biztonsági szabályzat
3. Kockázatmenedzsment stratégia
4. A compliance megvalósításáért felelős személy kijelölése
5. Intézkedési terv és annak mérföldkövei
6. A compliance erőforrás és a compliance tudatosság képzése

A hosszú, nehezen átültethető szabályzat szövegek kiváltása érdekében a keretrendszer mind a hat területét egy strukturált rendszermérnöki (systems-engineering) folyamatsablonná alakítottam át [100]. Ezek a sablonok pontosan meghatározzák a megvalósításhoz szükséges célkitűzéseket, szerepköröket, bemeneteket, folyamatlépéseket, kimeneteket, ellenőrzési pontokat, mérőszámokat és a felülvizsgálati (PDCA) ciklusokat [100].

A gyakorlati segédletek tehetik „élővé” a compliance működését.

IRODALOMJEGYZÉK

[1] Európai Bizottság: Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027 COM(2018) 434 final, 2018/0227(COD); https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A434%3AFIN

[2] Európai Bizottság. (2025). *State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future* (COM(2025) 290 final). Európai Bizottság.

[3] European Union Agency for Cybersecurity. (2023). Cybersecurity threats fast forward 2030., https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030 1

[4] Benedek P. (2012). Compliance Management – a New Response to Legal and Business Challenges. *Acta Polytechnica Hungarica, 9*(3), 135–148.

[5] Huang, C., Zhang, Z., Mao, B. és Yao, X. (2023). An Overview of Artificial Intelligence Ethics. *IEEE Transactions on Artificial Intelligence, 4*(4), 799–819. https://doi.org/10.1109/TAI.2022.3194503

[6] Gaudemet, A. (2020). What is Compliance? *RED, 2020*(1), 89–92. https://doi.org/10.3917/red.001.0089

[7] Bygrave, L. A. (2022). Automating Compliance: Artificial Intelligence and the Future of Legal Oversight. *Computer Law & Security Review, 47*, Article 105701. https://doi.org/10.1016/j.clsr.2022.105701

[8] Sloane, M., Moss, A. és Chowdhury, M. (2022). Participation is not a design fix for machine learning. *Proceedings of the ACM on Human-Computer Interaction*, *6*(CSCW2), 1–20. https://doi.org/10.1145/3555573

[9] Wu, Y. és Rooij, B. (2019). Compliance dynamism: Capturing the polynormative and situational nature of business responses to law. *Journal of Business Ethics*, *168*(3), 579–591. https://doi.org/10.1007/s10551-019-04234-4

[10] Silverman, M. (2008). *Compliance management for public, private, and nonprofit organizations*. McGraw Hill.

[11] Suyunov, D. K. (2021). Scientific foundation for implementation of the compliance control system at corporate enterprises. *The American Journal of Management and Economics Innovations*, *3*(6), 138–145. https://doi.org/10.37547/tajmei/Volume03Issue06-21

[12] Statista. (é. n.). *Estimated amount of data created on the internet in one minute*. https://www.statista.com/chart/25443/estimated-amount-of-data-created-on-the-internet-in-one-minute/

[13] Srinivasan, R. és Zielinska, A. (2020). *Data at the edge: Managing and activating information in a distributed world*. State of the Edge; Seagate Technology. https://www.stateoftheedge.com

[14] Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. és Byers, A. H. (2011). *Big data: The next frontier for innovation, competition, and productivity*. McKinsey Global Institute.

[15] Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures and their consequences*. SAGE Publications.

[16] Norori, N., Albornoz, D. és McBride, V. (2025). *Data and AI for science: Key considerations*. International Science Council. https://doi.org/10.24948/2025.11

[17] Shameli-Sendi, A., Aghababaei-Barzegar, R. és Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, *57*, 14–30. https://doi.org/10.1016/j.cose.2015.11.001

[18] ISO/IEC 22989:2022 (en), Information technology - Artificial intelligence - Artificial intelligence concepts and terminology; https://www.iso.org/obp/ui/#iso:std:iso-iec:22989:ed-1:v1:en.

[19] Statista. (2023). Artificial intelligence market size. https://www.statista.com/statistics/1365145/artificial-intelligence-market-size/

[20] Brynjolfsson, E., & McAfee, A. (2014). The Second Machine Age Work, Progress, and Prosperity in a Time of Brilliant Technologies. W. W. Norton. https://wwnorton.com/books/the-second-machine-age

[21] M.Raj and R. Seamans, "Primer on artificial intelligence and robotics," J. Organ. Des., vol. 8, no. 11, pp. 1–14, 2019. https://doi.org/10.1186/s41469-019-0050-0

[22] Riemann, U. és Ochs, T. (2025). *Machine learning get ready to measure the value for supply chain management: Understanding the value of machine learning in the context of business processes*. https://doi.org/10.1007/978-3-031-92184-1_7

[23] Furman, J. (2018). A mesterséges intelligencia és a gazdaság. NBER Working Paper No. 24689. https://www.nber.org/system/files/working_papers/w24689/w24689.pdf

[24] Marković, M. és Soleša, D. (2025). Security and data protection in artificial intelligence. *Journal of Process Management New Technologies*, *13*(1–2), 113–123. https://doi.org/10.5937/jpmnt13-58872

[25] Wang, R. Y. és Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. *Journal of Management Information Systems*, *12*(4), 5–33. https://doi.org/10.1080/07421222.1996.11518099

[26] Anderson, R. (2008). *Security engineering: A guide to building dependable distributed systems*. Wiley.

[27] Von Solms, R. és Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

[28] High-Level Expert Group on AI (2019). Ethics guidelines for trustworthy AI. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[29] Agrawal, A., Gans, J., & Goldfarb, A. (Eds.). (2019). Economics of artificial intelligence: Agenda. University of Chicago Press. https://www.nber.org/books-and-chapters/economics-artificial-intelligence-agenda

[30] Mayer-Schönberger, V., & Cukier, K. (2013). Big Data: A Revolution That Will Transform How We Live, Work and Think. Houghton Mifflin Harcourt. https://dl.acm.org/doi/10.5555/2588165

[31] National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf .

[32] Niskanen, T., Sipola, T. és Väänänen, O. (2023). *Latest trends in artificial intelligence technology: A scoping review*. JAMK University of Applied Sciences. https://doi.org/10.48550/arXiv.2305.04532

[33] Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., & al., e. (2014). Generative adversarial nets. NeurIPS. https://papers.neurips.cc/paper/5423-generative-adversarial-nets.pdf

[34] McKinsey. (2019Driving impact at scale from automation and AI., https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/driving-impact-at-scale-from-automation-and-ai

[35] Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2). https://doi.org/10.1177/2053951716679679 1

[36] Etzioni, A., Etzioni, O. (2017). Incorporating ethics into artificial intelligence. *The Journal of Ethics*, *21*(4), 403–418. https://doi.org/10.1007/978-3-319-69623-2_15

[37] Hodges, C. (2015). *Law and corporate behaviour: Integrating theories of regulation, enforcement, compliance and ethics*. Bloomsbury Publishing.

[38] Painter, R. W. (2017). *Ethics and compliance: The corporate guide*. Oxford University Press.

[39] Thompson, R. B. (2020). *Corporate governance after the financial crisis*. Oxford University Press.

