

A GENERATÍV MI-RENDSZEREK EGYES POLGÁRI JOGI KÁRTÉRÍTÉSI FELELŐSSÉGI KÉRDÉSEI

CIVIL LIABILITY ISSUES OF GENERATIVE AI SYSTEMS

Kézirat lezárásának dátuma: 2024.12.10.

TARTALOMJEGYZÉK

TARTALOMJEGYZÉK	3
BEVEZETÉS	4
1. A VIZSGÁLT TECHNOLÓGIA BEMUTATÁSA, KITÉRVE AZ ALKALMAZÁSBÉLI PROBLÉMÁIRA	5
1.1. A BLOKKLÁNCHÓZ KAPCSOLT NAGY NYELVI MODELL, MINT VIZSGÁLT TECHNOLÓGIA ÖSSZETEVŐI	5
1.1.1. Az OpenAI GPT típusú modellje	5
1.1.2. A közvetítő, avagy az API	6
1.1.3. Röviden a blokkláncról és a dApp-ról	7
1.2. A SELF CHAIN TECHNOLÓGIÁJÁNAK BEMUTATÁSA	9
1.3. A SELF CHAIN TECHNOLÓGIÁJA ÁLTAL OKOZOTT KÁR	10
1.4. HIPOTÉZIS	11
2. KONTRAKTUÁLIS FELELŐSSÉGI VIZSGÁLAT	12
2.1. A FELEK KÖZÖTTI SZERZŐDÉS LÉTREJÖTTE ÁLTALÁNOS SZERZŐDÉSI FELTÉTELEK ALKALMAZÁSÁVAL	12
2.2. A FELELŐSSÉGGIZÁRÓ- ÉS KORLÁTOZÓ KIKÖTÉSEK ÉS A HIBÁS TELJESÍTÉS VIZSGÁLATA	13
2.3. A SZERZŐDÉSSZEGÉS	19
2.4. BIZONYÍTÁSI KÉRDÉSEK A SZERZŐDÉSSZEGÉSSSEL OKOZOTT KÁRRÁ VONATKOZÓAN	20
2.4.1. A felek közötti szerződés típusának vizsgálata	20
2.4.2. Az elvárható gondosság hiányának vizsgálata	22
2.4.3. Az okozatosság és előreláthatóság vizsgálata	23
2.5. A KÁR BIZONYÍTÁSA	25
2.6. A KONTRAKTUÁLIS FELELŐSSÉGI VIZSGÁLAT ÖSSZEGZÉSE	26
3. A TERMÉKFELELŐSSÉGI VIZSGÁLAT	28
3.1. A GPT MINT TERMÉK	28
3.2. A TERMÉKHIBA MEGHATÁROZÁSA	29
3.3. A KÁR MEGHATÁROZÁSA	32
3.4. OK-OKOZATI KAPCSOLAT, BIZONYÍTHATÓSÁG	33
3.5. MENTESÜLÉS	35
3.6. A TERMÉKFELELŐSSÉGI VIZSGÁLAT ÖSSZEGZÉSE	36
4. A KONTRAKTUÁLIS ÉS DELIKTUÁLIS FELELŐSSÉGI SZABÁLYOK ÜTKÖZÉSE	36
5. DE LEGE FERENDA JAVASLAT, ZÁRSZÓ	40
FÜGGELÉK	41

<u>FOGALOMMAGYARÁZAT</u>	41
<u>FORRÁSOK JEGYZÉKE</u>	49
<u>IRODALOMJEGYZÉK</u>	49
<u>JOGFORRÁSOK</u>	51
<u>INTERNETES FORRÁSOK</u>	51

BEVEZETÉS

A dolgozat egy, a polgári jogi felelősségi szabályok alkalmazását kihívás elé állító technológiai megoldásra koncentrálnak. Ezen technológia bonyolultsága és újszerűsége ugyanis ütköző pályára állít két olyan felelősségi alakzatot, amelyeknek a konkurálása eddig nem volt jellemző, ezen kettő pedig a kontraktuális kárfelelősség és a termékfelelősség.

A dolgozat első részében ismertetem e speciális technológiát, amelynek lényege, hogy egy blokkláncon tranzakciókat elvégezni képes applikációba beépítésre kerül egy nagy nyelvi modell, azzal a céllal, hogy a felhasználókat kiszolgálva, nyelvi parancsok segítségével végezzék el bizonyos tranzakciókat, ezen technológia könnyebb megértése érdekében a függelékben több fontos technikai fogalmat, paramétert kifejtetek amelyre a technikai rész tárgyalása során több alkalommal is utalni fogok. Ezt az elvi technikai megoldást konkretizálom egy jelenleg még csak elképzelt, de megvalósítható gyakorlati alkalmazásban, amelynek segítségével végzem el a kiemelt kárfelelősségi alakzatok vizsgálatát a későbbiekben. Ennek érdekében azzal az előzetes hipotézissel élek, hogy mindkét felelősségi tényállás szerint vizsgálhatónak bizonyulhat az adott technológia által előidézett helyzet. E kutatás hátterét nemcsak a Polgári törvénykönyv, a kontraktuális és deliktuális felelősségi rendszer elválasztása és az ún. non-cumul szabály, hanem az elmúlt években elfogadott uniós jogszabályok is képezik, különös tekintettel az új termékfelelősségi irányelv megújított rendelkezéseire. Azt gondolom, azért is lényeges egy ilyen hipotetikus példát alkalmazni, mivel egyfajta mintaként szolgálhat számunkra, amelyen keresztül több hasonló – a jövőben megvalósuló – MI-alkalmazás jogi problémáit is vizsgálni tudjuk.

A dolgozat következő részében e sajátos MI alkalmazás használata során bekövetkezett károk kérdését elsőként a kontraktuális felelősségi alakzat, majd a termékfelelősségi alakzat mentén vizsgálom. Ezt követően pedig a két felelősségi alakzatot ütköztetem egymással több szempont szerint, amelynek a célja kettős. Egyrészt annak megállapítása, hogy melyik alakzat szerint állapítható meg a felelősség, másrészt pedig a felhasználó oldaláról melyik alakzat bizonyul előnyösebbnek.

Előre bocsátom, hogy jelen vizsgálat több problémát is igyekszik feltárni, úgymint a bizonyítási kérdések, az okozatosság, és megtérítendő kár. E problémákra pedig a dolgozat végén igyekszem megoldási javaslatokkal élni.

1. A VIZSGÁLT TECHNOLOGIA BEMUTATÁSA, KITÉRVE AZ ALKALMAZÁSBÉLI PROBLÉMÁIRA

1.1. A BLOKKLÁNCHOZ KAPCSOLT NAGY NYELVI MODELL, MINT VIZSGÁLT TECHNOLOGIA ÖSSZETEVŐI

1.1.1. AZ OPENAI GPT TÍPUSÚ MODELLJE

A GPT egy általános célú MI-rendszer, ami alatt az OpenAI legújabb, GPT 4o MI-modelljét értem. Ezt a modellt pedig, könnyen lehet, hogy az AI Act¹, kategorizálása alapján nem csupán általános célú MI-modellként határozhatjuk meg, hanem valószínűleg a rendszerszintű kockázatot jelentő általános MI-modellek táborát fogja erősíteni. Nincs erről hivatalos információ, de egy „kiszivárgott” adatok alapján a GPT 4 a tanítási fázisa alatt 2×10^{25} FLOP számítást végzett el.² Ez a számítási érték kétszerese az AI Act-ben meghatározott azon küszöbértéknek, amely alapján vélelmezhető, hogy nagy hatású képességekkel rendelkezik, ezáltal rendszerszintű kockázatot jelentő modellnek minősül.³ Mindez pedig az AI Act szerint azt jelenti, hogy a modellnek olyan kiterjedt képességei vannak, amelyek egy részét a forgalomba hozatal után lehet megismerni, továbbá jelentős hatással járhat akár piaci akár

¹ Európai Parlament és a Tanács (EU) 2024/1689 számú rendelete (2024. június 13.) 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 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról.

² Patrick McGuinness, GPT-4 Details Revealed, 2023.07.12., <https://patmcguinness.substack.com/p/gpt-4-details-revealed> (online, letöltve: 2024.10.06.)

³ Vö. AI Act, 111. preambulumbekkezdés, továbbá AI Act, 51. cikk (1) bekezdés a) pont és (2) bekezdés.

társadalmi folyamatokra.⁴ Amit érdemes tudni a GPT 4o modellről, hogy előtanított⁵, generatív⁶, multimodális⁷, és zárt forráskódú.⁸

A modell bemutatása után pedig térjünk rá, mitől is fog a GPT egy MI rendszerként működni, mintsem egyetlen önálló modellként. A GPT 4o MI-modellhez, amelyet betanítottak, finomhangoltak⁹, hozzákapcsolnak többek között egy felhasználói felületet, amelyen keresztül a végfelhasználók elérhetik. Legyen ez egy applikáció, vagy a weboldala (chatgpt.com). Továbbá a modell képes az internetről valós időben információkat feldolgozni, így nyilvánvaló, hogy valamilyen szoftver (egy másik MI) nyújt ehhez segítséget. Végül pedig a rendszer kimeneteit és bemeneteit egy szoftver folyamatosan naplózza, míg egy másik MI pedig moderálja azt valós időben. Természetesen ez csak néhány kapcsolódó szoftver, azonban ahhoz elég ennyit ismerni, hogy érezzük, amikor a GPT-t használjuk, nem csupán az MI-modellt használjuk, hanem egy komplex rendszert.

1.1.2. A KÖZVETÍTŐ, AVAGY AZ API

Egy nagy nyelvi modell API¹⁰ használata lehetővé teszi, hogy az API-on mint közvetítőn keresztül adjunk lekérdezéseket vagy utasításokat a modellnek anélkül, hogy saját hardveren kellene futtatnunk vagy a fejlesztéssel kellene foglalkoznunk. Informatikai értelemben beszélhetünk API-felhasználóról, aki hozzáférést kap az API-szolgáltató MI modelljéhez, azt utasíthatja. Az API bár hasonlóknak tűnik, mint a végfelhasználó általi használat, azonban ennél sokkal többet jelent. Az API-felhasználó amennyiben egy központi modelltől különálló, speciális feladatra tanított modellt kíván használni, úgy finomhangolhat egy modell magának. Ezt követően az API-felhasználó egy „saját”, a számára finomhangolt modellhez kap hozzáférést.

Rendkívül fontos, hogy az OpenAI sem a finomhangolt modell, sem a normál központi modell API felhasználására nem alkalmaz használati megkötéseket, egyszerűen kijelenti, hogy

⁴ Lásd: Függelék 7. pont

⁵ Lásd: Függelék 1. pont

⁶ Lásd: Függelék 2. pont

⁷ Lásd: Függelék 3. pont

⁸ Lásd: Függelék 4. pont

⁹ Lásd: Függelék 5. pont

¹⁰ Lásd. Függelék 6. pont

mind a bemenetekért, mind a kimenetekért az API-felhasználó tartozik felelősséggel. Továbbá az OpenAI az emberi felügyelet ellátását is az API-felhasználóra bízta¹¹, ennek fényében az API-felhasználás már nem tartozik a TaskUS¹² tevékenysége körébe – ha csak az API-felhasználó erre külön nem köt szerződést a TaskUS-el. Az OpenAI továbbá leszögezni, hogy közvetett károkozásért nem vállal felelősséget, sem valamelyik fél súlyos gondatlanságából, sem titoktartás megsértéséből, sem biztonság megértéséből fakadó károkért.¹³ Ugyanakkor az OpenAI, az API felhasználás esetén engedélyezi az API integrálását szolgáltatásokba, termékekbe, továbbá ezek elérhetővé tételét végfelhasználók számára. A modell viszont az API felhasználás ellenére is zárt forráskódú marad, tehát az API-felhasználó nem lát rá a modell működésére, forráskódjára.

1.1.3. RÖVIDEN A BLOKKLÁNCRÓL ÉS A DAPP-RÓL

A blokklánc lényegében egy adatbázis, amelyeken adatokat tárolhatunk, és mozgathatunk. Ehhez azonban több számítógép összekapcsolása szükséges, amelyek között adatforgalom zajlik. A Bitcoin rendszere ezen az elven alapszik, azonban a centralizált és decentralizált rendszerekkel szemben, ez osztott hálózatnak minősül. Hiszen itt nincs alá-fölérendeltség, minden csomópont (node) mellérendelt, továbbá minden csomópont kapcsolódik az összes többihez. Tehát egy központi irányítás nélküli hálózatról beszélünk. Amely nem sérül, amennyiben egy csomópontot kiiktatunk. Az említett csomópontok bárhol lehetnek a világon – akár mi is létrehozhatunk egyet. Minden egyes csomópont tartalmazza a blokkláncot (az eddigi összes tranzakció listáját), illetve ezeket megosztja más csomópontokkal és folyamatosan frissíti.¹⁴ Azonban egy blokklánc nem csak az említett adatbázisból áll, hanem hozzá lehet kapcsolni más kisebb szoftvereket is, mint például az Ethereum által létrehozott okos szerződések. Ezen szerződések a blokkláncon futnak, és valamilyen üzleti vagy más célú

¹¹ OpenAI, Business Terms, 2023.11.14., <https://openai.com/policies/business-terms/> (Online, letöltve: 2024.09.27.)

¹² A TaskUS egy az OpenAI partnercégei közül, amely tartalmak emberi munkaerővel történő ellenőrzését és moderálást végzi az OpenAI részére.

¹³ OpenAI, Business Terms, 2023.11.14., <https://openai.com/policies/business-terms/> (Online, letöltve: 2024.09.27)

¹⁴ Trinh Anh Tuan, Györfi András: A Blokklánc in Györfi András, Léderer András, Paluska Ferenc, Pataki Gábor, Trinh Anh Tuan: KR1PT0 PÉNZ ABC. HVG Könyvek, Budapest, 2019, 3. Fejezet, A Blokklánc, 26.-28. o.

folyamatot hitelesítenek. Az okos szerződések egy „ha–akkor” típusú feltétel teljesülése esetén automatikusan végrehajtanak egy előre meghatározott feladatot.¹⁵

A blokklánc adatbázisa, a hozzákapcsolt okos szerződésekkel minden node-on (csomóponton) fut, azonban ilyen csomópontok kialakításához egy rendkívül erős számítógépre van szükség, hiszen egy-egy ilyen blokklánc letöltése akár több száz GB-ot is kitehet. Így pedig más elérési utat kell biztosítani a blokkláncokhoz a nagyközönség számára. Erre a célra fejlesztették ki az ún. dApp-okat, vagyis a decentralizált applikációkat. Egy dApp hasonló, mint egy app (normál applikáció). Mindkettőnek van felhasználói felülete és háttér rendszer-része, viszont abban különböznek, hogy a háttér rendszer a dApp esetében a blokkláncot jelenti, nem egy központi szervert (felhőt). A lentebb említett Wallet pedig a dApp-ok egy kategóriáját jelenti, amely blokkláncon történő, kimondottan pénzügyi műveletek elvégzésére lett megalkotva.

Úgy gondolom szemléletesebb és célszerűbb, ha a dApp mint általános fogalom helyére egy valódi, létező Wallet-et helyezünk, olyat, amellyel működhetne a Self Chain lentebb kifejtett technológiája. Így az általam példaként választott kriptopénztárca a Trust. Az applikációja lehetővé teszi, hogy a beépített keresővel más blokkláncokhoz csatlakozhassunk, és azon keresztül végezzünk el tranzakciót, így ha a Trust a későbbiekben beépítene egy nagy nyelvi modellt az alkalmazásába, úgy a Self Chain technológiáját teljes egészében kihasználhatná, vagyis a lentebb említett „szándékkereső” és „szándékmegoldó” nyújtotta lehetőségek elérhetővé válnának.

Ha az eddigi három technológiát, a GPT-t, az API-t és a dApp-ot összekapcsoljuk, akkor a Trust tölti be a felhasználói felület funkcióját, amelyhez hozzákapcsolja API segítségével a GPT modellt, ez utóbbi kettő pedig képes lenne a Self Chain technológiáját használva automatikusan tranzakciókat végrehajtani akár több blokkláncon. Tehát a Trust mint az applikáció jelenne meg egyrészt, másrészt pedig mint az OpenAI egyik API-felhasználója, aki a saját applikációjában használja fel a modellt.

