

Szoftverek kiberbiztonsága és annak kapcsolata a társadalmi rezilienciával és fenntarthatósággal az Európai Unió stratégiai és kibebizotnsági joganyaga tükrében

Absztrakt

A tanulmány azt vizsgálja, hogy az Európai Unió szoftverbiztonsági szabályozása miként járul hozzá a társadalmi reziliencia megerősítéséhez. A kiberbiztonság – különösen a fejlesztési életciklusra (SDLC) és a forráskód hozzáférhetőségére vonatkozó előírások – nem pusztán technikai, hanem társadalmi jelentőséggel is bír. A tanulmány a security-by-design és resilience-by-design elvek mentén elemzi, hogyan válnak a biztonsági követelmények a demokratikus részvétel és a közbizalom strukturális feltételeivé. A Cybersecurity Act és a Cyber Resilience Act példáján keresztül bemutatásra kerül, hogy a szoftverek megbízhatóságát célzó jogi előírások hogyan épülnek be a kollektív digitális bizalom infrastruktúrájába. A tanulmány rávilágít: a fejlesztői és felhasználói tudatosság, valamint az átlátható és folyamatos frissítési gyakorlatok együttesen képesek erősíteni a társadalmi kohéziót. Az elemzés alátámasztja, hogy az EU kiberbiztonsági szabályozása nemcsak a szűken vett biztonsági logikát követ, hanem egy társadalom-technológiai modellt képvisel, amely illeszkedik az SDG 5, 10 és 16 célkitűzéseibe. A kiberbiztonság e keretben nem zárt szakterület, hanem a reziliens digitális demokrácia normatív alapköve.

Kulcsszavak

társadalmi reziliencia, szoftverbiztonság, kiberbiztonsági szabályozás, resilience-by-design, fenntarthatóság

I. BEVEZETŐ

A társadalmi reziliencia fogalma olyan képességekre utal, amelyek révén az egyének, közösségek és intézmények képesek alkalmazkodni a váratlan, működést megzavaró változásokhoz, fenntartva működőképességüket és társadalmi integritásukat.¹ Az elmúlt évtizedek során a kiberbiztonság egyre szorosabb kapcsolatba került ezzel a fogalommal. Az Európai Unió már 2013-as kiberbiztonsági stratégiájában felismerte az egyéni tudatosság fejlesztésének szükségességét a társadalmi ellenállóképesség megerősítése érdekében, míg a NATO 2018-tól kezdődően a társadalmi szintű kiberreziliencia kialakítását a kollektív védelem és hiteles elrettentés részévé tette. A világjárvány, majd az orosz–ukrán háború hatására ez a megközelítés tovább erősödött.

Ezzel párhuzamosan a szakirodalomban is egyre hangsúlyosabbá vált a szociotechnikai sérülékenységek vizsgálata, amely a kiberbiztonságot nem pusztán technikai, hanem társadalmi dimenzióban is értelmezi.² Az új kutatások olyan rezilienciaalapú megközelítések felé mutatnak, mint a resilience-by-design, amely szerint a technológiai rendszerek akkor válhatnak ellenállóvá, ha már tervezésük során figyelembe veszik a társadalmi működés komplexitását.³

¹ Cañizares et al., 2021.

² Cavelty et al., 2023.

³ Colabianchi et al., 2021.

E szemlélet különösen a szoftverfejlesztés és -használat terén kap kiemelt jelentőséget, ahol a fejlesztői tudatosság, a felhasználói döntések, valamint az átlátható és biztonságos frissítési mechanizmusok együttesen képesek hatással lenni a társadalmi kohézió és bizalom szintjére.

A tanulmány célja, hogy a szoftverbiztonsági szabályozás és a társadalmi reziliencia kapcsolatára irányítsa a figyelmet. A kérdés az, hogy az Európai Unió kiberbiztonsági stratégiai dokumentumai és jogalkotási eszközei – különösen a Cybersecurity Act, a Cyber Resilience Act – nemcsak technológiai, hanem normatív értelemben is a társadalmi reziliencia szolgáltatába állíthatók-e. A tanulmány ezt a kérdést a kiberbiztonsági stratégiák, az uniós idevágó jogszabályai és a releváns szakirodalom elemzésén keresztül vizsgálja, különös figyelemmel az SDG 5, 10 és 16 célkitűzéseire, amelyek a társadalmi egyenlőség, intézményi bizalom és inkluzív részvétel fenntartásának alapfeltételeiként értelmezik a digitális biztonságot.