[40] McKinsey. (2023). The state of AI in 2023: Generative Ais breakout year. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year

[41] Raji, I. D., Smart, A., White, R. N., et al. (2020). Closing the AI accountability gap: defining an end-to-end framework for internal algorithmic auditing. 2020. https://doi.org/10.1145/3351095.3372873

[42] McKinsey. (2021). The state of AI un 2021. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Analytics/Our%20Insights/Global%20survey%20The%20state%20of%20AI%20in%2021/Global-survey-The-state-of-AI-in-2021.pdf

[43] Danielsson, J., Macrae, R. és Uthemann, A. (2019). Artificial intelligence and systemic risk. *SSRN Electronic Journal*, 1–9. https://doi.org/10.2139/ssrn.3410948

[44] Cao, L. (2022). AI in finance: Challenges, techniques, and opportunities.*ACM Computing Surveys*, *55*(3), 1–38. https://doi.org/10.1145/3502289

[45] Nichols, P. M. (2025). Does compliance with the global anticorruption regime require the use of artificial intelligence? *American Business Law Journal*, *62*(3). https://doi.org/10.1111/ablj.70000

[46] Pandya, U. (2025). Enhancing cloud security and compliance through artificial intelligence: A conceptual framework. *International Journal of Emerging Trends in Computer Science and Information Technology*. https://doi.org/10.56472/ICCSAIML25-135

[47] Association of Certified Fraud Examiners: Occupational Fraud 2022: A Report to the Nations; https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf

[48] Becker, S. és mtsai. (2020). Continuous compliance. *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering*, 1–12. https://doi.org/10.1145/3324884.3416593

[49] López, H. A. és Hildebrandt, T. T. (2024). *Three decades of formal methods in business process compliance: A systematic literature review*. arXiv. https://arxiv.org/abs/2410.10906

[50] Rinderle-Ma, S., Winter, K. és Benzin, J.-V. (2022). *Predictive compliance monitoring in process-aware information systems: State of the art, functionalities, research directions*. arXiv. https://arxiv.org/abs/2205.05446

[51] Sharpe, L. K., Fong, P. S. és Seviora, R. E. (1998). Managing standards compliance. *IEEE Transactions on Software Engineering*, *24*(6), 471–484. https://doi.org/10.1109/32.824413

[52] Floridi, L. (2021). *The ethics of artificial intelligence*. Oxford University Press.

[53] Európai Bizottság. (2017). Beruházás az intelligens, innovatív és fenntartható iparba: Megújult uniós iparpolitikai stratégia (COM/2017/0479 final). https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52017DC0479

[54] Európai Parlament. (2017). Jelentés a robotika polgári jogi szabályairól szóló bizottsági ajánlásokkal (2015/2103(INL)). https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017IP0051

[55] Európai Tanács. (2017). Az Európai Tanács ülésének következtetései (EUCO 14/17). https://www.consilium.europa.eu/media/21607/19-euco-final-conclusions-hu.pdf

[56] Európai Bizottság. (2018). EU Nyilatkozat a mesterséges intelligenciával kapcsolatos együttműködésről. https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence

[57] Európai Bizottság. (2018). A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK A közös európai adattér kialakítása felé https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN)

[58] Európai Bizottság. (2018). Az Európai Parlament és a Tanács rendelete a Digitális Európa program létrehozásáról a 2021-2027-es időszakra (COM(2018) 434 final, 2018/0227(COD)). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A434%3AFIN

[59] Európai Parlament. (2019). Mesterséges intelligencia: Következtetések a mesterséges intelligenciával kapcsolatos összehangolt tervről (6177/19). https://data.consilium.europa.eu/doc/document/ST-6177-2019-INIT/en/pdf

[60] Európai Bizottság. (2020). Fehér Könyv a mesterséges intelligenciáról: Az európai megközelítés a kiválóság és a bizalom érdekében. https://eur-lex.europa.hu/legal-content/HU/ALL/?uri=CELEX:52020DC0065

[61] Európai Parlament és Tanács. (2024). Az Európai Parlament és a Tanács 2024. június 13-i (EU) 2024/1689 számú rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 számú rendeletek, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 számú irányelvek módosításáról (a mesterséges intelligenciáról szóló rendelet). https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[62] Európai Bizottság. (2025). *A mesterséges intelligencia általános célú gyakorlati kódexe*. https://digital-strategy.ec.europa.eu/hu/policies/contents-code-gpai

[63] Deming, W. E. (1986). *Out of the crisis*. MIT Press.

[64] Hammer, M., Champy, J. (1993). *Reengineering the corporation: A manifesto for business revolution*. Harper Business.

[65] Nizza, R. (2024). Assessing the impact of the EU AI Act on innovation: A multi-model analysis. Northwestern Pritzker School of Law. https://www.law.northwestern.edu/research-faculty/clbe/events/standardization/documents/nizza_assessing_impact_ai_act_innovation.pdf

[66] Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press.

[67] Veale, M. és Zuiderveen Borgesius, F. (2021). Demystifying the draft EU Artificial Intelligence Act. Computer Law & Security Review, 43, 105622. https://doi.org/10.1016/j.clsr.2021.105622

[68] Calo, R. (2017). Artificial Intelligence Policy: A Primer and Roadmap. SSRN https://ssrn.com/abstract=3015350, http://dx.doi.org/10.2139/ssrn.3015350

[69] van Rooij, B. és Sokol, D. D. (szerk.). (2021). The Cambridge handbook of compliance. Cambridge University Press. https://doi.org/10.1017/9781108759458

[70] OECD. (2022) OECD Framework for the Classification of AI systems. (OECD Digital Economy Papers, No. 323). OECD Publishing. https://doi.org/10.1787/cb6d9eca-en

[71] National Institute of Standards and Technology. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

[72] Talaseela, R. K. (2025). Real-time compliance and exception handling via artificial intelligence. Journal of Information Systems Engineering and Management, 10(58s). https://www.jisem-journal.com/

[73] Gösswein, G.: Mediation als Weg aus dem Compiance-Dilemma. Die Mediation (2) 2017. Magyar nyelvű fordítás: A mediáció mint a compliance dilemmából kivezető út (ford.: Csemáné Váradi E. – Jacsó J.), AKV Európai Szemle 1. (2017). pp. 122–127.

[74] Balogh M.: A munkaügyi compliance audit, Wolters Kluwer, Budapest, 2015. pp. 15.

[75] Bock, D.: Strafrechtliche Aspekte der Compliance-Diskussion – § 130 OWiG als zentrale Norm der Criminal Compliance, ZIS, 2. (2009). pp. 293.

[76] Rotsch, T.: 4. Compliance. In ACHENBACH, H., RANSIEK, A.: Handbuch Wirtschaftsstrafrecht. 3. kiad., C. F. Müller, Heidelberg, 2012. pp. 47.

[77] Ambrus, I., Mezei K., Molnár E.: Magyarázat a compliance jogszabályairól I., Általános és büntetőjogi compliance, Wolters Kluwer, Budapest, 2021 pp. 22.

[78] Antal, T. és Számadó, R. (2025). A hazai és a nemzetközi szakirodalomban használatos compliance fogalmának vizsgálata bibliometriai elemzéssel: Kísérlet az újradefiniálására. Hadmérnök, 20 (2), 161–187. https://doi.org/10.32567/hm.2025.2.10

[79] Pritchard, A. (1969). Statistical bibliography or bibliometrics. Journal of Documentation, 25(4), 348–349. https://doi.org/10.1108/eb026482

[80] Otlet, P. (1934). Traité de documentation: Le livre sur le livre, théorie et pratique. Edition Mundaneum.