¹⁵ Trinh Anh Tuan, Györfi András: A Blokklánc in Györfi András, Léderer András, Paluska Ferenc, Pataki Gábor, Trinh Anh Tuan: KR1PT0 PÉNZ ABC. HVG Könyvek, Budapest, 2019, 3. Fejezet, A Blokklánc, 33. o.

1.2.A SELF CHAIN TECHNOLÓGIÁJÁNAK BEMUTATÁSA

A Self Chain által kiadott Whitepaper¹⁶ alapján egy ilyen MI szerepe az lenne, hogy lehetővé teszi a Trust-on keresztül végzett pénzügyi műveletek egyszerűbb elvégzését. Mindezt a következőképpen: a felhasználó az MI-rendszernek természetes nyelven leír egy kérést, például: „Szeretnék, 500 USD értékben, a legjobb áron, Bitcoin-t vásárolni.”. Majd az MI ezt a parancsot egy nyelvi értelmezést követően megfelelő cselekvési részekre bontja, például az előbbi kérést a következőkre:

- Számlaegyenleg lekérdezés (ténylegesen van-e 500 dollár a számlánkon)
- Kérdezze le a legjobb árfolyamot (melyik tőzsdén adják a legjobb áron a Bitcoin-t)
- Tranzakciós költségek kiszámítása
- Legjobb út kiválasztása a tranzakcióhoz (olcsóbb és biztonságosabb út kiválasztása, az átváltások miatt)

A fenti parancsokat az MI elküldi a blokkláncon futó „intent searcher” -nek, amely úgy fordítható magyarra „szándékkereső”. Ez fog végrehajtani bizonyos parancsokat, például a számla egyenlegének lekérdezését. Majd miután megállapítja, hogy van elég pénz a számlánkon, kiszámítja a tranzakció lehetséges útvonalait és ezen útvonalak tranzakciós költségeit.¹⁷

Majd az „intent solver”, avagy magyarul „szándékvégrehajtó” kerül aktiválásra. A kereső által felkínált útvonalakat kvázi megversenyezteti, és a legbiztonságosabb és legolcsóbb útvonalat hajtja végre, vagyis aktiválja azon okos szerződéseket, amelyek a kiválasztott útvonalon keresztül végrehajtják a felhasználó által kívánt tranzakciót.¹⁸ Például a legjobb áron megveszi a Bitcoin-t, azt pedig hozzáírja a felhasználó Bitcoin számlájához, így az összeg megjelenik a felhasználói applikációban.

¹⁶ Self Chain, A modular intent-centric blockchain for enhanced security and user-friendliness, 2023.

¹⁷ Self Chain, A modular intent-centric blockchain for enhanced security and user-friendliness, 2023. 12.-13. o.
https://github.com/selfchainxyz/selfchain-docs/blob/main/Selfchain_Whitepaper_v0.1.3.pdf (Online, letöltve: 2024.11.15.)

¹⁸ Self Chain i.m. 14.-15. o.

1.3.A SELF CHAIN TECHNOLÓGIÁJA ÁLTAL OKOZOTT KÁR

Kár alatt jelen példában olyan anyagi hátrány okozását értem, amely az MI-rendszer hibás kimenetéből adódik, arra visszavezethető, azon tranzakciók elvégzése esetén, amelyet a felhasználó rábízott az MI-rendszerre.

Fontos, hogy olyan tranzakcióra irányuljon a kérés, amely megfelel az MI rendeltetésszerű és ésszerűen előrelátható használatának, továbbá olyan kriptovalutával kapcsolatos kérést intézzon az MI-hez, amely az adott Wallet esetén kezelhető. Ezen kívül lényeges, hogy a kár olyan módon történjen, ami a tranzakció ideális végrehajtása során elkerülhető lett volna.

Ilyen hiba általában akkor fordulhat elő, ha az MI például hibásan értelmezi a felhasználó kérését, vagy a kérést hibás parancssorra bontja fel, ezen kívül kár származhat abból is, ha az MI kihagy fontos műveleteket. Ezen hibák a generatív modell statisztikai, nem-determinisztikus, továbbá inkonzisztens működéséből adódnak. A statisztikai működés azt eredményezi, hogy a válasz kiszámíthatatlan, előre meghatározhatatlan. A nem determinisztikusság úgy jelenik meg, hogy azonos bemenetre különböző kimeneteket adhat a modell, az inkonzisztencia pedig úgy jelenik meg, hogy ezen különböző kimenetek akár egymásnak is ellentmondhatnak. Ezekből adódóan fennáll a veszélye, hogy egy értelmes és ésszerű bemenetre hibás kimenetet generáljon a modell.

A kérdés az, hogyan lesz a hibás kimenetből anyagi hátrány, kár. Lényegében, a kimenet alatt azokat a parancssorokat értem, amiket a modell a blokkláncon futó végrehajtó szoftverek felé továbbít. Ez a kimenet lehet bizonyos műveletek végrehajtására adott utasítás, de lehet konkrét okos szerződés is, amit a modell generált. Ez esetben, ha ezen műveleteket hibásan végzi el az MI-rendszer, akkor akár a blokkláncon végzett tranzakciók során fizetett ún. „gáz-díjak”¹⁹ (ez a kriptovaluta-tranzakciók során a tranzakciós díjnak feleltethető meg) megnövekedhetnek, illetve amennyiben nem a megfelelő kriptotőzsdén ad el vagy vásárol az MI-rendszer, úgy akár gazdaságilag sokkal kedvezőtlenebb tranzakciókat is végrehajthat.

¹⁹ A gáz-díj (avagy angolul gas fee) kifejezést az Ethereum használta először, amely arra a költségre utal, amelyet a rendszer használatért kell fizetni, a szerint hogy a tranzakció mekkora számítási teljesítményt igényel, továbbá a blokklánc-rendszer mekkora leterheltség alatt van.

Például, ha a felhasználó kifejezetten kéri, hogy a „legjobb áron” vásároljon, de az ennek megfelelő parancsot nem küldi tovább az MI-rendszer, akkor ez azt is eredményezheti, hogy a kért mennyiségű kriptovalutát lényegesen drágábban vásárolja meg az MI-rendszer, tehát ezzel anyagi veszteséget okoz. Ha pedig rossz okos szerződéseket aktivál, akkor pedig az ún. „gáz-díj” fog lényegesen megnövekedni. Ezzel további anyagi hátrányt okozva a felhasználónak.

A továbbiakban pedig, a kár alatt az ebben az albekezdésben tárgyalt anyagi hátrányt értem, amely - hipotetikusán - a Trust applikációjába épített GPT modell hibás kimenetéből adódik, vagyis azon parancsokból, amelyeket a modell küld a blokkláncon futó szoftvereknek.

1.4. HIPOTÉZIS

A fenti hibás kimenetből eredő kár vonatkozásában azt a hipotézist kívánom felállítani, hogy mind a kontraktuális kártérítési felelősségi szabályok, (így különösen a 2013. évi V. törvény, a Ptk. és a 373/2021. Korm. rendelet szabályai²⁰), mind a termékfelelősségi szabályok (pontosabban az új termékfelelősségi irányelv²¹ rendelkezései) egyaránt alkalmazhatók lesznek. Mivel egyidőben állhat fent az a helyzet, hogy a fogyasztó a gyártóval közvetlen szerződéses kapcsolatban áll, továbbá hogy az MI rendszer hibás működése egyidejűleg jelent a szerződéses viszonyban hibás teljesítést és az irányelv alkalmazása körében termékhibát. Ezen felelősségi alakzatok alkalmazhatóságát azonban a Ptk. 6:145. §-a, azaz a non-cumul szabály fogja befolyásolni. Ez akadályt jelenthet a termékfelelősség alkalmazhatóságát illetően akkor is, ha ez a felelősségi alakzat bizonyul járhatóbb útnak az igényérvényesítés tekintetében.

Tekintettel arra, hogy az MI rendszerek kiszámíthatatlanok és átláthatatlanok, amennyiben egy generatív MI-rendszer részét képezi egy tényszerű bizonyítási eljárásnak, mint amilyen a kontraktuális felelősség vizsgálatakor lefolytatott bizonyítási eljárás, úgy az MI szingularitásként viselkedik. Tehát a bizonyítás során feltehetőleg a szükséges szempontok szerint nem lesz vizsgálható, illetve nem lesz annyira átlátható ez az MI-rendszer, hogy a bizonyítás megvalósításához szükséges következtetéseket le lehessen vonni. Ezen hipotézis,

²⁰ Vö. 373/2021. (VI. 30.) Korm. rendelet a fogyasztó és vállalkozás közötti, az áruk adásvételére, valamint a digitális tartalom szolgáltatására és digitális szolgáltatások nyújtására irányuló szerződések részletes szabályairól.

²¹ Az Európai Parlament és a Tanács (EU) 2024/2853 irányelve (2024. október 23.) a hibás termékekért való felelősségről és a 85/374/EGK tanácsi irányelv hatályon kívül helyezéséről (EGT-vonatkozású szöveg) *OJ L*, 2024/2853, 18.11.2024, ELI: <http://data.europa.eu/eli/dir/2024/2853/oj>.

pedig a következő esetre áll fent: Egy fogyasztónak minősülő természetes személy használni kezdi a Trust alkalmazását, amelybe már beépítésre került a GPT modell. A modell azonban a fogyasztó kriptovaluta vételi kérését rosszul értelmezni, ezért a modell hibás parancsai miatt a tranzakció nem megfelelően kerül végrehajtásra, amely miatt a fogyasztót kár éri.

2. KONTRAKTUÁLIS FELELŐSSÉGI VIZSGÁLAT

2.1. A FELEK KÖZÖTTI SZERZŐDÉS LÉTREJÖTTE ÁLTALÁNOS SZERZŐDÉSI FELTÉTELEK ALKALMAZÁSÁVAL

A felek közötti szerződés létrejöttét és tartalmát az alkalmazott, általános szerződési feltételek tükrében kell vizsgálni. Ez azt jelenti, hogy az egyedi szerződéskötési alkut az egyik fél által tömeges szerződéskötésre előkészített szerződési feltételek váltják fel, amelyek esetén a másik fél mint passzív közreműködő jelenik meg, vagyis csupán megismerni és elfogadja e feltételeket.²² Az ÁSZF fogalma a Ptk. 6:77. § 1) bekezdésben található, amely szerint: „Általános szerződési feltételnek minősül az a feltétel, amelyet az alkalmazója többszerződés megkötése céljából egyoldalúan, a másik fél közreműködése nélkül előre meghatározott, és amelyet a felek egyidejűleg nem tárgyalnak meg.” Ennek mentén, a következőképpen történik a szerződéskötés: az Trust a letöltést követően felkínálja, hogy a felhasználó regisztráljon be egy új pénztárcát. A Trust szolgáltatásai csak a regisztrációt követően válnak hozzáférhetővé, ugyanakkor a szerződés a szolgáltatások egészéhez vagy részéhez történő hozzáféréssel vagy azok használatával hatályosul a felek között. Ugyanis szerződés rendelkezései alapján, a fogyasztó a használttal illetve a hozzáféréssel igazolja, hogy megismerte, és magára nézve

²² Csehi Zoltán (szerk.), 2013. évi V. Törvény A Polgári Törvénykönyvről Kommentárja, Magyar Közlöny Lap- és Könyvkiadó Kft., Budapest, 2021, XV. Fejezet, Tókey Balázs, A szerződés megkötése és értelmezése, 1458.-1459. o.

kötelezőnek fogadta el a szerződési feltételeket.²³ Ilyen módon a fogyasztó és a DApps Platform Inc. között szerződés jön létre.

A DApps Platform Inc. nem alkalmaz külön fogyasztói szerződési feltételeket, ugyanazon szerződés vonatkozik minden felhasználóra. A szerződés, ugyanakkor nem tartalmazza az uniós fogyasztóvédelmi szabályokat, úgy mint például az OpenAI EU Terms of Use, ehelyett aláveti magát a fogyasztó által alkalmazandó jognak. Olyan módon, hogy amennyiben a szerződés valamely része érvénytelen vagy nem végrehajtható az alkalmazandó jogból kifolyólag, úgy a szerződésnek csak az alkalmazandó joggal összhangban álló részei maradnak érvényesek.²⁴

2.2. A FELELŐSSÉGGKIZÁRÓ- ÉS KORLÁTOZÓ KIKÖTÉSEK ÉS A HIBÁS TELJESÍTÉS VIZSGÁLATA

A Ptk. diszpozitív szabályainak köszönhetően a felek a kockázatmegosztás felől saját igényeik szerint rendelkezhetnek, így alkalmazhatnak olyan szerződéses kikötéseket, melyek a szerződésszegésért való felelősséget kizárják vagy korlátozzák. A felek például dönthetnek arról, hogy mely körülményeket tekintik ellenőrzési körükbe tartozónak, vagy például milyen tevékenységet vagy mulasztást szankcionálnak. Mindez azonban nem vezethet a mellérendeltség és egyenjogúság követelményének megsértéséhez. Amennyiben pedig a klauzula indokolatlanul hátrányos, úgy akár a jóhiszeműség és tisztesség elve mentén is vizsgálható annak érvényessége.²⁵ Ennek fényében nézzük meg közelebbről az alábbi konkrét felelősségkizáró- és korlátozó kikötéseket.

²³ DApps Platform Inc., Trust Wallet Terms of Service, 2022. aug. 25. <https://trustwallet.com/terms-of-service> (Online, letöltve: 2024.11.20.)

²⁴ DApps Platform Inc., Trust Wallet Terms of Service, 2022. aug. 25. <https://trustwallet.com/terms-of-service> (Online, letöltve: 2024.11.20.)

²⁵ Fazekas Zoltán József, 4. fejezet: A szerződésszegéssel okozott károkért való felelősség, 182. o. in Barta Judit, Barzó Tímea, Csák Csilla (szerk.), Magyarázat a Kártérítési jogról, Wolters Kluwer Hungary Kft., Budapest, 2018.

Az OpenAI a szerződés²⁶ – azaz a használati feltételek – tárgyát a szolgáltatások nyújtásában határozza meg, a szolgáltatások pedig magát az MI-modelleket jelentik, mint például Dall-E, ChatGPT és egyéb. A vállalat az EU Terms of Use című anyagában kifejti, hogy a szolgáltatások részére bemenetet adhatunk, amire válaszként a szolgáltatás generál egy kimenetet. A bemenet és a kimenet együtt tekintendő tartalomnak.²⁷ Tehát a tartalom maga a rendszerrel történő kommunikáció, amelyet jelen példában úgy fordíthatunk át, hogy a tartalom részének kell tekinteni a blokklánc felé küldött parancssort is. A tartalomról szóló bekezdést viszont úgy folytatja az OpenAI, hogy a tartalomért amennyiben az alkalmazandó jogszabályt vagy a szerződési feltételt megsérti, kizárólag a felhasználó felel. Ugyanakkor kijelenti, hogy a gépi tanulás statisztikai működési jellegéből adódóan olyan kimenet is generálódhat, mely nem tükröz a valóságnak megfelelően embereket, tényeket, helyzeteket. Ha e két bekezdés tartalmát összevetjük, akkor arra juthatunk, hogy az OpenAI MI-modellje ugyan bármikor hibázhat, azonban függetlenül a hiba jellegétől, súlyától és kiváltó okától, a felhasználó viseli a következményeket. Ezzel összevág a Trust szabályozása, mivel nem vállal semmilyen felelősséget a digitális eszközök feldolgozási hibái, megszakításai, vagy késedelmei miatt, továbbá nem vállal semmilyen felelősséget a szerverhibákért, illetve a szoftverben lévő hibákért sem. Amennyiben egy a Trust-ba épített GPT modell kárt okoz, úgy sem az OpenAI GPT-re vonatkozó, sem a DApps Platform Inc. Trust-ra vonatkozó szerződése nem teszi lehetővé, hogy a fogyasztó kártérítési igénnyel éljen. Hiszen az OpenAI a tartalomra vonatkozóan zárja ki a felelősségét, míg a DApps Platform Inc. a szerver- és szoftverhibákért.

