Jog-Állam-Politika, 2024/2.49
DOI: 10.58528/JAP.2024.16-2.49

KELEMEN ROLAND

Az Egyesült Államok hírszerző tevékenységének alkotmányos alapjai és kiberbiztonsági kapcsolódásai[1]

ABSTRACT

In the unique constitutional structure of the United States, the activities of the intelligence community are based on a constitutional mandate, which is essentially derived from the Preamble's directive for common defence. However, these activities are also subject to constitutional checks and balances. Today, the activities of most of these empowered bodies have moved into cyberspace, where they operate within constitutional standards. The laws and strategies developed at the intersection of cybersecurity and intelligence in the United States can be summarised by three characteristics: first, increased efficiency, continuous review and correction; second, deep cooperation between state and non-state actors for efficiency and resilience; and third, constitutional control by the legislature and the judiciary.

Keywords: intelligence ■ constitutional ■ cybersecurity ■ intelligence agencies ■ resilience

I. BEVEZETÉS

Jelenkorunk biztonsági gondolkodásának egyik kiemelt fókuszpontja a kibertér és a hozzá kapcsolódó rendszerek, ugyanis napjaink állama, gazdasága és társadalma óriási mértékben hálózatosodott és összekapcsolt a digitális környezetnek is köszönhetően, ami pedig rendkívüli módon kitetté teszi ezeket a rendszereket az ártó szándékú aktoroknak, legyenek azok állami vagy nem állami szereplők. A kibertér jelentette geopolitikai lehetőségeket a hibriditás révén a hadviselési stratégiák szintjére emelő orosz, kínai, észak-koreai és iráni állam sajátos autoriter

[1] Jelen tanulmány a Kulturális és Innovációs Minisztérium ÚNKP-23-4-II-SZE-65 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

és totaliter rezsimei a belső kibertér totális kontrollján alapuló környezetét felhasználva próbálják főként az euroatlanti térség jogállamainak hálózati és kognitív biztonságát aláásni saját érdekeik érvényre juttatása érdekében. Minderre a biztonsági kockázatra és veszélyre viszont e térség államainak olyan megoldásokat kell találniuk, amelyek önazonosak, vagyis a jogállami standardokat nem veszélyeztetik, sőt valójában azokat megerősítve kell válaszokat kidolgozniuk és megvalósítaniuk.

E kérdéskörnek az egyik sarokpontja a kibertérrel kapcsolatos hírszerző, a magyar szakzsargon szerint nemzetbiztonsági ágens olyan megerősítése a kibertérrel kapcsolatos hatáskörök terrénumában, amely nem eredményez jogállami deficitet. E területen (is) mintaadó állam lehet az Egyesült Államok, ahol az alkotmányos struktúra erősen körbebástyázza az alapvető jogokat, az intézmények feletti alkotmányos kontroll mechanizmusai az egyes hatalmi ágak viszonyrendszerében régóta kidolgozott rendszert eredményeznek.

Így e tanulmány arra vállalkozik, hogy bemutassa az Egyesült Államok hírszerző szerveinek alkotmányos felhatalmazottságát, valamint e szerveknek adott kiberbiztonsággal kapcsolatos hatásköröket és feladatokat.

II. A HÍRSZERZÉS ALKOTMÁNYOS ALAPJAI AZ EGYESÜLT ÁLLAMOKBAN

Az amerikai alkotmányos struktúrában, az alkotmány szentségének és mindenekfelettiségének elveiből kiindulva,[2] minden állami tevékenységi körbe tartozó intézmény felhatalmazása levezethető az alkotmányból, így természetesen nincs ez másként a hírszerzési tevékenység esetében sem.

Az Amerikai Egyesült Államok alkotmányának a Preambuluma az alkotmányos felfogásuk szerint saját jogi erővel rendelkezik, amely egyfajta hatálybaléptető záradék, mivel az alkotmány elfogadásának a tényét jelenti. A Preambulum kollektív akaratot fejez ki az alkotmány megalkotására és a benne foglalt célokra, azokat a hatalmi ágak fölé emelve. A Preambulum az alkotmány létrehozásának okaként, céljaként határozza meg a belső nyugalom biztosítását, a közös védelemről való gondoskodást, valamint a szabadság áldásainak biztosítását.[3] Tehát „kinyilvánított cél egy olyan kormány létrehozása, amely megfelel az emberek szükségleteinek".[4] Viszont ezek a célmeghatározások nem adnak önmagukban hatásköröket egyetlen hatalmi ágnak sem.[5] A Legfelsőbb Bíróság az 1905-ös Jacobson vs. Massachusetts-ügyben meg is erősítette ezt az alábbi érvelésével: „Az Egyesült Államok az Alkotmány Preambulumából nem meríti lényegi hatáskörét. Nem gyakorolhat semmilyen hatalmat az Alkotmány kinyilvánított céljai-

[2] Képes, 2003.
[3] Az Amerikai Egyesült Államok Alkotmánya, Preambulum.
[4] Chemerinsky – Stokes Paulsen, é.n.
[5] Chemerinsky, é.n.

nak biztosítására, hacsak a preambulumon kívül nem található ilyen hatalom az alkotmány valamely kifejezett felhatalmazásában, vagy ha az nem következik megfelelően az alkotmány valamely kifejezett felhatalmazásából. Bár az Alkotmány szellemét nem kevésbé kell tiszteletben tartani, mint betűjét, a szellemét elsősorban a szavaiból kell meríteni."[6]