[81] Garfield, E. (1955). Citation indexes for science: A new dimension in documentation through association of ideas. Science, 122(3159), 108–111. https://doi.org/10.1126/science.122.3159.108

[82] van Eck, N. J., és Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics, 84(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

[83] Allam, Z. és Dhunny, Z. A. (2019). On big data, artificial intelligence and smart cities. Cities, 89, 80–91. https://doi.org/10.1016/j.cities.2019.01.032

[84] Li, J., Greenwood, D. és Kassem, M. (2019). Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases. Automation in Construction, 102, 288–307. https://doi.org/10.1016/j.autcon.2019.02.005

[85] Tandon, A., Dhir, A., Islam, A. K. M. N. és Mantymäki, M. (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Computers in Industry, 122, 103290. https://doi.org/10.1016/j.compind.2020.103290

[86] Cram, W. A., D'Arcy, J. és Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. MIS Quarterly, 43 (2), 525–554. https://doi.org/10.25300/MISQ/2019/43.2.09

[87] Bernal Bernabe, J., Luis Canovas, J., Hernandez-Ramos, J. L., Torres Moreno, R. és Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. IEEE Access, 7, 164908–164940. https://doi.org/10.1109/ACCESS.2019.2950872

[88] Majumdar, A., Shaw, M. és Sinha, S. K. (2020). COVID-19 debunks the myth of socially sustainable supply chain: A case of the clothing industry in South Asian countries. Sustainable Production and Consumption, 24, 150–155. https://doi.org/10.1016/j.spc.2020.07.001

[89] Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J. és Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security, 88, 101653. https://doi.org/10.1016/j.cose.2019.101653

[90] Mackey, T. K., Kuo, T.-T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., Obbad, K., Barkovich, R. és Palombini, M. (2019). Fit-for-purpose? – challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Medicine, 17 (1), 68. https://doi.org/10.1186/s12916-019-1296-7

[91] D'Arcy, J. és Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. Information Systems Journal, 29 (1), 43–69. https://doi.org/10.1111/isj.12173

[92] Attaran, M. (2020). Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management, 15 (1), 70–83. https://doi.org/10.1080/20479700.2020.1843887

[93] Giuditta, T., Hilde, V. M., Alessandra, P., Annick, S., Arthi, A., Artur, Z., … Justine, G. (2024). Supporting measures to improve biosecurity compliance in poultry farms: the NetPoulSafe project. In: 8th International conference on poultry intestinal health, 108–109.

[94] Bálint, F. (2023). Anti-money laundering with a special focus on the cyber security threats and vulnerabilities. National security review: Periodical of the military national security service, 2023(2), 144–157.

[95] Delpont, M., Salazar, L. G., Dewulf, J., Zbikowski, A., Szeleszczuk, P., Dufay-Lefort, A.-C., … Paul, M. C. (2023). Monitoring biosecurity in poultry production: an overview of databases reporting biosecurity compliance from seven European countries. Frontiers in veterinary science, 10. http://doi.org/10.3389/fvets.2023.1231377

[96] Dunay, P. (2020). Arms Control Arrangements under the Aegis of the OSCE: Is There a Better Way to Handle Compliance? In: Times of Eroding Cooperative Security: How to Save Conventional Arms Control in Europe, 51–69.

[97] Bicaku, A., Schmittner, C., Rottmann, P., Tauber, M., & Delsing, J. (2019). Security Safety and Organizational Standard Compliance in Cyber Physical Systems. Infocommunications Journal, 11(1), 2–9. http://doi.org/10.36244/ICJ.2019.1.1

[98] Barta, G. (2018). Challenges in the compliance with the General Data Protection Regulation: Anonymization of personal information and related information security concerns. In Knowledge – economy – society. business, finance and technology as protection and support for society, 115–121.

[99] Dunay, P. (2000). The CFE Compliance record a decade after treaty signature. S + F: Sicherheit und frieden: security and peace, 18(4), 327–333.

[100] Antal, T. és Számadó, R. (2026). Design and evaluation of a compliance management framework for business operations: A system engineering perspective. Journal of Engineering Management and Systems Engineering, 5 (2), 120–136. https://doi.org/10.56578/jemse050201

[101] Dhal, S. B., és Kar, D. (2025). Leveraging artificial intelligence and advanced food processing techniques for enhanced food safety, quality, and security: A comprehensive review. *Food Control*, 155, 110024. https://doi.org/10.1016/j.foodcont.2024.110024

[102] Chen, D., et al. (2025). Optimizing the compliance third-party supervision workflow of involved enterprises using artificial intelligence ant colony algorithm. *Scientific Reports*, 15, 12202. https://doi.org/10.1038/s41598-025-97115-y

[103] Ali, S., Razzaque, M. A., Yousaf, M., és Shan, A. (2025). Cloud security automation through symmetry: Threat detection and response. Symmetry, 17(6), 859. https://doi.org/10.3390/sym17060859

[104] Filipović, A. M., Bralić, V., és Tripalo, S. (2025). Automated analysis of SSL/TLS certificates and network communication security in compliance with the Cybersecurity Act. Crisis Management Days. https://ojs.vvg.hr/index.php/DKU/article/view/760

[105] Isazade, A., Malik, A., & Alshawki, M. B. (2025). Blockchain-enabled GDPR compliance enforcement for IIoT data access. *Journal of Cybersecurity and Privacy*, 5(4), 84. https://doi.org/10.3390/jcp5040084

[106] Jacsó, J. (2019). A pénzmosás compliance a hazai és európai dimenzióban a társadalmi innováció tükrében. Miskolci Jogi Szemle, 2(1), 397–410.

[107] Institute of Internal Auditors. (2020). THE IIA'S THREE LINES MODEL. An update of the Three Lines of Defense

[108] Financial Markets Standards Board. (2020). The 3 Lines Model: A lens on risk management frameworks. https://fmsb.com/publication/the-3-lines-model-a-lens-on-risk-management-frameworks/

[109] Eulerich, M. (2022). The new three lines model... Corporate Ownership & Control, 18(2), 183–191. https://doi.org/10.22495/cocv18i2art15

[110] Magyar Nemzeti Bank. (2022. augusztus 11.). 12/2022. (VIII.11.) számú ajánlása. https://www.mnb.hu/letoltes/12-2022-belso-vedelmi-vonalak-ajanlas.pdf

[111] Alrawashdeh, N., Jawad, M. A., Masoud, M., Al-Afeef, M. A., Al-Smadi, R. W., és Al Ibbini, O. A. (2025). Intelligent finance: Exploring the convergence of AI and fintech. In *Studies in systems, decision and control* (pp. 695–708). Springer International Publishing. https://doi.org/10.1007/978-3-031-90271-0_49

[112] Salama, R., Cacciagrano, D., Al-Turjman, F. (2025). Connecting AI and Blockchain to Improve Security of Financial Services. In: Barolli, L. (eds) Advances on P2P, Parallel, Grid, Cloud and Internet Computing. 3PGCIC 2024. Lecture Notes on Data Engineering and Communications Technologies, vol 232. Springer, Cham. https://doi.org/10.1007/978-3-031-76462-2_7

[113] Magyar Nemzeti Bank. (2022). A belső védelmi vonalak kialakításáról és működtetéséről, a pénzügyi szervezetek irányítási és kontroll funkcióiról (Ajánlás No. 12/2022. (VIII.11.)). https://www.mnb.hu/letoltes/12-2022-belso-vedelmi-vonalak-ajanlas.pdf

[114] George, B. és Vondra, A. (2023). Building a culture of compliance in life sciences organizations. Journal of Commercial Biotechnology, 28(1), 1-8. https://doi.org/10.5912/jcb1005

[115] Borbás, Gy., Leitner, Gy., Bogsch, E. és Brázay, A. (2012). A gyógyszer-kommunikáció etikai kódexe. Magyarországi Gyógyszergyártók Országos Szövetsége.

