BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Infrastructurile critice prin lentila teoriei securizării

Critical Infrastructure through a Securitization Theory Lens

Drd. Sorina-Denisa POTCOVARU (DRAGNE)*
Prof. univ. Dr. Habil. Marinel-Adi MUSTAȚĂ**

*Școala Doctorală Interdisciplinară, Universitatea Națională de Apărare "Carol I", București
e-mail: dragne.sorina@adlunap.ro
**Facultatea de Securitate și Apărare, Universitatea Națională de Apărare "Carol I", Bucharest
e-mail: mustata.adi@unap.ro

Abstract

Infrastructurile critice au devenit un punct central al guvernanței europene în materie de securitate, pe fondul creșterii complexității amenințărilor fizice, digitale și hibride. Acest articol aplică teoria securizării, bazându-se atât pe formularea clasică a Școlii de la Copenhaga, cât și pe dezvoltările sale sociologice, pentru a analiza modul în care Uniunea Europeană construiește și guvernează infrastructurile critice prin Directiva CER și Directiva NIS2. Cele două acte normative dezvăluie o logică dual a securizării bazată pe continuitate operațională fizică și integritate sistemică digitală. Prin corelarea teoriei securizării cu politica materială a guvernanței infrastructurilor, articolul demonstrează că infrastructura critică nu este doar un domeniu tehnic, ci o arenă esențială prin care securitatea europeană contemporană este definită și pusă în practică.

Critical infrastructures have become a central concern of European security governance in the context of the growing complexity of physical, digital, and hybrid threats. This article applies securitization theory, drawing on both the classical formulation of the Copenhagen School and its sociological developments, to analyse how the European Union constructs and governs critical infrastructure through the CER Directive and the NIS2 Directive. The two legal instruments reveal a dual securitization logic grounded in physical operational continuity and digital systemic integrity. By linking securitization theory with the material politics of infrastructure governance, the article demonstrates that critical infrastructure is not merely a technical domain but a key arena through which contemporary European security is defined and enacted.

Cuvinte-cheie:
teoria securizării; infrastructuri critice; reziliență; securitate cibernetică; Directiva CER; Directiva NIS2; guvernanța Uniunii Europene; servicii esențiale; rețele și sisteme informatice.

Keywords:
Securitization Theory; Critical Infrastructure; Resilience; Cybersecurity; CER Directive; NIS2 Directive; European Union Governance; Essential Services; Network and Information Systems.

Info articol
Primit: 12 octombrie 2025; Evaluat: 3 noiembrie 2025; Acceptat: 4 decembrie 2025; Disponibil online: 9 ianuarie 2026

Citare: Potcovaru (Dragne), S.D. și M.A. Mustață. 2025. „Infrastructurile critice prin lentila teoriei securizării." *Buletinul Universității Naționale de Apărare „Carol I"*, 14(4): 48-61. https://doi.org/10.53477/2065-8281-25-27

Introducere

Guvernanța infrastructurilor critice a devenit o preocupare centrală a politicilor contemporane de securitate, determinată de interdependența tot mai accentuată a societăților europene și de expansiunea riscurilor hibride, cibernetice și sistemice (atacuri de tip ransomware, sabotajul conductelor Nord Stream (2022), întreruperea comunicațiilor satelitare). Dacă abordările timpurii privind protecția infrastructurilor critice se bazau, în principal, pe managementul riscurilor și standarde tehnice, legislația recentă a Uniunii Europene (UE) evidențiază o restructurare profundă a modului în care protejarea caracterului critic este construită și guvernată din punct de vedere politic. Adoptarea Directivei privind reziliența entităților critice (Directiva CER) și a Directivei privind măsuri pentru un nivel comun ridicat de securitate cibernetică (Directiva NIS2) marchează o tranziție decisivă de la evaluările sectoriale ale vulnerabilităților la un cadru mai amplu, în care serviciile esențiale, dependențele digitale și sistemele socio-tehnice sunt ridicate la rangul de chestiuni de importanță existențială.

Teoria securizării, dezvoltată de Școala de la Copenhaga și extinsă, ulterior, prin perspective sociologice și material-discursive, oferă un cadru conceptual robust pentru înțelegerea acestei transformări. În loc să trateze infrastructurile ca obiecte neutre ale unui management tehnic, teoria securizării evidențiază modul în care actorii politici și de reglementare construiesc serviciile esențiale, infrastructurile digitale și sistemele în rețea ca entități amenințate existențial, a căror protecție justifică aranjamente de guvernanță extraordinare. În acest context, infrastructura critică nu este doar un ansamblu de active, ci un obiect de referință produs prin practici juridice, instituționale și discursive, care îi conferă un statut privilegiat în ierarhia priorităților societale. Aplicarea teoriei securizării permite, astfel, o înțelegere mai profundă a modului în care legislația UE mobilizează narațiuni privind vulnerabilitatea, interdependența și riscul societal, pentru a extinde autoritatea de reglementare și a reconfigura responsabilitățile atât ale statelor, cât și ale operatorilor.

