A digitalizáció sok tekintetben demokratizálta a technológiai fejlesztéseket

Interjú dr. Kovács Zoltán alezredessel, a Mesterséges Intelligencia kutatás vezetőjével

A Köz-Gazdaság interjút készített Kovács Zoltán alezredessel az általa vezetett kutatásról a mesterséges intelligencia témakörében. Az interjúban megfogalmazódnak a mesterséges intelligencia használatából fakadó veszélyek a pozitív hatások mellett. Fontos üzenete a kutatásnak, hogy a parttalan verseny a vállalatok, vagy az államok között a technológiát társadalomellenes irányba fordíthatja, ezért minden eszközt meg kell ragadni a hatékony és eredményes szabályozás érdekében.

Köz-Gazdaság: Az Ön vezetésével jelentős kutatás folyt a mesterséges intelligencia hatásáról, lehetséges kockázatairól. Mi volt a kutatás legfontosabb tanulsága, félni vagy bízni kell a mesterséges intelligenciában?

Kovács Zoltán: A mesterséges intelligencia (MI) megítélése kapcsán két markánsan eltérő vélemény fogalmazódik meg a témával foglalkozó kutatók körében. A MI-optimisták úgy tarják, hogy az új technológia soha nem látott fejlődést és jólétet hoz az emberiség számára. A MI – a kiemelkedő adatfeldolgozási képességek miatt – megold olyan problémákat (rákbetegség, globális felmelegedés, energiahiány), amik hosszú ideje fennállnak. A MI-pesszimisták ezzel szemben úgy vélik, hogy a MI elterjedése fenyegetést jelent az emberekre, szélsőséges esetben a puszta létünket is veszélyeztetheti. Szerintem mindkét tábornak igaza van.

Már eddig is tapasztalhattuk, hogy a technológiai fejlődés mennyivel könnyebbé tette a mindennapi életünket, ezért nehéz lenne vitatni annak kedvező hatásait. A tudományos fejlődés következtében kevesebb munkával jobb életkörülményeket teremthetünk magunknak, mint bármikor az emberiség történetében. A jó táplálkozás és egészségi ellátás miatt életkilátásaink kedvezőek. Ez a tendencia valószínűleg a jövőben is folytatódik.

DOI: https://doi.org/10.14267/RETP2022.04.02

Fontos kiemelni ugyanakkor, hogy már a MI fejlődésének jelenlegi, korai szakaszában is jól látszanak a technológia elterjedésének kedvezőtlen hatásai. Talán a legnyilvánvalóbb a technológiai függés. A modern társadalom olyan mértékben rá van utalva a technológiára, hogy már rövid ideig tartó kiesése is jelentős károkat okozhat a pénzügyi rendszereben és az ellátási láncokban. Egyebek mellett az ipar és a kereskedelem is nagymértékben támaszkodik a modern technológiára. Annak csupán részleges kimaradása is komolyan veszélyeztetheti az ellátási láncokat. További zavart okozhat a MI ellenőrizhetősége. Ahogy az algoritmusok mind összetettebbé válnak, egyre nehezebbé válik a szakemberek számára azok működésének megértése. Ez a jelenség már most is több területen tapasztalható. Jó példa néhány, főleg kínai bank által alkalmazott hitelminősítő algoritmus, ami egészen váratlan tényezőket is figyelembe vesz egy lehetséges ügyfél hitelképességének vizsgálatakor és a rendszer bonyolultsága miatt nem lehet egyértelmű választ adni egy döntés hátterét firtató kérdésre. Szinén fontos rámutatni az emberi társadalomra gyakorolt hatására. Az emberi kapcsolatok megkerülhetetlen színterévé váló közösségi média több szempontból is sérülékeny a MI miatt. A különböző platformokat működtető cégek a haszon maximalizálás vagy ideológiai okok miatt (Twitter levelezés) pontosan adagolják az egyes felhasználóknak a tartalmakhoz való hozzáférést. Ez vezet a véleménybuborékok kialakulásához, ami veszélyesen torzítja a felhasználók gondolkodását. Még súlyosabb probléma lehet, amikor államok, politikai pártok vagy magáncégek manipulációs kampányokat folytatnak fejlett algoritmusok támogatásával állampolgárok, szavazók és ügyfelek magatartásának befolyásolására. Az átlag felhasználó nincs felkészülve az ilyen próbálkozások kezelésére ezért ezek különösen veszélyesek lehetnek.