Mindemellett viszont a szellemével ellentétes alkotmányértelmezést is kizárja, így annak elvitatása sem lehetséges, hogy az Alkotmány egyáltalán azért létezik, hogy hatékony kormányzást teremtsenek a nemzet számára. A Legfelsőbb Bíróság ennek megfelelően a Martin v. Hunter's Lessee-ügyben a Preambulumra is hivatkozva kimondta, hogy az Alkotmányt a nép hozta létre, nem pedig a tagállamok saját szuverén minőségükben, ahogy fogalmaz: „kevés kétség merülhet fel afelől, hogy a népnek joga volt megtiltani az államoknak minden olyan hatáskör gyakorlását, amely megítélése szerint összeegyeztethetetlen az általános szerződés céljaival… Az Egyesült Államok kormánya tehát nem tarthat igényt olyan hatáskörökre, amelyeket az Alkotmány nem biztosít számára, és a ténylegesen biztosított hatásköröknek olyanoknak kell lenniük, amelyeket kifejezetten vagy szükségszerűen hallgatólagosan adtak meg."[7] Ez az érvelés pedig elvárja John Jay – többek között a Legfelsőbb Bíróság főbírájának – szavaival élve, hogy forduljunk vissza az Alkotmányhoz, amelyben a szuverén, alkotmányozó nép hat általános célt fogalmazott meg,[8] amelynek pedig oszthatatlan részét képezi a „közös védelemről való gondoskodás". Ugyanis az Alapítóatyák számára a szövetségi kormány elsődleges és központi feladata a közös védelemről való gondoskodás.[9] E közös védelem pedig a Kongresszus és az Elnök közös feladata, amelyet az Alkotmány konkrét rendelkezései tesznek lehetővé. Ez pedig bővíti a Kongresszus (és nyilván a végrehajtó hatalom) hatáskörét, hogy megtehessen bármilyen intézkedést a közös védelem érdekében.[10] Amely vélekedést megalapozza, hogy a Kongresszus hatásköreit tartalmazó 1. cikk 8. §-a szerinti taxáció utolsó eleme kimondja a szükséges és elégséges klauzulát, amely lehetővé teszi a felsorolt hatáskörök korokhoz, élethelyzetekhez igazodó értelmezését. Így e cél szavatolása érdekében mind a Kongresszust, mind pedig az Elnököt különleges hatáskörök illetik meg. [11]

E különleges helyzetekben pedig a megalapozott döntések meghozatalához elengedhetetlen az azokat alátámasztó információk és adatok birtoklása is. Így nem meglepő, hogy az amerikai alkotmányos felfogás abból indul ki, hogy a demokratikus társadalom stabilitását veszélyeztető erőszakos fenyegetésekkel szemben a hatékony védelem csak akkor valósítható meg, ha az ehhez szükséges informá-

[6] Jacobson v. Massachusetts, 197 U.S. 11 (1905).
[7] Martin v. Hunter's Lessee, 14 U.S. 304 (1816).
[8] Story, 1873, 341.
[9] Eaglen, 2011.
[10] Story, 1873, 339.
[11] Kelemen, 2020, 107-120.

ciók rendelkezésre állnak.[12] Ahhoz, hogy az állam biztonsága szavatolva legyen, ahhoz hozzátartozik a hírszerző szolgálatok tevékenysége is. Ez így volt már a kezdetekkor is, hiszen George Washington is számos ügynököt alkalmazott, ami befolyásolta a függetlenségi háború kimenetelét.[13] A fentiekből is adódóan, ennek jogszabályi kereteit a Kongresszus tudja megteremteni, emellett viszont annak gyakorlati megvalósítása abból vezethető le, hogy „az elnököt minden végrehajtó hatalom megilleti… ez különösképpen vonatkozik a háborúk és a nemzetbiztonság kérdéseire, mivel az elnök a fegyveres erők főparancsnoka".[14]

A hírszerző tevékenység egyik alkotmányos alapja így a közös védelem szavatolásához szükséges információk megszerzésének igényén nyugszik, amelyek az elnököt illetik meg, akinek eme joga a II. cikk 2. § első bekezdéséből vezethető le. Emellett, ahogy Philip A. Lacovara kiemeli, a külföldi hírszerző tevékenység elnöki jogkörként megjelenő alkotmányos alapját a II. cikk második bekezdése is adja, ugyanis eredményes külkapcsolatok és külpolitika folytatása elképzelhetetlen volna a megfelelő információk hiányában.[15]

A fentiek ellenére – követve a nemzetközi folyamatokat – maga a hírszerzői tevékenység szervezeti keretek között váratott magára. A katonai hírszerzés létrejötte megelőzte a polgári hírszerzést, azonban a 19. század végéig gyakorlatilag csak háborús időszakban létezett az amerikai hadseregben hírszerző osztály. A haditengerészet berkein belül 1882-ben állították fel a Hírszerzési Hivatalt, amely ekkor inkább a tengerészet fejlesztésének motorjaként működött. Húsz évvel a polgárháború után, 1885-ben jött létre a Katonai Információs Osztály, ami 1903-ban alakult át a Tábornoki Főhadiszállás Második Osztályává. A két világháború nyilvánvalóan megkövetelte a katonai hírszerzés létezését, azonban ez leginkább a kialakult helyzethez való igazodást jelentette. 1946 hozta el a Katonai Hírszerző Osztály dominanciáját, majd az azt követő negyven év hatásainak (hidegháború, technológiai fejlődés, hadviselés átalakulása) köszönhetően a haderő minden ágában megjelent a hírszerző részleg. A hadsereg berkein belül a kibertérrel kapcsolatos hírszerző szervezetet, a Sixteenth Air Force-t, vagy másnéven Air Forces Cyber-t 2019-ben állították fel.[16]