II. KIBERBIZTONSÁGI KÖVETELMÉNYEK A SZOFTVEREKKEL SZEMBEN: RESILIENCE-BY-DESIGN, SECURITY-BY-DESIGN ELVEI

A kibertér és a teljes digitális ökoszisztéma, valamint azok részegységeként megjelenő információs és kommunikációs technológiák nem egyszerűen újraformálják a mindennapi életet, hanem mélyebben, szinte észrevétlenül, annak működési logikáját is átírják. A technológiai újítások ilyen rohamos volta azonban gyakran egyre mélyülő sebezhetőséget hordoz magában, ugyanis ezek a kibertámadások ma már nem elszigetelt "zavarok", hanem rendszerszintű mintázatokat követnek, élesen kihasználva a célba vett infrastruktúrák jellemzőit és azok hiányosságait. Ebben a megvilágításban a biztonság többé nem tekinthető pusztán technikai kérdésnek - összetettebb jelenség, amely előfeltételezi a (társadalmi) rezilienciát is. A problémakör egyik központi eleme a szoftverbiztonság kérdésében jelenik meg. Ha elfogadjuk - ahogyan Cavelty és szerzőtársai (2023) is hangsúlyozzák -, hogy a kiberbiztonság eredendően társadalmi és technológiai tényezők összjátéka, akkor kiemelt jelentőséggel bír azon szoftverek biztonsága, amelyeket az emberek a hétköznapijaik során használnak.⁴ E területen fontos kérdés, hogy mennyiben férhetünk hozzá magához a forráskódhoz. A zárt (proprietary) és a nyílt forráskódú (open-source, OSS) modellek eltérő fejlesztési szemléletet, eltérő biztonsági következményeket és más-más kockázati logikát hordoznak - és mindez nemcsak technikai, hanem társadalmi értelemben is jelentőséggel bír.

A forráskód - leegyszerűsítve - nem más, mint egy utasítássorozat, amelyet ember által is olvasható formában írnak meg, még azelőtt, hogy gépi futtatásra alkalmas alkalmazássá alakítanak. A zárt rendszerekben ez a kód a fejlesztő kizárólagos ellenőrzése alatt marad, a felhasználók hozzáférését pedig szigorú licencszerződések szabályozzák. Ilyen környezetben a biztonság szinte teljes egészében a szolgáltató kezében összpontosul - elég csak a Microsoft vagy az Apple példájára gondolni -, akik komoly erőforrásokat fordíthatnak belső biztonsági protokollokra, beépített védelmi mechanizmusokra és rendszeres frissítésekre. Bár e zártság önmagában magasabb fokú biztonságot eredményezhet, a korlátozott átláthatóság és a szolgáltatófüggés éppen a rendszer ellenállóképességét gyengítheti.⁵

⁴ Cavelty et al., 2023.

⁵ Guo et al., 2022.

A nyílt forráskódú modellek⁶ egészen más logikát követnek. Itt a forráskód már eleve nyilvános, ez a működés egyik alaptétele. Olyan projektekről van szó, mint a Linux vagy az Apache, amelyek nyílt fejlesztésű rendszerek, gyakran olyan platformokon keresztül működnek, mint a GitHub - ott bárki megtekintheti a kódot, javaslatokat tehet, vagy akár módosíthat is rajta. A mögöttes elv egyszerű: a nyilvánosság gyorsabb hibafeltárást tesz lehetővé. A centralizált rendszerekkel ellentétben a nyílt forráskódú projektek mögött nem áll egységes szervezeti háttér: a frissítések rendszertelenek lehetnek, a dokumentáció hiányos, a kódellenőrzés pedig gyakran attól függ, hogy éppen van-e idő, bizalom vagy elérhető közreműködő. Ez a közösségi alapú modell kétségtelenül rugalmas és gyors tud lenni, különösen, ha a sérülékenységek felismeréséről van szó, de ezzel együtt komoly kockázatokkal is jár: a nyilvánosan elérhető kódhoz ugyanolyan hozzáférése van a rosszindulatú szereplőknek, mint a jóhiszemű fejlesztőknek; a minőségbiztosítás és a biztonsági auditok nem mindig következetesek; a támogatás, a dokumentáció és a frissítések gyakorisága pedig projektfüggően nagy szórást mutathat.⁷

A Log4Shell sebezhetőség pontosan a fentiekre mutat rá, amely soha nem pusztán egy szoftverhiba volt; sokkal inkább olyan jelzésértékű eseményként kell kezelnünk, amely élesen és egyértelműen megmutatta, hogy akár egy alig észlelhető törésvonal is elegendő lehet ahhoz, hogy egész rendszereket, intézményi struktúrákat, sőt akár a közszolgáltatások infrastruktúráját is megbénítsa. Rámutatott arra, hogy a digitális bizalom nem tartható fenn ötletszerű hiba foltozgatásokkal. Tudniillik az a fajta bizalom, amelyre egy komplex digitális ökoszisztéma épülhet, csak rendszerességen, összehangoltságon és megosztott felelősségen alapuló karbantartási gyakorlatok révén fenntartható - méghozzá úgy, hogy ez nem utólagos technikai toldalék, hanem kezdettől fogva beágyazott strukturális elvként jelenik meg. Ezt a bizalmat nem lehet csupán alkalmi, elszigetelt javításokkal fenntartani. A tanulság világos: a szoftverkarbantartás nem lehet esetleges; annak tudatos és összehangolt stratégia mentén kell történnie.⁸ Ennek azonban legalább annyira része a felhasználó is, így ez nem csupán technikai kötelesség, hanem társadalmi tudatosságot is előfeltételez.

A szoftverbiztonság garantálásának kulcseleme a gyenge pontok feltérképezése. A kódfelülvizsgálat – ha valóban alapos – nemcsak hibakeresésről szól. Akár soronkénti ellenőrzésről van szó, akár automatizált vizsgálatról, a cél az, hogy ne maradjanak észrevétlenül a törékeny, gyenge láncszemek. A hálózati forgalom elemzése (network sniffing) már egészen más jellegű módszer: nem avatkozik be, hanem figyel. Figyeli, hogyan áramlik az információ a rendszeren belül, és elkapja azt is, aminek nem kellett volna láthatóvá válnia. Ami átcsúszik a réseken az nagyon sokszor az, amit eleve biztonságosnak feltételeztünk. A penetrációs tesztelés ezzel szemben aktív beavatkozást jelent: valós támadási scénáriókat szimulál annak érdekében, hogy feltárja, hol maradtak ki a védekezés szempontjából kritikus elemek. Ezek a módszerek önmagukban is működőképesek – de igazán akkor válnak hatékonyá, ha a teljes fejlesztési életciklusba (System Development Life Cycle – SDLC) szervesen beépülnek. A legkorábbi tervezési fázisoktól a rendszeres karbantartásig támogatják azt a proaktív

⁶ Hadi et al., 2024.