[116] Miftari, C. S., és Aliu, A. (2025). Designing a tailored ERP system with localized architecture for North Macedonian enterprises. 1991–1996. https://doi.org/10.1109/mipro65660.2025.11131743

[117] Shah, R., Shah, S., és Pathak, P. (2025). Metaverse work culture: The emergence of virtual-first companies and HR's role. *Strategic HR Review*, *24*(5), 195–200. https://doi.org/10.1108/shr-03-2025-0029

[118] Singh, B., és Dutta, P. K. (2025). Cloud native engineering for AI-driven ERP systems: Enhancing security, compliance and data privacy. In *Advances in computers* (o. 439–463). Elsevier BV. https://doi.org/10.1016/bs.adcom.2025.06.009

[119] Singh, K. R., Khanna, M., és Singh, R. (2026). The role of digital twin technology in sustainable smart cities. In *Elsevier eBooks* (o. 233–249). Elsevier BV. https://doi.org/10.1016/b978-0-443-27388-9.00007-6

[120] Soares B. R. Filho, W., de Sousa, L. A. N., Pinto, H. A., Fontes, R. S., Caldeira Silva, G. J. P., Martins Fernandes, F. B., Barbalho, I. M. P., de Morais, A. H. F., Arrais Júnior, E., de Oliveira Barreto, T., Teixeira, C., Henriques, J., Machado, G. M., Valentim, J. L. R. S., Coutinho, K. D., és Valentim, R. A. M. (2026). Brazilian national telediagnosis platform: A data report for scientific research and public health improvement. *Frontiers in Digital Health*, *8*, 1766606. https://doi.org/10.3389/fdgth.2026.1766606

[121] Grant, O. és Agoro, H. (2021). Trends in network compliance and regulatory challenges. ResearchGate. https://www.researchgate.net/publication/389674261_Trends_in_Network_Compliance_and_Regulatory_Challenges

[122] Song, X., Liu, X., Yang, X., Si, C., Zuo, X., He, J., és Cui, Y. (2025). Strategizing data compliance in intelligent healthcare: A four-step solution. *Chinese Medical Journal*, *138*(10), 1254–1256. https://doi.org/10.1097/cm9.0000000000003434

[123] Ананьєва, О., és Гончар, В. (2026). Analysis of modern AI technologies in business: Algorithms and optimization methods, advantages and risks of application. *Scientific Notes of the UniversityKROK*, 88–94. https://doi.org/10.31732/2663-2209-2026-81-88-94

[124] Bârsan-Moigrădean, M. A. (2025). Legal aspects of the Lisbon Treaty on the European. *Cluj University Journal Interdisciplinary Social Sciences and Humanities*, *3*(3-4), 7–20. https://doi.org/10.61846/cuji-ssh.2025.3-4.02

[125] Ebrahim, A. (2025). *Enhancing domestic revenue mobilization in a reformed international financial architecture: Strategies for developing countries in a globalized tax landscape* [Jelentés]. https://doi.org/10.35188/unu-wider/usuc9887

[126] Khezam, Y. B., Gamarnik, I. A., és Gendon, A. L. (2026). The use of artificial intelligence technologies for regulatory risk monitoring in the internal audit system. *Ekonomika i Upravlenie Problemy Resheniya*, *4/2*(169), 200–207. https://doi.org/10.36871/ek.up.p.r.2026.04.02.022

[127] Lakhamraju, M. V. (2025). The strategic role of workday payroll in addressing enterprise challenges. *2*(1), 3–6. https://doi.org/10.69517/cser.2025.02.01.0002

[128] Vankayalapati, R. K. (2025). Security and compliance in hybrid cloud models. https://doi.org/10.70593/978-81-984306-5-6_8

[129] Eurostat. (2023). Use of artificial intelligence in enterprises. Európai Bizottság. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Use_of_artificial_intelligence_in_enterprises

[130] Európai Bizottság. (2022). Digital Economy and Society Index (DESI) 2022: Hungary. https://digital-strategy.ec.europa.eu/en/policies/desi-hungary

[131] Európai Bizottság. (2023). 2023. évi jelentés a digitális évtized helyzetéről: Magyarország. https://digital-strategy.ec.europa.eu/hu/library/2023-report-state-digital-decade-hungary

[132] Cahn, E. S. (2018). The King Midas monoculture. *Tikkun*, 33(1), 36–41. https://doi.org/10.1215/08879982-6817889

[133] Andorka, R. (2006). Bevezetés a szociológiába. Osiris.

[134] Carrapico, H., & Farrand, B. (2024). Cybersecurity trends in the European Union: Regulatory mercantilism and the digitalisation of geopolitics. *Journal of Common Market Studies*. Advance online publication. https://doi.org/10.1111/jcms.13654

[135] Frederica, D., & Murwaningsari, E. (2021). The effect of the use of artificial intelligence and operational risk management on banking performance with the implementation of regulation as a moderation variable. *DeReMa (Development Research of Management)*, 20(1). https://doi.org/10.1877/degres.v20i1.50

[136] Hutchinson, J., Stilinovic, M., és Gray, J. (2024). Data sovereignty: The next frontier for internet policy? *Policy & Internet*. https://doi.org/10.1002/poi3.386

[137] Ijaiya, H., & Adeniyi, I. A. (2024). AI and personal data privacy in the U.S: Balancing customer convenience with privacy compliance. *ABUAD Law Journal*, 12(1). https://doi.org/10.53982/alj.2024.1201.03-j

[138] Li, Y., Wang, S., & Khaskheli, M. B. (2024). Integrating artificial intelligence into service innovation, business development, and legal compliance: Insights from the Hainan Free Trade Port era. *Systems*, 12(11), 463. https://doi.org/10.3390/systems12110463

[139] Maitra, R., & Shrivastav, A. (2024). The data advantage: Artificial intelligence in ophthalmology. *Delhi Journal of Ophthalmology*. https://doi.org/10.4103/dljo.dljo_178_24

[140] McKenna, B., Cai, W., és Tuunanen, T. (2024). Transforming to a sustainable visitor economy with information systems. *Information Systems Journal*. https://doi.org/10.1111/isj.12573

[141] Mokale, M. (2021). Navigating global data privacy regulations: A guide for telecom operators. *International Journal for Multidisciplinary Research*, 3(4). https://doi.org/10.36948/ijfmr.2021.v03i04.39051

[142] Nanumura, U., & Kumara, I. N. (2024). Including GRC principles in IoT security: A comparison of current approaches and future prospects. *International Journal of Innovative Science and Research Technology (IJISRT)*, 9(3). https://doi.org/10.38124/ijisrt/ijisrt24mar227

[143] Rajamäki, J., Jarzemski, D., Kucera, J., Nyman, V., Pura, I., Virtanen, J., Herlevi, M., & Karlsson, L. (2024). Implications of GDPR and NIS2 for cyber threat intelligence exchange in hospitals. *WSEAS Transactions on Computers*, 23, 1. https://doi.org/10.37394/23205.2024.23.1

[144] Shchavinsky, Y., Muzhanova, T., Yakymenko, Y., & Zaporozhchenko, M. (2023). Application of artificial intelligence for improving situational training of cybersecurity specialists. *Information Technologies and Learning Tools*, 97(5). https://doi.org/10.33407/itlt.v97i5.5424

[145] Zahid, A., & Sharma, R. (2023). Personalized health care in a data-driven era: A post–COVID-19 retrospective. *Mayo Clinic Proceedings: Digital Health*, 1(2). https://doi.org/10.1016/j.mcpdig.2023.04.002

[146] Berwer, R. K., Indora, S., Atal, D. K., & Yadav, V. (2024). Blockchain technology for Industry 4.0. In *Blockchain technology and applications*. https://doi.org/10.1002/9781394216147.ch6

[147] Dimitrov, W. (2020). Analysis of the need for cyber security components in the study of advanced technologies. In *INTED2020 Proceedings*. https://doi.org/10.21125/inted.2020.1423

[148] Dorairajan, V. (2024). Cybersecurity and organisational performance – the interplay. *ARPHA Conference Abstracts*. https://doi.org/10.3897/aca.7.e129255