Köz-Gazdaság: A kutatás egyik sajátossága volt az interdiszciplinaritás. Visszanézve, hogy értékeli az együttműködés szintjét a különböző tudományterületek képviselői között?

Kovács Zoltán: Ezen a területen rendkívül jók a tapasztalataim, az együttműködés beváltotta a hozzá fűzött reményeket. A kutatásba bevont 19 terület kutatói között többrétegű együttműködés alakult ki. Hasznos terepe volt a közös munkának a csoport számára kialakított közös internetes felület és jól beváltak az elmúlt évben megtartott workshopok is, amelyek során lehetőségünk volt megismerni egymás eredményeit. Ezek során rendszeresen élénk beszélgetések alakultak ki a kutatók között és olyan kérdések is fölmerültek, amelyeket elszigetelt kutatóként nehéz feltárni. Mindenképpen érdemesnek tartom a kipróbált együttműködési módszert fenntartani.

Köz-Gazdaság: A kutatás alapján azonosíthatóak-e a főbb veszélyforrások a mesterséges intelligencia fejlesztések kapcsán? Honnan származnak ezek: a felelőtlen fejlesztőktől, a profitvezérelt vállalatoktól vagy az egyes országok, régiók geopolitikai küzdelmeiből?

Kovács Zoltán: A MI fejlesztések kapcsán abban látom a legnagyobb veszélyt, hogy nem tudjuk felmérni az új technológia pontos hatásait. Ezért is tartom kiemelten fontosnak a jelenlegi kutatásunkat. Nem csak azzal kell foglalkozni, hogy egy bizonyos területen milyen következményei vannak a MI elterjedésének – bár ez önmagában is nehéz feladat –, hanem azzal is, hogy az egyes területeken tapasztalt hatások hogyan befolyásolják az összképet.

Evolúciós szempontból az ember nem a modern technikai társadalom gyorsan változó környezetére, hanem viszonylag szerény adatbevitelű és állandó körülményekre van optimalizálva. Az élet különböző területein kialakult alrendszerek olyan bonyolult módon változnak a fejlesztések hatására, aminek feldolgozása nehézséget jelent a felhasználóknak még akkor is, ha a változtatások a tervezettnek megfelelően következnek be. Erre a kockázatra jönnek még rá a fejlesztők hibái és a szándékos rosszakarat, amelyek negatív hatást gyakorolhatnak az életünkre.

Az alkalmazások fejlesztésénél azt tartom a legnagyobb kockázatnak, hogy a fejlesztőmérnökök úgy próbálnak megoldásokat találni a megrendelő által felvetett problémára, hogy nincsenek részletes ismereteik arról. Ez egyrészt megnehezíti, hogy a fejlesztés megfelelő választ adjon a megoldandó kérdésre, másrészt az esetleges nem szándékolt következmények előzetes feltárása is problémás. Ezeket úgy lehet legkönnyebben elkerülni, ha a megrendelők és a fejlesztők a lehető legszorosabban együttműködnek a termék (például egy ügyfélszolgálati chatbot) fejlesztésekor. Egyre nagyobb jelentősége lesz az egyéni igények alapján elkészített termékeknek, amelyek kialakításához a már meglévő MI alkalmazások adhatnak segítséget.

A vállalatok részéről a folyamatos fejlesztési kényszer jelenti a legnagyobb kockázatot. A piaci verseny egyre kiélezettebb és egyre gyorsabban váltják egymást a termékek generációi. A puszta túlélés érdekében minden vállalatnak elemi érdeke, hogy lépést tartson a technológiai fejlődés ütemével. A fejlesztés ütemének felgyorsítása azt okozza, hogy a piacra dobott termékek sok esetben hibákat tartalmaznak. A Microsoft operációs rendszerei nem ok nélkül váltak hírhedtté az ilyen jellegű problémák miatt. A fokozódó verseny következtében egyre gyakrabban várható félkész vagy nem kellően tesztelt szoftverek megjelenése, amelyek biztonsági problémákat generálhatnak.