⁷ Shan et al., 2022.

⁸ Pigola – Meirelles, 2024.

gondolkodásmódot, amelyben a reziliencia nem utólagos kiegészítés, hanem eleve strukturális alapelv (resilience-by-design).⁹

Tehát a szoftverbiztonság hatékony kezelése messze túlmutat a forráskód hozzáférhetőségén (még ha attól nem teljesen független). Valójában egy olyan szemléletet igényel, amely a teljes fejlesztési életciklusra (SDLC) biztonságtudatos megközelítéssel tekint, még hozzá úgy, hogy közben nem feledkezik meg a tágabb társadalmi-technológiai összefüggésekről sem. Valódi biztonság és reziliencia csak akkor érhető el, ha a biztonsági követelményeket és kontrollokat következetesen már a legelső fejlesztési lépésekbe integráljuk – a „security by design” elve mentén, összhangban a „resilience-by-design” koncepcióval is – egészen a termék élettartamának végéig.¹⁰ Ha ez a szemlélet már a korai fázistól kezdve elmaradt, akkor olyan kockázatokkal nézünk szembe, amelyek később nehezen vagy magasabb költségek és kár mellett lesznek orvosolhatóak. A termékbe vetett bizalom meginoghat, és ennek a hatásai nem maradnak meg a technikai rendszerek hatókörén belül. A biztonsági szempontok korai szakaszban történő integrálása tehát nem pusztán hasznos javaslat, hanem alapvető követelmény: így hatékonyabban szűkíthető a támadási felület, gyorsabban és költséghatékonyabban orvosolhatók a hibák, és ami talán a legfontosabb a lehetséges károk mértéke is jóval kezelhetőbbé válik.

A fejlesztési életciklus (SDLC) fogalma szorosan összefügg az informatikai szektorban tapasztalható technológiai avulás gyors ütemével. Ez az összefüggés nemcsak azt teszi szükségessé, hogy a szoftvertermékeket folyamatosan technikailag naprakészen tartsuk, hanem azt is, hogy a reziliencia – társadalmi és technológiai értelemben egyaránt – tudatosan épüljön be a teljes életciklus menedzsmentjébe. Az SDLC főbb szakaszai,¹¹ és azok sajátos biztonsági jelentősége – különös tekintettel a társadalom-technológiai sérülékenységek kezelésére – a következőképpen vázolhatók fel:

Bevezetési szakasz: A termék ekkor lép piacra. Ebben a korai fázisban különösen kritikus, hogy a „security by design” elve, valamint a szélesebb körű „resilience by design” megközelítés következetesen érvényesüljön. Ide tartozik a biztonsági követelmények világos meghatározása, a kezdeti fenyegetésmodellezés, amelynek figyelembe kell vennie a technikai és a felhasználói szintű kockázatokat egyaránt, továbbá a biztonságos kódolási gyakorlatok és a belső protokollok korai kialakítása is.

Növekedési szakasz: A felhasználói kör és a piaci láthatóság bővülésével párhuzamosan nő a rendszer komplexitása, ezzel együtt pedig a potenciális támadási felület is. Ebben az időszakban fokozottan szükség van a folyamatos és egyre mélyebb biztonsági tesztelésre (például penetrációs vizsgálatokra), valamint egy hatékony és időszerű frissítési rendszerre, amely képes reagálni a felmerülő sérülékenységekre. Ezen a ponton a társadalmi és technológiai tényezők közötti kölcsönhatás is láthatóvá válik: a frissítések sikeressége ugyanis nem csupán a szolgáltatótól, hanem a felhasználók tudatosságától és együttműködésétől is nagymértékben függ.

⁹ Wang et al., 2023.

¹⁰ Colabianchi et al., 2021.

¹¹ Khan et al., 2022.

Érettségi szakasz: A szoftverek esetében ez jellemzően a leghosszabb időszak, amikor a működésbeli stabilitás válik az elvárások központi elemévé. Idővel a hangsúly természetes módon eltolódik a funkcionális bővítésről a stratégiai karbantartás irányába. A frissítések rendszeres alkalmazása és a javítások időben történő végrehajtása egyre inkább a kockázatkezelés beépített eszközeivé válnak. Ebben a fázisban a sérülékenységek kezelése már megelőző logika mentén kell, hogy működjön. Különös érzékenységgel kell lennie a működési metodikának azokra a rejtett gyengeségekre, amelyek csak hosszabbtávú, valós környezetben történő működés során válnak láthatóvá. A végfelhasználói interakciók és a hosszabb időszakot lefedő használati adatok nem pusztán visszajelzésként szolgálnak, hanem kvázi diagnosztikai eszközként is: olyan társadalom-technológiai töréspontokra világítanak rá, amelyeket a szokványos tesztelési eljárások önmagukban nem képesek feltárni.