[149] Herath, H.M.S.S., Herath, H.M.K.K.M.B., Madhusanka, B.G.D.A., Guruge, L.G.P.K. (2024). Data Protection Challenges in the Processing of Sensitive Data. In: Hewage, C., Yasakethu, L., Jayakody, D.N.K. (eds) Data Protection. Springer, Cham. (pp.155-179). https://doi.org/10.1007/978-3-031-76473-8_8

[150] Kazi, M. R., P., S., Buvaneswari, R., és Kumar, S. S. (2024). *Modern commerce*. https://doi.org/10.61909/amkedtb112437

[151] Maguluri, K. K. (2025). Foundations of artificial intelligence in healthcare IT: An overview of innovation. In *How Artificial Intelligence is Transforming Healthcare IT: Applications in Diagnostics, Treatment Planning, and Patient Monitoring* (pp. 1-15). Deep Science Publishing. https://doi.org/10.70593/978-81-984306-1-8_1

[152] Maguluri, K. K. (2025). Natural language processing in healthcare: Unlocking insights from clinical data. In *How Artificial Intelligence is Transforming Healthcare IT: Applications in Diagnostics, Treatment Planning, and Patient Monitoring* (pp. 72-88). Deep Science Publishing. https://doi.org/10.70593/978-81-984306-1-8_5

[153] Rane, N. L., Paramesha, M., Rane, J., & Mallick, S. K. (2024). Policies and regulations of artificial intelligence in healthcare, finance, agriculture, manufacturing, retail, energy, and transportation industry. In N. L. Rane (Ed.), *Artificial Intelligence and Industry in Society 5.0* (pp. 67-81). Deep Science Publishing. https://doi.org/10.70593/978-81-981271-1-2_4

[154] Sargiotis, D. (2024). Future Trends in Data Governance: Preparing for Tomorrow. In: Data Governance. (pp. 365-390) Springer, Cham. https://doi.org/10.1007/978-3-031-67268-2_12

RÖVIDÍTÉSJEGYZÉK

Rövidítés	Kifejtés
AI	Artifical Intelligence
ChatGPT	Generative Pre-trained Transformer
CFE	Conventional Armed Forces in Europe
EBESZ	Európai Biztonsági és Együttműködési Szervezet
ENISA	European Union Agency for Cybersecurity (Európai Hálózat- és Információbiztonsági Ügynökség)
ESG	Environmental (környezeti), Social (társadalmi) és Governance (irányítási) keretrendszer
EU	Európai Unió
EUCO	European Council (Európai Tanács)
EU HLEG	European Union High-Level Expert Group on MI (EU Mesterséges Intelligenciával Foglalkozó Magas Szintű Szakértői Csoportja)
H	Hipotézis
HR	Human resources (Humánerőforás)
IDC	International Data Corporation
IKT	Info-kommunikációs technológia
IP	Internet Protocoll
KK	Kutatási kérdés
KKV	Kis- és középvállalkozás
MTMT	Magyar Tudományos Művek Tára
NIS2	Network and Information Security Directive 2. (Hálózat- és információbiztonsági irányelv 2.)
NIST AI RMF	National Institute of Standards and Technology Artificial Intelligence Risk Management Framework
MI	Mesterséges intelligencia
MS Excel	Microsoft Excel
OECD	Organisation for Economic Co-operation and Development (Gazdasági Együttműködési és Fejlesztési Szervezet)

PDCA	Plan–Do–Check–Act (tervezés–cselekvés–ellenőrzés–beavatkozás)
SCI	Science Citation Index
SPSS	Statistical Package for the Social Sciences
VOSViewer	Visualization of Similarities Viewer
WoS	Web of Science
ZB	Zetabyte

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

FÜGGELÉK

1. számú függelék: Gyakorlati segédletek: Ajánlások, Compliance keretrendszer

Compliance ajánlások

I. Vállalkozások részére 10 compliance módszertani kérdés megvizsgálását javaslom a mesterséges intelligencia alkalmazása esetében.

II. Vállalkozások részére 8 compliance ajánlást teszek a mesterséges intelligencia bevezetésére, használatára.

III. Vállalkozások részére konkrét mesterséges intelligencia megoldási lehetőségeket javaslok a compliance feladatok ellátásakor.

I. Vállalkozások részére 10 compliance módszertani kérdés megvizsgálását javaslom a mesterséges intelligencia alkalmazása esetében:

1. Milyen előnyt biztosít a mesterséges intelligencia a szervezetnek?
2. Hozzájárul-e a humánerőforrás minőségi munkavégzéséhez?
3. Hogyan biztosítható a mesterséges intelligencia ellenőrzése?
4. Hogyan illeszkedik a mesterséges intelligencia a meglévő folyamatokba és a szervezeti stratégiába, továbbá milyen módon fejleszti azokat?
5. Hogyan történik a mesterséges intelligencia alkalmazásának szabályozása?
6. A meglévő irányítás és a folyamatok elégségesek-e ahhoz, hogy megfeleljenek a törvényeknek és rendeleteknek?
7. Az átláthatóság biztosítása folyamat és technológia szinten megfelelően biztosítható-e?
8. Milyen kockázatok merülnek fel a mesterséges intelligencia alkalmazásakor?
9. Hogyan és milyen folyamatokkal biztosítják a kockázatok valószínűségének és/vagy a hatásának a minimalizálását, illetve károkozás esetén milyen szabályozások érvényesülnek?
10. A mesterséges intelligencia bevezetésének, fejlesztésének, fenntartásának költségei megtérülnek-e?

II. Vállalkozások részére 8 compliance ajánlást teszek a mesterséges intelligencia bevezetésére, használatára.

1. Compliance megközelítésű mesterséges intelligencia stratégia kidolgozása.

2. Támogatás és tudás megszerzése partnerektől és külső szervezetektől.
3. Folyamatos nyomon követése a mesterséges intelligencia trendeknek, kockázatoknak, hogy meghatározhatóak legyenek azok a mesterséges intelligencia eszközök, melyek támogathatják az egyes belső folyamatokat.
4. Szervezet működési folyamatainak és felelőseinek meghatározása.
5. Dokumentálás biztosítása.
6. A munkavállalók mesterséges intelligenciára vonatkozó képességeinek felmérése, képzések szervezése.
7. Biztosítani szükséges a felhasználható adatok gyűjtését és kezelését.
8. Szükséges a mesterséges intelligencia rendszerek működési folyamatai során kifejtett hatásainak értékelése.

III. Vállalkozások részére konkrét mesterséges intelligencia megoldási lehetőségeket javaslok a compliance feladatok ellátásakor.

1. adatszolgáltatások teljesítése gépi automatizált folyamatokkal;
2. belső szabályzatok aktualizálása, jogszabályi változások nyomon követése;
3. digitális kockázatértékelés, kezelés;
4. jelentéstétel;
5. tesztelési eljárások alkalmazása;
6. ügyfélhitelesítés online ügyfélazonosítással, viselkedésminták azonosítása, monitorozása;
7. üzleti folyamatok automatizálása.

A compliance keretrendszer

1. A szervezeti működés és üzleti folyamatok meghatározása
2. Compliance-biztonsági szabályzat
3. Kockázatmenedzsment stratégia
4. A compliance megvalósításáért felelős személy kijelölése
5. Intézkedési terv és annak mérföldkövei
6. A compliance erőforrás és a compliance tudatosság képzése

I. Terület: A szervezeti működés és üzleti folyamatok meghatározása

Célkitűzés: Az átfogó rendszer megállapítása, az elfogadható MI-használat, az adatkezelési korlátok és a jogi megfelelési elvárások meghatározása a szervezet egészére vonatkozóan.
Szerepkörök: Vezetőség (Jóváhagyás), Compliance vezető (Kialakítás és végrehajtás).

Bemenetek: Hatályos jogszabályi keretek (pl. EU AI Act, GDPR), vállalati stratégiai célok, meglévő IT biztonsági alapelvek és iparági szabványok (pl. ISO/IEC 42001).