A nemzetállamok közötti ellentétekben is új eszközt jelentenek a fejlett technológiák. A kibertér jelentőségének növekedésével a kormányzati fegyveres testületek jelentős erőfeszítéseket tesznek hatékony védelmi és támadó eszközök kifejlesztésére és rendszerbe állítására. Az ukrajnai konfliktus is jól mutatja a kibertámadások veszélyességét. Az állami szereplők mellett azonban terrorista csoportok és a szervezett bűnözés is igyekeznek kihasználni az új lehetőségeket. A kibertér e csoportok számára is kedvező terepet teremt megfélemlítő és anyagi haszonszerzésre irányuló tevékenységre.

Köz-Gazdaság: Mit tehet az Európai Unió és Magyarország ezek tompítása érdekében? Lát-e globális egyeztetési mechanizmust a mesterséges intelligencia, illetve tágabban a kibertér szabályozása irányába? Milyen időtávon tudja elképzelni egy jól működő intézmény létrehozását, és mennyire lehet hatékony a globális szabályozás?

Kovács Zoltán: Kifejezetten jó hír, hogy az EU már idejekorán felismerte a MI jelentette kockázatokat és jogszabályokat alkotott azok kezelésére. Az már kevésbé jó hír, hogy ezek hatékonysága kétséges. A 2016-os GDPR sok tekintetben látszatintézkedés, hiszen például az egyik leglátványosabb eleme, a süti használat szabályozása a legtöbb felhasználó számára érthetetlen és fölösleges adminisztratív lépés egy weboldal látogatása előtt. Az EU 2021-ben elfogadott MI stratégiája pedig sok elemében kifejezetten káros. Mivel liberális ideológiai alapon közelíti meg a kérdést, alkalmazása – az adatokhoz való hozzáférés korlátozása miatt – versenyhátrányt okoz Kína és Oroszország, de bizonyos tekintetben még India és az Amerikai Egyesült Államok vonatkozásában is. Pontosan ezért tartom túlzottan optimistának az EU vezetőinek álláspontját, miszerint a többi ország követendő példaként tekint majd az EU MI stratégiájára.

A helyzet azonban kritikus és nem kerülhetjük meg a megfelelő szabályozást. Ennek megvalósítása azonban nem egyszerű. Még az egyes államokon belül sem könnyű a politikai és a gazdasági célokat egyeztetni, szövetségi és globális szinten pedig leküzdhetetlennek tűnő akadályok látszanak. Mindenképp először nemzeti szinten kell határozott álláspontot kialakítani és ezt követően kerülhet sor a regionális és globális egyeztetésre. Sajnos nem tudok javaslatot tenni a szabályozás megvalósítására, de az biztosnak látszik, hogy kidolgozásában politikai, jogi, gazdasági és informatikai szakértőknek egyaránt részt kell majd venni.

Köz-Gazdaság: A techcégek minden államban a gazdaságpolitikai szabályozása középpontjában állnak. Lehet ezeket a cégeket szabályozni? A szabályozó intézmények ráadásul teljesen új helyzetben vannak, hiszen a techcégek a gazdaság, és az élet egészét átfogják, digitális életvilág jött létre. Az államigazgatás mely területének lesz feladata a techcégek ellenőrzése és szabályozása: a fogyasztóvédelemé, a katonai területé, az adatvédelmi hivataloké vagy a titkosszolgálatoké?

Kovács Zoltán: A digitalizáció sok tekintetben demokratizálta a technológiai fejlesztéseket, mivel már nem csak államok és multinacionális cégek képesek maradandót alkotni. Ezért vált jelentős tényezővé néhány startup vállalat a közelmúltban. Fontos azonban leszögezni, hogy a MI fejlesztések legfontosabb eszköze az adat. Minél több adat áll egy szereplő rendelkezésére, annál jobb lehetőségei vannak a további fejlesztésekre és a versenyelőny kiépítésére. A nyugati féltekén jelenleg a Google, a Facebook és a Tesla áll legjobban a rendelkezésre álló hasznos adat tekintetében és szorosan követi őket a kínai Alibaba, Tencent és Tiktok. Ezek a cégek átszővik a társadalom minden rétegét, és a megszerzett adatok, illetve az általuk nyújtott szolgáltatások következtében kiemelkedő anyagi erőforrásokra, ebből adódóan jelentős befolyásra, esetleg hatalomra is szert tesznek. A nyugati demokráciák és az azt működtető pártok sok tekintetben anyagilag függnek a nagy cégektől, ezért ezekben az országokban a cégeknek jelentős lobbi erejük van, amivel befolyásolni tudják a politikai döntéseket és így formálhatják az őket szabályoznia akaró politikai szándékot. Ironikusnak tűnhet, hogy a központosított – autoriter, vagy egyenesen pártállami berendezkedés – alkalmasabbnak lehet a kontroll megvalósítására.