Az Egyesült Államokban a modernkori polgári hírszerzés születését a Központi Hírszerző Ügynökség (CIA) 1947-es felállításához kötik. Az Egyesült Államok modern polgári hírszerzési és nemzetbiztonsági tevékenysége, valamint annak szabályozása 1947-re tehető, ekkor fogadta el a Kongresszus a National Security Act of 1947-et, vagyis a nemzetbiztonsági törvényt. E törvény mai napig a vizsgált terület legfontosabb jogszabálya. A törvény megalkotásának célja: átfogó szabályozást adni az Egyesült Államok biztonsága érdekében, hogy az érintett minisztériumok, ügynökségek egységes és átfogó irányelvek és eljárások

[12] Ez jelenik meg már John Jay Föderalista levelekben közzétett gondolataiban is. Lásd: Morris, é.n.
[13] Kelly, 2019, 95.
[14] Spalding, 2011, 64.
[15] Lacovara, 1976, 107.
[16] Finnegan – Danysh, 1998.

mentén végezzék tevékenységüket, felszámolja a párhuzamos tevékenységeket és átfogó irányítást és ellenőrzést biztosítson az ágazat felett. A törvény kiadáskori hatályos állapota szerint a hírszerző közösség vezetője a központi hírszerzés igazgatója volt (director of central intelligence), aki egyidejűleg a Központi Hírszerző Ügynökség igazgatója is volt.[17] 1981-ben Ronald Reagen létrehozta a Hírszerző Közösséget (Intelligence Community), amelyhez ekkor tizenhat nemzetbiztonsági szervezet/ügynökség tartozott.[18]

A fékek és ellensúlyok rendszeréből adódóan az amerikai alkotmány nem engedi a hírszerző tevékenység területén sem az elnöknek, hogy monopolizált helyzetet teremtsen, vagyis e területen is elszámoltathatónak kell lennie a Kongresszus és a Legfelsőbb Bíróság irányába. A Kongresszus ezen, felügyeleti jogköre nyilvánvaló módon pedig szintén az Alkotmányból eredeztethető, mégpedig az I. cikk 8. § védelmi jellegű felhatalmazásaiból.[19] A polgári hírszerzés esetében kezdetben a hidegháborús viszonyok miatt nem volt összeütközés a két hatalmi ág között e kérdéskörben, vagyis az 1970-es évek közepéig a Kongresszus két házának albizottságai csak névlegesen gyakoroltak felügyeletet a hírszerzés felett, azonban a Watergate-ügy változásokat hozott, amelyet követően az évtized végére a Kongresszus mindkét háza állandó bizottságot állított fel[20] a hírszerzés ellenőrzésére. E két bizottságnak joga a hírszerzési titkok teljeskörű megismerése és a hírszerzési költségvetések jóváhagyása, ezáltal pedig felügyelet gyakorlása a hírszerzési szervezetrendszer felett.[21]

Jelentős változást hoztak 2001. szeptember 11. tragikus eseményeinek hírszerzési negatív tapasztalatai, amelynek következtében Bush elnök kezdeményezésére a ház elfogadta 2004-ben a hírszerzési tevékenység reformját jelentő törvényt, amely létrehozta a Hírszerző Közösség irányítására a Nemzeti Hírszerző Igazgató pozícióját és annak hivatalát. Az Igazgató hírszerzési és nemzetbiztonsági kérdésekben közvetlenül az elnöknek jelent, továbbá éves beszámolással tartozik a Kongresszus szakági bizottságának. A Nemzeti Hírszerző Igazgató Hivatalába integráltan több központ jött létre,[22] amely az eredetihez képest kibővült a Kiberfenyegetettségi Hírszerzési Integrációs Központtal (Cyber Threat Intelligence Integration Center, 2015) és a Külföldi Rosszindulatú Befolyásolásellenes Központtal (Foreign Malign Influence Center, 2022). Így napjaikra az elnök és kongresszus felügyelete mellett már a Nemzeti Hírszerző Igazgató Hivatalába integrálva is működik a kiberbiztonság mindkét ágensére (hálózatbiztonságra és kognitív biztonságra) fókuszáló szervezeti egység, ami

[17] From Director of Central Intelligence to Director of National Intelligence.

[18] Béres, 2018, 66.

[19] Többek között a háború és béke kérdése, haderő alkalmazása, a haderő fenntartása, a haderő szervezetének meghatározása, a haderő irányítása.

[20] U.S. Senate Select Committee on Intelligence (1976) és House Permanent Select Commitee on Intelligence (1977).

[21] Ransom, 1987, 43-50.

[22] Intelligence Reform and Terrorism Prevention Act of 2004.

jól mutatja e terület kiemelt szerepét, mindemellett pedig a fentieket követve az is rögzíthető, hogy e szervek a hírszerző tevékenységüket a kibertérben vagy ahhoz kapcsolódóan is alkotmányos felhatalmazás alapján végzik.

III. EGYES KIBERBIZTONSÁGI JOGSZABÁLYOK HÍRSZERZÉSI RELEVANCIÁI

E fejezet arra vállalkozik, hogy az előzőekben bemutatott alkotmányos kereteket a kiberbiztonság terrénumában milyen hatáskörökkel, feladatokkal tölti fel a jogalkotó annak érdekében, hogy biztosítani tudja a rezilienciát és az együttműködést az egyes állami és civil szervezetekkel, továbbá a kritikus és kapcsolódó infrastruktúrák biztonságának fokozását. Ennek érdekében érdemes röviden megnézi, hogy a hírszerzési szereplők ezen területen milyen hatáskörrel bírnak.