Directiva CER și Directiva NIS2 oferă o bază solidă pentru o analiză comparativă, deoarece reprezintă două forme distincte, dar interconectate, de securizare. Directiva CER construiește continuitatea serviciilor esențiale, precum energia, transportul, apa, sănătatea și administrația publică, ca fiind indispensabilă pentru funcțiile vitale ale societății și pentru stabilitatea economică. Prin contrast, Directiva NIS2 securizează fiabilitatea și integritatea rețelelor și sistemelor informatice care susțin aceste funcții, definind securitatea cibernetică nu ca pe un domeniu tehnic, ci ca pe o condiție pentru funcționarea pieței interne și pentru reziliența serviciilor dependente de mediul digital. În pofida unei suprapuneri sectoriale considerabile, cele două directive formulează obiecte de referință diferite, mobilizează manifestări distincte ale amenințării și utilizează mecanisme de guvernanță separate. Compararea lor evidențiază modul în care UE articulează vulnerabilități fizice, organizaționale și digitale la multiple niveluri ale sistemului socio-tehnic.

Acest articol utilizează teoria securizării pentru a analiza modul în care infrastructura critică este construită ca obiect de protecție în dreptul UE și pentru a compara Directivele CER și NIS2 ca fiind cadre complementare, dar conceptual distincte. Analiza demonstrează că UE operează astăzi cu o logică dublă a securizării: una centrată pe reziliența critică și pe furnizarea neîntreruptă a serviciilor esențiale, iar cealaltă centrată pe securitatea cibernetică și pe integritatea rețelelor și a sistemelor informatice.

Din perspectivă metodologică, cadrul conceptual al acestui articol este fundamentat pe teoria securizării, care oferă instrumentele necesare pentru realizarea unei analize legislative și comparative a două acte normative ale Uniunii Europene privind infrastructura critică. În acest sens, studiul examinează modul în care Directiva privind reziliența entităților critice (CER) și Directiva NIS2 își construiesc obiectele de referință, actorii de securitizare, audiențele și imaginarul de amenințare. Analiza este structurată prin intermediul unei grile analitice cu trei niveluri, nivelul valoric, nivelul actorilor/operatorilor și nivelul fizic-tehnic, aplicată în mod simetric ambelor directive pentru a asigura coerența conceptuală. Perspectivele rezultate din acest cadru sunt, ulterior, integrate într-o evaluare comparativă care identifică convergențe, divergențe și complementarități în abordarea Uniunii Europene privind guvernanța infrastructurilor critice. Metodologia adoptată este, așadar, una interpretativă și nu empirică, concentrându-se asupra modului în care instrumentele legislative formulează amenințări existențiale și autorizează intervenții de guvernanță într-o arhitectură europeană de securitate multinivel.

Cu toate acestea, această abordare metodologică prezintă anumite limite inerente. În primul rând, întrucât se bazează, în principal, pe analiza textuală și conceptuală a legislației Uniunii Europene, studiul nu surprinde în mod exhaustiv diversitatea practicilor naționale de implementare sau variațiile sectoriale existente între statele membre.

Teoria securizării și relevanța sa pentru infrastructurile critice

Teoria securizării, dezvoltată inițial de Școala de la Copenhaga, conceptualizează securitatea ca un proces operativ și intersubiectiv prin care actorii politici construiesc anumite probleme ca amenințări existențiale, care justifică măsuri extraordinare (Buzan, Wæver și de Wilde 1998; Taureck 2006, 54–55). Elementul central al acestui cadru este afirmația că securitatea reprezintă un *speech act*: prin declararea unei probleme ca fiind o chestiune de supraviețuire, un actor învestit cu autoritate o transformă într-una tratată în afara limitelor politicii obișnuite. Teoria clasică a securizării subliniază, astfel, rolul actorilor elitiști, obiectul de referință prezentat ca aflat sub amenințare, audiența a cărei acceptare este necesară pentru ca securizarea să reușească, precum și tranziția de la guvernanța de rutină la măsuri politice excepționale (Taureck 2006, 55; Balzacq 2019, 3–4).

Balzacq (2011) reformulează teoria dincolo de fundamentul său lingvistic, distingând între o abordare filosofică și una sociologică, aceasta din urmă ancorând securizarea în practici mai largi, contexte instituționale și relații de putere. Pentru Balzacq, securizarea reușește nu doar prin performanță retorică, ci prin alinierea așteptărilor audienței, rezonanței contextuale și a ceea ce el numește un *dispozitiv* de practici, instrumente și dispoziții culturale care conferă sens anumitor construcții ale amenințării. Enunțurile de securitate își derivă astfel forța din ancorarea lor în condiții sociale și istorice, mai degrabă decât din semantica propriu-zisă. Această orientare sociologică deplasează teoria de la un accent restrâns pe limbaj către o explicație mai cuprinzătoare a modului în care amenințările sunt produse, circulate și stabilizate în mediile politice.

O altă abordare este oferită de Balzacq, Léonard și Ruzicka (2016), care susțin faptul că securizarea este cel mai bine înțeleasă ca un proces prin care se stabilește caracterul de securitate al problemelor publice și se conturează opțiunile de politică considerate legitime ca răspuns. Autorii reconceptualizează securizarea ca pe o fuziune între operativitate și o „analitică a guvernării", în care securitatea este înfăptuită prin rutine birocratice, practici profesionale, sisteme de date și instrumente juridice, nu doar prin acte discursive. Ei evidențiază patru dimensiuni reteoretizate (audiența, contextul, relațiile de putere și practicile), demonstrând că teoria securizării a evoluat într-un program de cercetare flexibil, preocupat de modul în care amenințările sunt construite și instituționalizate în diverse domenii, de la migrație și sănătate la energie și securitate cibernetică.