Ezen felül az OpenAI további kötelezettséggel terheli a felhasználókat, mint például a felhasználó köteles ellenőrizni a kimenet pontosságát, értékelnie azt, továbbá nem használhatja fel azt a kimenetet, amely „*jogi vagy anyagi hatással lehet az adott személyre*”.²⁸ Ebből pedig könnyedén belátható, hogy az OpenAI lényegében csak a szolgáltatások zavartalan, és folyamatos nyújtására vállal kötelezettséget, ellenben a szolgáltatás minőségéért nem vállal

²⁶ Az OpenAI szerződési feltételeit párhuzamosan kívánom vizsgálni a DApps Platform Inc. (Trust) feltételeivel, mivel a DApps Platform Inc (Trust) jelenleg nem foglalkozik nagy nyelvi modellekkel, így az OpenAI erre vonatkozó szerződéses kikötései kiegészíthetik a Trust szerződéses kikötéseit, hiszen a két szerződés rendkívül hasonlóan bizonyul releváns kérdésekben.

²⁷ OpenAI, EU Terms Of Use, 2024.10.23., <https://openai.com/policies/eu-terms-of-use/> (Online, letöltve: 2024.09.22.)

²⁸ OpenAI, EU Terms Of Use, 2024.10.23., <https://openai.com/policies/eu-terms-of-use/> (Online, letöltve: 2024.09.22.)

semmiféle felelősséget. Ugyanez elmondható a DApps Platform Inc. esetében is, ahol szintén csak az applikáció elérhetővé tételét, és folyamatos elérhetőségét jelölik meg saját kötelezettségként. Azt gondolom, ez a szabályozás felvetheti a tisztességtelenség gyanúját. Érdeemes belegondolni, hogy a hiba abban az esetben is felmerülhet, ha a felhasználó rendeltetészerűen használja a rendszert.

Annak megállapításához, hogy az említett felelősségkizáró- illetve korlátozó kikötés érvényes-e, mérceként a Ptk. 1:3.§-ába foglalt jóhiszeműség és tisztesség elvét alkalmazom, amely a következőképpen szól: *„A jogok gyakorlása és a kötelezettségek teljesítése során a felek a jóhiszeműség és tisztesség követelményének megfelelően kötelesek eljárni.”*. Lényeges, hogy a jóhiszeműség és tisztesség megragadásához ide kell emelnünk az ellentét fogalmát, vagyis a tisztességtelen magatartást. Így adódik a kérdés: Tisztességtelen-e az a gyakorlat, amely a teljes felelősséget a károsultra hárítja, annak ellenére, hogy a károsult egy szolgáltatást vesz igénybe a másik féltől, kárt pedig e szolgáltatás teljesítése során szenved, tekintettel arra, hogy a szolgáltatást rendeltetésének megfelelően használja.

Ha a példánknál maradunk, vagyis a Trust saját alkalmazásában használja a GPT modellt, és a hibás kimenet, mint hibás eredmény miatt a tranzakció nem tartalmaz egy fontos lépést, például a modell nem utasítja a többi szoftvert, hogy kérdezze le „a legjobb árfolyamot”, ami miatt a felhasználót jelentős többletköltség terheli. Mind az OpenAI mind a DApps Platform Inc. szerződési feltételei szerint ezért is a felhasználó viseli a kockázatot. Mindezekről azt gondolom, teljességgel tisztességtelen. Mivel pedig a végfelhasználó természetes személyként, önálló foglalkozásának és szakmájának körén kívül jár el példánkban, úgy hatályos rá a fogyasztókra vonatkozó szabályozás. A Ptk. 6:104. § 2) bekezdésének h) pontja szerint, fogyasztó és vállalkozás között ellenkező bizonyítása erejéig tisztességtelennek kell tekinteni azt a kikötést, amely kizárja vagy korlátozza a fogyasztó jogszabályokon alapuló jogait a vállalkozás szerződésszegése esetén. Míg a Ptk. 6:103§ 3) szerint, a tisztességtelen feltétel a fogyasztó és a vállalkozás között semmis. Tehát a felelősségkizárás semmissé tételét ily módon lehet megkísérelni. Amennyiben semmissé tesszük a felhasználóra rótt ezen tisztességtelen feltételeket, lehetőségünk nyílik, hogy a kimenetek esetén bizonyos minőségi követelményt megállapítsunk, hiszen ha a kimenet mint eredmény anyagi hátrányt okoz a végfelhasználónak, az - bizonyos esetben - szerződésszegésként értelmezhető.

Amennyiben semmissé tudjuk tenni azon kikötéseket, amelyek a végfelhasználóra hárítanak a kimenet mint eredmény miatti szinte minden felelősséget, rátérhetünk a 373/2021 (IV. 30.) Korm. rendelet a fogyasztó és a vállalkozás közötti, az áruk adásvételére, valamint a

digitális tartalom szolgáltatására és digitális szolgáltatások nyújtására irányuló szerződések részletes szabályairól (továbbiakban: Korm. rendelet) szerint annak megállapítására, hogy a hibás kimenet nem szerződésszerű teljesítésnek tekinthető-e, vagyis a szolgáltatót terheli-e bizonyos kötelezettség a kimenet minőségét illetően. A Korm. rendelet viszont kizárólag a visszterhes szerződésekre nézve hatályos, ám a Trust applikáció nem alkalmaz semmilyen díjazást, így pedig a visszterhességet az adatok kezelésének függvényében kell vizsgálnunk. A Korm. rendelet 1. § 1) pontjának b) bekezdése szerint a rendelet hatályos az olyan fogyasztó és vállalkozás közötti szerződésekre, amelyekben a vállalkozás digitális szolgáltatást nyújt, a fogyasztó pedig kifizeti a vételárat, vagy vállalja, hogy kifizeti. Míg a 3) bekezdés a) pontja szerint, az előző rendelkezést kell alkalmazni, amennyiben a fogyasztó személyes adatot szolgáltat a vállalkozásnak, az pedig ezen adatokat a digitális szolgáltatás nyújtásán, és a jogszabályoknak való megfelelésen más célra is nyújtja. Ennek keretében mind a DApps Platform Inc. mind az OpenAI kiemeli a szerződési feltételeiben, hogy a szolgáltatás fejlesztésére is felhasználják ezen személyes adatokat, továbbá a Trust szabályzata tartalmaz olyan kikötést miszerint „belső üzleti célokra” is felhasználják. Így pedig a szolgáltatás visszterhesnek mondható.

A szerződésszerű teljesítést a Korm. rendelet 17. § szerint értelmezve, e szakasz (1) bekezdése alapján, a vállalkozás a szerződéskötést követően köteles indokolatlan késedelem nélkül szolgáltatni a fogyasztónak a digitális szolgáltatást, a rendelkezésre álló legfrissebb verzióban. A GPT-t, mint digitális szolgáltatást a Korm. rendelet 4. § 4. pontjának, a) bekezdés szerint, a következőképpen tudjuk meghatározni: *„olyan szolgáltatás, amely lehetővé teszi a fogyasztó számára, hogy digitális adatokat hozzon létre, kezeljen, tároljon, vagy azokhoz hozzáférjen”*. A generatív MI-modellek működési elvéből, és rendeltetésszerű használatából könnyen levezethető, hogy ezen modelleknek illetve a kapcsolt más szoftvereknek pontosan az adatok létrehozása, kezelése a céljuk. Azonban, ha a digitális szolgáltatás alatt az adatok létrehozását, és kezelését értjük, míg digitális tartalom alatt az adatok digitális úton történő rendelkezésre bocsátást, akkor ha a digitális szolgáltatáskor az adatok a fogyasztó számára tartósan hozzáférhetővé válnak - letöltheti például -, úgy a két fogalom átfedésbe kerül. Ez esetben a megkülönböztetést úgy tudjuk megtenni, ha a tartalom nem letölthető a fogyasztó eszközére, hanem újra és újra le kell hívni a szolgáltató szerveréről, úgy digitális szolgáltatásról

beszélünk.²⁹ A GPT esetében pedig ez azért lehet speciális, mert az általunk vizsgált speciális esetben kérdéses, hogy a tartós hozzáférhetőség biztosítva lehet-e, ezért inkább érdemes a digitális szolgáltatás felől megközelíteni. Ezen szolgáltatásokat (MI-modelleket) pedig az OpenAI a szerződéskötést követően késedelem nélkül nyújtja, ez a Trust esetében is megvalósul, vagyis a regisztrációt követően rögtön használható az applikáció.. Ám ha azt a fordulatot elemezzük, miszerint „a szerződéskötéskor rendelkezésre álló legfrissebb verzióban” köteles nyújtani a digitális szolgáltatást, egy másfajta problémakörhöz érünk. Ami a Trust esetében speciális esetet teremt, hiszen az MI-t bár az OpenAI fejleszti, a blokkláncon történő műveletek, tranzakciók végrehajtásához mégis egy módosított, finomhangolt modellre van szükség. Ezen speciális, finomhangolt modelleket pedig az OpenAI nem frissíti automatikusan, ezért a frissítést a DApps Platform Inc.-nek külön kérnie kell. Tehát a Trust minden egyes frissítés kiadásakor köteles új, frissített modellt használni, és azt nyújtani tovább a végfelhasználóknak. Amennyiben ezt elmulasztja, úgy a teljesítés nem lehet szerződésszerű. Ahogyan a Korm. rendelet 21.§-a kimondja, a 17. § (1) bekezdésben foglalt kötelezettségek elmulasztásáért a vállalkozás felel, illetőleg a vállalkozást terheli annak bizonyítása, hogy az általa nyújtott szolgáltatás megfelel-e az említett szakasznak. Továbbá a 17. § (3) bekezdése szerint a vállalkozásnak biztosítani kell, hogy a fogyasztó a frissítéseket, különösen a biztonsági frissítéseket megkapja. A Korm. rendelet 17. § (4) bekezdés a) pontja szerint a fenti kötelezettségnek a vállalkozás a szerződés időtartama alatt köteles eleget tenni.

A frissítés kérdéskörén túl a Korm. rendelet egy további rendelkezése szerint is vizsgálhatjuk a hibás teljesítés esetét, ami leginkább a minőségre, teljesítményre és biztonságra koncentrál. A Korm. rendelet 5. § (3) bekezdésének b) pontja tartalmazza, hogy a szerződés tárgyát képző szolgáltatásnak rendelkeznie kell a fogyasztó által ésszerűen elvárható azon mennyiséggel, minőséggel, teljesítménnyel és egyéb jellemzőkkel, amely azonos típusú szolgáltatás szerint szokásos. Ez a rendelkezés szintén fontos lehet annak vizsgálatakor, hogy a hibás, károkozó kimenet vajon hibás teljesítésként értelmezhető-e. Azt gondolom, hogy jelen példában, vagyis a blokkláncon tranzakciókat elvégző MI-esetében mint minőségi, teljesítménybeli és biztonsági kritériumok terén is az AI Act rendelkezéseit kell alapul venni. Amennyiben a GPT 4o modellen gondolkodunk, azt el kell helyezni az AI Act által meghatározott kategóriák egyikében, amely alapján a GPT 4o modell tekintettel arra, hogy

²⁹ Vö. https://www.gesetze-im-internet.de/bgb/_327.html; Thomas Riehm, Verträge über digitale Dienstleistungen, in: Martin Schmidt-Kessel, Christina Möllnitz (szerk.) Grundfragen des Digitalvertragsrechts, Mohr Siebeck, Tübingen, 2022, 4.-5. o.

jelenleg a legmodernebb általános generatív modellnek tekinthető, továbbá a modell által a tanítás során elvégzett lebegőpontos műveletek száma meghaladja az AI Act által meghatározott küszöbértéket³⁰ rendszerszintű kockázatot jelentő általános modellnek vehető. Tehát ez a modell nagyhatású képességekkel rendelkezik, vagyis egy rendkívül nagy teljesítményű, továbbá a modell zárt forráskódú voltából adódóan pedig alapvetően biztonságos generatív modellnek tekinthető. Úgy gondolom a példába szereplő felhasználás magas szintű nyelvi képességeket kíván meg, ami azt jelenti, hogy teljesítményt, mint a rendelet 5.§ (3) bekezdése b) pontjának egyik kritériumát tekintve leginkább egy nagy hatású képességgel rendelkező modell alkalmas azt elvégezni. Ami pedig a minőségi kritériumokat illeti, úgy gondolom leginkább a Trust által finomhangoláshoz használt – jellemzően kisebb – tanulóadatmennyiség minőségére, továbbá az előtanítás során alkalmazott – jellemzően óriási – tanulóadatmennyiség minőségére vonatkoztatható. Az azonban akadályt jelenthet ezek vizsgálata esetén, hogy mind a finomhangolásra, mind a modell előtanítására használt tanulóadatmennyiség összehasonlítható kell, hogy legyen más, hasonló MI felhasználások tanulóadatbázisával. Azonban rendkívül fontos, hogy alapjában ha csak a GPT 4o modellt vesszük alapul, akkor minden egyes fogyasztó, API-felhasználó és egyéb alkalmazó ugyanolyan előtanításon átesett modellt használ, ezért az előtanítás szempontjából ezek egymással való összehasonlítása értelmetlen. Más gyártó modelljeinek tanulóadatai sem hasonlíthatók a GPT előtanítási adataival, más modellek a GPT-hez képest némiképp eltérő felépítése, és működése miatt. Így a minőségi kritérium esetében, leginkább a finomhangoláshoz szükséges kisebb adathalmazra kell koncentrálni, ahol is több hasonló MI felhasználás során használt tanulóadatmennyiséget vethetünk össze egymással.

Amennyiben pedig a fentiek alapján azt találjuk, hogy egy Trust szintű generatív MI felhasználás nem nagyhatású képességgel rendelkező modellt alkalmaz, arra a célra, hogy képes legyen akár a finom nyelvi, megfogalmazásbeli árnyalatokat is értelmezni, úgy akár nem megfelelő teljesítményű modell alkalmazásáról beszélhetünk. Továbbá ha a finomhangoláshoz használt adatok minősége és mennyisége nem megfelelő, a többi hasonló MI alkalmazáshoz használt tanulóadatok minőségi és mennyiségi tulajdonságaitól elmarad, úgy a minőségi kritériumok megsértése miatt beszélhetünk nem megfelelő teljesítésről.

Azonban a Korm. rendelet 18. § (2) szerint, nem állapítható meg hibás teljesítés, ha a szerződés megkötésekor a fogyasztó külön tájékoztatást kapott arról, hogy a digitális

³⁰ Lásd: Függelék: 7. pont

tartalom vagy szolgáltatás valamely konkrét tulajdonsága eltér az 5. § (3) bekezdésben meghatározott valamely követelménytől, és a szerződés megkötésekor ezt a fogyasztó külön, kifejezetten elfogadta. A kifejezett elfogadás pedig, másfajta gyakorlatot követel meg a DApps Platform Inc.-től, mivel ezideáig a szerződés elfogadása a szolgáltatáshoz való hozzáféréssel és használattal valósul meg. Azonban, akár arról tartalmaz külön rendelkezést a szerződés, hogy a modell nem rendelkezik kellően nagy teljesítménnyel, vagy akár nem a más alkalmazások által használt minőségű és mennyiségű tanulóadatbázist használ a modell finomhangolására, külön fel kell hívnia rá a felhasználók figyelmét. Ez azt a problémát is maga után vonja, hogy akár olyan kockázatokat is hordozhat a rendszer, amelyek bár a külön tájékoztatás és a kifejezett elfogadás esetén Korm. rendelet szerint nem tekinthetők hibás teljesítésnek, de az AI Act gyakorlati kódexének egyes rendelkezéseibe ütközhetnek, mint például bizonyos kockázatok felmérésére és kockázatok kiküszöbölésére vonatkozó kötelezettségek. Amelyekhez szükséges bizonyos minőségi és teljesítménybeli kritériumoknak való megfelelés, bár jelenleg ezen részletes szabályok még kidolgozás alatt vannak.³¹ Ehhez segít mindkét félnek, akár a fogyasztónak a külön rendelkezések értelmezéséhez, és a vállalkozásnak az AI Act általi követelmények és más vonatkozó jogszabályok általi követelményeknek való megfeleléshez, azon törekvés, amely arra irányul, hogy megfelelő tájékoztatást kapjon minden szereplő az AI-ra vonatkozó uniós szabályokról, és az annak való megfelelésről.³²

2.3. A SZERZŐDÉSSZEGÉS

A Ptk. 6:137. § szerint a szerződésszegés bármely kötelezettség szerződésszerű teljesítésének elmaradása. Ez történhet a szerződésből fakadó valamely főkötelezettségnek vagy mellékkötelezettségnek a megszegésével. Amennyiben a szerződésszegés oka emberi magatartás akkor az megvalósulhat tevőleges magatartással vagy mulasztással.³³ A szerződésszegés tehát akkor áll fenn, ha a teljesítés a szerződés tartalmának valamilyen módon

³¹ European Commission, AI Pact, 2024. december 3., <https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice> (Online, letöltve: 2024.12.09.)