A 2002-es Homeland Security Act a belbiztonsággal kapcsolatos hírszerző és nemzetbiztonsági tevékenység kereteit határozza meg, létrehozva a Belbiztonsági Minisztériumot (Department of Homland Security). A jogszabály konkrét rendelkezéseket tartalmaz a kibertérrel és kiberbiztonsággal kapcsolatban. E törvény rendelkezései szerint a Minisztériumnak létre kell hoznia – a 2004-es hírszerzési reformtörvény előírásainak megfelelően – az átfogó informatikai architektúrát a Hírszerzési és Elemzési Hivatal (Office of Intelligence and Analysis) számára. A Hivatal a Minisztérium 2007-ben felállított polgári hírszerzési részlege, amely tagja a Hírszerzési Közösségnek. A létrehozott architektúra lényege, hogy a Hivatalt összekapcsolja a minisztérium hírszerző részlegeinek adatbázisaival, elősegítve a belső információcserét.[23] Szintén egy törvény állította fel és szabályozza a Kiberbiztonsági és Infrastruktúra-biztonsági Ügynökséget (Cybersecurity & Infrastructure Security Agency [CISA]), az Egyesült Államok egyik legjelentősebb kiberbiztonsági intézményét.[24] Szintén a törvény írta elő, hogy a Belbiztonsági Miniszternek létre kellett hoznia és fenn kell tartania egy nemzeti adatbázist olyan rendszerekről, amelyeket a tagállami belbiztonsági tisztviselőkkel konzultálva létfontosságúnak minősítenek, az alapján, hogy a bennük lévő adatok elvesztése, hozzáférhetetlenné tétele vagy megsemmisülése jelentős hatással lenne az Egyesült Államok, illetve bármely tagállam vagy helyi önkormányzat gazdaságára, közegészségügyére vagy biztonságára, továbbá olyan egyéb rendszerek, amelyeket a miniszter ilyennek minősít. A kritikus infrastruktúrákról kialakított adatbázist a miniszter az elnök hetedik számú belbiztonsági irányelvével összhangban állítja össze. Az adatbázist a miniszter évente frissíti, amelyhez a szükséges adatokat a tagállami belbiztonsági tisztviselők szolgáltatják. Az adatbázis célja, hogy a megfelelő tervezés felkészítsen a lehetséges jövőbeli fenyegetések kezelésére. E tevékenységéről a miniszter évente beszámolót készít a Szenátus belbiztonsági és kormányzati ügyekkel

[23] Department of Homeland Security Appropriations Act, Sec. 205-206.
[24] Department of Homeland Security Appropriations Act, Title XXII.

foglalkozó bizottságának, a beszámoló kiemelt része a terrorizmussal leginkább fenyegetett infrastruktúrák listája, valamint a minisztérium és a magánszektor közötti koordináció mértékének ismertetése.[25]

A 2014-es Szövetségi információbiztonság korszerűsítéséről szóló törvényt a digitalizáció magas foka hívta életre. A módosítás célja többek között a következők: átfogó keretrendszer létrehozása a szövetségi szervek működését és eszközeiket támogató erőforrások információbiztonsági ellenőrzésének hatékonyabbá tétele, valamint a kapcsolódó információbiztonsági kockázatok hatékony kormányzati szintű kezelésének és felügyeletének a biztosítása, továbbá szövetségi információs rendszerek és információk védelméhez szükséges szabályozási minimumok kidolgozása és betartatása érdekében.[26]

A törvény osztott hatáskört állapít meg a belbiztonsági miniszter és a Nemzeti Szabványügyi és Technológiai Intézet igazgatója között. Utóbbi feladata a törvény szerint, hogy felügyelje az információbiztonsági szabályzatokat és módszereket, ebbe beleértve többek között az elvek, szabványok és iránymutatások kidolgozásának és végrehajtásának a felügyeletét, továbbá, hogy az ügynökségek a jogszabályban kihirdetett szabványokkal összhangban határozzák meg és biztosítsák az információbiztonsági védelmet, amelynek arányosnak kell lennie a felmerülő biztonsági kockázatokból eredő károkkal, valamint a szabványok és iránymutatások kidolgozásának összehangolása azon szervek között, amelyek nemzetbiztonsági rendszereket üzemeltetnek vagy azok felett ellenőrzést gyakorolnak. A miniszter az igazgatóval konzultálva felügyeli az információs rendszerekre vonatkozó információbiztonsági szabályok és gyakorlatok végrehajtását, kivéve a nemzetbiztonsági rendszereket. E tevékenységükről legkésőbb minden év március 1-ig jelentést tesznek a Kongresszusnak. Az igazgatóra vonatkozó hatásköröket a Védelmi Minisztériumhoz kapcsolódó szervek esetében a védelmi miniszter, míg a Hírszerző Közösség vagy ahhoz kapcsolódó valamely gazdasági szervezet, illetve ilyen nevében e területen eljáró más szervezet tekintetében a Nemzeti Hírszerző Igazgató gyakorolja. A törvény lehetőséget biztosít a miniszter számára, ha potenciális támadást lehetőségét észlelik, hogy ennek elhárítása érdekében azonnali szabványt, gyakorlatot vagy módszertani módosításokat tartalmazó utasításokat adjon az érintett szerv számára.[27]