A hatékony ellenőrzés alapja a megfelelő jogalkotás, ami természetesen a parlamentek feladata, de elengedhetetlen a megfelelő szakértői háttér igénybe vétele a munkában. A jogszabályok alkalmazásának ellenőrzésekor a különböző állami intézmények szerepe területenként merül fel. Az adatvédelmi hatóság és a fogyasztóvédelem mellett a rendőrség, az ügyészség és a nemzetbiztonsági szolgálatok is fontos szerepet játszanak saját szakterületükön.

Köz-Gazdaság: Az orosz-ukrán konfliktus jelentős része a kibertérben zajlik. Az eddigi fejlemények alapján milyen kibertechnikai fejlesztések várhatóak különös tekintettel a mesterséges intelligenciára? Kibervédelmi szempontból melyek a tanulságai a konfliktusnak például a mi térségünkre nézve? Tovább egységesül-e a kibervédelem a NATO-n belül, vagy erre nincs szükség?

Kovács Zoltán: A háború az első jelentős fegyveres konfliktus, amelyben a felek kiterjedt kiberműveleti tevékenységet folytatnak. Oroszország már a tényleges invázió kezdete előtt széleskörű kibertámadást indított az

ukrán kritikus infrastruktúra (elsősorban energetikai és telekommunikációs vállalatok, pénzügyi szervezetek és médiaszolgáltatók) ellen azzal a céllal, hogy káoszt teremtsen és ellehetetlenítse az ukrán védelmet. Ukrajna – nyugati hatalmak és a magánszféra segítségével – a korábbi tapasztalatokra építve jól felkészült az orosz támadásra, amelyek hatásossága elmaradt az előzetes értékelések alapján vártnál.

Az információs műveletek tudati dimenziójában végzett orosz műveletek ugyanakkor, bár Nyugaton és Ukrajnában sikertelenül kísérelték meg a közvélemény formálását, sikeresen közvetítették az orosz narratívát a saját közvélemény irányában. Az orosz propagandát honi területén jól támogatta a kínai kormányzat is, sikerült továbbá semleges álláspontot kialakítani az indiai, az afrikai és a közel-keleti közvéleményben, illetve néhány latin-amerikai országban.

A mesterséges intelligencia jelentős segítséget nyújt az ukrán haderőnek a védelmi műveletekben. Jó példa a „Diia" nevű MI alapú alkalmazás, amit bárki feltelepíthet mobiltelefonjára. Az alkalmazás képes fogadni az állampolgárok hadműveleti helyzethez kapcsolódó megfigyeléseit. Csatlakozás után bárki képes megosztani olyan információkat, ami az orosz haderő tevékenységére utal (például, hogy hol milyen katonai eszközöket, vagy csapatmozgást láttak). A bejövő információkat egy algoritmus elemzi é az ukrán felderítés számára. Az eszköz rendkívül hatékonynak bizonyul a beérkező információk kezelésére és a védelmi műveletek támogatására.

A NATO 2002-ben vette fel a kibertér védelmét a politikai napirendjére. A technológiai fejlődéssel egyre nagyobb jelentőséget kapott a terület, míg 2016-ban a Szövetség önálló hadműveleti területként definiálta a kiberteret. Ez azt jelenti, hogy a szárazföld, a tengerek, a levegő és a világűr után a kibertér is dedikált katonai tevékenységek színterévé vált. A NATO értékelése szerint a Szövetség komplex, romboló és erőszakos kiberfenyegetésekkel szembesül, amelyek egyre gyakrabban jelennek meg. A NATO folyamatosan alkalmazkodik az új fenyegetésekhez és felkészül azok hatékony elhárítására. A tagállamok önállóan is jelentős lépéseket tesznek a kiberfenyegetések elhárítására, de a többi védelmi területhez hasonlóan szükség van az erőfeszítések egyeztetésére a kibervédelemben is.

Köszönjük szépen a beszélgetést!