Balzacq (2019) aprofundează această direcție abordând tensiunile cheie care persistă în domeniu: dacă securizarea derivă, în primul rând, din performanța elitelor sau din interacțiuni co-constitutive cu audiențele și dacă securizarea depolitizează sau intensifică lupta politică. Pentru a reconcilia aceste dezbateri, el propune conceptul de *regimuri de practici*, care integrează mecanisme discursive și materiale ce modelează modul în care amenințările devin social „aderente". În această formulare, securizarea este inseparabilă de politica extraordinarului, o competiție pentru legitimitate în care actorii se luptă să impună reprezentări autoritative ale pericolului. Această abordare situează securizarea în cadrul puterii productive mai largi a practicilor de guvernanță care structurează vizibilitatea, expertiza și reacțiile instituționale la amenințările percepute.

Stritzel (2014) oferă una dintre cele mai influente critici ale teoriei clasice, argumentând că arhitectura conceptuală a Școlii de la Copenhaga este insuficient teoretizată și intern inconsistentă, în special în ceea ce privește relația dintre actele de vorbire, audiențe, context și putere. El arată că teoria oscilează între o perspectivă austiniană asupra securizării ca act ilocuționar, o focalizare poststructuralistă pe indeterminare și o interpretare bourdieusiană a câmpurilor de putere, fără a reconcilia aceste poziții. Stritzel susține, în consecință, o abordare discursiv-pragmatică și sensibilă la context, în care sensul securității provine din practici istorice de traducere, negociere și putere.

Completând această dezbatere, Taureck (2006) clarifică distincția dintre teoria securizării drept cadru analitic și studiile de securizare ca formă mai largă de critică normativă. Ea argumentează că multe dintre critici interpretează eronat teoria, reproșându-i lipsa unei orientări morale, deși scopul său este unul diagnostic: teoria urmărește să explice cum actorii construiesc amenințări și mobilizează măsuri excepționale, nu să evalueze dacă ar trebui sau nu să facă acest lucru. Prin trasarea acestei frontiere, Taureck repoziționează teoria securizării ca un instrument metodologic neutru pentru urmărirea proceselor de securizare și desecurizare.

În pofida acestor progrese, aplicarea teoriei securizării la infrastructurile critice rămâne insuficient dezvoltată. Aradau (2010) subliniază că o mare parte a literaturii tratează infrastructurile ca obiecte pasive, mai degrabă decât ca ansambluri material-discursive constituite activ ca fiind „critice" prin standarde inginerești, clasificări juridice și practici de evaluare a riscurilor. Această perspectivă contestă tendința dominantă de a privilegia actele lingvistice și acceptarea din partea audienței, ignorând capacitatea materială de a acționa a infrastructurilor și practicile socio-tehnice care stau la baza guvernanței lor. Prin urmare, abordările de securizare ajung adesea să adopte o perspectivă managerială bazată în principal pe managementul riscurilor, ignorând faptul că infrastructurile contribuie activ la formarea logicilor de securitate și că însăși noțiunea de „criticitate" este construită prin procese instituționale și tehnice. Intervenția lui Aradau evidențiază, astfel, necesitatea unei perspective mai integrate care să conecteze teoria securizării cu politica materială a guvernanței infrastructurilor.

Abordare a rezilienței entităților critice din perspectiva teoriei securizării

Aplicarea teoriei securizării la Directiva privind reziliența entităților critice (Directiva CER) demonstrează că principalul obiect de referință nu este infrastructura fizică în sine, ci continuitatea serviciilor esențiale care susțin funcțiile vitale ale societății și stabilitatea economică. Directiva poziționează explicit entitățile critice ca fiind indispensabile pentru „menținerea funcțiilor vitale ale societății sau a activităților economice", stabilind continuitatea serviciilor drept valoarea existențială aflată în joc (European Union 2022b, Considerentele 1–3). În termenii teoriei securizării, potențiala perturbare a acestor servicii esențiale și consecințele societale și economice în cascadă constituie amenințarea existențială care necesită măsuri de guvernanță excepționale.

Această încadrare securizată este operaționalizată printr-o concepție în trei straturi a obiectului de referință: stratul valoric, stratul actorilor/operatorilor și stratul fizic. La nivel valoric, Directiva identifică servicii esențiale, precum energia, transporturile, sectorul bancar, sănătatea, infrastructura digitală și alimentarea cu apă drept funcțiile societale fundamentale a căror furnizare neîntreruptă trebuie protejată. Aceste servicii susțin stabilitatea pieței interne și bunăstarea publică și, prin urmare, justifică intervenția armonizată la nivelul UE.

La nivelul actorilor sau operatorilor, obiectul de referință este constituit din entitățile critice, operatori publici și privați, responsabile pentru menținerea acestor servicii esențiale. Articolul 1 afirmă că scopul Directivei este de a asigura „reziliența entităților critice", astfel încât acestea să poată furniza servicii esențiale „în mod neîngrădit", chiar și în condiții perturbatoare (European Union 2022b, art. 1). Operatorii devin, astfel, intermediari funcționali a căror incapacitate ar amenința direct valorile societale esențiale securizate la stratul superior.