³² European Commission, General-Purpose AI Code of Practice, 2024. november 21., <https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice> (Online, letöltve: 2024.12.09.)

³³ Fuglinszky Ádám, Kártérítési Jog, HvgOrac Kiadó, Budapest, 2015., 101. o.

nem felel meg. A szerződés tartalmát jelenti a felek megállapodása, a kógens jogszabályok, illetve – eltérő rendelkezés hiányában – a diszpozitív jogszabályok is.³⁴

A probléma viszont akkor következik be, ha azt vizsgáljuk, hogy bár a károkozás megtörténik, ugyanakkor sem

(1) minőségi azaz tanulóadatokat tekintve, sem

(2) teljesítménybéli, sem

(3) biztonsági téren

nem lehet jelentős különbséget találni a modell és más hasonló felhasználású modell között, figyelembe véve, hogy a legfrissebb verziót használja. Ekkor ugyanis a bizonyítási eljárásnak - akár a fenti szempontok alapján - érintenie kell az MI-rendszer „belső működését”, hiszen ha az MI-t körbevevő intézkedésekben nem találunk lényeges hibát, akkor magát a rendszert kell elkezdünk vizsgálni. Hiszen ha a rendszeren kívüli, azt leíró intézkedések és tulajdonságok terén nem tudunk érdemi hibát feltárni, akkor a tervezési és működési hibákat kell elkezdenünk vizsgálni, amik szintén kimeríthetik az előbbi három kategóriát, azonban sokkal nehezebb, ha egyáltalán lehetséges ezen hibákat felismerni, a rendszer bonyolultságából, zártságából adódóan.

2.4. BIZONYÍTÁSI KÉRDÉSEK A SZERZŐDÉSSZEGÉSSSEL OKOZOTT KÁRRÁ VONATKOZÓAN

2.4.1. A FELEK KÖZÖTTI SZERZŐDÉS TÍPUSÁNAK VIZSGÁLATA

A kapcsolódó szolgáltatás nem más, mint olyan termékbe épített technológiai megoldás, mellyel adatokat hozhatunk létre, illetve magunk vagy más személy által létrehozott adatokon végezhetünk bármilyen műveletet. A német polgári törvénykönyv (Bürgerliches Gesetzbuch; BGB) 327.§ 1. bevezető rendelkezése, amelyet azon fogyasztói szerződésekre kell alkalmazni, amelynek tárgya digitális tartalom vagy digitális szolgáltatás, kimondja, hogy a digitális

³⁴ Csehi Zoltán (szerk.), 2013. évi V. Törvény A Polgári Törvénykönyvről Kommentárja, Magyar Közlöny Lap- és Könyvkiadó Kft., Budapest, 2021, XXII. Fejezet, Bársony Eszter, A szerződésszegés, 1557.-1558. o.

szolgáltatásokat és digitális tartalmakat egyenrangúnak kell tekinteni, vagyis mindkettőt digitális termék kategóriájába sorolja.³⁵ Azonban a Trust és a GPT esetét a digitális szolgáltatás felől közelítettük. Thomas Riehm kiemeli, hogy a digitális szolgáltatásokra vonatkozó szerződések sokfélesége miatt nem lehet ezen szerződéstípusokat egységesen osztályozni, ezért vegyes típusú szerződésnek tekinti, mivel több szerződés típus elemei megjelennek benne.³⁶

Ugyanakkor a digitális szolgáltatások központi eleme jellemzően a szerver-infrastruktúra rendelkezésre állásának és fenntartásának a kötelezettsége, amely leginkább a „szolgáltatási szerződések” körébe sorolható, hiszen ez a szerződés időtartama alatt a saját teljesítési készség fenntartását és a szolgáltatásra jogosult fél utasítására a szerződésben vállalt tevékenység elvégzését tartalmazza. A digitális szolgáltatásokra vonatkozó szerződés ez alapján az orvosi és a ügyvédi tanácsadói szerződéshez hasonlítható, vagyis a tevékenységen túl, további sikerrel nem tartozik, amelyeket a szerződő fél garantál. Ami viszont elvárható a féltől, az az objektív, ellenőrizhető tevékenység elvégzése.³⁷ Összegzőként elmondható, hogy az irányelv német implementációja azzal a következménnyel járt, hogy a digitális szolgáltatások vonatkozásában a hibás teljesítés jogkövetkezményei akkor is alkalmazandók, ha egyébként a felek jogviszonya a szolgáltatási szerződés típusához áll a legközelebb.

Azt a kérdéskört, hogy az adós a szolgáltatási cselekménnyel vagy szolgáltatás eredménnyel tartozik-e, Szászy István is vizsgálta: az adóstól csak a tőle telhető eredmény kifejtését várhatjuk el, annak érdekében, hogy a szolgáltatás célja elérhető legyen, vagy pedig a cél valós elérését. Szászy szerint alapvetően az adós a szolgáltatási eredménnyel tartozik. Kivételként említi viszont, a rendkívüli- és tömegjelenségeket, amelyek indokolhatják, hogy az adós mentesüljön, amennyiben minden tőle telhetőt megtett az eredmény előállításáért.³⁸

Mindebből, illetve az előzőekben – a felelősség kizáró és korlátozó kikötések alfejezetben – tárgyalta szerződési feltételek ismeretében kijelenthetjük, hogy alapvetően szolgáltatási kötelemről beszélhetünk, amely a hazai jogban a megbízási típusú azaz a gondossági kötelemként sorolható be. E szerint a kimenet mint eredmény „sikeréért” vagyis a kimenet helyességéért a szolgáltató nem tartozik felelősséggel, kizárólag a szerver-infrastruktúra elérhetővé tételéért és folyamatos biztosításáért. Az irányelv magyar átültetése

³⁵ Riehm, i.m. 4.-5. o.

³⁶ Riehm, i.m. 5.-6. o.

³⁷ Riehm, i.m. 12.-13. o.

³⁸ Szászy István, A kötelmi jog általános tanai, Grill Károly Könyvkiadóvállalata, Budapest, 1943., 51.-52. o.

során konkrét jogszabályi rendelkezés híján egyértelmű tisztázást nem nyert, hogy a kötelezett felelőssége ilyen gondossági kötelemények esetében nem terjedne-e ki a kimenet hibája miatt a hibás teljesítésért való helytállásra. Viszont az irányelv maximumharmonizációt célzó rendelkezéseit csorbító értelmezés lenne, ha ezt a megoldást követnénk. Ugyanígy megkövetelhetjük a kötelezettől a szolgáltatás célja elérése érdekében elvárható gondos magatartás tanúsítását, ahogy a megbízott sem jogosult a díjazásra, ha az eredmény részben vagy egészben a felróható magatartása miatt maradt el.³⁹ Ebben az értelemben, mivel gondossági kötelemről beszélünk, úgy a szerződés szerű teljesítés a feladat gondos ellátását foglalja magában, így a nem szerződés szerű teljesítés a „nem gondos” eljárással egyenlő.⁴⁰

2.4.2. AZ ELVÁRHATÓ GONDOSSÁG HIÁNYÁNAK VIZSGÁLATA

Úgy gondolom, minden olyan magatartás elvárható, amely a technika jelen állása szerint megvalósítható, vagy akár az AI Act, továbbá a 373/2021 Korm. rendelt vagy más jogszabályok előírják, illetve az adott szakterületen bevett gyakorlatok, melyek ismertek és alkalmasak az adott hibás kimenet korrigálására, enyhítésére. A Trust mint API-felhasználó esetében többek között elvárható, hogy az AI Act 55. cikkében szereplő korrigáló, enyhítő és megelőző intézkedéseket tegyen.⁴¹ Továbbá a Korm. rendelet 17.§-ban található friss verzió kritériumának, ezzel együtt az 5. § 3) bekezdésében támasztott minőségi, teljesítménybeli és biztonsági kritériumoknak eleget tegyen. A probléma akkor merül fel, ha mindezen intézkedések ellenére is bekövetkezik a károkozás, tekintettel a modell megfelelő teljesítményére, továbbá ha a tanulóadatbázis minőségéről és mennyiségéről nem állapítható meg egyértelműen annak elégtelensége. Ebben az esetben pedig a felperesnek, azaz a károsultnak azt kellene bizonyítania, hogy egyrészt ilyen károkozás már egyszer megtörtént, hogy vizsgálható legyen a megfelelő korrekciós intézkedések esetleges elmaradása. Mivel mind a GPT modell, mind a hozzá kapcsolt, a kimeneteket ellenőrző és módostó moderátor MI zárt

³⁹ Vö. Ptk. 6:276. § (1) bekezdés.

⁴⁰ Leszkoven László: Szerződészegés a polgári jogban. 2. kiadás, Wolters Kluwer, Budapest, 2018, 81–82. o.

⁴¹ Lásd. Függelék 8. pont

forráskódú, továbbá rendkívül komplex és átláthatatlan generatív rendszerek, a megfelelő korrekciós intézkedés gyorsan megfoghatatlan fogalommal halványul. Azért lesz a definíció megfoghatatlan, mivel azt várjuk el, hogy a korrekciós intézkedés, és az enyhítés nagymértékben csökkentse, vagy szüntesse meg az adott hiba előfordulásának valószínűségét. Azonban az, hogy mely intézkedések milyen mértékben képesek csökkenteni vagy megszüntetni az adott hibás kimenetek generálásának esélyét, előre beláthatatlan. Mivel a moderálás is tartalmazhat hibát, például hibás kimeneteket engedhet át, vagy akár hibás információval egészíti ki a kimenetet, vagy helyes információt szűr ki. Az elvárható gondosság ugyanakkor nem szűkíthető le kizárólag a jogszabály betartására, mivel a hiba szüntelen fennállása miatt, kárigények maradhatnak kielégítetlenül. Ez rendkívül negatív hatással járna a károsultakra. Ha pedig túlterjeszkedünk a jogszabályi kritériumokon, rendkívüli technikai nehézséggel állunk szembe, hiszen nem tudjuk megállapítani, mely intézkedések milyen mértékben segítettek vagy rontottak volna a helyzeten, a modell komplexitása és átláthatatlansága miatt.

2.4.3. AZ OKOZATOSSÁG ÉS ELŐRELÁTHATÓSÁG VIZSGÁLATA

Az ok-okozati összefüggés vizsgálata során egyrészt a *conditio sine qua non* kritériuma szerint kell eljárni, amely a természettudományos okozatosságot jelenti, vagyis minden előzmény okozatos, mely nélkül a kár nem következett volna be, ez azonban különbözik a jogi okozatosságtól. Ezért második lépésben okszűrő szempontokat kell alkalmazni, vagyis meg kell állapítani a felsorolt, tényszerű okok közül melyek játszanak jelentősebb szerepet a felelősség megállapításában. Ilyen okszűrő szempont lehet az általános élettapasztalat; a szokásos, rendszerinti következmény; tipikus, életszerű következmény; és a szerves kapcsolat. Végül pedig a több azonosított és relevanciával rendelkező okok egymáshoz való súlyát kell megállapítani.⁴²

Másrészt pedig, az okozatosságon alapuló felelősség megállapítást ésszerű módon korlátozni is szükséges, melyet az előreláthatósági korláttal ér el a jog. A magyar bírói gyakorlat továbbra is vizsgálja az okozatosságot, illetve az előreláthatóságot.⁴³ Így a két szempont

⁴² Fuglinszky, i.m., 2015., 244.-250. o.

⁴³ Fuglinszky, i.m. 2015., 109.-110. o.

egyfajta kettős védelmi mechanizmust lát el, vagyis az okozatosság vizsgálata kiszűri az alaptalan túlzó igényeket, ezen belül pedig az előreláthatóság alapján megállapítható mely károkat kell, illetve nem kell megtérítenie a károkozónak. Az okozatosság kapcsán, lényeges megvizsgálni, hogy az okfolyamatba nem ékelődött-e be semmilyen lényeges mozzanat, amely az oksági láncot megszakítaná.⁴⁴

A *conditio-sine-qua-non* szerint azon előzményeket kell számbavenni, amelyeket oknak tekinthetünk. Egy generatív MI esetében a ténybeli okok a következők lehetnek:

- Egy generatív nagy nyelvi modell több százmilliárd paraméterből áll, a modell paramétereit tartalmazhatják a hibát, azonban ennek megismerése rendkívüli nehézséget okoz.
- A tanulódatok adathibái is előidézhettek bizonyos hibás kimeneteket, azonban ezen hibák visszakövetése a tanulási időszakban sem mindig vezet vissza az adatsorra, így ezen hibák okai rejtve maradhatnak.
- A moderátori rendszerek célja, hogy a modell kimeneteit pontosítsák, javítsák, viszont a moderátori rendszerek is statisztikai, gépi tanulási alapon működnek így a kimenetekre gyakorolt hatásai gyakran kiszámíthatatlanok.

Természetesen ez csak néhány a felmerülő okok közül. Ezen okokat ún. okszűrők alkalmazásával ki kellene szűrni, vagyis azon okokat kivenni a vizsgálat alól, amelyek nem játszhattak jelentős szerepet a következményben, azaz a kár bekövetkeztében. Ekkor érkezünk el a nagy dilemmához, mivel a jelenleg alkalmazott okszűrő szempontok nem működnek. Tegyük egy próbát. Azt kell az okszűrő szempontokkal megállapítani, hogy melyik ténybeli ok nem játszott jelentős szerepet a hibás kimenet generálásába. Az első okszűrő szempont amit vizsgálunk, az a szokásos rendszerinti következmény. Ez annak a vizsgálatát jelenti, hogy a kár a károkozó magatartás szokásos, rendszerinti következménye-e. Ez annyit jelent, hogy az ok, az események rendszerinti lefolyása mellett alkalmas-e az eredmény létrehozására. Ennek vizsgálatakor azonban, olyan problémába sodródunk mely jó eséllyel azt eredményezi, hogy mindhárom előzményből levezethető a következmény külön-külön. Ezen előzmények további szűréséhez pedig, különleges, speciális technikai vizsgálatra van szükség, amely nem bizonyos hogy a technika jelen állása szerint megvalósítható.

Ha pedig a szerves kapcsolatot mint okszűrő szempontot vesszük figyelembe, amely az előzmény és a következmény közötti szerves kapcsolatot követeli meg, vagyis az okfolyamatba

⁴⁴ Fuglinszky, i.m. 2015., 109.-110. o.

nem szabad beékelődnie olyan lényeges mozzanatnak, amely miatt a vizsgált károkozó magatartás relevanciája csökken. Ekkor a vizsgálat megállapíthatja, hogy olyan részfolyamatok játszanak közre mindhárom ténybeli ok esetében, melynek kihatása megismerhetetlen a rendszer komplexitásából adódóan.

Egyrészt nem rendelkezünk elegendő technikai információval az említett előzményekről, másrészt, ha rendelkeznénk is speciális szakértelemre lenne szükség, azonban még speciális szakértelem és információk birtokában sem bizonyos, hogy ezen okokat képesek lennénk szűrni, hiszen nem rendelkezünk jelenleg a szükséges technikai felkészültséggel. Ennek oka, az MI-rendszer statisztikai jellege, nagyfokú komplexitása, és nem determinisztikus működése. Ha ezen okokat kvázi szűretlenül vinnénk tovább, vagyis feltételeznénk, hogy egyenlő súlyt képviselnek a kár bekövetkeztében, akkor a következő vizsgálati szempont szintén nem lenne megoldható, vagyis az okok egymáshoz való viszonyának megítélése újfent lehetetlen az MI-rendszer természetéből adódóan. Tehát a rendszer zártóságából és komplexitásából adódóan lehetetlennek, vagy legalább rendkívül nehéznek bizonyul a következményhez vezető ok vagy okok megtalálása.

Továbbá úgy gondolom, az előreláthatóság, mint követelmény sem értelmezhető a generatív rendszerek viszonylatában, mivel a rendszer által a jövőben generált konkrét kimenetek, a szolgáltató előtt is rejtve maradnak, illetve mint említettem a moderátor rendszer is bizonyos hatást képes gyakorolni a kimenetre, amely előre megjósolhatatlan, mind a szerződéskötés időpontjában mind utána. Ezekből tisztán látszik, hogy a kontraktuális felelősségre vonatkozó vizsgálatkor olyan nehézségekbe ütközünk, amelyek az igényérvényesítést nemhogy megnehezítik, de el is lehetetlenítik.