A Homeland Security Act felhatalmazása alapján a miniszter engedélyezheti behatolásfelderítési és -megelőzési eszközök használatát, ha közvetlen veszély fenyegeti a rendszereket, ha a korábban ismertetett felhatalmazások nem eredményeznének időbeni reagálást, ha az eszközök alkalmazásából eredő károk mértéke nem haladja meg a potenciális kár mértékét, továbbá erről értesíti az érintett ügynökséget, annak informatikai vezetőjét és az ügynökség szerint érintett kongresszusi bizottságot. A törvény azt is előírja, hogy az egyes ügynökségeknek minden évben el kell végezniük az információbiztonsági programjuk és gyakorlatuk

[25] Department of Homeland Security Appropriations Act, Sec. 2214.
[26] Federal Information Security Modernization Act of 2014, Sec. 3351.
[27] Federal Information Security Modernization Act of 2014, Sec. 3553.

független értékelését. A független értékelést a szabványügyi intézet főfelügyelője vagy az általa meghatározott külső szereplő végzi. A nemzetbiztonsági rendszerek esetében minden egyes nemzetbiztonsági rendszert működtető vagy azt ellenőrző ügynökség esetében az értékelést, ami a nemzetbiztonsági rendszerre vonatkozik, kizárólag az ügynökség vezetője által kijelölt szerv végezheti. A törvénynek megfelelően, a miniszter szövetségi információbiztonsági incidensközpontot állított fel, amelynek feladata technikai segítségnyújtás a biztonsági incidensekkel kapcsolatban, beleértve az észlelést és a kezelést is, az ezekkel kapcsolatos adatok összegyűjtése és elemzése, az alárendelt ügynökségek tájékoztatása a potenciális veszélyforrásokról, adott esetben pedig hírszerzési és egyéb információkat szolgáltat kiberfenyegetésekről, sebezhetőségekről és incidensekről az ügynökségeknek. A nemzetbiztonsági rendszerekkel kapcsolatban előírja, hogy minden nemzetbiztonsági rendszert működtető vagy azt felügyelő ügynökségnek meg kell osztania az ilyen típusú információkat a szövetségi információbiztonsági incidensközponttal, azonban csak olyan mértékben, hogy az az érintett rendszerekre vonatkozó jogszabályokkal és elnöki utasításokkal összhangban legyen, ezzel is elősegítve a polgári szervek hatékonyabb feladatellátását.[28]

A nemzetbiztonsági rendszerekkel kapcsolatban kifejti, hogy annak vezetője felelős annak biztosításáért, hogy olyan információbiztonsági védelmet valósítsanak meg, amely arányos az ilyen rendszerben tárolt adatok jogosulatlan hozzáféréséből, megzavarásából, nyilvánosságra hozatalából, módosításából vagy megsemmisítéséből eredő károk kockázatával, továbbá a szervezet végrehajtja a rendszereire vonatkozó jogszabályokba, elnöki utasításokba foglalt szabványokat és gyakorlatokat.[29]

A 2015-ös Cybersecurity Act egyik elvárása, hogy a minősített adatok, a hírszerzési források és módszerek védelmével, valamint a szabadságjogokkal összhangban a Nemzeti Hírszerző Igazgató (DNI), a belbiztonsági miniszter, a védelmi miniszter és a főügyész a hatáskörrel rendelkező szerv vezetőjével konzultálva, közösen eljárásokat dolgozzanak és adjanak ki (például kiberfenyegetettségi mutatókat és védelmi intézkedéseket, információ megosztására és legjobb gyakorlatokra).[30] Az ilyen eljárások lényege az, hogy ezáltal biztosítani tudják az információk valós idejű megosztását, amit a lehető legteljesebb mértékig be kell építeni az egyes szövetségi és nem szövetségi szervek meglévő folyamataiba, beleértve az ágazatspecifikus információmegosztó és -elemző központokat is, de mindeközben a személyes adatokat a lehető legteljesebb módon tiszteletben tartva. Nagyon fontos része a szabályozásnak, hogy a vállalati szféra számára is lehetővé teszi a csatlakozást ebbe az információmegosztási rendszerbe. A törvény szerint kidolgozott eljárásokat a felhatalmazott szerveknek be kell nyújtaniuk a Kongresszushoz, így megvalósítva a hírszerzés, nemzetbiztonság feletti alkotmányos kontrollt.[31]

[28] Federal Information Security Modernization Act of 2014, Sec. 3554-3556.
[29] Federal Information Security Modernization Act of 2014, Sec. 3557.
[30] Cybersecurity Act of 2015, Sec 103.(a).
[31] Cybersecurity Act of 2015, Sec 103.(b)-(c).

A törvény a fentieknek köszönhetően lehetővé teszi, sőt a hatékony információáramlás érdekében előírja eljárások kidolgozását arra, hogy a hírszerzési, nemzetbiztonsági szervek irányítói szükséges esetben adatokat és információkat szolgáltassanak a kibertámadással fenyegetett vagy érintett szerv vezetőjének, emellett a megfelelő felkészülés érdekében a legjobb gyakorlatok megosztását is előírja. Ezeknek köszönhetően a hírszerzési ernyőszervek vezetői egy felgyorsított információáramlást valósíthatnak meg egymás és az érintett szövetségi és nem szövetségi szervek vezetői között.[32]