În cele din urmă, la nivelul fizic, Directiva include infrastructurile, activele și sistemele prin care operatorii furnizează serviciile esențiale. Aceste componente fizice și digitale, rețele, facilități, tehnologii, sunt încadrate ca obiecte de referință instrumentale. Articolul 2 definește infrastructura critică drept orice activ sau sistem „necesar pentru furnizarea unui serviciu esențial", subliniind rolul său de suport în raport cu straturile operator și valoric (European Union 2022b, art. 2).

Privită prin prisma teoriei securizării, Directiva CER construiește, așadar, un obiect de referință ierarhizat: funcțiile societale esențiale ce trebuie protejate, operatorii responsabili de furnizarea lor și infrastructurile care le permit funcționarea. Această încadrare stratificată deplasează accentul de la protecția tradițională centrată pe infrastructură către protejarea continuității serviciilor, tratată ca o chestiune de importanță existențială pentru Uniunea Europeană, legitimând astfel măsuri extinse de reglementare și de supraveghere în statele membre.

Aplicarea teoriei securizării la Directiva privind reziliența entităților critice (Directiva CER) evidențiază o constelație multistratificată și multinivel a actorilor de securizare. Securizarea se desfășoară atât la nivel juridic-instituțional, prin acte legislative, cât și la nivel operațional, prin practici de implementare și de supraveghere, care traduc Directiva în guvernanța cotidiană. Fiecare strat operează simultan la nivelul UE și la nivel național, rezultând o arhitectură complexă de autoritate distribuită în procesul de securizare.

La nivelul juridic-instituțional al UE, principalii actori de securizare sunt Parlamentul European și Consiliul, acționând pe baza unei propuneri a Comisiei Europene. Prin adoptarea Directivei, aceste instituții realizează mișcarea de securizare fundamentală: ele încadrează formal continuitatea serviciilor esențiale ca indispensabilă pentru funcționarea sistemelor societale și economice vitale, identifică o gamă largă de amenințări, de la dezastre naturale și terorism la atacuri hibride și interdependențe (amenințări precum cutremurul din Italia din 2016 sau atacul cibernetic asupra rețelei electrice a Ucrainei), și justifică impunerea unor obligații armonizate de reziliență în statele membre. În termenii teoriei securizării, actul legislativ constituie *actul autoritar,* care ridică continuitatea serviciilor esențiale la rangul de prioritate existențială pentru Uniune (European Union 2022b, Considerentele 1–3).

La nivelul juridic-instituțional național, statele membre și autoritățile competente desemnate devin actori secundari de securizare. Acestea sunt obligate să adopte strategii naționale, să efectueze evaluări naționale ale riscurilor și să identifice

entitățile critice a căror perturbare ar avea efecte societale semnificative (European Union 2022b, art. 3–6). Prin aceste desemnări și prin transpunerea internă a normelor europene, autoritățile naționale reproduc și înscriu mișcarea de securizare inițiată la nivelul UE în structurile lor teritoriale de guvernanță, extinzând astfel autoritatea acesteia în multiple domenii administrative și de reglementare.

La nivel operațional al UE, securizarea este pusă în practică de organisme precum Grupul pentru Reziliența Entităților Critice, care coordonează implementarea, elaborează orientări și facilitează schimbul transfrontalier de informații. Deși aceste organisme nu produc norme obligatorii, ele operaționalizează și stabilizează încadrarea securizată prin modul în care influențează interpretarea, monitorizarea și integrarea obligațiilor de reziliență în rutinele administrative curente. Activitatea lor asigură menținerea cadrului excepțional introdus de legiuitorul european prin practici continue de supraveghere și de coordonare.

La nivel operațional național, autoritățile competente, organismele de supraveghere și chiar entitățile critice însele materializează securizarea prin activități cotidiene de conformare. Autoritățile naționale efectuează inspecții, impun măsuri corective și supraveghează respectarea obligațiilor de reziliență, în timp ce entitățile critice realizează evaluări ale riscurilor, adoptă măsuri de reziliență organizațională și fizică și raportează incidente perturbatoare (European Union 2022b, art. 18–21). Aceste practici încorporează logica securizată în operațiunile de rutină ale operatorilor de infrastructuri, transformând încadrarea abstractă a continuității serviciilor esențiale în cerințe organizaționale și comportamentale concrete.

Privită în ansamblu, Directiva CER instituie o arhitectură de securizare cu două niveluri, operând atât la nivelul UE, cât și la nivel național. Instituțiile europene inițiază și instituționalizează securizarea prin acte legislative și prin mecanisme de coordonare de nivel înalt, în timp ce autoritățile naționale și entitățile critice o concretizează, implementează și aplică prin practici de reglementare și operaționale. Prin această configurație distribuită de actori, continuitatea serviciilor esențiale este construită și menținută ca o chestiune de importanță existențială pentru Uniune, legitimând astfel supravegherea extinsă și intervențiile orientate spre consolidarea rezilienței.