2.5. A KÁR BIZONYÍTÁSA

Azt gondolom, a kár bizonyítása okoz a legkevesebb gondot, hiszen a tranzakció káros kimenetét kell visszakövetni, egészen az MI kimenetéig, vagy pusztán az MI-parancssorát megvizsgálni, és feltárni annak hiányosságai, hibáit. Például, ha olyan kérést intézünk az MI felé, hogy vegyen X mennyiségű Bitcoin-t a legjobb áron, akkor ha a parancssorban nem szerepel arra vonatkozó utasítás, hogy a szoftverek a legjobb áron hajtsák végre a tranzakciót, és ez jelentős többletköltséggel járt a fogyasztónak, úgy természetesen kárról beszélhetünk, és a szükséges dokumentumokkal, naplókkal és egyéb információkkal bizonyítható. Nyilvánvalóan utánajárást igényel, de megvalósítható ennek bizonyítása. Mivel a jogosult

vagyonában következik be kár, így következménykárrol beszélhetünk, vagyis a Ptk. 143. § 2) bekezdése lép életbe, ezzel pedig ez előreláthatósági korlát.

A Ptk. 6:143. § (2) bekezdése rendelkezik a kártérítés mértékéről szerződésszegés esetén, a következőképpen: *„A szerződésszegés következményeként a jogosult vagyonában keletkezett egyéb károkat és az elmaradt vagyoni előnyt olyan mértékben kell megtéríteni, amilyen mértékben a jogosult bizonyítja, hogy a kár mint a szerződésszegés lehetséges következménye a szerződés megkötésének időpontjában előre látható volt.”* Azt gondolom, nem kell messzire menni ahhoz, hogy az eddig tárgyaltak alapján belássuk, a szerződéskötés időpontjában a konkrét károkozás nem volt előrelátható, semmilyen mértékben, tehát a jogosult az előreláthatóságot nem képes bizonyítani, így pedig nem illeti meg kártérítés kontraktuális alapon. Hiszen dacára az AI Act által megkövetelt kötelezettségeknek, illetve az önként vállalt kötelezettségeknek, a gyártó avagy vállalkozás ha előre is láthatta - valamilyen módon - a hibát, az erről szóló dokumentációkat, méréseket, és naplókat nem köteles a kontraktuális felelősség alapján kiadni a fogyasztónak, amennyiben pedig valahogy mégis a fogyasztóhoz kerülnek ezen dokumentumok, úgy rendkívüli tudományos és technikai nehézséggel áll szemben, ha azokat fel kívánja dolgozni. Továbbá, a kontraktuális alapon történő kártérítés mértékének megállapításához lényeges, hogy figyelembe vegyük a szerződésben kikötött felelősségkizáró- vagy korlátozó kikötéseket. Amelyeket ha nem sikerül semmissé tenni, a fentebb említett módon, úgy szintén nem illeti meg kártérítés a fogyasztót, az őt ért kár esetén.

2.6. A KONTRAKTUÁLIS FELELŐSSÉGI VIZSGÁLAT ÖSSZEGZÉSE

Ebben a részben megállapítottuk, hogy amennyiben a Trust GPT modellt használ, úgy eleget kell tennie bizonyos minőségi, teljesítményre vonatkozó, és biztonsági követelménynek, amely alapulhat mind az AI Act gyakorlati szabályain, mind a Korm. rendelet rendelkezésein. Azonban azt is megvizsgáltuk, hogy ha valamely kritérium sérül, úgy hibás teljesítésről beszélhetünk, azonban ezen kritériumok sérelme nem feltétlen „jól látható” helyen jelenik meg, úgy mint a finomhangolásra használt adatok egyértelmű hibája, vagy egy gyengébb modell használata. Mindez azt mutatja, hogy bizonyos körülmények között vizsgálat akár az MI-modell belső vizsgálatát is megkívánhatja, amely rendkívüli módon bonyolulttá teheti a bizonyítást. Ezt tovább erősítendő, a felek közötti szerződés gondossági típusú, vagyis az

elvárható gondosság hiányát, az okozatosságot és előreláthatóságot kell bizonyítani, amelyek bizonyítása szintén a modellen belülré mutathat. Ez pedig úgy kezelhetjük, hogy mintegy lehetetlenné teszi a szerződésszegés gondosságon alapuló bizonyítását.

3. *A TERMÉKFELELŐSSÉGI VIZSGÁLAT*

A termékfelelősségi vizsgálatot az Európai Parlament és a Tanács (EU) 2024/2853 irányelve⁴⁵ (továbbiakban: termékfelelősségi irányelv) alapján fogom elemezni. A 2024. október 23-án elfogadott új irányelv átültetését a tagállamoknak 2026. december 9-ig kell végrehajtaniuk, ezért láttam szükségesnek, hogy a felmerült kártérítési kérdést előre tekintve, már az új irányelv tükrében vizsgáljam. Az előző fejezethez hasonlóan, a hipotézisem bizonyítása céljából, az alábbiakban is arra keresek válaszokat, vajon a termékfelelősségi irányelv szerint lehetséges-e igényt érvényesíteni a példában meghatározott esetben.

3.1. *A GPT MINT TERMÉK*

A termékfelelősségi irányelv a termék fogalmát – az eddigi szabályoktól eltérően – kiterjeszti a szoftverekre is, azonban ki kell térnünk rá, hogy a magyar jogban is felmerült a szoftver mint termék megítélése, különösen a robotok és hasonló alkalmazás során ún. „tárgyasult szellemi termékek” megjelenése kapcsán.⁴⁶ Az új definíció az irányelv 4. cikkének 1. pontja szerint így hangzik: *„minden ingó dolog, abban az esetben is, ha azt egy másik ingó dologba vagy ingatlanba építették be, vagy ha az egy másik ingó dologhoz vagy ingatlanhoz kapcsolódik; a „termék” magában foglalja a villamos energiát, a digitális gyártási fájlokat, a nyersanyagokat és szoftvereket;”* Láthatjuk, hogy a villamos energia mellé a digitális gyártási fájlokat és a szoftvereket is beemelte az uniós jogalkotó, azonban a dolgozat témáját adó nagy

⁴⁵ Az Európai Parlament és a Tanács (EU) 2024/2853 irányelve (2024. október 23.) a hibástermékekért való felelősségről és a 85/374/EGK tanácsi irányelv hatályon kívül helyezéséről. *OJ L*, 2024/2853, 18.11.2024, ELI: <http://data.europa.eu/eli/dir/2024/2853/oj>.

⁴⁶ Fazekas Zoltán József, 4. fejezet: A szerződésszegéssel okozott károkért való felelősség, 182. o. in Barta Judit, Barzó Tímea, Csák Csilla (szerk.) *Magyarázat a Kártérítési jogról*, Wolters Kluwer Hungary Kft., Budapest, 2018.

nyelvi modellek nem minden esetben önálló, a fogyasztó eszközén futó – termékként – szoftverként jelennek meg, így szükség lesz némileg árnyalni a képet. Az egyszerűség kedvéért ebben a részben csupán a GPT modellre fogom értelmezni a termék fenti fogalmát, mivel egyrészt maga a dApp, mint például a Trust egyértelműen terméknek tekinthető, hiszen a felhasználó eszközén futó szoftverről beszélünk, másrészt a témánk bár érinti a blokkláncot, ennek termékfelelősségi értékelése nem játszik fontos szerepet, ezért ettől eltekintek.

Maga a GPT modell egy szoftvernek tekinthető, azonban tudjuk, hogy a GPT nem különálló szoftverként használható, hanem egy szoftver- és hardverrendszer részeként. Hiszen nem a felhasználó eszközén fut, hanem egy felhőn, továbbá különböző API szoftvereken, avagy közvetítőkön keresztül érhető el a felhasználó számára. Ezért a termék definíciója mellé segítségül kell hívnunk a termékfelelősségi irányelv (13) preambulumbekzdését. Amely egyértelműen kimondja, hogy akkor is terméknek minősül a szoftver, amennyiben egy felhőn keresztül érhető el, illetőleg beépítették más termékbe alkotóelemként. Ezek alapján a GPT egy termék, amely alkotóelemként kerül beépítésre a Trust-ba mint applikáció, vagyis a felhasználói felületbe kerül beépítésre.

3.2. A TERMÉKHIBA MEGHATÁROZÁSA

Le kell szögezni, hogy a generatív MI-rendszerek esetében leginkább tervezési hibákról beszélhetünk mintsem gyártási hibákról. Mivel az MI-rendszerek rendkívül komplex algoritmusokat tartalmaznak, amelyek tervezése számos tényezőt foglal magába. Mint például képzési adatokat, modell architektúrát, tanulási algoritmusokat, és döntéshozatali szabályokat. Míg a gyártás szabványosított szoftver- és hardverkomponensek másolását és telepítését foglalja magában, ezeket azonban ellenőrzött környezetben végzik, aminek köszönhetően a hibák többsége nem a gyártásból adódik, mint például hibás összeszerelés, vagy az alkatrészek meghibásodása. Ebből következik, hogy az MI-rendszerek pedig rendkívüli mértékben támaszkodnak a szoftverkomponensekre, az ezt érő tervezési hibák bizonyítása pedig rendkívüli terhet róhat a felperesekre.⁴⁷ Ezért a termék hiba meghatározásakor a tervezési hibákra kell leginkább összpontosítani, ha a hiba egyes aspektusaira kívánunk kitérni.

⁴⁷ Miriam C. Buiten, Product Liability of defective AI, European Journal of Law and Economics, (2024) 57, 239–273, 2024.02.27. 257.-258. o.

A termékfelelősségi irányelv 7. cikkének (1) bekezdése szerint a termék akkor hibás, ha nem nyújtja a bárki által jogosan elvárható biztonságot. A cikk (2) bekezdése felsorolja azon kritériumokat⁴⁸, amelyeket figyelembe kell venni ennek megítélésakor, így többek között⁴⁹:

- a termék ésszerűen előrelátható használata,
- a vonatkozó termékbiztonsági követelmények,
- az az időpont, amikor a terméket forgalomba hozták, vagy használatba vették, vagy amennyiben a gyártó ez időpont után is megőrzi a termék feletti ellenőrzést, illetve az az időpont, amikor a termék kikerült a gyártó ellenőrzése alól.

A termék ésszerűen előrelátható használata, úgy gondolom a termék azon felhasználására vonatkozik, amelyek annak a célnak az elérésére törekednek, amelyekre a terméket a gyártója szánta. Ez esetben a Trust alkalmazásába épített GPT egyértelműen azt a célt hivatott szolgálni, hogy meghatározott blokkláncon, meghatározott tranzakciókat segítsen elvégezni, legyen az eladás, vétel, átváltás és egyéb. Az ésszerűen előrelátható használat értelemszerűen ezen célok elérésére történő használatot foglal magában. Ez egyrészt a gyártó felelőssége, hiszen neki biztosítania kell a termék olyan minőségét, és biztonságát amely képessé teszi a rendeltetésére történő használatra. Másrészt pedig a fogyasztó felelőssége, mivel köteles a terméket ésszerűen előreláthatóan, a rendeltetésének, céljának megfelelően használni. Azt gondolom, egy hibás, károkozó kimenet bekövetkeztekor, a fogyasztó által adott bemenetet könnyedén lehet értékelni aszerint, hogy a rendeltetésnek megfelelő célt kívánt-e elérni vagy sem. Azonban ha a válasz igen, akkor viszont a terméket további vizsgálatoknak kell alávetni, hiszen minden bizonnyal termékhibáról lehet szó. Éppen ezért rátérhetünk a termékbiztonsági követelményekre.

A termékbiztonsági követelmények esetében pedig az AI Act rendelkezései lesznek segítségünkre. Az általam vizsgált MI-alkalmazás viszont, még a modell finomhangolással történő módosítása ellenére sem sorolható a nagy kockázatú kategóriába. Így továbbra is az AI Act 55. cikke⁵⁰ vonatkozik rá. Eszerint a modell működését a szolgáltatónak folyamatosan figyelnie és dokumentálnia kell. A felmerülő rendszerszintű kockázatokat értékelniük és

⁴⁹Tekintettel arra, hogy több szempontot is felsorol a termékfelelősségi irányelv, igyekeztem azokat kiválogatni amelyek a leginkább fontosak jelen témában, ezért kihagytam több olyan, a témát tekintve nem releváns szempontot, mint például a csomagolásra vonatkozó kikötések.

⁵⁰ Lásd. Függelék 8. pont

enyhíteniük kell, továbbá megfelelő kiberbiztonsági intézkedéseket kell tenniük annak érdekében, hogy a rendszert ne érhesse támadás. Ezeknek egy részéért természetesen az OpenAI mint gyártó a felelős, úgy mint a kiberbiztonság követelményének való megfelelés. Azonban az enyhítés és korrigálás ez esetben, ha a Trust mint API-felhasználó nyújtja a szolgáltatást, azt fogja jelenteni, hogy a szükséges frissítéseket kellően elvégezte. Amennyiben pedig indokoltnak látszik, akár a tanulóadatbázis minőségén javítani és újra tanítani a modellt, továbbá más beállításokon használni. Ezeken kívül a Trust-nak kötelezettsége még naplót vezetni a tartalomról, azaz a bemenetről és a modell kimenteiről, úgy mint a fogyasztónak elküldött válasz, és a blokklánc felé továbbított parancsok. Szükséges esetén pedig ezeket értékelnie és felülvizsgálnia kell. Amennyiben hibát tapasztal, úgy az AI Act szerint reagálnia kell rá, vagyis korrigáló, enyhítő intézkedéseket kell tennie. Azt gondolom ez mind a termékbiztonság körébe beleérthető, amennyiben ezeket elmulasztja, úgy hibás termékről beszélhetünk.

A gyártó ellenőrzése alól való kikerülés időpontja lesz számunkra érdekes, mivel a finomhangolás eleve a modell gyártó ellenőrzése alól való kikerülésével történik meg, mivel az API-felhasználó, a példában a Trust végzi el a gyártó manuális ellenőrzésén kívül. Ennek vizsgálatakor olyan szempontok játszanak szerepet, mint a finomhangolást követő frissítések és javítások elvégzése. Hiszen ha az API alkalmazást követően lát napvilágot egy hiba, amely addig ismeretlen volt – nagyhatású képességgel rendelkező modellek esetében ez gyakran előfordulhat – akkor az API-felhasználó köteles, a gyártó által kínált a frissítést, hibajavítást alkalmazni. Így pedig annak a ténye, hogy a digitális termékek – eltérően a fizikai termékektől – nem egyszer kerülnek átadásra, hanem folyamatos frissítéseknek vannak alávetve, egyrészt szükségtelenné teszi a „jobb termékek” későbbi megjelenésére vonatkozó kikötést, továbbá a gyártó felelősségét tovább terjeszti azon a ponton, amikor a terméket használatba veszik.⁵¹

Mindezt pedig abban az esetben kell vizsgálni, ha a jogosan elvárható biztonság sérül. A jogosan elvárható biztonság tekintetében először ki kell emelni, hogy nem egy adott személy esetében beszélünk jogosan elvárható biztonságról, hanem amit objektíve a „nagy

⁵¹ European Law Institute, – Guiding Principles for Updating the Product Liability Directive for the Digital Age 6.-7. oldal (Guiding Principle 6)
https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Guiding_Principles_for_Updating_the_PLD_for_the_Digital_Age.pdf

nyilvánosság” elvárhat.⁵² Ez esetben, mivel tisztán anyagi kárról beszélhetünk, helyesebben anyagi kár felmerülésének kockázatáról. A végfelhasználók esetében tehát a biztonság az anyagi javaik védelmét jelenti elsősorban, ez akkor tekinthető megsértettnek, ha az MI hibájából adódóan, anyagi hátrány éri a végfelhasználókat.

A kérdés az, milyen szintű biztonság várható el jogosan egy ilyen MI-rendszertől. Azt gondolom, az olyan MI-cselekvés még biztonságosnak tekinthetők, melyek bagatell mértékű kárhoz vezetnek, vagy olyan hibák melyek nem vezetnek anyagi kárhoz egyáltalán. Azonban, ha súlyosabb anyagi kár a végeredmény, úgy már a jogosan elvárható biztonság sérül, mivel a rendszer használatával a fél nem abba egyezik bele, hogy akár súlyosabb anyagi hátrány is érheti. Természetesen a súlyosság szubjektív kategória, így azt véleményem szerint mindig az adott esetben kell vizsgálni. Erre vonatkozóan felmerült egy olyan álláspont, mi szerint a digitális termékeket, mint például a GPT, nem hibás termékként azonosíthatnánk, hanem „nem biztonságos” termékként⁵³, amely meghatározás véleményem szerint is pontosabb képet fest le a helyzetről.