Folyamatlépések:

1. A megfelelő szereplők bevonásával dokumentált compliance-biztonsági szabályzat kidolgozása.
2. A célkitűzések, hatókörök, szerepkörök és felelősségek definiálása.
3. A jogszabályoknak és szabványoknak való megfelelés biztosítása.
4. A szabályzat jóváhagyása és a felelősségvállalás rögzítése.
5. A szabályzat megfelelő kihirdetése és a gyakorlati alkalmazás biztosítása.

Kimenetek: Dokumentált, verziókövetett Szervezeti Compliance-Biztonsági Szabályzat.

Ellenőrzési pontok: Kötelező szabályzat-elfogadás (aláírás) minden munkavállaló számára, mielőtt hozzáférést kapnának a vállalati MI eszközökhöz vagy a hálózati erőforrásokhoz.

Mérőszámok: A szabályzatot aláíró munkavállalók aránya; a hálózati tűzfalak által blokkolt, nem engedélyezett MI eszközök száma.

Felülvizsgálati ciklus (PDCA): A szabályzat meghatározott időközönkénti, valamint biztonsági incidensek vagy jogszabályi változások (Check/Act) bekövetkezése utáni frissítése.

II. Terület: A compliance megvalósításáért felelős személy kijelölése

Célkitűzés: Központosított elszámoltathatóság kijelölése az MI compliance rendszer **folyamatos** nyomon követésére, karbantartására és érvényesítésére, biztosítva az emberi felügyelet integrálását az irányítási architektúrába.

Szerepkörök: Szervezet vezetője (Kinevező hatóság), Compliance felelős (Rendszertulajdonos).

Bemenetek: Szervezeti felépítés, humánerőforrás-költségvetés, compliance-biztonsági szabályzat előírásai.

Folyamatlépések:

1. A szervezet vezetője kijelöli a compliance működtetéséért felelős személyt.
2. Megfelelő szintű függetlenség biztosítása a kijelölt személy számára.
3. A felelős személy felhatalmazása a szervezeti compliance-biztonsági szabályzatnak való megfelelés koordinálására, fejlesztésére és fenntartására.
4. A célok eléréséhez szükséges erőforrások (képzés, eszközök, technológia, támogató személyzet) biztosítása a szervezet vezetője által.

Kimenetek: Formális kinevezési okmány; elkülönített és jóváhagyott compliance költségvetés.

Ellenőrzési pontok: A vezetőség félévente felülvizsgálja az erőforrások elégségességét, biztosítva, hogy a felelős személy rendelkezzen a feladatai ellátásához szükséges kapacitással.

Mérőszámok: A jelentett compliance incidensek megoldási ideje; compliance költségvetés felhasználási aránya.

Felülvizsgálati ciklus (PDCA): Folyamatos operatív felhatalmazás, amelyet az éves teljesítményértékelések során vizsgálnak felül az erőforrások szükség szerinti kiigazítása érdekében.

III. Terület: Intézkedési terv és annak mérföldkövei

Célkitűzés: A compliance szabályzat gyakorlati megvalósítása egy strukturált, mérhető ütemterv révén, amely összehangolja a technikai MI-integrációt a kockázatkezelési és üzleti célokkal.

Szerepkörök: Compliance felelős (Vezető), IT menedzsment, részlegvezetők.

Bemenetek: Compliance-biztonsági szabályzat, azonosított működési szűk keresztmetszetek, technológiai beszerzési tervek, korábbi incidensadatok.

Folyamatlépések:

1. Eljárásrend bevezetése a szervezeti szintű compliance-biztonsági és kockázatkezelési intézkedési tervek kidolgozására és fenntartására.
2. A helyreállító intézkedések dokumentálása a kockázatokra való megfelelő reagálás érdekében.
3. A menedzsment felé történő jelentéstételi kötelezettségek teljesítése.
4. Minden lépés és intézkedés dokumentálása a folyamat átláthatósága és nyomon követhetősége érdekében.

Kimenetek: Dinamikus compliance intézkedési terv; mérföldkő-követő irányítópultok; helyreállító intézkedések naplója.

Ellenőrzési pontok: Havi státuszértekezletek a mérföldkövek előrehaladásának értékelésére az alaptervekhez képest.

Mérőszámok: Az ütemterv szerint elért mérföldkövek százalékos aránya; a tervezett és a tényleges helyreállítási idők közötti különbség.

Felülvizsgálati ciklus (PDCA): Az intézkedési terv negyedéves frissítése a végrehajtott intézkedések értékelése és a folyamatos monitoring visszacsatolásai alapján.

IV. Terület: Kockázatmenedzsment stratégia

Célkitűzés: Az MI-alkalmazáshoz kapcsolódó kockázatok (pl. algoritmikus torzítás, adat-hallucinációk, szellemi tulajdon megsértése) szisztematikus azonosítása, értékelése és mérséklése a hibatűrés és a rendszerszintű ellenállóképesség biztosítása érdekében.

Szerepkörök: Kockázatkezelési vezető / Compliance felelős, adatgazdák, rendszertulajdonosok.

Bemenetek: Iparági kockázati keretrendszerek (pl. NIST AI RMF), belső incidensnaplók, tervezett MI felhasználási esetek, rendszerarchitektúra-modellek.

Folyamatlépések:

1. Átfogó kockázatkezelési stratégia kidolgozása (elkerülés, áthárítás, csökkentés, elfogadás).
2. A kockázatelemzési módszertan és a kockázati értékek meghatározása.
3. A kockázatkezelés összehangolása a compliance és biztonsági folyamatokkal, valamint a stratégiai és operatív folyamatokkal.
4. A kockázatokkal és felügyeletükkel kapcsolatos feltételezések és korlátok dokumentálása.
5. A kockázatkezelési tevékenységek nyomon követése, dokumentálása és az eredmények megosztása az érintettekkel.

Kimenetek: MI kockázati regiszter; fenyegetésmodellek; mérséklési protokollok; kockázatértékelési jelentések.

Ellenőrzési pontok: „Go/No-Go" (Mehet/Nem mehet) kapu-felülvizsgálatok az MI modellek tesztkörnyezetből éles üzembe történő átállítása előtt.

Mérőszámok: Azonosított magas szintű sebezhetőségek száma; incidensek gyakorisága; mérséklési intézkedések végrehajtási sebessége.

Felülvizsgálati ciklus (PDCA): Az üzemelő MI rendszerek folyamatos monitorozása és a stratégia rendszeres frissítése a szervezeti változásokra reagálva.

V. Terület: A szervezeti működés és üzleti folyamatok meghatározása

Célkitűzés: Funkcionális dekompozíció végrehajtása: annak pontos feltérképezése, hol és hogyan lépnek interakcióba az MI eszközök a magfolyamatokkal és az adatláncokkal, egyértelmű interfész-definíciók kialakításával.

Szerepkörök: Folyamatgazdák, rendszermérnökök, compliance felelős.

Bemenetek: Vállalati architektúra diagramok, üzletmenet-folytonossági tervek, osztályszintű munkafolyamatok, MI eszközök funkcionális specifikációi.

Folyamatlépések:

1. A szervezeti célok és alapfunkciók meghatározása, figyelembe véve a compliance biztonságot és a működési kockázatokat.
2. Az alapfunkciókból adódó compliance igények meghatározása és az információk sérüléséből fakadó károk azonosítása.
3. Az alapfeladatok, funkciók és kapcsolódó védelmi követelmények dokumentálása.

Kimenetek: Dokumentált folyamattérképek; interfész-szabályozó dokumentumok (Interface Control Documents); funkcionális képesség-meghatározások.

Ellenőrzési pontok: A folyamattérképek építészeti felülvizsgálata annak biztosítására, hogy ne jöhessen létre „árnyék-MI" integráció az adatkontrollok megkerülésével.