Aplicarea teoriei securizării la Directiva privind reziliența entităților critice (Directiva CER) arată că principala audiență a mișcării de securizare este reprezentată de statele membre, care acționează ca autoritățile juridice și politice principale responsabile pentru punerea ei în aplicare. În mod formal, Directiva este „adresată statelor membre" (European Union 2022b, art. 29), obligându-le să o transpună, să adopte strategiile naționale necesare, să identifice entitățile critice și să efectueze evaluări naționale ale riscurilor. În termenii teoriei securizării, acceptarea lor este una juridică și administrativă: prin integrarea acestor obligații în dreptul intern, statele membre confirmă că asigurarea continuității serviciilor esențiale constituie o preocupare existențială care justifică măsuri de reziliență armonizate și intruzive.

O a doua audiență importantă este reprezentată de entitățile critice însele, operatori publici și privați supuși în mod direct obligațiilor prevăzute în Capitolul III al Directivei. Articolul 1(b) prevede că Directiva „stabilește obligații pentru entitățile critice" pentru a le asigura capacitatea de a furniza servicii esențiale în orice condiții, în timp ce articolul 6 impune ca entitățile desemnate să fie notificate oficial cu privire la statutul lor și informate despre obligațiile specifice care li se aplică (European Union 2022b, art. 1(b), 6). Securizarea operațională depinde, astfel, de acceptarea de către aceste entități a rolului lor consolidat: nu mai sunt simpli furnizori de servicii, ci actori a căror performanță este încadrată ca fiind crucială pentru stabilitatea societală, iar a căror incapacitate ar putea genera perturbări în cascadă și cu efecte transfrontaliere.

În cele din urmă, Directiva se adresează implicit unei audiențe societale și economice mai largi, incluzând investitori, companii și utilizatori de servicii. Considerentul 6 subliniază că un sistem rezilient de entități critice generează „încredere și fiabilitate", prezentate ca fiind esențiale pentru buna funcționare a pieței interne. Deși această audiență nu este supusă unor obligații directe, Directiva urmărește să o reasigure, semnalând că serviciile esențiale sunt protejate prin măsuri coordonate de reziliență. În acest sens, securizarea se extinde dincolo de actorii de reglementare și de operatori pentru a include publicul larg, ale cărui așteptări privind servicii esențiale stabile și fiabile susțin încrederea societății.

Privite în ansamblu, Directiva CER stabilește o structură de audiență multistratificată. Statele membre constituie audiența politico-juridică principală, responsabilă pentru instituționalizarea mișcării de securizare; entitățile critice formează audiența operațională însărcinată cu implementarea obligațiilor de reziliență; iar o audiență societală și economică mai largă reprezintă publicul difuz a cărui încredere Directiva urmărește să o consolideze. Această configurare stratificată întărește încadrarea Directivei privind continuitatea serviciilor esențiale ca o chestiune de importanță existențială pentru Uniunea Europeană.

Aplicarea teoriei securizării la Directiva NIS2 relevă că principalul obiect de referință este securitatea și continuitatea rețelelor și sistemelor informatice (NIS) care susțin serviciile esențiale și importante din întreaga Uniune Europeană. În loc să trateze securitatea cibernetică drept un scop în sine, Directiva încadrează infrastructurile digitale ca fiind indispensabile pentru funcționarea pieței interne și pentru stabilitatea activităților societale și economice critice. Astfel, amenințarea existențială este înțeleasă ca potențiala perturbare, degradare sau compromitere a sistemelor digitale, a căror deficiență ar putea genera efecte sistemice și transfrontaliere.

La nivelul valoric, Directiva identifică funcționarea pieței interne și continuitatea activităților societale și economice dependente de mediul digital ca obiecte fundamentale de protecție. Articolul 1(1) afirmă explicit că obiectivul este asigurarea „unui nivel comun ridicat de securitate cibernetică în întreaga Uniune, în vederea îmbunătățirii funcționării pieței interne" (European Union 2022a, art. 1(1)). Aceste

valori sistemice, stabilitatea pieței, reziliența economică și fiabilitatea serviciilor digitale esențiale constituie bunurile existențiale a căror protecție justifică obligațiile armonizate de securitate cibernetică.

La nivelul actorilor sau operatorilor, Directiva desemnează entitățile esențiale și importante ca obiecte de referință indirecte. Acestea includ operatori din sectoare precum energia, transporturile, sectorul bancar, infrastructura digitală, sănătatea, apa potabilă, serviciile TIC și administrația publică (European Union 2022a, art. 3). Operațiunile lor sunt securizate, deoarece dependența lor digitală le conferă un rol central în menținerea stabilității societale. Eșecul acestor entități de a proteja sau de a asigura integritatea sistemelor lor digitale este încadrat ca o amenințare care ar putea produce efecte în cascadă în multiple sectoare.

La nivelul fizic-tehnic, Directiva tratează rețelele și sistemele informatice ca obiectul direct de referință operațional. Articolul 6 definește NIS drept sisteme digitale interconectate și sisteme de prelucrare a datelor, a căror compromitere poate submina confidențialitatea, integritatea, autenticitatea și disponibilitatea (European Union 2022a, art. 6). Obligațiile impuse operatorilor, de la măsuri de gestionare a riscurilor la raportarea incidentelor (art. 20–21), sunt concepute pentru a securiza aceste infrastructuri digitale ca substrat material prin care amenințările se manifestă. În termenii teoriei securizării, vulnerabilitatea acestor sisteme constituie punctul de ancorare al logicii Directivei privind intervenția normativă excepțională.