Hanyatlási szakasz: Amint a karbantartási ciklusok kifutnak, és a hivatalos támogatás megszűnik, a rendszer egy minőségileg új típusú kitettségi állapotba lép, ahol a kockázat már nem elméleti lehetőség, hanem strukturálisan beágyazott adottság. A biztonsági frissítéseket már nem kapó, előregedő rendszerekre való további támaszkodás nem a periférián, hanem a működés középpontjában rögzíti a sebezhetőséget. A probléma nem az, hogy ezek a rendszerek meghibásodnak, hanem épp az, hogy tovább működnek. Működés közben tágitják ki észrevétlenül a kitettség határait, ugyanis a működőképesség önmagában nem jelent stabilitást. Egy rendszer akkor is üzemelhet, amikor közben fokozatosan lebontja a saját biztonsági tartalékait. Ilyen összefüggésben a reziliencia nem azonos a folytonossággal, hanem azzal mérhető, mennyire képes egy struktúra elnyelni a becsapódást, amikor ez a folytonosság megtörik.

A strukturált és biztonságos fejlesztési folyamatok mögött olyan nemzetközi szabványok állnak, mint az ISO/IEC 27001, amelyek nem csupán eljárásrendi útmutatást adnak, hanem egy átfogó keretet kínálnak a kiberbiztonság kezelésére egy folyamatosan változó környezetben.¹² Ezzel párhuzamosan a modern fejlesztési gyakorlatok – mint a DevOps, illetve annak biztonságközpontú kiterjesztése, a DevSecOps – arra törekednek, hogy a biztonság, sőt, ennél is mélyebben a reziliencia beépüljön a fejlesztési életciklus minden rétegébe. Ezek az agilis és iteratív megközelítések, amelyekben a tesztelés nem egyszerű ellenőrzés, hanem kérdésfeltevés, a visszacsatolás pedig nem formaiság, hanem a továbblépés feltétele, nem egy jól körülhatárolható célállapot felé vezetnek, hanem egy állandó felülvizsgálat felé.¹³ Itt válik a „resilience by design” elve többlettartalmúvá: nem valamiféle statikus mérceként, hanem működési logikaként, amely épp a nyomás alatt nyer értelmet – ahogyan azt Colabianchi és munkatársai (2021) is hangsúlyozzák. Ők a „security by design” ethosát automatizált kontrollmechanizmusokon keresztül operacionalizálják, és egy olyan fejlesztői kultúra megerősödését támogatják, amely a társadalom-technológiai sérülékenységeket nem anomáliákként, hanem a digitális rendszerek sajátos, belső tulajdonságaiként ismeri fel.¹⁴

Sem a zárt, sem a nyílt forráskódú modell nem jelent önmagában garanciát a kiberbiztonságra. Mindkettőnek megvannak a maga strukturális erősségei – és vele együtt a belső korlátai is. Ami

¹² Kang – Kim, 2022.

¹³ Alghawli – Radivilova, 2024.

¹⁴ Colabianchi et al., 2021.

igazán számít, az nem maga a modell, hanem az a fegyelmezett hozzáállás, amellyel a kockázatokat a szoftver teljes életciklusa során kezeljük: teszteléssel, auditálással, a fejlesztési ciklusba szervesen beépített kontrollokkal, a nemzetközi szabványok követésével, időszzerű javításokkal, valamint olyan fejlesztési és üzemeltetési módszerekkel, amelyek a biztonságot nem végpontként, hanem folyamatos feladatként értelmezik. E nézőpont térnyerésében azonban jelentős szerepe van az államnak és a jogi szabályozásnak is.

III. ELŐÍRVA A KÖVETELMÉNYEKET – AZ EURÓPAI UNIÓ KIBERBIZTONSÁGI JOGI ELŐÍRÁSAI A SZOFTVEREK TERÜLETÉN

A 2020-as évektől kezdődően a társadalmi reziliencia fogalma egyre hangsúlyosabb szerepet kap az Európai Unió biztonsági és szabályozási diskurzusaiban. A kiberbiztonság és a demokratikus kormányzás közötti kapcsolat mára nem csupán egy új szakpolitikai nézőpontot tükröz, hanem mélyebb paradigmaváltásra utal. A digitális környezet biztonsága többé nem kezelhető pusztán technológiai vagy nemzetbiztonsági kihívásként. A biztonságos digitális terekhez való hozzáférés, az állampolgárok digitális kompetenciái és részvételi képességei, valamint a platformalapú fenyegetések kormányzása együttesen erősítik a társadalom szélesebb értelemben vett rezilienciáját, nemcsak technikai, hanem politikai és kulturális dimenzióban is.¹⁵ Ez a megközelítés egyúttal egy társadalom-technológiai kormányzási modellre is épít, amelyben a technikai szabályozás és a társadalmi együttműködés egymást erősítő tényezőként jelennek meg a közösségi ellenállóképesség szempontjából. Mindez több fenntartható fejlődési célhoz (SDG) is hozzájárul, különösen az SDG 5 (nem egyenlőség), SDG 10 (egyenlőtlenségek csökkentése) és SDG 16 (béke, igazságosság és erős intézmények) célkitűzéseikhez.¹⁶