3.3. A KÁR MEGHATÁROZÁSA

A kárt a termékfelelősségi irányelv 6. cikke határozza meg. E cikk (1) bekezdésének a) pontja szerint haláleset vagy személyi sérülés, beleértve a lelki egészség orvosilag elismert sérülését is. Míg a b) pont tartalmazza, hogy bármilyen javak károsodása vagy megsemmisülése, kivétel ha maga a hibás termék, nem szakmai célokra használt adatok, a gyártó ellenőrzése alatt álló alkotóelem károsodik vagy semmisül meg, míg a Ptk. 6:552. § b) pontja szerint, a termékkár, a termék által más dolgokban okozott károkra terjed ki. A 6. cikk 2) bekezdése ugyanakkor kitér rá, hogy a fenti 1) bekezdésben szereplő esetekből eredő valamennyi anyagi veszteségre kiterjed a kártérítés.

A példában kárként például a rossz tranzakciós folyamat miatt elszenvedett „extrém” „gázdíj” – tranzakciós költség a blokkláncon – szerepel, illetve a rendkívül kedvezőtlen

⁵² Jean-Sébastien Borghetti, Adapting Product Liability to digitalization: Trying Not to put New Wine Into Old Wineskin, 149.-150. o. in Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer VII, Nomos Verlagsgesellschaft, Baden-Baden, Germany, 2023.

⁵³ ELI– Guiding Principles for Updating the Product Liability Directive for the Digital Age 6.-7. oldal (Guiding Principle 6)

árfolyamon végrehajtott tranzakció. Ez esetben pedig a javak károsodása vagy megsemmisülése irányából tudunk közelíteni. Amelyek közül a megsemmisülést el is hagyhatjuk, ugyanis ez esetben a pénz nem semmisül meg, csupán csökken a mennyisége, amely inkább a károsodás irányába mutat. Mivel ahogy az ELI kifejti, a digitális korszakban a sérülés és megsemmisülés már nem csak a fizikai tárgyakra, hanem a vagyon, például a bankszámla, vagy nem banki számlán lévő pénz csökkenése.⁵⁴ Hiszen ha úgy értelmezzük, a fogyasztó pénzügyi tőkéje „károsodik”, mivel veszít a felhasználhatóságából, értékéből. Így ha a mennyiségbeli csökkenést értékcsökkenésként értékeljük, ezt pedig a felhasználhatóságának részbeni elvesztéseként, akkor a károsodás megáll, ez esetben pedig a (2) bekezdés alapján kártérítési igény érvényesíthetünk.

A termékfelelősség mivel a deliktuális felelősségi szabályok körébe tartozik, így a Ptk. 6:522. § vonatkozik rá, e szakasz 1) bekezdése szerint, a károkozó köteles megtéríteni a károsult teljes kárát, a 2) bekezdés a) pontja szerint ide tartozik a károsult vagyonába beállott értékcsökkenés, továbbá a c) pont szerint a károsultat ért vagyoni hátrányok kiküszöböléséhez szükséges költségeket. Amint látható, ezen rendelkezés nem határoz meg olyan speciális kikötéseket mint a kontraktuális felelősség, így objektíve a károsultat ért teljes kárt megtéríteni köteles a károkozó. Azt gondolom az általam vizsgált példában, ez a sokkal inkább megvalósítható szabályozás, hiszen nem ró többlet-bizonyítási terhet a felperesre, a károsultra. Ptk. 6:552. § b) pontja ugyanakkor megemlíti, a termékkárra vonatkozó értékhatárt, amely a kár bekövetkeztekor 500 Euróban került megállapításra, tehát ennél nagyobb összegű kár esetén lehetséges igényt érvényesíteni a termékfelelősség alapján.

3.4. OK-OKOZATI KAPCSOLAT, BIZONYÍTHATÓSÁG

Ha azt az esetkört vesszük alapul, amikor a Trust alkalmazásával összekapcsolt GPT modell okoz kárt egy fogyasztónak, akkor fontos, hogy a termék hibáját illetve a hiba és a kár közötti okozatossági kapcsolatot bizonyítani tudjuk. Ilyen hiba lehet például, ha a gyártó által ismert hibát nem korrigálta, például frissítéssel.

A hibát ilyen módon bizonyítottnak is vehetjük, azonban a hiba és a kár oksági kapcsolata már lényegesen nehezebb kérdés. Hiszen az MI konkrét döntési mechanizmusát

⁵⁴ ELI– Guiding Principles for Updating the Product Liability Directive for the Digital Age 8.-9. oldal (Guiding Principle 7)

kellene vissza fejtenünk, hogy ezt a kapcsolatot tételesen bizonyíthassuk, ami nem megoldható. Ezért a termékfelelősségi irányelv 10. cikkének (2) és (3) bekezdését kell figyelembe vennünk.

A (2) bekezdés b) pontja szerint vélelmezni kell a termék hibáját, ha a felperes bizonyítja, hogy a termék nem felelt meg az uniós vagy nemzeti jog által előírt termékbiztonsági követelményeknek. Ilyen lehet a már említett AI Act által előírt kötelezettségeknek való megfelelés, illetőleg a termékfelelősségi irányelv szabályainak, továbbá más speciális jogszabályoknak való megfelelés, amennyiben valamelyik vonatkozó uniós vagy nemzeti jogi szabálynak nem felel meg, úgy az annak bizonyítékeként értékelhető, hogy a termék hibás.

A (3) bekezdés szerint a termék hibája és a kár közötti ok-okozati összefüggést vélelmezni kell, amennyiben megállapítást nyer, hogy a termék hibás, és az okozott kár jellemzően összefügg a kérdéses hibával. Ez a rendelkezés akkor alkalmazandó, amikor egy ismert hibával állunk szemben, például, ha többször is előfordul egy modell esetében, hogy bizonyos kriptovalutával végzett tranzakciót elront, akkor ez egy ismert hiba, így ha ez a későbbiekben is bekövetkezik, akkor feltehető, hogy az okozott kár feltehetőleg összefügg a már ismert hibával. Azonban, ha egyedi eset történik, egyedi hiba, akkor ezen rendelkezés nem alkalmazható. A kérdés pedig abból adódik, hogy amennyiben egy ismert hibát a szolgáltató igyekszik korrigálni, de ennek ellenére – merthogy ez a termékfelelősségi szabályok betartásának dacára is előfordulhat – ismét bekövetkezik, úgy azt még jellemző összefüggésnek lehet-e tekinteni, vagy nem ismert hibának. Azt gondolom, ez a kérdés a gyakorlatra fog maradni.

Vélelmet állít fel még a termékfelelősségi irányelv 10. cikkének (4) bekezdése is, e szerint vélelmezni kell a termék hibáját, ha a felperes különösen műszaki vagy tudományos szempontból felmerülő összetettség miatt rendkívüli nehézségekkel szembesül a termék hibája vagy a hiba és a kár közötti ok-okozati összefüggés vagy mindkettő bizonyítása tekintetében. Továbbá a felperes bizonyítja, hogy valószínű, hogy a termék hibás, vagy ok-okozati kapcsolat áll fent a termék hibája és a kár között. Azt gondolom ezen szabályozás pedig arra az esetkörre vonatkozik, amikor sem ismert hiba, sem pedig jogszabálysértés nem mutatható ki, de a hibás kimenet és a kár ennek ellenére is bekövetkezett. Ez esetben a felperes elsőként annak valószínűségét bizonyítja, hogy a termék hibás, amely véleményem szerint történhet akár úgy is, hogy a felperes bemutatja az általa beküldött bemenetet, amely megfelel az ésszerűen előrelátható használatnak és rendeltetésnek, majd pedig bemutatja a hibás kimenetet amely következtében a kárt elszenvedte, illetőleg, hogy kellően körültekintően járt el. Ez már valószínűsítheti a hibát. A termékhibáról szóló részben tárgyalt módszer, miszerint a modell

blokkláncnak küldött bemenetét igyekszünk végig vezetni a tranzakciós folyamaton, vagy pedig kielemezni magát a kimenetet, és feltárni azon hibákat amelyeket a modell elkövetett. Azt gondolom ilyen módon, ha tényszerűen nem is bizonyítható, de valószínűsíthető a hiba és a hiba és a kár közötti ok-okozati összefüggés.

3.5. MENTESÜLÉS

A mentesülési körülményeket a termékfelelősségi irányelv 11. cikke tartalmazza, az 1) bekezdés c) pontja alapján a gazdasági szereplő nem tartozik felelősséggel, ha a bizonyítja, hogy kárt okozó hiba nem állt fenn a termék forgalomba hozatalakor, használatbavételekor. Azt gondolom, hogy ez a mentesülési körülmény némileg ellentmond a nagy hatású képességekkel rendelkező modellek AI Act által meghatározott fogalomnak. Hiszen ezen modelleket az AI Act olyan MI-modelleknek tartja, amelyek bizonyos képességét a forgalombahozatal után képes még a gyártó is megismerni. Nem is beszélve az olyan API-felhasználókról mint a Trust, amely nem hogy a tervezésben nem vett részt, de még a modell egyes paramétereit, kódját, tanulóadatait, felépítését sem látja, így rendkívül nehéz bizonyítania, hogy ez a hiba nem állt fent. Hiszen azt sem tudhatja - még a gyártó sem - hogy a finomhangolásra használt adatok mennyiben befolyásolták a modell hibás működését.

Ugyanezen cikk e) pontja ugyanakkor olyan körülményt ír elő, amely szerint a használatba vétel időpontjában a tudományos és műszaki ismeretek objektív állása szerint nem volt előrelátható a hiba. Amennyiben nem ismert a hiba, úgy a termékhibára vonatkozó vélelem a 10. cikk (4) bekezdése alapján fennállhat, azonban, ha a gyártó bizonyítja, hogy ezen hibát annak ismeretlensége és kiszámíthatatlansága miatt a tudomány és technika objektív állása szerint nem látta és nem is láthatta volna előre, úgy mentesülhet a felelősség alól. Azt gondolom, ezen rendelkezés leginkább a gyártó a fogyasztóval szembeni többlet információja és szakértelme miatt került bevezetésre. Ismét az AI Act rendelkezéseit kell ideemelnünk, hiszen érezhető, hogy a rendszerszintű kockázatot jelentő modellek esetében kötelezően alkalmazandó rendelkezések nem alkalmasak egy ilyen mentesülési körülmény kellő alátámasztására. Hiszen ez a fajta, azaz a „tudomány és technika objektív állása szerinti előreláthatatlan hiba” megállapítása olyan fokú monitorozási és nyomonkövetési intézkedéseket követel meg, amely kizárólag a nagy kockázatú MI alkalmazások esetében válik kötelezettséggé, azt viszont már fentebb kifejtettem, hogy ezen alkalmazás csupán

rendszerszintű kockázatot jelentő modellként kategorizálható. Azonban az AI Act (131) Preambulumbekezdése lehetővé teszi, hogy a gyártók önkéntes alapon alkalmazzák a saját rendszerükre a nagy kockázatú modellekre vonatkozó intézkedéseket. Ennek fényében pedig, amennyiben a gyártó ezt nem alkalmazza, úgy a fogyasztó könnyebben tudja a vélelmet használni, mint a gyártó a kimentést, így pedig a termékfelelősségi irányelv arra predesztinálja a gyártót, hogy a szigorúbb intézkedéseknek vesse alá magát.

3.6. A TERMÉKFELELŐSSÉGI VIZSGÁLAT ÖSSZEGZÉSE

A termékfelelősség tekintetében megállapítottuk, hogy az új irányelv a távoli felhőn futó szoftvert is termékként határozza meg, vagyis a GPT modellt termékként kezelhetjük. A termékhiba vizsgálata pedig a bizonyítás megkönnyítése miatt egyszerűbben kezelhető. Hiszen a termékfelelősségi irányelv megóvni látszik a károsultat a modell „belső működésébe” hatoló vizsgálat lehetetlensége alól. Továbbá azt gondolom, az irányelv a mentesülési feltételekkel arra próbálja vezetni a gyártókat, hogy éljenek az AI Act nyújtotta önkéntesség lehetőségével, amely a szigorúbb szabályok önként történő betartásáról szól, ezzel növelve az átláthatóságot és a biztonságot.

4. A KONTRAKTUÁLIS ÉS DELIKTUÁLIS FELELŐSSÉGI SZABÁLYOK ÜTKÖZÉSE

Amint azt már a kontraktuális felelősségről szóló részben kifejtettem, a Trust mint a GPT modell API-felhasználója és a fogyasztó között szerződéses viszony van, amely életre hívja a Ptk. ún. non-cumul szabályát. A Ptk. 6:145. § a párhuzamos kártérítési igények kizárásáról a következőképpen rendelkezik: „A jogosult kártérítési igényét a kötelezettel szemben akkor is a szerződésszegéssel okozott károkért való felelősség szabályai szerint érvényesítheti, ha a kár a kötelezett szerződésen kívül okozott károkért való felelősségét is megalapozza.” A jogosult a kártérítési igényét tehát akkor is kizárólag a kontraktuális szabályok szerint érvényesítheti, ha a kár egyébként megalapozná a deliktuális felelősség alkalmazását is. Ebben az értelemben az elnevezés is téves, hiszen nem a párhuzamos igényérvényesítést zárja ki, hanem kizárólagossá

teszi a kontraktuális felelősség alkalmazását, azt zárja ki, hogy a felperes megválassza a kártérítési követelésének jogalapját.⁵⁵ Ahogy Fazekas Judit is utal rá, előfordulnak olyan esetek, amikor a gyártó a szerződés alanyaként jelenik meg, azonban az ilyen esetekben a non-cumul akadályozza az irányelv maximumharmonizációját, hiszen a tagállami jogrendszer nem állapíthat meg szigorúbb szabályokat sem mint a termékfelelősség, ennél fogva, a nemzeti jogban nem lehet szerződésszegési szabályokat előírni termékfelelősség helyett.⁵⁶

Miskolczi-Bodnár Péter ugyanakkor felhívja a figyelmet arra, hogy a Ptk.-ban a károsultnak továbbra és kétféle kárigénye van, ha kárát más károkozótól is igényelheti, például ha a szerződő félen kívül a gyártóval szemben is eljárhat.⁵⁷ Így amennyiben a fogyasztó nem a Trust ellen, hanem például az OpenAI mint gyártó ellen kíván igényt érvényesíteni, úgy természetesen eljárhat a termékfelelősség szerint, azonban ez a fajta lehetőség csupán látszólagos, mivel az igényérvényesítés problémába ütközik, ha figyelembe vesszük a következőket.

A termékfelelősségi irányelv 8. cikke szerint, elsődlegesen a hibás termék gyártóját terheli a felelősség. Ezzel szemben abban az esetben, ha a hibát egy alkotóelem idézte elő, úgy a hibás alkotóelem gyártója felel. Feltéve, hogy az említett alkotóelemet a gyártó ellenőrzése alatt álló termékkel összekapcsolták, és az említett termék meghibásodását okozta. Amennyiben viszont sem a termék sem az alkotóelem gyártójának nincs székhelye az Európai Unióban, úgy az importőr, ennek hiányában a gyártó meghatalmazott képviselője, ha ilyen szereplők nincsenek, úgy a logisztikai szolgáltatót terheli a felelősség. Ezeken felül bármely természetes vagy jogi személy, amely a gyártó ellenőrzési körén kívül lényegesen módosít valamely terméket, majd azt forgalomba hozza vagy használatba veszi. Látható, hogy minden esetben a gyártó felelősségét kell elsődlegesen vizsgálni. Amennyiben ez akadályba ütközik, úgy, az irányelv logikája mentén a többi felmerülő szereplőt terhelheti a felelősség.

⁵⁵ Menyhárd Attila, Veress Emőd, Kontraktuális felelősség a magyar és román jogban, Magyar Jog, 2020/5., 288-296.,

⁵⁶ Fazekas Judit, Kontraktuális és deliktuális felelősség viszonya az új Polgári Törvénykönyvben különös tekintettel a párhuzamos igényérvényesítést kizáró non-cumul szabályra, 47.-48. o. in Fazekas Judit, Kőszegi Ákos, Csítei Béla, Állandó és változás, tanulmányok a magánjogi felelősség köréből, Gondolat kiadó, Budapest, 2017.,

⁵⁷ Miskolczi-Bodnár Péter, A jogi felelősség és a polgári jogi felelősség alapkérdései a Ptk. kártérítési szabályainak rendszere, a deliktuális és kontraktuális felelősség szétválasztása, 32. o. in Barta Judit, Barzó Tímea, Csák Csilla (szerk.) Magyarázat a Kártérítési jogról, Wolters Kluwer Hungary Kft., Budapest, 2018.