Privită în ansamblu, Directiva NIS2 construiește un obiect de referință stratificat, centrat pe continuitatea și fiabilitatea infrastructurilor digitale care fac posibile serviciile esențiale. La nivel macro, piața internă și stabilitatea societală constituie valorile existențiale ce trebuie protejate; la nivel intermediar, entitățile esențiale și importante funcționează ca operatori a căror postură de securitate cibernetică este crucială pentru această protecție; iar la nivel micro, rețelele și sistemele informatice formează baza materială a securizării. Directiva ridică astfel continuitatea digitală la rangul de chestiune de importanță existențială pentru Uniunea Europeană și legitimează o guvernanță extinsă a securității cibernetice ca răspuns necesar.

Analiză comparativă a obiectului de referință în Directivele CER și NIS2

O analiză comparativă a Directivei privind reziliența entităților critice (Directiva CER) și a Directivei NIS2 prin perspectiva teoriei securizării arată că, deși ambele instrumente urmăresc protejarea continuității funcțiilor societale și economice esențiale, ele construiesc obiecte de referință diferite în centrul logicilor lor de securizare. În Directiva CER, principalul obiect de referință este continuitatea serviciilor esențiale, incluzând energia, transporturile, apa, sănătatea, infrastructura digitală și administrația publică, a căror furnizare neîntreruptă este prezentată ca indispensabilă pentru funcțiile vitale ale societății și pentru funcționarea pieței interne. Aceste servicii esențiale constituie valorile existențiale aflate în joc, întrucât

perturbarea lor este de așteptat să genereze consecințe în cascadă, transsectoriale. În sprijinul acestui strat valoric se află un obiect de referință secundar: entitățile critice responsabile de furnizarea acestor servicii. Reziliența lor organizațională și operațională este încadrată ca fiind crucială pentru menținerea stabilității societale. La nivel operațional, Directiva CER tratează infrastructurile fizice și organizaționale utilizate de aceste entități ca obiecte de referință instrumentale, relevante în măsura în care permit continuitatea serviciilor.

Prin contrast, Directiva NIS2 își construiește obiectul de referință într-un registru digital și sistemic. Principala sa preocupare este securitatea și fiabilitatea rețelelor și sistemelor informatice (NIS), care susțin serviciile esențiale și importante din întreaga Uniune Europeană. Stratul valoric este, așadar, articulat în jurul funcționării pieței interne și al stabilității activităților societale și economice dependente de mediul digital, expuse din ce în ce mai mult amenințărilor cibernetice. La nivelul actorilor, Directiva identifică entitățile esențiale și importante a căror postură de securitate cibernetică modelează direct integritatea și fiabilitatea ecosistemului digital mai larg. La nivel operațional, NIS2 se concentrează asupra infrastructurilor tehnice, precum sistemele de prelucrare a datelor, rețelele de comunicații electronice și platformele TIC, care constituie fundația materială a continuității digitale.

Privite împreună, cele două directive dezvăluie logici de securizare complementare, dar distincte. Directiva CER securizează continuitatea serviciilor esențiale în domeniul fizic și organizațional, în timp ce Directiva NIS2 securizează condițiile digitale care permit funcționarea acestor servicii. În cadrul CER, criticitatea rezultă din potențiala perturbare a funcțiilor vitale ale societății; în NIS2, ea rezultă din compromiterea infrastructurilor digitale esențiale pentru piața internă. Deși ambele urmăresc protejarea rezilienței societății europene, ele identifică niveluri diferite ale sistemului socio-tehnic ca obiecte centrale ale securizării, generând două forme paralele, dar interconectate, de securizare: una ancorată în continuitatea operațională fizică și cealaltă în fiabilitatea sistemică digitală.

Analiză comparativă a sectoarelor de servicii esențiale (CER) și a categoriilor de infrastructuri (NIS2)

Regulamentul delegat al Directivei CER definește serviciile esențiale drept acele servicii necesare pentru menținerea funcțiilor societale vitale, a activității economice, a siguranței publice și a sănătății publice. Aceste servicii esențiale sunt grupate în unsprezece sectoare largi, incluzând energia, transporturile, infrastructura digitală, sectorul bancar, sănătatea, apa potabilă și apele uzate, alimentația, spațiul, administrația publică și serviciile de mediu precum gestionarea deșeurilor. Factorul determinant pentru includere este măsura în care întreruperea acestor servicii ar genera consecințe sociale sau economice grave. Prin urmare, cadrul CER centrează protecția pe continuitatea serviciilor ca obiect principal și identifică sectoarele în funcție de indispensabilitatea lor pentru societate.