Az Európai Unió 2020-as Kiberbiztonsági Stratégiája kifejezetten a digitális biztonságot nevezi meg a társadalmi reziliencia egyik alappilléreként. A dokumentum újdonságát az adja, hogy a kiberbiztonságot nem csupán technológiai vagy biztonságpolitikai kérdésként kezeli, hanem olyan összefüggésként, amely szorosan kapcsolódik az alapvető jogokhoz, a demokratikus intézmények működéséhez, valamint a zöld és digitális átmenet társadalmi feltételrendszeréhez is. Az egyik visszatérő fogalmi kerete a „reziliencia”, amelyet nem egyszerűen rendszerszintű ellenállóképességként értelmez, hanem – bár közvetett módon – az állampolgári részvétel, a közösségi tudatosság és az oktatáshoz való hozzáférés függvényeként is. Fontos mozzanat, hogy a stratégia a „security by design” elvét nemcsak a kritikus infrastruktúrák és szolgáltatások esetében hangsúlyozza, hanem a digitális eszközök, munkahelyek és platformok tervezésére is kiterjeszti, mindezt a társadalmi reziliencia technológiai előfeltételeként értelmezve. A biztonságos szoftver tehát nem pusztán technikai kérdés, hanem annak a kérdése is, hogy mire bízunk rá azokat a rendszereket, amelyek között élünk. Azzal, hogy a biztonságért és a sérülékenységek kezeléséért a fejlesztőket és a gyártókat teszi elsődlegesen felelőssé, a stratégia közvetlen kapcsolatot jelöl ki a kódsorok és az alkotmányos értékek között. Azt sugallja, hogy a közbizalom azokban a digitális eszközökben kezdődik, amelyeket nap mint nap használunk. Ebben az értelemben a biztonságos digitális környezet és a mindennapi kiberhigiénia nem marginális tényezők – épp ezek teszik lehetővé a részvételt, és ezek tartják össze a társadalmi

¹⁵ Farkas – Vikman, 2024.

¹⁶ Közös közlemény az Európai Parlamentnek és a Tanácsnak – Az EU kiberbiztonsági stratégiája a digitális évtizedre.

kohézió szövetét. A stratégia egyértelművé teszi: a kiberbiztonság nem önálló cél, hanem alapfeltétele a fenntartható fejlődésnek, és egyben záloga azoknak az alapértékeknek, amelyeket az Európai Unió a legfontosabbnak tart: a szabadságnak, a demokráciának és a jogállamiságnak. Ugyanakkor az ehhez vezető út nem csupán tűzfalakkal és megfelelőségi listákkal van kikövezve. Az álhírek elleni fellépés, a hibrid fenyegetésekre adott válasz, a digitális írástudásba való befektetés, valamint a női jelenlét erősítése és gyermekek célzott védelme nem önálló szakpolitikai szigetek, hanem a kiberbiztonság területén is ezekkel együtt kell felrajzolni egy átfogó kiberbiztonsági stratégiai törekvés körvonalait. Ezáltal pedig egy olyan társadalom képe bontakozik ki, amely nem csupán digitális eszközökkel felszerelt, de azt képes is értő módon használni, ezzel pedig megteremtve a kiberbiztonság területén és azon is túlmutató tudatos és digitális kompetens európai polgárt. Ebben az összefüggésben a Fenntartható Fejlődési Célokhoz való illeszkedés nem pusztán szimbolikus: az SDG 5 és SDG 16 nem lábjegyzetek e projektben, hanem annak strukturális alapelemei. A biztonságos és inkluzív digitális tér nem csupán kívánatos cél, hanem előfeltétele többek között a nemek közötti egyenlőségnek és a demokratikus együttélésnek.¹⁷

A 2025-ös Internal Security Strategy (ProtectEU) ezt a gondolatmenetet viszi tovább: élesíti, kiszélesíti, és mélyebben beépíti az uniós intézményrendszer reflexeibe. A dokumentum kiindulópontja egyértelmű: a kiberbiztonság nem csupán technikai szintér, hanem a társadalmi reziliencia egyik strukturális alappillére. Az erre adott válaszok többretegűek – jogi, technológiai és állampolgári szinten – éppúgy, ahogyan maguk a fenyegetések is hibrid természetűek. A szoftverbiztonság ebben az értelmezésben nem egyszerű technikai paraméterként jelenik meg, hanem mint strukturális töréspont, amely átszövi a teljes digitális infrastruktúrát. Ugyanis a szoftverek (és teljes digitális ökoszisztéma) esetében nem pusztán az kérdés, hogy biztonságos és jól működik-e a szoftver, hanem az, hogy megbízhatunk-e azokban a rendszerekben, amelyekre nap mint nap támaszkodunk. Ebben az értelemben a kötelező fejlesztési protokollok és a tanúsítási követelmények bevezetése nem pusztán szabályszigorítás, hanem sokkal inkább azon kérdésekre adott válaszok, hogy ki viseli a felelősséget, ha a rendszer meghibásodik, valamint hogyan alkothatunk olyan rendszereket, amelyek nemcsak működnek, hanem ki is érdemlik a társadalmi bizalmat? A stratégiai szerint itt válik valóban jelentőssé a NIS2 irányelv és a Cyber Resilience Act, nem mint távoli szabályozási háttér, hanem mint a rendszertervezés szerves része. Ezekre nem úgy kell tekinteni, mint kívülről rákényszerített korlátokra, hanem akként, hogy ezek egységes szemlélet mentén rámutatnak arra, hogyan épül fel a bizalom, hogyan oszlik meg a felelősség, és miként maradnak stabilak a rendszerek akkor is, amikor nyomás alá kerülnek. Nem csupán elvárják a biztonságot, de megkövetelik, hogy az előre megtervezett, mérnökiileg megalapozott és mindennapokban is gyakorolt valóság legyen. Emellett a stratégia rámutat arra is, hogy a Digital Service Act (DSA) megalkotásával az európai közösség a platformkormányzást kiemeli a magánérdekű mérlegelés szférájából, és áthelyezi a közérdekű elszámoltathatóság terébe. E felfogás üdvözlendő, azonban eredményessége még erősen vitatható, de legalább lépéseket tett az EU ennek érdekében.¹⁸ Az azonban egyértelműen

¹⁷ Közös közlemény az Európai Parlamentnek és a Tanácsnak – Az EU kiberbiztonsági stratégiája a digitális évtizedre.