A fentiekből két szereplő lesz érdekes a számunkra. Az első a gyártó, amelyet a termékfelelősségi irányelv 4. cikk 10. pontjában határoz meg: „*minden olyan természetes vagy jogi személy, aki: a) terméket fejleszt, gyárt vagy állít elő; b) terméket terveztet vagy gyártat, vagy aki nevének, védjegyének vagy egyéb megkülönböztető jegyeinek a terméken való feltüntetésével annak gyártójaként jelenik meg; vagy c) saját használatra fejleszt, gyárt vagy állít elő terméket;*” Ez esetben pedig jól látható, hogy az OpenAI tekinthető gyártónak, hiszen ő fejlesztette és állította elő a modellt. A másik szereplő a forgalmazó, a termék felelősségi irányelv 4. cikkének 14. pontja szerint: „*az ellátási láncban belül a termék gyártójától vagy importőrétől különböző természetes vagy jogi személy, aki vagy amely terméket forgalmaz;*” Láthatjuk, hogy a forgalmazó értelmezéséhez, a forgalmazás definíciója szükséges, amely ugyanezen cikk 7. pontjában található, a következőt jelenti: „*az uniós piacon valamely termék kereskedelmi tevékenység keretében történő rendelkezésre bocsátása értékesítés, fogyasztás vagy használat céljára, akár ellenérték fejében, akár díjmentesen;*” A forgalmazó a mi esetünkben nem feltétlenül ugyanarra a célra kínálja a terméket vagy alkotóelemet mint azt a gyártó teszi. A példában, a Trust a GPT modellt nem általános kérdés-megválaszolásra nyújtja, hanem pénzügyi tranzakciók elvégzéséhez. A forgalmazó státuszát pedig a Trust tölti be, mivel az uniós piacon használatra bocsátja a terméket, ez esetben a modellt. A kiindulópont szerint az OpenAI a gyártó, míg a Trust a forgalmazó, a termékfelelősségi irányelv szerint pedig elsődlegesen a gyártót terheli a felelősség, a probléma viszont akkor áll fent, ha a forgalmazó átveszi a gyártó helyét.

API-felhasználóból is alapvetően két kategória van, az egyik, aki egy általános tudású központi modellt használ, a másik pedig aki különálló, speciális feladatra finomhangolt modellt. A blokkláncon történő tranzakciók végrehajtása, olyan speciális feladatnak tűnik, amely kizárólag egy erre finomhangolt modellel elképzelhető, ezért meg kell vizsgálni, hogy a finomhangolás lényeges módosításnak minősül-e. Mégpedig a finomhangolás a termékfelelősségi irányelv 4. cikkének 18. pontjának b) bekezdését teljes mértékben kielégíti, amely szerint: „*amely a termék eredeti teljesítményének, céljának vagy típusának anélküli megváltoztatásával jár, hogy ezt a gyártó kezdeti kockázatértékelése előre jelezte volna; és amely megváltoztatja a veszély jellegét, új veszélyt teremt vagy növeli a kockázati szintet.*” Mivel a finomhangolás a blokkláncc felé küldött parancsok végrehajtására, olyan újfajta kockázatot teremt, amelyre az OpenAI nem láthatott rá az eredeti, általános modell

tervezésekor. A modell⁵⁸ utasítása a blokkláncon futó szoftverek felé pedig olyan újfajta veszélyt tartalmaz, amely az eredeti, általános használatú modell esetében nem merülhet fel. Így alkalmazható rá a termékfelelősségi irányelv 8. cikkének (2) bekezdése, mely szerint, bármely természetes vagy jogi személy, aki vagy amely a gyártó ellenőrzésén kívül lényegesen módosít valamely terméket, majd azt forgalomba hozza vagy használatba veszi, gyártónak minősül. Fontos leszögezni, hogy magát a finomhangolást az API-felhasználó végzi el, az OpenAI rendszerén keresztül, automatikusan, tehát manuális ellenőrzés és felügyelet nélkül. Továbbá az üzleti feltételekben az OpenAI minden felelősséget az API-felhasználóra helyez, amelyben még olyan elemek is szerepet kapnak mint a naplózás és a moderáció, mint az API-felhasználó felelősségi körébe tartozó kötelezettségek. A használat pedig a modell és Trust összekapcsolásával megvalósul. Tehát ebben az értelemben az OpenAI felelőssége mondhatni megszűnik, mivel a Trust az ő helyébe lép.

Ekkor visszatérünk az eredeti problémához, vagyis a gyártó a szerződő félként lesz jelen, hiszen az OpenAI-al szemben, a termékfelelősség szerint nem járhatunk el, hiszen a gyártó már a Trust lesz, ugyanakkor pedig a Ptk. 6:145. § szerint mivel a Trust és a fogyasztó között szerződéses viszony van, így csak kontraktuális alapon lehet igényt érvényesíteni a fentebb tárgyalt bizonyítás során előálló problémák miatt. A Ptk. 6:146. § a alapján pedig már önmagában az is elegendő, hogy a károkozás a szerződés teljesítése során következzen be, mert a károsult a vagyonában bekövetkezett kár megtérítését ezesetben is a szerződésszegéssel okozott károkért való felelősség szabályai szerint követelheti. A non-cumul szabálya e szerint hiába kötelezi a felet a kontraktuális felelősség szerinti eljárásra, az a rendkívüli bizonyítási nehézségek miatt falakba ütközik, míg a termékfelelősség szerint képes lehetne eljárni.

Úgy gondolom ezen a ponton válik nyilvánvalóvá, hogy a non-cumul szabály egyrészt megfosztja a jogosultat a termékfelelősség szabályai alapján való igényérvényesítés lehetőségétől, másrészt pedig olyan útra kötelezi a károsultat, amelyet alkalmazva – a technika jelen állása szerint - szinte képtelenség igényt érvényesíteni, a fent kifejtett bizonyítási nehézségekből adódóan. Továbbá, a termékfelelősségi irányelv 3. cikke megtiltja a fogyasztók és természetes személyek eltérő szintű védelmének alkalmazását. Tehát a non-cumul egyrészt az igényérvényesítést, másrészt a jogharmonizáció akadályozó rendelkezésnek bizonyul. E problémakörhöz hasonlóan, Fazekas Judit azt az esetkör említi, amikor a termék gyártója nem állapítható meg, ezért azt a forgalmazót kell gyártónak tekinteni, akivel a károsult szerződéses

⁵⁸ A GPT modell mint termék meghatározását, lásd.: A termék meghatározása részben

viszonyban áll a károsult nem érvényesíthet igényt a termékfelelősség alapján, e tekintetben pedig a termékfelelősségi irányelv és a Ptk. nincs összhangban. A kollízió úgy lett volna feloldható, ha a kódex (Ptk.) a termékfelelősségi jogalap kivételként megállapítaná.⁵⁹ Úgy gondolom az általam vizsgált helyzet kísértetiesen hasonlít erre, annyi különbséggel, hogy bár a gyártó ismert, viszont az API-felhasználó által elvégzett finomhangolás miatt az API-felhasználó belép a gyártó helyébe, így ugyanaz a helyzet áll fent, mivel a gyártóként megjelenő API-felhasználó⁶⁰ és a végfelhasználó szerződéses viszonyban áll egymással.

5. *DE LEGE FERENDA JAVASLAT, ZÁRSZÓ*

Ahogy a dolgozatban igyekeztem rámutatni, a probléma kettős természetű. Egyrészt a gondossági kötelem esetén történő szerződésszegés bizonyítása majdnem hogy lehetetlenül. Másrészt pedig, a non-cumul megakadályozza a termékfelelősség alkalmazását, annak ellenére, hogy a példában szereplő és hasonló esetben alkalmazható lenne.

Azt gondolom, hogy minden olyan károkozásnál, ahol MI okozott kárt, ott érdemes lehet a non-cumul alól egy olyan kivételt meghatározni, amely rendkívüli tudományos és technikai bonyolultság esetén, a termékfelelősség szabályait alkalmazhatóvá teszi. Hiszen a termékfelelősségi szabályok alapján sokkalta kezelhetőbbek az MI-rendszerek, azáltal, hogy a fogyasztóra nem rónak olyan bizonyítási terhet, amelynek nem képes eleget tenni.

A kontraktuális felelősség esetében pedig kérdéses, hogy szükséges-e ezeken a szabályokon változtatni, hiszen a technológia kihívásaiból adódóan leginkább a bizonyítási eljárás intézményét és a kártérítés mértékére vonatkozó szabályokat lenne szükséges átgondolni. mivel az MI-modellek bonyolultsága miatt, az előreláthatóság és okozatosság már nem értelmezhető a hagyományos módon, hiszen olyan dolgokról beszélünk, amelyeket még a gyártója sem képes teljesen átlátni. Éppen ezért a rendszeren belülré mutató bizonyítást ki kellene küszöbölni, akár vélelmekkel, ahol a gyártót terhelé a többlet bizonyítási teher, arra tekintettel, hogy a gyártó rendelkezik többlet információval és tudással. Ezt pedig leginkább

⁵⁹Fazekas Judit, Kontraktuális és deliktuális felelősség viszonya az új Polgári Törvénykönyvben különös tekintettel a párhuzamos igényérvényesítést kizáró non-cumul szabályra, 47.-48. o. in Fazekas Judit, Kőszegi Ákos, Csítei Béla, Állandó és változás, tanulmányok a magánjogi felelősség köréből, Gondolat kiadó, Budapest, 2017.

⁶⁰ Vagyis a Trust, ebben a példában a Trust és az API-felhasználó ugyanaz a személy

azon sérelem okozására lehetne fordítani, amelyre nem lehet a termékfelelősségi szabályokat alapozni.

Jelen dolgozatban igyekeztem egy olyan példát bemutatni, ami bár még a gyakorlatban nem létezik, mégis sok változata lesz akár 1 - 1,5 éven belül. Ilyenek lesznek például a banki applikációba megjelenő MI-rendszerek, vagy akár a biztosítók által alkalmazott MI-rendszerek, továbbá abban is biztos vagyok, hogy a dolgozatban szereplő blokklánc-alkalmazás és megjelenik előbb-utóbb a piacon. A dolgozat egyik célkitűzése az volt, hogy részben előre gondolkodjon olyan problémákat illetően, amely már szinte itt van a küszöbön.

FÜGGELÉK

FOGALOMMAGYARÁZAT

1. PONT ELŐTANÍTÁS

Az előtanítás célja, hogy nagy mennyiségű adat alapján a modell megtanulja megjósolni a következő szót (nagy nyelvi modellek esetében). Ebben a fázisban tehát, még nem tanul speciális feladatot a modell, csupán a következő szót megjósolni egy adott szövegben. Ez a folyamat többféle tanítási mechanizmus szerint történhet, azonban a GPT esetében autoregresszív tanítási módot használják, vagyis a modellnek úgy kell kitalálnia a következő szót, hogy egy adott mondatban nem látja a szöveg folytatását, így az előző szavakból kell kiindulnia.⁶¹

2. PONT GENERATÍV MODELL

A generatív modell, olyan gépi tanulási modell, amelynek célja, hogy megtanulja a tanulóadatok mögöttes mintáit és ez alapján új, hasonló adatokat hozzon létre. Lényegében, mintha megtanítanánk a gépet, hogy adatokat „álmodjon meg” a korábban látott adatok

⁶¹ Kushal Shah, Pre-training, fine-tuning, and in-context learning in Large Language Models (LLMs), 2022.08.06. <https://medium.com/@atmabodha/pre-training-fine-tuning-and-in-context-learning-in-large-language-models-llms-dd483707b122> (Online, leöltve: 2024.09.02.)

alapján.⁶² Fontos, hogy a modell működéséből adódóan az előrejelzések statisztikai alapon történnek.

A generatív modell kockázatai:

- I. A kitalált „tények” és
- II. a hallucináció esete: Amikor a modell tényeket talál ki, és hamis indoklást ad hozzá, ez az ártalmatlan tényektől, akár a jogilag támadható tényekig terjedhet.⁶³
- III. Szerzői jogi kockázatok: A modell tanításához használt tanulóadatok tartalmazznak e szerzői jogi védelem alatt álló műveket? Ennek a kérdésnek az eldöntéséhez elengedhetetlen, hogy a modell képzési adatai ismertek és átláthatók legyenek.⁶⁴
- IV. Elfogult kimenetek: A generatív modellek ki vannak téve annak a kockázatnak, hogy a kimeneteik elfogultak legyenek, a Stable Diffusion például a "vállalati vezérigazgatók" képeinek megjelenítésére vonatkozó kérés alapján kizárólag fehér férfiakat ábrázoló képeket állíthat elő.⁶⁵
- V. Deepfake-ek generálása generatív modell segítségével. Híres deepfake volt például Ferenc Pápa pufferdzsekiben⁶⁶, és különböző kitalált helyzetekben, például volt olyan deepfake, amely azt ábrázolta, hogy Ferenc Pápa a rendőrök előtt futott el éppen.

3. PONT MULTIMODÁLIS

Először is meg kell határoznunk, mit értünk modalitás alatt. A mesterséges intelligencia és a gépi tanulás kontextusában a modalitás, az adatok típusát jelenti, ezek a következők lehetnek:

⁶² Abid Ali Awan, What is Generative Model?, 2023. 08. 22., <https://www.datacamp.com/blog/what-is-a-generative-model> (Online, letöltve: 2024.09.02.)

⁶³ Manasi Vartak, Six Risks Of generative AI, 2023. 06. 29., <https://www.forbes.com/sites/forbestechcouncil/2023/06/29/six-risks-of-generative-ai/?sh=796df0273206> (Online, letöltve: 2024.09.02)

⁶⁴ Manasi Vartak, i.m.

⁶⁵ Manasi Vartak, i.m.

⁶⁶ Sabrina Ortiz, Top 5 biggest risks of generative AI, according to an expert, 2023.04.25., <https://www.zdnet.com/article/the-5-biggest-risks-of-generative-ai-according-to-an-expert/> (Online, letöltve: 2024.09.02)

- Szöveg
- Kép
- Hang
- Videó

Az unimodális modellek kizárólag egyetlen adattípust képesek kezelni, mint például a GPT-3 amely csak a szöveges adatok kezelésére képes, illetve csak szöveges adatot képes előállítani. Ezzel szemben a multimodális modellek képesek egynél több fajta kimenetet előállítani.⁶⁷

Multimodális modell kockázatai

- I. Átláthatóság hiánya: Bár ez mind a generatív mind az alapmodellek tekintetében is igaz, viszont egy multimodális modell még ezeknél is bonyolultabb, így a multimodális modell döntési eljárása felfedhetetlen.
- II. A multimodális modellek is áldozatul eshetnek annak a működési hibának, amely diszkriminációval jár, illetve tartalmazhatnak olyan elfogultságot, amely a diszkriminációt akár súlyosbíthatja.
- III. Az adatvédelmi kockázatai nagyban megnőnek a multimodális modelleknek, hiszen több forrásból származó különböző típusú adatot dolgoznak fel, ezek sok esetben személyes adatokat is tartalmazhatnak.⁶⁸

4. PONT ZÁRT/NYÍLT FORRÁSKÓDÚ MI-MODELL

A nyílt mesterséges intelligenciát azok a rendszerek jelentik, ahol a forráskódját, az algoritmust a tanulóadatokat, adott esetben a modell tanításához használt szoftvert nyilvánosan

⁶⁷ Margaret Rouse, Multimodal AI (Multimodal Artificial Intelligence), 2023.06.24., <https://www.techopedia.com/definition/multimodal-ai-multimodal-artificial-intelligence> (Online, letöltve: 2024.09.02)

⁶⁸ Javiel Canales Luna, What is Multimodal AI, 2024.02.22., <https://www.datacamp.com/blog/what-is-multimodal-ai> (Online, letöltve: 2024.09.02)

hozzáférhetővé teszik. Ez lehetővé teszi a nyilvánosság számára a hozzáférhetőséget, az ellenőrzés, a módosítást, az együttműködést és az innovációt.⁶⁹

Ellenben a zárt mesterséges intelligencia esetében, nem nyilvánosak sem az adatok, sem az algoritmus, sem pedig a forráskód és egyéb szoftver. Ez esetben a felhasználók egy API segítségével férhetnek hozzá a mesterséges intelligenciához (erről a következőkben beszélek). A zárt MI rendszerek biztonságosak, képesek megvédeni a személyes adatokat és egyéb jogokat, viszont átláthatatlanabbak, és kiszámíthatatlanabbak.⁷⁰

Fontos, hogy a zártság- és nyíltságnak vannak fokozatai, amelyek a következők: a modellre vonatkozó információk, a tanulóadatokra vonatkozó információk, illetve azon szoftverek, amelyeket a modell tanításához használtak.⁷¹

5. PONT FINOMHANGOLÁS

Az előtanítás után, van a kezünkben egy úgynevezett PLM (Pre-trained language model), ez egy általános nyelvi tudással rendelkező modell, ha konkrét feladatokra szeretnénk használni, akkor finomhangolnunk kell. Amihez már jóval kevesebb adatra van szükség, mint az előtanításhoz. Ennek során egy kisebb adatkészlettel betanítják kimondottan egy konkrét feladat elvégzésére.