TABELUL 1. Comparație între sectoarele de servicii esențiale din cadrul CER și categoriile de infrastructuri digitale critice din NIS2

Sector/Categorie	Regulamentul Delegat CER: Servicii esențiale	Directiva NIS2: Categorii de infrastructuri digitale critice
Energie	Electricitate, termoficare, petrol, gaze – servicii esențiale pentru societate	Operatorii de electricitate, petrol și gaze ca entități dependente de infrastructuri digitale; rețele și sisteme informatice ale operatorilor energetici
Transporturi	Servicii feroviare, aeriene, maritime, rutiere	Operatorii de transport unde sistemele TIC sunt critice; sisteme digitale care susțin traficul aerian, semnalizarea feroviară, operațiunile maritime
Infrastructură digitală	Incluse ca servicii esențiale (ex. IXP, DNS, cloud)	Sector central în NIS2: DNS, cloud, centre de date, CDN-uri, servicii de încredere, rețele de comunicații electronice
Sector bancar și piețe financiare	Tratate ca servicii esențiale datorită indispensabilității economice	Tratate ca esențiale din cauza riscului cibernetic asupra stabilității financiare
Sănătate	Spitale, servicii medicale, lanț de aprovizionare farmaceutic	Furnizorii de servicii medicale ca entități dependente de sisteme cibernetice ce trebuie securizate
Apă potabilă și ape uzate	Esențiale pentru sănătatea publică și supraviețuire	Incluse datorită dependenței de sisteme SCADA și control digital al proceselor
Alimentație	Producția și distribuția produselor alimentare esențiale	Nu este o categorie digitală centrală în NIS2, decât dacă este parte a producției cu sisteme TIC critice
Gestionarea deșeurilor	Esențială pentru protecția mediului și sănătatea publică	Acoperită doar indirect, atunci când operațiunile depind de sisteme digitale
Administrație publică	Funcții centrale de guvernare societală	Guvernele centrale sunt incluse explicit ca entități digitale esențiale
Spațiu	Operațiuni satelitare ce susțin servicii esențiale	Incluse în NIS2 doar dacă serviciile spațiale depind de furnizori TIC critici (ex. stații la sol)
Sectoare de mediu și chimice	Esențiale pentru siguranță, mediu, manipularea substanțelor chimice	Incluse în sectoarele de producție NIS2 când riscurile de securitate cibernetică sunt ridicate

Directiva NIS2, în schimb, identifică sectoarele nu în funcție de esențialitatea serviciilor fizice, ci în funcție de criticitatea infrastructurilor digitale și a dependențelor TIC. Anexele I (entități esențiale) și II (entități importante) ale Directivei clasifică entitățile ale căror rețele și sisteme informatice sunt fundamentale pentru funcționarea pieței interne și reziliența activităților dependente de mediul digital. Aceste categorii includ infrastructura digitală (furnizori de servicii DNS, centre de date, cloud computing, rețele de livrare de conținut), servicii de management TIC, rețele de comunicații electronice, și sectoare, precum energia,

transporturile, apa potabilă, apele uzate, sănătatea, sectorul bancar, infrastructurile pieţelor financiare şi administraţia publică. Deşi există o suprapunere sectorială largă cu CER, NIS2 reconfigurează aceste sectoare prin prisma securităţii cibernetice: ceea ce devine „critic" nu este serviciul în sine, ci reţelele şi sistemele informatice care susţin sau operează aceste servicii.

Diferenţa esenţială rezidă în logica de clasificare. CER protejează serviciile esenţiale pentru funcţionarea societăţii, indiferent de gradul lor de intensitate digitală, în timp ce NIS2 protejează infrastructurile digitale şi operatorii dependenţi de TIC, a căror perturbare ar putea compromite securitatea cibernetică, stabilitatea pieţei şi continuitatea digitală. În numeroase sectoare, energie, transporturi, sănătate, apă şi administraţie publică, aceleaşi entităţi apar în ambele cadre, însă ele sunt securizate din motive diferite. În CER, ele sunt esenţiale datorită importanţei lor fizice şi organizaţionale pentru societate; în NIS2, ele sunt esenţiale, deoarece se bazează pe infrastructuri digitale a căror compromitere poate genera riscuri sistemice. Astfel, deşi domeniul sectorial se suprapune parţial, obiectele de referinţă şi mecanismele criticităţii diferă: CER se concentrează asupra serviciilor esenţiale ca atare, în timp ce NIS2 se concentrează asupra reţelelor şi infrastructurilor digitale care le fac posibile.

Deşi atât CER, cât şi NIS2 acoperă multe dintre aceleaşi sectoare, raţiunea includerii lor diferă semnificativ. Aceasta demonstrează că cele două directive protejează straturi distincte ale sistemului socio-tehnic european: CER apără continuitatea fizică şi organizaţională a serviciilor esenţiale, în timp ce NIS2 protejează securitatea cibernetică şi integritatea sistemelor digitale care fac posibile aceste servicii.

Concluzii

Acest articol examinează modul în care Uniunea Europeană construieşte şi guvernează infrastructurile critice prin procese de securizare integrate în două cadre legislative esenţiale: Directiva privind reziliența entităților critice (Directiva CER) şi Directiva NIS2. Bazându-se pe teoria securizării atât în forma sa clasică, cât şi în dezvoltările sociologice ulterioare, analiza a arătat că aceste instrumente articulează logici de securizare distincte, dar interconectate, care operează pe multiple niveluri instituţionale şi operaţionale.