¹⁸ Gosztönyi, 2021.

visszatükröződik a dokumentumból, hogy nézőpontja szerint a biztonság többé nem jó szándék kérdése, hanem a demokratikus létfeltétel, és mint ilyen, kötelezően kezelendő.¹⁹

A dokumentum jelentősége azonban nem csupán abban áll, hogy az EU szabályozását rendszerbe foglalja, hanem abban is, hogy miként gondolja újra a reziliencia fogalmát. A társadalmi kohézió itt nem elvont eszményként jelenik meg, hanem mint törékeny konstrukció, amelyet az online radikalizáció, a gyűlöletbeszéd és a közös valóságérzékelés felbomlása fenyeget. A javasolt intézkedések nem egyszerű technikai korrekciók vagy válságkezelő protokollok. A stratégia sokkal inkább szemléletváltást indít el: az eddigi reaktív felfogás helyébe egy strukturális előrelátáson alapuló megközelítés lép. A digitális válságkezelési keretrendszerek, a gyermekeket védő intézkedések megerősítése és a platformokra vonatkozó új elszámoltathatósági kötelezettségek nem alkalmi megoldásokat jelentenek, hanem egy olyan kormányzási modell korai jeleit, amely nem csupán válaszolni kíván, hanem előre látni. Ezen állammodell – amely illeszkedik a cyberfare state modell fejlődési pályáihoz – a „resilience by design” és „security-by-design” elveinek gyakorlati megnyilvánulását jelenti. Annak felismerése, hogy a társadalom nem kizárólag a technológiai megoldásoktól válik ellenállóképessebbé, hanem a digitális tudatosság minőségének javítása révén, amelyhez hozzá tartozik az eszközökhöz való minőségi hozzáférés mellett a tudatos eszközválasztás, beleértve a szoftvereket is (ezt segíti például a CRA is), amelynek eredménye lehet az inkluzív, részvételen alapuló és önreflektív demokratikus társadalom kialakulása. Ilyen módon pedig a stratégia nemcsak az SDG 5 és SDG 16 célkitűzéseivel kapcsolódik, hanem az SDG 10-hez is, vagyis az egyenlőtlenségek csökkentését nem járulékos hozadékként, hanem alapkérdésként kezeli. Ami ebből a stratégiai törekvésből formálódik, az a társadalom-technológiai modell legteljesebb értelmében olyan rendszer megteremtése, amelyben a kiberbiztonsági keretek, a jogi garanciák és a kulturális normák nem különálló logikák, hanem ugyanannak a demokratikus rendszernek egymást feltételező rétegei. És éppen ez a rétegekből álló egymásrautaltság az, ami lehetővé teszi, hogy a digitális reziliencia végre azzá váljon, aminek mindig is lennie kellett: társadalmi minőséggé, amely természetesen a 2020-as stratégia nemzeti biztonságot erősítő célját is kiemelkedően szolgálni tudja.²⁰

Érdemes röviden áttekinteni, hogy a stratégiákban hivatkozott, kiberbiztonsággal kapcsolatos jogszabályok – különösen a szoftverbiztonságot érintő rendelkezések – miként járulnak hozzá a korábban vázolt célkitűzésekhez.

A Cybersecurity Act nem csupán egy tanúsítási rendszert vezet be – hanem újraértelmezi a kiberbiztonságot mint a demokratikus kormányzás strukturális elemét. Azáltal, hogy az ENISA-t állandó ügynökséggé nyilvánítja stratégiai és operatív hatáskörökkel, a rendelet a digitális biztonságot a technikai szakpolitikák szintjéről az intézményi folytonosság kérdésévé emeli. Olyan kormányzási modell képe bontakozott ki ezzel, amelyben a kiberbiztonság nem válik el a politikai rend tágabb szövetétől, hanem a közbizalom és a társadalmi reziliencia intézményi architektúrájának része. Az egységes uniós tanúsítási keretrendszer létrehozása finom, de érdemi elmozdulást jelezett, bár formailag önkéntes, a rendelet rétegzett logikája hosszú távon

¹⁹ A Bizottság közleménye a ProtectEU-ról: Európai belső biztonsági stratégia.