Mérőszámok: Teljes körűen dokumentált kulcsfolyamatok aránya; az auditok során észlelt jogosulatlan folyamateltérések gyakorisága.

Felülvizsgálati ciklus (PDCA): A szervezeti célok és funkciók meghatározott időközönkénti felülvizsgálata és módosítása a változó környezeti feltételekhez igazodva.

VI. Terület: A compliance erőforrás és a compliance tudatosság képzése

Célkitűzés: Humán-rendszer ellenállóképesség építése az MI-vel dolgozó munkavállalók összetett biztonságtudatosságának (tudás, attitűd, viselkedés) növelése és az emberi tényezők integrálása révén.

Szerepkörök: HR, compliance felelős, IT biztonsági csoport.

Bemenetek: Képzettségi hiányelemzések, fenyegetéselemzések, frissített szabályzatok, felhasználói visszajelzések.

Folyamatlépések:

1. A compliance feladatokhoz szükséges készségek meghatározása és szerepkör alapú képzési programok kidolgozása.
2. Compliance karrierutak kialakítása a szakmai fejlődés ösztönzése és a kompetenciák intézményesítése érdekében.
3. Felhasználói tudatossági képzések kidolgozása és lebonyolítása, beleértve a tudásszintek mérését is.
4. A képzések lebonyolításának dokumentálása (jelenléti ívek, tanúsítványok) és a résztvevők fejlődésének nyomon követése.
5. A belső és külső eseményekből levont tanulságok beépítése a képzési anyagokba és az eszköztárba.

Kimenetek: Képzési tanterv; jelenléti naplók; kompetenciamérési pontszámok; compliance karrierfejlesztési tervek.

Ellenőrzési pontok: Az MI eszközökhöz való hozzáférés automatikus korlátozása azon munkavállalók számára, akik nem teljesítik a kötelező képzési ciklusokat vagy nem érik el az alapvető kompetenciaszintet.

Mérőszámok: Képzési befejezési arány; átlagos kompetenciateszt-pontszámok; emberi hibából fakadó biztonsági incidensek számának csökkenése.

Felülvizsgálati ciklus (PDCA): A képzési és figyelemfelhívó anyagok rendszeres felülvizsgálata a relevanciájuk megőrzése érdekében, különösen jelentős események után vagy a visszajelzések alapján.

2. számú függelék „Compliance (megfelelőség) és mesterséges intelligencia kutatás a magyar kkv szektorban” című kérdőívben feltett kérdések

- **A vállalkozás neve?**
- **A vállalkozás székhelye (település neve)?**
- **Vállalkozás fő tevékenysége (TEÁOR’08)?**
- **A kérdőív kitöltője, a cég:** vezetője / tulajdonosa / egyéb?
- **Milyen területen dolgozik a szervezetében?** HR / Marketing / Könyvelés / Menedzsment / Ügyfélszolgálat / Adminisztráció / IT / Egyéb szakmai feladatok (pl.: mérnök).
- **A vállalkozás hány főt foglalkoztat?** Mikro-; vagy kisvállalat (kevesebb, mint 50 fő alkalmazott) / Középvállalat (50–250 fő alkalmazott) / Nagyvállalat (több, mint 250 fő alkalmazott).
- **Mi az a három dolog, ami a compliance (megfelelőség) és a mesterséges intelligencia kifejezések hallatán először eszébe jut?**
- **Használ az Ön cége bármilyen mesterséges intelligencián alapuló eszközt?** Igen / Nem / Nem tudom.
- **Amennyiben az előző kérdésre „Igen” volt a válasza, melyek ezek? (Több választ is megjelölhet egyszerre).** Dall-E / ChatGPT / DeepL / Brickabrack AI / Gemini / Claude / Midjourney / Character.AI / QuillBot / Microsoft Copilot / TensorFlow / SAP / Bard / Novel AI / CapCut / Janitor AI / Civitai / Az előző kérdésre „nem” volt a válaszom. / Egyéb
- **Mely területeken tapasztalta, hogy vállalkozása mesterséges intelligencián alapuló alkalmazást/eszközt használ? (Egyszerre több válaszlehetőséget is megjelölhet).** Nem használ ilyet a szervezetem. / Nem vagyok érintett. / Könyvelés, számvitel / HR / Ügyfélszolgálat, támogatás / Adminisztráció / Marketing / Üzletfejlesztés / Menedzsment / Egyéb (pl.: termelés, piackutatás).
- **A szervezetén belül hol látná a legnagyobb előnyét annak, ha mesterséges intelligenciát használnának?**
- **Kérem, fejezze be a mondatot! „Azért használok mesterséges intelligenciát, mert…**
- **Kérem, fejezze be a mondatot! „Azért nem használok mesterséges intelligenciát, mert…**
- **Hogyan értékeli az előnyöket a mesterséges intelligencia eszközök használatában? (Táblázat)**

  - Megkönnyíti, egyszerűsíti, gyorsítja a munkavégzést.
  - Versenyelőny a vállalkozásnak.
  - Fejleszti a szervezeti folyamatokat.

- Marketing lehetőség.
- Növeli az alkalmazkodóképességet.

- **Hogyan értékeli a kockázatokat a mesterséges intelligencia eszközök használatában? (Táblázat)**
  - Pénzügyi korlátok (pl.: üzembe helyezés és működtetés összköltségei).
  - Működési nehézségek (pl.: szakértelemhiány).
  - Informatikai, biztonsági kihívások.
  - Jogi bizonytalanságok.
  - Felhasználási esetek hiánya.
  - Egyéb.
- **Tapasztalt bármilyen kibertámadást, vagy ahhoz hasonlót, amit közvetlenül vagy közvetve egy mesterséges intelligencián alapuló eszköz okozott?** Igen / Nem.
- **Léteznek a munkahelyén felhasználói, biztonsági előírások a mesterséges intelligencián alapuló eszközök használatáról? Ha az előző válaszra „Nem" volt a válasza, válassza a harmadik rubrikát.** Igen / Nem / Az előző kérdésre nem volt a válaszom.
- **Ha az előző kérdésre igennel válaszolt, mennyire érzi megfelelőnek, hasznosnak ezeket az előírásokat a biztonság fenntartása érdekében?** Skála: Teljesen biztonságosnak érzem. – Egyáltalán nem érzem biztonságosnak.
- **Mennyire érzi biztonságosnak a munkahelyén használt mesterséges intelligencián alapuló eszközöket?** Skála: Teljesen biztonságosnak érzem. – Egyáltalán nem érzem biztonságosnak.
- **Évente hányszor tartanak a munkahelyén informatikai biztonsággal kapcsolatos tréninget, avagy bármilyen ebbe a témakörbe tartozó oktatást?** Kevesebb, mint egyszer / Évente egyszer / Kétszer / Kettőnél többször / Egyéb.
- **Ezek az oktatások mennyire aktuálisak, hasznosak?** Skála: Teljesen aktuálisak és hasznosak. – Egyáltalán nem aktuálisak és hasznosak.
- **Van compliance (megfelelőség) előírása, szabályzata a vállalkozásnak?** Van. / Nincs. / Nem tudom. / Egyéb.
- **A vállalkozása milyen gyakran vizsgálja felül a compliance (megfelelőség) szabályrendszerét?** Évente. / Időszakosan. / Akkor, amikor valami új kockázati tényező felmerül. / Soha. / Nem tudom. / Nincs ilyen szabályrendszer.
- **Mire használja jelenleg az Ön szervezete a megfelelőségi (compliance) szabályokat? (Több választ is megjelölhet).** Nem használ ilyet a szervezetem. / Nem vagyok érintett. / Jogszabályok változásainak nyomon követésére. / Képzési és tanúsítási követelmények

kezelésére. / Reputáció céljából. / Előírások és jóváhagyások nyomon követésére és kezelésére. / Egyéb.