A törvény lehetővé teszi a kiberbiztonsági fenyegetések megelőzése, felderítése, elemzése és mérséklése érdekében, hogy a felhatalmazott szervek a kiberbiztonsági célok érdekében figyelemmel kísérjék szövetségi és nem szövetségi szervek és csatlakozó magánjogi alanyok információs rendszerét, illetve az általuk felügyelt információs rendszerben tárolt, feldolgozott vagy azon áthaladó információt. Ezen lehetőség azonban semmi esetben sem értelmezhető akként, hogy az felhatalmazást adna az adott információs rendszer megfigyelésére vagy az ilyen megfigyelés során szerzett információk felhasználására az előzőektől eltérő körben, illetve a megfigyelt, egyébként jogszerű tevékenység korlátozására.[33] Olyannyira, hogy a törvény kizárja annak is a lehetőségét, hogy ilyen megfigyelés során szerzett – a megfigyelés jogcímével nem összeegyeztethető – információ felhasználásával nem indítható vagy tartható fenn kereset civil személlyel vagy szervezettel szemben.[34] Ezek a garanciák azért kifejezetten fontosak, mivel ezek növelhetik a kormányzatba vetett bizalmat vállalkozói oldalról, így növelve a programhoz való csatlakozást is.[35] A programhoz való csatlakozás pedig kötelezi a magánszféra vállalkozását is a szükséges kiberbiztonsági mutatók és eljárások átvételére, és rájuk is vonatkozik a jelentéstéli kötelezettség. Mindezeknek köszönhetően pedig egy egységesebb és hatékonyabb kiberbiztonsági közeg alakítható ki.[36]

A szervezetek feletti törvényhozási kontrollt tovább erősíti, hogy egy évvel a törvény hatályba lépése után jelentést kellett tenniük, lényegében annak tartalmi végrehajtásáról. Emellett a jogszabály előírta az első két év utáni, majd folyamatosan, legalább kétévente való jelentéstételi kötelezettséget a Kongresszus irányába. Ezen ügynökségközi jelentéseket a feljogosított szövetségi szerveknek a főfelügyelői, valamint a ODNI főfelügyelője (Inspector General of the Intelligen-

[32] A magyar fegyveres védelmi ágazat esetében (nem csak kiberbiztonság területén) Farkas Ádám évek óta az ilyen típusú információáramlást szorgalmazza az egyes ágazatokon belül és ágazatok között. Lásd: Farkas, 2019.

[33] Cybersecurity Act of 2015, Sec 104.

[34] Cybersecurity Act of 2015, Sec. 106.

[35] Ez a fajta kooperációs együttműködés elengedhetetlen ahhoz, hogy az autoriter rezsimek jelentette kibertéri fenyegetéseket jogállami keretek között tudják kezelni az euroatlanti térség államai. Lásd: Kelemen, 2023, 13-42.

[36] Cybersecurity Act of 2015, Sec. 106.

ce Community)[37] és Pénzügyi Felügyelet Főfelügyelőinek Tanácsa, egymással konzultálva, közösen készítik el és nyújtják be.[38] A felhatalmazás Kongresszus általi ellenőrzés, kiterjed egyfelől a szervek által előterjesztett szakmai kontrollra, valamint a feljogosított szervek törvényességi, szakszerűségi ellenőrzését megvalósító főfelügyelők által előterjesztett revízióra is.

Az Egyesült Államok kiberbiztonságának javítása érdekében a törvény hatálybalépését követő 180 napon belül a DNI-nak a Gazdálkodási és Költségvetési Hivatal igazgatójával és más ügynökségek vezetőivel egyeztetve azonosítaniuk kellett minden olyan, nem minősített információs rendszert, amely hozzáférést biztosít olyan információkhoz, amelyek egy szembenálló szereplő (akár állam, akár nem állami) számára lehetőséget biztosíthatnak olyan információk megszerzésére, amelyek egyébként minősítettnek minősülnének, továbbá felmérik az azonosított minden egyes, nem minősített információs rendszer megsértéséből eredő kockázatokat, valamint felmérik az abból eredő költségeket, ha az ilyen rendszert később nemzetbiztonsági rendszerré minősítenék.[39]

A törvény jelentős előnye volt a kiberbiztonság területén, hogy egy hatalmas lépést tett a vállalati szférával való együttműködés felé a vállalati biztonság, végső soron pedig a nemzetbiztonság érdekében. Az önkéntes alapú csatlakozás következtében a vállalatok információkat kaphatnak a kiberfenyegetésekről, azokkal kapcsolatos eljárásokról, de a vállalattal kapcsolatos kiberbiztonsági indikátorok megoszthatóak a szövetségi ügynökségekkel és nem szövetségi szervezetekkel, nyilvánvalóan anonimizált módon.[40] Ez pedig segít kidolgozni legjobb gyakorlatokat, figyelemmel kísérni az ártó szándékú szereplőket, valamint tapasztalatokat adhat azok szerveződéséről.

Lathrop azonban megfogalmazta azt a kritikát a törvénnyel kapcsolatban, hogy a gyakorlatban csak visszafogottan hatott a kibertámadások folyamatos eszkalálódására, ez szerinte főként azért volt, mert nem számolt a mesterséges intelligencia ilyen, jelentős fejlődésével, amit a kiberbűnözők és külső államok is felhasználtak.[41] 2015-ben a jogalkotó a hibriditás ekkora volumenű térnyerésére, a biztonsági környezet ilyen arányú változására vagy az ártó szándékú szereplők jelentős szaporodására valószínűleg nem számított, és talán nem is számíthatott.[42]

Nagy lépést jelent az önkéntes rendszerhez képest, hogy 2022-ben elfogadták a Cyber Incident Reporting for Critical Infrastructure Act-et (CIRCA), amely a kritikus infrastruktúrák esetében már kötelezővé teszi a bejelentést kiberinci-

[37] IG támogatja a nemzeti hírszerzés igazgatóját (DNI) annak biztosításában, hogy a DNI irányítása alá tartozó programokat és tevékenységeket hatékonyan és eredményesen hajtsák végre, az alkotmánnyal, a szövetségi törvényekkel és a vonatkozó szabályzatokkal összhangban, valamint csalástól, pazarlástól és visszaélésektől mentesen. (Ld. Office of the Director of National Intelligence: Divisions and Offices).