²⁰ A Bizottság közleménye a ProtectEU-ról: Európai belső biztonsági stratégia.

olyan irányt vetít előre, amelyben a tanúsított biztonság válik az általánossá, nem pedig kivétellé. A normaszöveg hangsúlyozza a „security by design” és a „security by default” elveit, nem mint absztrakt mérnöki eszményeket, hanem mint rendszerszintű elvárásokat. Egyértelmű üzenetet küld fejlesztőknek és gyártóknak: a szoftversebezhetőség nem pusztán technikai mulasztás, hanem a társadalmi stabilitás potenciális kockázati pontja. Ebben az olvasatban a rendelet a reziliencia nyelvén szól, még ha a fogalmat nem is nevezi meg nyíltan. A digitális szolgáltatások megbízhatóságát a demokratikus részvétel társadalmi előfeltételeihez köti. Az infrastruktúrába vetett bizalmat a jogállamisággal kapcsolja össze. Implicit módon illeszkedik az SDG 16 célkitűzéséhez is. Azáltal, hogy a rendelet kiemelten kezeli az alapvető szolgáltatások biztonságát, közvetetten az SDG 5 és SDG 10 céljaival is összhangba kerül: olyan feltételeket határoz meg, amelyek révén a nők, a gyermekek és a társadalmilag kiszolgáltatott csoportok aránytalan kockázat nélkül férhetnek hozzá a technológiához. Ebben a keretben a kiberbiztonság többé nem a rendszer mögé helyezett pajzs, hanem maga is a rendszer tartószerkezetének része.²¹

A Cyber Resilience Act nem csupán technikai előírásokat rögzít, hanem víziót is kínál a digitális bizalom újraértelmezéséhez. Azzal, hogy horizontális kiberbiztonsági követelményeket ír elő minden digitális elemet tartalmazó termék számára, a biztonságot nemcsak az eszközök tervezésébe szövi bele, hanem a kollektív reziliencia egész architektúrájába. A „resilience-by-design”, a „security-by-design” és „security-by-default” elvek nem csupán mérnöki preferenciaként jelennek meg, hanem strukturális feltételek is annak érdekében, hogy fenntartható legyen a társadalmi bizalom a mindinkább digitalizált államban és társadalomban. A rendelet valódi súlyát nem a technikai kötelezettségek felsorolása adja, hanem az, hogy a biztonságot hosszú távú intézményi felelősségként szabályozza. A digitális biztonság nem kezelhető többé statikus terméktulajdonságként; a szabályozás azt folyamatos, fejlődő kötelezettségként határozza meg, amely az eszköz teljes életciklusában jelen van. Az elvárás nem csupán annyi, hogy a gyártók működőképes terméket bocsássanak ki, hanem az is, hogy tartósan felelősséget vállaljanak annak biztonságáért. A rendszeres frissítések, az átlátható sérülékenységi jelentések és az elszámoltatható javítási eljárások nem egyszerű megfelelési szempontok: ezek képezik annak a társadalmi szerződésnek a feltételeit, amelyre a digitális bizalom épül. A jelentési kötelezettségek is új értelmet nyernek: a nemzeti hatóságok és az ENISA irányába történő bejelentések a jelentős eseményekről és kihasználható sebezhetőségekről már nem csupán utólagos reakciók, hanem a kollektív védekezés eszközei. Az átláthatóság és a koordinált válasz a digitális érettség alapkövetelményévé vált. A rendelet hatálya – az okoseszközöktől az ipari irányítórendszerekig – biztosítja, hogy a szabályozás hatása ne korlátozódjon szűk technológiai szegmensekre, hanem a mindennapi élet egészébe beágyazódjon. Ezzel a CRA nemcsak szűk értelemben vett kiberbiztonsághoz járul hozzá, hanem a digitális egyenlőséghez is: annak biztosításához, hogy a biztonságos technológiai hozzáférés ne kiváltság, hanem jog legyen. Ez összhangban áll az EU tágabb fenntarthatósági célkitűzéseivel, különösen az SDG 5 (nemzeti egyenlőség), SDG 10 (egyenlőtlenségek csökkentése) és SDG 16 (békés és inkluzív társadalmak építése) értékeivel. Ugyanakkor a rendelet a reziliencia fogalmát a felhasználói oldalra is kiterjeszti. A gyártók számára előírt

²¹ Az Európai Parlament és a Tanács (EU) 2019/881 rendelete.

információszoftáratási kötelezettségek – például a termék biztonsági jellemzőinek, támogatási időtartamának és frissítési lehetőségeinek közlése – azt a célt szolgálják, hogy erősítsék a felhasználói döntések mögötti tudatosságot. Ebben a keretben a társadalmi reziliencia nem azt jelenti, hogy a felhasználókat passzívan védjük, hanem azt, hogy képessé tesszük őket az aktív, tájékozott részvételre. Az egyéni döntéshozatali képesség ilyen típusú megerősítése közvetlenül járul hozzá a közösség egészének biztonságához.²²

V. KONKLÚZIÓ

A tanulmányban vizsgált stratégiák és jogszabályok alapján világossá válik, hogy az Európai Unió célja nem pusztán a digitális térben megjelenő fenyegetések elleni védekezés, hanem annak aktív alakítása is: annak meghatározása, miként ágyazódik be ez a tér a társadalom egészébe. A kiberbiztonság – különösen a szoftverbiztonság szabályozása – nemcsak önálló célként jelenik meg, hanem időnként eszközként is: olyan szabályozási kapocsként, amelyen keresztül a technológiai megbízhatóság társadalmi kohéziót, állampolgári részvételt és intézményi bizalmat megalapozó szerkezeti feltétellé válik. Ez a megközelítés nem technokrata, hanem normatív és inkluzív: a digitális környezet biztonsága alakítható, konfigurálható komponensként épül be a társadalmi reziliencia fogalmába.