- **Hogyan tájékoztatják szervezeténél a munkavállalókat, szerződött feleket és más felelős személyeket a vállalkozás megfelelőségi (compliance) mechanizmusairól?** (Több választ is megjelölhet). Képzésekkel. / Belső szabályozókkal (pl.: Etikai kódex vagy Mesterséges intelligencia eszköz felhasználási útmutató). / Belső kommunikációval. / Belső, céges weboldal használatával. / Tudatosságnövelő események szervezésével. / Egyéb.
- **Milyen compliance területen használná a mesterséges intelligenciát?** Nem használ ilyet a szervezetem. / Nem vagyok érintett. / Kockázatkezelés. / Folyamatok monitorozása. / Jelentés készítése.

3. számú függelék: Az interjúalanyok főbb jellemzői és interjúkérdések

Táblázat 17: Az interjúalanyok főbb jellemzői (Saját szerkesztés)

	Interjúalany neme	**Interjúalany kora**	**Interjúalany végzettsége**	**Interjúalany pozíciója**
1.	Férfi	40–50	Történész, az MTA doktora, vezető kutató	Professzor
2.	Férfi	50–60	Pénzügy, számvitel, közgazdász	Részlegvezető
3.	Férfi	30–40	Informatikus	Biztonságtechnikai szakember
4.	Férfi	40–50	Villamosmérnök, elektronikus információbiztonsági vezető	IT kockázatkezelési szenior menedzser, oktató
5.	Férfi	40–50	Programozó	Digitális coach mesterséges intelligencia területen
6.	Nő	50–60	Jogász, közgazdász	Főiskolai docens, CEO
7.	Férfi	40–50	Etnográfus, kulturális antropológus, PhD	Tudományos főmunkatárs
8.	Férfi	30–40	Közgazdász, regionális tudományok doktora.	Egyetemi docens
9.	Férfi	30–40	Matematikai közgazdász	Beszerzési igazgató
10.	Férfi	40–50	Közgazdász, szociológus	Partner

„Compliance (megfelelőség) és mesterséges intelligencia kutatás a magyar kkv szektorban” című interjúkérdések

1. Mi az első három dolog, ami a compliance (megfelelőség) és a mesterséges intelligencia (MI) kifejezések hallatán először eszébe jut?
2. Hogyan lehet összekapcsolni a compliance és a mesterséges intelligencia témakörét?
3. Milyen új fogalmi elemei lehetnek a compliance-nek a mesterséges intelligencia trendben?
4. Milyen új funkciói lehetnek a compliance-nek?
5. Elegendő a check list típusú megfelelés a biztonságos működéshez?
6. Hogyan van jelen, és milyen tartalmi jegyekkel bír a compliance szemlélet a hazai KKV-knál?
7. Milyen mesterséges intelligencián alapuló használati szokásokkal, tapasztalatokkal rendelkeznek a magyar kis- és közepes méretű vállalkozások?
8. Milyen compliance területeken lehet MI eszközöket alkalmazni?
9. Az új kihívásokra, technológiai trendekre milyen válaszokat lehet adni a compliance területen keresztül?
10. Konkrét példákat tudna-e mondani, amelyek nehézséget okoznak a compliance működtetésében?
11. Hogyan lehetne a kockázatként megjelenő mesterséges intelligenciát a compliance eszközévé tenni?
12. Milyen menedzsment módszerekkel lehet beilleszteni a szervezeti kultúrába a compliancet, mint menedzsment eszközt?
13. Mi a legnagyobb kihívás a menedzsment számára?
14. Milyen konkrét változtatásokkal könnyíthető meg és segíthető elő a compliance működtetését?
15. Van olyan hazai best practise, akár nemzetközi példa, amelyet követendőnek tart a compliance szempontból?

4. számú függelék: Kérdőív és interjú kérdések megfeleltetési táblázat

Táblázat 18: Kérdőív és interjú kérdések megfeleltetési táblázat (Saját szerkesztés)

Kérdőív kérdés	Interjú kérdés	Megfeleltetés típusa	Kategória
Mi az a három dolog, ami a compliance és a mesterséges intelligencia kifejezések hallatán először eszébe jut?	Mi az a három dolog, ami a compliance és a mesterséges intelligencia kifejezések hallatán először eszébe jut?	Teljes átfedés	Compliance és MI fogalom
Használ az Ön cége bármilyen MI alapú eszközt?	Milyen MI alapú használati szokásokkal, tapasztalatokkal rendelkeznek a KKV-k?	Teljes átfedés	MI használat, tapasztalat összevetése
Mely területeken tapasztalta, hogy vállalkozása MI alkalmazást használ?	Milyen compliance területeken lehet MI eszközöket alkalmazni?	Részleges átfedés	MI alkalmazási területek vs. compliance-hez kapcsolódás
A szervezetén belül hol látná a legnagyobb előnyét MI használatának?	Új kihívásokra milyen válaszok adhatók compliance területen keresztül? Konkrét példák nehézségekre a compliance működtetésében? Van hazai vagy nemzetközi best practice a compliance-ban?	Részleges átfedés	MI előnyök és compliance válaszok összekapcsolása
Hogyan értékeli az előnyöket és kockázatokat a mesterséges intelligencia eszközök használatában?	Hogyan lehet a kockázatként megjelenő MI-t compliance eszközzé tenni?	Részleges átfedés	Kockázatok és lehetőségek compliance szempontú kezelése
Van compliance előírása a vállalkozásnak?	Hogyan van jelen, milyen tartalmi jegyekkel bír a compliance szemlélet a hazai KKV-knál? Milyen új fogalmi elemei lehetnek a compliance-nek az MI trendben? Milyen új funkciói lehetnek a compliance-nek	Teljes átfedés	Compliance fogalom
Mennyire érzi biztonságosnak a munkahelyi MI eszközöket?	Elegendő a check list típusú megfelelés a biztonságos működéshez?	Részleges átfedés	Biztonságérzet és megfelelőségi eljárások hatékonysága
Hogyan tájékoztatják a munkavállalókat a compliance mechanizmusokról?	Milyen menedzsment módszerekkel lehet beilleszteni a compliance-t a szervezeti kultúrába?	Részleges átfedés	Kommunikáció és menedzsment szerepe
Mi a legnagyobb kihívás a menedzsment számára?	Mi a legnagyobb kihívás a menedzsment számára? Milyen konkrét változtatásokkal lehet könnyíteni a compliance működtetésén?	Teljes átfedés	Menedzsment kihívás

Kérem, fejezze be: „Azért használok MI-t, mert…” és „… nem használok MI-t, mert…”	Hogyan lehet összekapcsolni a compliance és az MI témakörét?	Részleges átfedés	Motivációk és MI és compliance kapcsolódás

KÖSZÖNETNYILVÁNÍTÁS

Kiemelt köszönettel tartozom a témavezetőmnek, Dr. Számadó Róza adjunktus asszonynak, aki mindenkor hitt bennem, folyamatosan támogatott és biztatott. Mindig rendelkezésemre állt a felmerülő kérdések megvitatására, figyelemmel kísérte a kutatási tevékenységemet, és ellátott tanácsaival, átsegített a nehézségeken. Nélküle nem jöhetett volna létre ez az értekezés.

Köszönettel tartozom az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának, hogy befogadott. Külön köszönöm Prof. Dr. Rajnai Zoltán professzor úrnak, Farkasné Hronyecz Erikának és Lévay Katalinnak a folyamatos támogatást.

Köszönöm férjemnek, ikerlányaimnak, szüleimnek, a családomnak és a barátaimnak, hogy végig mellettem álltak és támaszaim voltak.