[38] Cybersecurity Act of 2015, Sec. 107.

[39] Cybersecurity Act of 2015, Sec. 107.

[40] Panetta – Schroth, 2015.

[41] Lathrop, 2020, 501-533.

[42] Farkas, 2022, 113-124.

densek esetében. Megalkotásának az indoka, hogy az amerikai kritikus infrastruktúrák elleni kibertámadások komoly nemzetbiztonsági fenyegetést jelentenek, és a törvényt megelőzően egyetlen amerikai kormányzati ügynökség sem rendelkezett rálátással az amerikai létfontosságú infrastruktúrák ellen naponta elkövetett összes kibertámadásra, így az ezekkel arányos válaszlépéseket sem tudták megtenni. A törvény ennek megfelelően eszközöket biztosít az amerikai kritikus infrastruktúrák elleni zsarolóprogramokat és más kibertámadásokat végrehajtó külföldi kormányzati és bűnszervezetek azonosításához, figyelmeztetéséhez és az ellenük való védekezéshez. A CIRCA előírja a Kiberbiztonsági és Infrastruktúrabiztonsági Ügynökség (CISA) számára, hogy dolgozzon ki és hajtasson végre olyan szabályozást, amely előírja az érintett szervezetek számára, hogy jelenteniük kell a CISA-nak az érintett kiberincidenseket és váltságdíjfizetéseket. A törvény kötelezi a kritikus infrastruktúrával foglalkozó szervezeteket, hogy 72 órán belül jelentsenek a CISA-nak, ha jelentős kiberbiztonsági incidenst észlelnek, valamint 24 órán belül jelenteniük kell, ha váltságdíjat fizetnek ransomware-támadás esetén. A többi szövetségi ügynökséget is kötelezi arra, hogy osszák meg a kapott jelentéseket a CISA-val.[43]

IV. ÖSSZEGZÉS

Az Egyesült Államok alkotmányos rendszeréből adódóan, a kibertérrel kapcsolatos hírszerzési tevékenység is alkotmányos felhatalmazottság mellett és alkotmányos kontrollmechanizmusokkal körbebástyázva valósul meg.

A kiberbiztonság és hírszerzés kapcsolódásain megalkotott jogszabályok az Egyesült Államok esetében három jellemzőben ragadhatóak meg: 1. hatékonyság növelése, folyamatos felülvizsgálat és korrekció; 2. állami és nem állami szereplők közötti mélységi kooperáció a hatékonyság és reziliencia érdekében; 3. a törvényhozás és az igazságszolgáltatás alkotmányos kontrollja mellett.

Az első esetkör már önmagában a jogszabályok időközönkénti, folyamatos felülvizsgálatán is érzékelhető, viszont maguk a jogszabályok is előírják a felhatalmazott szervezetek számára, hogy az általuk kidolgozott szabályok megvalósítását folyamatosan monitorozniuk kell, de emellett az érintett szerveknek is a hatékonyság növelése érdekében felül kell vizsgálniuk saját eljárásaikat, újra kell értékelni folyamataikat, amelyekről jelentést kell tenniük. Ez pedig folyamatos fejlődésre ösztönzi a szereplőket, hiszen mindenki érdeke a gördülékeny együttműködés.

Ezt segíti még a második jellemző, a kooperáció ösztönzése, amelybe nem csupán az egyes hírszerzési szereplőket vonta be a jogalkotó, hanem – a hírszerzési érdekek és alapjogok megsértése nélkül – más érintett szövetségi vagy

[43] Cyber Incident Reporting for Critical Infrastructure Act of 2021, Sec. 2241-2242.

tagállami intézményeket is, emellett pedig magánjogi jogalanyokat is. Az információs együttműködés elősegíti, hogy a hatóságok teljesebb képet kapjanak a kiberfenyegetésekről, átfogó, összehangolt eljárásokat dolgozzanak ki, illetve szereplőkön átnyúló legjobb gyakorlatokat tudnak kialakítani, a másik oldal pedig gyorsabban fog tudni reagálni az incidensekre, esetlegesen még az incidenst megelőzően értesülhet a lehetséges támadásról, emellett a saját gazdasági kapacitásához képest magasszintű kiberbiztonsági protokollokat és legjobb gyakorlatokat ismerhet meg.

A harmadik pillér pedig egy fontos cezúrát jelent az autokratikus/totaliter cyberfare rezsimek és a demokratikus, jogállami keretek között létező digitális államok között, hiszen minden, ezzel kapcsolatos hírszerzési tevékenység törvényhozási kontroll mellett valósítható meg, sőt a szabályozás az igazságszolgáltatás útján is védi a magánjogi jogalanyok alapjogait. Nyilván ezen rendszer is érdekközpontú, ami esetenként visszaéléseket eredményez, azonban a szabályozási és szervezeti törekvések a jogállami standardok megtartását kívánják meg.