Az előtanítás során szerzett tudással, a modell képes lesz több feladatot is ellátni, azonban igazán hatékony és specifikus csak a finomhangolás után lesz, egy alapmodellt éppen ezért több feladatra is lehet finomhangolni. Ez azért is hasznos, mivel az előtanítási fázis akár hónapokat is igénybe vehet, míg a finomhangolás viszonylag gyors.⁷²

⁶⁹ Arttteo, Open vs Closed AI: What's the difference and which suits your business the most, 2024.02.6., <https://www.linkedin.com/pulse/open-vs-closed-ai-whats-difference-which-suits-your-business-most-fz1vf> (Online, letöltve: 2024.09.05)

⁷⁰ Arttteo, i.m.

⁷¹ George Lawton, Attributes of open vs closed AI explained, 2024.07.08., <https://www.techtarget.com/searchenterpriseai/feature/Attributes-of-open-vs-closed-AI-explained> (Online, letöltve: 2024.09.05)

⁷² Kushal Shah, Pre-training, fine-tuning, and in-context learning in Large Language Models (LLMs), 2022.08.06. <https://medium.com/@atmabodha/pre-training-fine-tuning-and-in-context-learning-in-large-language-models-llms-dd483707b122> (Online, letöltve 2024.09.01.)

6. PONT API – APPLICATION PROGRAMMING INTERFACE

Az API (vagy Application Programming Interface, avagy magyarul: alkalmazás programozási interfész), olyan szabályok és protokollok összessége, amely lehetővé teszi szoftveralkalmazások számára, hogy egymással kommunikáljanak az adatok, funkciók, vagy működésmódok cseréje érdekében.⁷³ Tehát minden API egy interfész, ez olyan közvetítőt jelent, amivel az ügyfél⁷⁴ illetve a kiszolgáló⁷⁵ rendszere egymással kapcsolatba léphet, illetőleg lehetőséget biztosíthat az ügyfélnek, hogy a kiszolgáló rendszerének működését, ha korlátozottan is, de megváltoztassa.

Jelen példában az API-felhasználó (Tust) az ügyfél, az OpenAI pedig a kiszolgáló. Az ügyfél ekkor a GPT-hez mint a kiszolgáló rendszeréhez intézhet utasításokat, és végezhet el bizonyos módosításokat - utasítás formájában.

7. PONT AZ AI ACT EGYES FOGALMAI

Az AI Act 3. cikkében szereplő, egyes fogalmakat sorolom fel, és magyarázom jelen pontban, amelyek jórészt a téma technikai érthetőségét segítik elő.

- a) Az **MI-rendszert** az AI Act, a 3. cikk 1. pontjában a következőképpen határozza meg:
„gépi alapú rendszer, amelyet különböző autonómiaszinteken történő működésre terveztek, és amely a bevezetését követően alkalmazkodóképességet tanúsíthat, és amely a kapott bemenetből – explicit vagy implicit célok érdekében – kikövetkezteti, miként generáljon olyan kimeneteket, mint például előrejelzéseket, tartalmakat, ajánlásokat vagy döntéseket, amelyek befolyásolhatják a fizikai vagy a virtuális környezetet
- b) Az általános célú **MI-modellt** mint kategóriát szintén definiálja az AI Act, a következőképpen: *„olyan MI-modell – ideértve azt is, amikor az ilyen MI-modell tanítása nagy adatmenynyiséggel, nagy léptékű önfelügyelet mellett történik –, amely*

⁷³ Michael Goodwin, What is an API? (application programming interface), 2024.04.09., <https://www.ibm.com/topics/api> (Online, letöltve 2024.09.01.)

⁷⁴ az API szempontjából az egyik fél

⁷⁵ az API szempontjából a másik fél, többnyire ez a fejlesztőt jelenti, vagy a fejlesztő szolgáltatását, amit az ügyfél elkíván érni

jelentős általánosságot mutat, és forgalomba hozatalának módjától függetlenül, különféle feladatok széles körének elvégzésére képes, valamint többféle downstream rendszerbe vagy alkalmazásba integrálható, azon MI-modellek kivételével, amelyeket a forgalomba hozatalukat megelőzően kutatási, fejlesztési vagy prototípus-alkotási tevékenységekre használnak;”

- c) **Rendszerszintű kockázatot jelentő MI-modellek:** Ezek közé tartoznak azon modellek, amelyek nagyhatású képességekkel rendelkeznek, vagy a bizottság határozata szerint tekintendők nagy hatású képességgel rendelkező modelleknek. Az AI Act 51. cikke szerint a modelltől vélelmezni kell, hogy nagyhatású képességekkel rendelkezik, ha a tanításához használt összesített számítási teljesítménye, lebegőpontos műveletekben mérve eléri vagy meghaladja a 10^{25} FLOP-ot.⁷⁶ Az AI Act 111. Preambulumbekezdése részletezi a kategória létrehozásának értelmét, amely dióhéjban a következő: Ezen kategóriának meghozatal az olyan általános MI-rendszereket érinti, melyek nagyhatású képességekkel rendelkeznek, vagy jelentős hatással vannak a belső piacra. Nagyhatású képességekről akkor beszélünk, ha az adott MI-modell képességei megfelelnek a legfejlettebb általános célú MI-modell képességeinek, vagy meghaladják azokat. Ezen túlmenően az adott modell képességeit jobban meg lehet érteni a forgalombahozatal után, vagy akkor, amikor az alkalmazók interakcióba lépnek vele. E képességeknek a méréséhez a technika jelen állása szerint, azon lebegőpontos műveletek összegét vesszük, amelyet a modell fejlesztésének folyamán a modell elvégzett. Amennyiben ez az érték meghaladja az AI Act-ben meghatározott – fentebb írt – küszöbértéket, úgy rendszerszintű kockázatot jelentő modellnek minősül.

8. PONT AZ AI ACT RENDELKEZÉSEI A RENDSZERSZINTŰ KOCKÁZATOT JELENTŐ MODELLEKRE VONATKOZÓAN

⁷⁶ A FLOP-érték azt a mérőszámot jelenti, hogy egyetlen iteráció során hány lebegőpontos műveletet hajt végre az MI-rendszer. Egy iteráció magában foglalja a forward pass-t, amikor a rendszer a kapott bemenetet feldolgozza és a kimenetet előállítja, valamint a backward pass-t, amikor a rendszer frissíti a súlyait vagyis tanul. Egy tanítás során rendkívül sok iteráció történik. Például, ha egy modell egy bemenet feldolgozásához 10^{12} műveletet végez el, és a tanítás során 100.000 iteráció történik, akkor az összesített FLOP érték 10^{17} lesz, mivel a tanítás során ennyi lebegőpontos műveletet hajtott végre. Ez a mérőszám rendkívül fontos a modell számítási igényének és hatékonyságának megállapításához.

A rendszerszintű kockázatot jelentő általános MI-rendszerekre vonatkozóan a fentiekén kívül, plusz kötelezettséget ró az AI Act 55. cikke, ide értve a modellértékelést, amelyben a rendszerszintű kockázatot azonosítják és enyhítik; értékelniük és enyhíteniük kell az általános célú MI-rendszer forgalomba hozatalából, üzembe helyezéséből eredő rendszerszintű kockázatokat. Továbbá nyomon kell követniük, dokumentálniuk és jelenteniük kell az MI-hivatal – adott esetben a nemzeti hatóságok - felé a súlyos váratlan eseményekre, és azok kezelésére meghozott korrekciós intézkedéseket. Végül pedig megfelelő szintű kiberbiztonságot kell nyújtaniuk az általános célú MI-modell és a fizikai infrastruktúrája számára.

FORRÁSOK JEGYZÉKE

IRODALOMJEGYZÉK

1. Györfi András, Léderer András, Paluska Ferenc, Pataki Gábor, Trinh Anh Tuan, KR1PT0 PÉNZ ABC, HVG Könyvek, Budapest, 2019.
2. Self Chain, A modular intent-centric blockchain for enhanced security and user-friendliness, 2023.
3. Csehi Zoltán (szerk.), 2013. évi V. Törvény A Polgári Törvénykönyvről Kommentárja, Magyar Közlöny Lap- és Könyvkiadó Kft., Budapest, 2021,
4. Barta Judit, Barzó Tímea, Csák Csilla (szerk.) Magyarázat a Kártérítési jogról, Wolters Kluwer Hungary Kft., Budapest, 2018.
5. Fuglinszky Ádám, Kártérítési Jog, HvgOrac Kiadó, Budapest, 2015.
6. Leszkoven László, Szerződészegés a polgári jogban, Wolters Kluwer Kft., Budapest, 2016.
7. Thomas Riehm, Verträge über digitale Dienstleistungen, in: Martin Schmidt-Kessel, Christina Möllnitz (szerk.) Grundfragen des Digitalvertragsrechts, Mohr Siebeck, Tübingen, 2022,

8. Szászy István, A kötelmi jog általános tanai, Grill Károly Könyvkiadóvállalata, Budapest, 1943.
9. Miriam C. Buiten, Product Liability of defective AI European Journal of Law and Economics, (2024) 57, 239–273, 2024.02.27.
10. Fazekas Judit, Kőszegi Ákos, Csitéi Béla, Állandó és változás, tanulmányok a magánjogi felelősség köréből, Gondolat kiadó, Budapest, 2017.
11. European Law Institute – Guiding Principles for Updating the Product Liability Directive for the Digital Age, 2021.
12. Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer, Liability for AI, Münster Colloquia on EU Law and Digital Economy VII, Nomos Verlagsgesellschaft, Baden-Baden, Germany, 2023.
13. Menyhárd Attila, Veress Emőd, Kontraktuális felelősség a magyar és román jogban, Magyar Jog, 2020/5.
14. Piotr Machnikowski : Regulation of Damages on National or European Level, in: Reiner Schulze, Dirk Staudenmayer, Sebastian Lohsse (szerk): Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps. Münster Colloquia on EU Law and Digital Economy II, Nomos Verlagsgesellschaft, Baden-Baden, Germany, 2017, 141-154.
15. Sebastian AE Martens: Contracts for the Supply of Digital Content – Consequential Loss in: Reiner Schulze, Dirk Staudenmayer, Sebastian Lohsse (szerk): Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps. Münster Colloquia on EU Law and Digital Economy II, Nomos Verlagsgesellschaft, Baden-Baden, Germany, 2017, 155–168
16. Leszkóven László: Szerződészegés a polgári jogban. 2. kiadás, Wolters Kluwer, Budapest, 2018.

JOGFORRÁSOK

1. 373/2021 (IV. 30.) Korm. rendelet a fogyasztó és a vállalkozás közötti, az áruk adásvételére, valamint a digitális tartalom szolgáltatására és digitális szolgáltatások nyújtására irányuló szerződések részletes szabályairól

2. az Európai Parlament és a Tanács (EU) 2024/2853 Irányelve (2024. október 23.) a hibástermékekért való felelősségről és a 85/374/EGK tanácsi irányelv hatályon kívül helyezéséről
3. az Európai Parlament És a Tanács (EU) 2019/770 Irányelve (2019. május 20.) a digitális tartalom szolgáltatására és digitális szolgáltatások nyújtására irányuló szerződések egyes vonatkozásairól
4. Az Európai Parlament és a Tanács (EU) 2024/1689 számú rendeletének, (2024. június 13.) 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 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelvmódosításáról (a mesterséges intelligenciáról szóló rendelet)
5. 2013. évi V. törvény, A Polgári Törvénykönyvről

INTERNETES FORRÁSOK

1. Patrick McGuinness, GPT-4 Details Revealed, 2023.07.12., <https://patmcguinness.substack.com/p/gpt-4-details-revealed> (online, letöltve: 2024.10.06.)
2. OpenAI, Business Terms, 2023.11.14., <https://openai.com/policies/business-terms/> (Online, letöltve: 2024.09.27.)
3. OpenAI, EU Terms Of Use, 2024.10.23., <https://openai.com/policies/eu-terms-of-use/> (Online, letöltve: 2024.09.22.)
4. Kane Pepi, Trust Wallet Review 2024 – Everything You need to know, 2024.04.04., <https://www.techopedia.com/cryptocurrency/trust-wallet-review> (Online, leöltve: 2024.11.21.)
5. Kushal Shah, Pre-training, fine-tuning, and in-context learning in Large Language Models (LLMs), 2022.08.06. <https://medium.com/@atmabodha/pre-training-fine-tuning-and-in-context-learning-in-large-language-models-llms-dd483707b122> (Online, leöltve: 2024.09.02.)
6. Abid Ali Awan, What is Generative Model?, 2023. 08. 22., <https://www.datacamp.com/blog/what-is-a-generative-model> (Online, letöltve: 2024.09.02.)
7. Manasi Vartak, Six Risks Of generative AI, 2023. 06. 29., <https://www.forbes.com/sites/forbestechcouncil/2023/06/29/six-risks-of-generative-ai/?sh=796df0273206> (Online, letöltve: 2024.09.02)

8. Manasi Vartak, Six Risks Of generative AI, 2023. 06. 29, <https://www.forbes.com/sites/forbestechcouncil/2023/06/29/six-risks-of-generative-ai/?sh=796df0273206> (Online, letöltve: 2024.09.02)
9. Sabrina Ortiz, Top 5 biggest risks of generative AI, according to an expert, 2023.04.25., <https://www.zdnet.com/article/the-5-biggest-risks-of-generative-ai-according-to-an-expert/> (Online, letöltve: 2024.09.02)
10. Margaret Rouse, Multimodal AI (Multimodal Artificial Intelligence), 2023.06.24., <https://www.techopedia.com/definition/multimodal-ai-multimodal-artificial-intelligence> (Online, letöltve: 2024.09.02)
11. Javiel Canales Luna, What is Multimodal AI, 2024.02.22., <https://www.datacamp.com/blog/what-is-multimodal-ai> (Online, letöltve: 2024.09.02)
12. Arttéo, Open vs Closed AI: What's the difference and which suits your business the most, 2024.02.6., <https://www.linkedin.com/pulse/open-vs-closed-ai-whats-difference-which-suits-your-business-most-fz1vf> (Online, letöltve: 2024.09.05)
13. George Lawton, Attributes of open vs closed AI explained, 2024.07.08., <https://www.techtarget.com/searchenterpriseai/feature/Attributes-of-open-vs-closed-AI-explained> (Online, letöltve: 2024.09.05)
14. Kushal Shah, Pre-training, fine-tuning, and in-context learning in Large Language Models (LLMs), 2022.08.06. <https://medium.com/@atmabodha/pre-training-fine-tuning-and-in-context-learning-in-large-language-models-llms-dd483707b122> (Online, letöltve 2024.09.01.)
15. Michael Goodwin, What is an API? (application programming interface), 2024.04.09., <https://www.ibm.com/topics/api> (Online, letöltve 2024.09.01.)
16. DApps Platform Inc., Trust Wallet Terms of Service, 2022. aug. 25. <https://trustwallet.com/terms-of-service> (Online, letöltve: 2024.11.20.)
17. European Commission, General-Purpose AI Code of Practice, 2024. november 21., <https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice> (Online, letöltve: 2024.12.09.)
18. European Commission, AI Pact, 2024. december 3., <https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice> (Online, letöltve: 2024.12.09.)