Az SDG 5, 10 és 16 célkitűzéseikhez való illeszkedés nem retorikai gesztus, hanem tartalmi és gyakorlati kapcsolódás. Az EU által képviselt rezilienciafelfogás a digitális egyenlőtlenségek csökkentésére, a befogadó intézmények megerősítésére és a biztonsághoz való univerzális hozzáférés biztosítására épül. Ami így kirajzolódik, az nem csupán egy biztonsági keretrendszer, hanem egy társadalom-technológiai modell, amelyben sem a technológia, sem a biztonság nem önmagáért való fogalom, elvárás vagy szabályozási kérdés, hanem azoknak sokkal inkább végső célja egy reziliens társadalom megvalósítása, amelynek révén egy hatékony nemzeti biztonsági környezet alakulhat ki úgy, hogy közben akár polgárok jogai még tágabb körben tudnak érvényesülni (például a digitális képességek magasabb minősége következtében élni tudnak a digitális környezet által nyújtott részvételi lehetőségekkel), így a cyberfare state demokratikus oldalát adó államok éppoly hatékonyan, de önképüket megtartva tudják szavatolni saját társadalmaik biztonságát jelenkorunk totális biztonsági környezetében.

²² Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete.

Irodalom

- Alghawli, A. – Radivilova, T. (2024): Resilient Cloud cluster with DevSecOps security model, automates a data analysis, vulnerability search and risk calculation. In: *Alexandria Engineering Journal*, 107, 136–149, <https://doi.org/10.1016/j.aej.2024.07.036>.
- Cañizares, J. – Copeland, S. – Doorn, N. (2021): Making Sense of Resilience. In: *Sustainability*, 2021/15. sz., <https://doi.org/10.3390/su13158538>.
- Cavelty, M. – Eriksen, C. – Scharte, B. (2023): Making cyber security more resilient: adding social considerations to technological fixes. In: *Journal of Risk Research*, 2023/7. sz., <https://doi.org/10.1080/13669877.2023.2208146>.
- Colabianchi, S. – Costantino, F. – Gravio, G. – Nonino, F. – Patriarca, R. (2021): Discussing resilience in the context of cyber physical systems. In: *Computers & Industrial Engineering*, 160, <https://doi.org/10.1016/j.cie.2021.107534>.
- Farkas Ádám – Vikman László (2024): Information Operations as a Question of Law and Cyber Sovereignty. In: *ELTE Law Journal* 2024/2. sz., <https://doi.org/10.54148/ELTELJ.2024.2.187>
- Gosztonyi Gergely (2021): Az internetes tartalomszabályozás európai típusú szabályozásának kezdetei, avagy irányelvektől a rendeletekig (TWF, AVMS, E-Comm, DSA, DMA). In: *Jog Állam Politika* 2024/4. sz.
- Guo, W. – Fang, Y. – Huang, C. – Ou, H. – Lin, C. – Guo, Y. (2022): HyVulDect: A hybrid semantic vulnerability mining system based on graph neural network. In: *Computers & Security*, 121 (102823), <https://doi.org/10.1016/j.cose.2022.102823>.
- Hadi, H. – Ahmad, N. – Aziz, K. – Cao, Y. – Alshara, M. (2024): Cost-Effective Resilience: A Comprehensive Survey and Tutorial on Assessing Open-Source Cybersecurity Tools for Multi-Tiered Defense. In: *IEEE Access*, 12 (194053-194076), <https://doi.org/10.1109/ACCESS.2024.3510533>.
- Kang, S. – Kim, S. (2022): CIA-level driven secure SDLC framework for integrating security into SDLC process. In: *Journal of Ambient Intelligence and Humanized Computing*, 13, 4601–4624, <https://doi.org/10.1007/s12652-021-03450-z>.
- Khan, R. – Khan, S. – Akbar, M. – Alzahrani, M. (2022): Security risks of global software development life cycle: Industry practitioner's perspective. In: *Journal of Software: Evolution and Process*, 2022/3. sz., <https://doi.org/10.1002/smr.2521>.
- Pigola, A. – De Souza Meirelles, F. (2024): Unraveling trust management in cybersecurity: insights from a systematic literature review. In: *Information Technology and Management*, <https://doi.org/10.1007/s10799-024-00438-x>.
- Shan, C. – Gong, Y. – Xiong, L. – Liao, S. – Wang, Y. (2022): A Software Vulnerability Detection Method Based on Complex Network Community. In: *Security and Communication Networks*. 2022/1. sz., <https://doi.org/10.1155/2022/3024731>.
- Wang, Z. – Wen, Y. – Wang, Z. – Zhi, P. (2023): Resilience-based design optimization of engineering systems under degradation and different maintenance strategy. In: *Structural and Multidisciplinary Optimization*, 66(219), <https://doi.org/10.1007/s00158-023-03671-0>.

Jogforrások

- A Bizottság közleménye a ProtectEU-ról: *Európai belső biztonsági stratégia*, COM (2025) 148 final, 2025. március 27. (Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52025PC0148>. Letöltés ideje: 2025.05.01.)

- Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az EU kiberbiztonsági stratégiája a digitális évtizedre, JOIN (2020) 18 final, 2020. december 16. Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52020JC0018>.Letöltés ideje: 2025.05.01.)
- Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Unió Kiberbiztonsági Ügynökségéről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (Cybersecurity Act) (Elérhető: <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32019R0881>.Letöltés ideje: 2025.05.01.)
- Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828 irányelv módosításáról (Cyber Resilience Act) (Elérhető: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>.Letöltés ideje: 2025.05.01.)