Directiva CER instituie o dinamică de securizare centrată pe continuitatea serviciilor esenţiale, poziţionând funcţiile vitale ale societăţii ca bunuri existenţiale a căror perturbare necesită măsuri armonizate şi intruzive de reziliență. Această construcţie aduce în prim-plan entităţile critice şi infrastructurile acestora ca intermediari indispensabili în protejarea stabilităţii societale. Prin contrast, Directiva NIS2 securizează condiţiile digitale care susţin serviciile esenţiale, identificând securitatea şi fiabilitatea reţelelor şi sistemelor informatice ca obiect de referinţă. În acest cadru, piaţa internă şi activităţile dependente de mediul digital sunt încadrate ca fiind ameninţate existenţial de incidente cibernetice, ceea ce motivează impunerea unor obligaţii stricte de securitate cibernetică pentru entităţile esenţiale şi importante.

Analiza comparativă demonstrează că aceste directive instituie forme paralele, dar complementare, de securizare. Directiva CER abordează vulnerabilitățile din domeniul fizic și organizațional al serviciilor esențiale, în timp ce NIS2 vizează infrastructurile digitale care permit funcționarea acestor servicii. Împreună, cele două instrumente dezvăluie o arhitectură de securitate stratificată la nivelul UE, în care continuitatea fizică și integritatea digitală reprezintă dimensiuni reciproc dependente ale rezilienței infrastructurilor critice. Această structură dual de guvernanță ilustrează modul în care UE gestionează din ce în ce mai mult riscul nu prin măsuri sectoriale izolate, ci prin cadre integrate și transsectoriale care reflectă complexitatea materială și socio-tehnică a sistemelor infrastructurale contemporane.

Într-o perspectivă mai largă, concluziile contribuie la teoria securizării, demonstrând că logica securității depășește actele discursive și se extinde în practici de reglementare, standarde tehnice și rutine instituționale. Directivele arată cum amenințările sunt construite, circulate și operaționalizate prin instrumente juridice, proceduri administrative și cerințe impuse operatorilor publici și privați. Ele evidențiază, de asemenea, necesitatea ca cercetarea în domeniul securizării să ia în considerare capacitatea materială a infrastructurilor și centralitatea sistemelor socio-tehnice în formele contemporane de guvernanță.

Analiza Directivelor CER și NIS2 are, de asemenea, implicații importante pentru statele membre, al căror rol este esențial în operaționalizarea logicii duale de securizare promovate de Uniunea Europeană. La nivel practic, statele membre trebuie să transpună cadrul juridic privind continuitatea serviciilor esențiale și integritatea sistemelor digitale în strategii naționale coerente, reforme instituționale și măsuri de reglementare specifice fiecărui sector. Acest proces presupune consolidarea capacităților naționale de evaluare a riscurilor, îmbunătățirea cooperării între actorii civili, militari și privați, precum și asigurarea faptului că autoritățile competente dispun de expertiza tehnică și de resursele necesare pentru a supraveghea respectarea obligațiilor legale.

În esență, Directivele CER și NIS2 arată că abordarea Uniunii Europene privind infrastructurile critice este modelată de un proces de securizare multistratificat, multinivel și ancorat material. Prin diferențierea, dar și interconectarea protecției serviciilor esențiale și a infrastructurilor digitale, UE construiește reziliența ca pe un imperativ simultan fizic și cibernetic-sistemic. Această analiză evidențiază nu doar complexitatea tot mai mare a guvernanței infrastructurilor critice, ci și extinderea cadrului de securizare ca instrument de înțelegere a modului în care politicile contemporane definesc, prioritizează și protejează ceea ce consideră a fi existențial pentru ordinea lor societală și economică.

Referințe

Aradau, Claudia. 2010. "Security That Matters: Critical Infrastructure and Objects of Protection." *Security Dialogue* 41 (5): 491–514. https://doi.org/10.1177/0967010610382687.

Balzacq, Thierry. 2011. "A Theory of Securitization: Origins, Core Assumptions, and Variants." In *Securitization Theory: How Security Problems Emerge and Dissolve*, edited by Thierry Balzacq, 1–30. London: Routledge.

___. 2019. *Securitization Theory: Past, Present, and Future*. London: Routledge.

Balzacq, Thierry, Sarah Léonard și Jan Ruzicka. 2016. "Securitization: Toward a Theory of the Making of Security." *European Journal of International Relations* 22 (4): 493–516.

Buzan, Barry, Ole Wæver și Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner.

European Union. 2022a. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*.

___. 2022b. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive). *Official Journal of the European Union*.

European Commission. 2024. Commission Delegated Regulation (EU) 2023/503 supplementing Directive (EU) 2022/2557 by establishing a list of essential services. *Official Journal of the European Union*.

Stritzel, Holger. 2014. *Security in Translation: Securitization Theory and the Localization of Threat*. London: Palgrave Macmillan.

Taureck, Rita. 2006. "Securitization Theory and Securitization Studies." *Journal of International Relations and Development* 9 (1): 53–61.

Taureck, Rita. 2006. "Securitization – An Analytical Tool." In *Approaches to Security*, edited by Kai Michael Kenkel, 53–72. London: Routledge. *(If needed; optional depending on whether both texts were used.)*

Wæver, Ole. 1995. "Securitization and Desecuritization." In *On Security*, edited by Ronnie D. Lipschutz, 46–86. New York: Columbia University Press.