IRODALOM

- Béres János (szerk.) (2018): *Külföldi nemzetbiztonsági szolgálatok.* Zrínyi Kiadó, Budapest.
- Chemerinsky, Erwin – Stokes Paulsen, Michael (é.n.): The Preamble. In: *National Constitution Center.* (Elérhető: https://constitutioncenter.org/the-constitution/preamble/interpretations/37. Letöltés ideje: 2024.02.04.).
- Chemerinsky, Erwin (é.n.): Giving Meaning to the Preamble. In: *National Constitution Center* (Elérhető: https://constitutioncenter.org/the-constitution/preamble/interpretations/37. Letöltés ideje: 2024.02.04.).
- Eaglen, Mackenzie (2011): Why Provide for the Common Defense? In: *The Heritage Foundation.* (Elérhető: https://www.heritage.org/defense/report/why-provide-the-common-defense. Letöltés ideje: 2024.02.04.).
- Farkas Ádám (2019): *Az állam fegyveres védelmének alapvonalai*. Katonai Nemzetbiztonsági Szolgálat, Budapest.
- Farkas Ádám (2022): The Status and Role of Law and Regulation in the 21st-Century Hybrid Security Environment. In: *Acta Universitatis Sapientiae Legal Studies.* Vol. 2/2022.
- Finnegan, John Patrick – Danysh, Romana (1998): *Military Intelligence.* Center of Military History United States Army, Washington D. C.
- Kelemen Roland (2020): Az Amerikai Egyesült Államok kivételes hatalmi rendszerének fejlődése a hosszú 19. században. In: *Iustum Aequum Salutare.* 2020/3. sz.
- Kelemen Roland (2023): Cyberfare State modelljei: A digitális állam lehetséges irányai. In: Farkas Ádám – Kelemen Roland (szerk.): *A fejlődés fogságában? Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből.* Gondolat Kiadó, Budapest.
- Kelly, William E. (2019): The President and Intelligence Communities. In: *American Intelligence Journal.* Vol. 2/2019.
- Képes György (2003): *A tökéletes unió: Az Amerikai Egyesült Államok alkotmánya.* Gondolat Kiadó, Budapest.

• Lacovara, Philip A. (1976): Presidential Power to Gather Intelligence: The Tension Between Article II and Amendment IV. In: *Law and Contemporary Problems.* 1976/Summer. DOI: https://doi.org/10.2307/1191394.
• Lathrop, Bert (2020): The Inadequacies of the Cybersecurity Information Sharing Act of 2015 in the Age of Artificial Intelligence. In: *Hastings Law Journal.* Vol. 2/2020.
• Morris, Richard B. (é.n.): *Essay: John Jay and the Constitution. Based on the Notes of Professor Richard B. Morris (1904-1989) and his Staff, Originally Prepared for Volume 3 of the Papers of John Jay.* (Elérhető: https://dlc.library.columbia.edu/jay/jay_constitution. Letöltés ideje: 2024.02.04.).
• Panetta, Joseph J. – Schroth, R. Andrew (2015): *Cybersecurity Act of 2015 Review – What it Means for Cybersecurity Governance and Enterprise Risk Management*. Kogod Cybersecurity Governance Center, Washington.
• Ransom, Harry Howe (1987): The Intelligence Function and the Constitution. In: *Armed Forces & Society.* 1987/Fall.
DOI: https://doi.org/10.1177/0095327x8701400104.
• Spalding, Matthew (2011): *Az Amerikai Függetlenségi Nyilatkozat és Alkotmány alapelvei.* Századvég Kiadó, Budapest.
• Story, Joseph (1873): *Commentaries on the Constitution of the United States: with a Preliminary Review of the Constitutional History of the ColoniesPreliminary Review of the Constitutional History of the Colonies and States Before the Adoption of the Constitutionand States Before the Adoption of the Constitutio.* Little, Brown and Company, Boston. DOI: https://doi.org/10.4135/9781071800942.n14.

EGYÉB FORRÁSOK

• Az Amerikai Egyesült Államok Alkotmánya.
• Cyber Incident Reporting for Critical Infrastructure Act of 2021. (Elérhető: https://www.congress.gov/bill/117th-congress/house-bill/5440/text. Letöltés ideje: 2024.02.04.).
• Cybersecurity Act of 2015. (Elérhető: https://www.intelligence.senate.gov/sites/default/files/legislation/Cybersecurity-Act-Of-2015.pdf. Letöltés ideje: 2024.02.04.).
• Department of Homeland Security Appropriations Act, 2022. (Elérhető: https://www.congress.gov/bill/117th-congress/house-bill/4431/text. Letöltés ideje: 2024.02.04.).
• Federal Information Security Modernization Act of 2014. (Elérhető: https://www.congress.gov/bill/113th-congress/senate-bill/2521. Letöltés ideje: 2024.02.04.).
• From Director of Central Intelligence to Director of National Intelligence. In: Jeffrey T. Richelson (szerk.): *National Security Archive Electronic Briefing Book No. 144.* Washington D.C., National Security Archive, 2004. (Elérhető: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB144/index.htm. Letöltés ideje: 2024.02.04.).
• Intelligence Reform and Terrorism Prevention Act of 2004. (Elérhető: https://www.congress.gov/bill/108th-congress/senate-bill/2845. Letöltés ideje: 2024.02.04.).
• Jacobson v. Massachusetts, 197 U.S. 11 (1905) (Elérhető: https://supreme.justia.com/cases/federal/us/197/11/. Letöltés ideje: 2024.02.04.).
• Martin v. Hunter's Lessee, 14 U.S. 304 (1816) (Elérhető: https://supreme.justia.com/cases/federal/us/14/304/. Letöltés ideje: 2024.02.04.).
• Office of the Director of National Intelligence: Divisions and Offices (Elérhető: https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-about-us/icig-divisions. Letöltés ideje: 2024.02.04.).

Szerényi Gábor grafikája