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

Confidențialitate, loialitate și responsabilitate: triada etică în managementul sistemelor informaționale în domeniul securității naționale

Confidentiality, Loyalty, and Responsibility: The Ethical Triad in Information Systems Management in the Field of National Security

Conf.univ.dr. Florentina-Loredana DRAGOMIR*
*Universitatea Națională de Apărare „Carol I", București
e-mail: Dragomir.Loredana@unap.ro

Abstract

Prezentul articol analizează triada etică formată din confidențialitate, loialitate și responsabilitate în managementul sistemelor informaționale din domeniul securității naționale, subliniind nevoia unei guvernanțe informaționale adaptate complexității actuale. În centrul analizei se află rolul sistemelor informaționale inteligente (SII), care, prin integrarea tehnologiilor de inteligență artificială, învățare automată și analiză comportamentală, oferă un suport decisiv în modernizarea arhitecturilor de securitate și în consolidarea unei culturi organizaționale etice. În acest sens, articolul susține că integrarea SII nu mai reprezintă o alegere tehnologică opțională, ci o necesitate strategică pentru organizațiile care gestionează informații clasificate și resurse critice. Prin abordarea sa multidisciplinară și prin argumentele fundamentate teoretic și normativ, studiul contribuie la delimitarea unui cadru conceptual robust privind guvernanța etică a informației în instituțiile de securitate națională.

This article analyzes the ethical triad of confidentiality, loyalty, and responsibility in the management of information systems in the field of national security, highlighting the need for information governance adapted to the current complexity. At the heart of the analysis is the role of intelligent information systems (IIS), which, by integrating artificial intelligence, machine learning, and behavioral analysis technologies, provide decisive support in modernizing security architectures and strengthening an ethical organizational culture. In this sense, the article argues that the integration of IIS is no longer an optional technological choice, but a strategic necessity for organizations that manage classified information and critical resources. Through its multidisciplinary approach and theoretically and normatively grounded arguments, the study contributes to the delimitation of a robust conceptual framework regarding the ethical governance of information in national security institutions.

Cuvinte-cheie:
sisteme informatice inteligente; securitate națională; guvernanță etică; decizii strategice; confidențialitate.

Keywords:
Intelligent Information Systems; National Security; Ethical Governance; Strategic Decision-Making; Confidentiality.

Info articol
Primit: 30 aprilie 2025; Evaluat: 28 mai 2025; Acceptat: 30 mai 2025; Disponibil online: ? iunie 2025
Citare: Dragomir, F.L. 2025. „Confidențialitate, loialitate și responsabilitate: triada etică în managementul sistemelor informaționale în domeniul securității naționale". *Buletinul Universității Naționale de Apărare „Carol I"*, 14(2): 80-93. https://doi.org/10.53477/2065-8281-25-14

Gestionarea etică a sistemelor informaționale în domeniul securității naționale a devenit o provocare strategică majoră. Instituțiile militare și de securitate se confruntă cu necesitatea de a echilibra transparența proceselor operaționale cu protecția informațiilor sensibile într-un mediu în care confidențialitatea, loialitatea și responsabilitatea constituie parametrii esențiali ai încrederii instituționale. În actualul climat strategic, profund marcat de digitalizare accelerată și volatilitate geopolitică, protejarea informațiilor sensibile reprezintă un obiectiv prioritar pentru organizațiile din domeniul securității naționale. În paralel, exigențele privind transparența proceselor și responsabilitatea instituțională devin din ce în ce mai pregnante, inclusiv în sectorul militar. Astfel, se conturează o dilemă etică fundamentală: cum poate fi asigurat un echilibru sustenabil între nevoia de transparență operațională și imperativele confidențialității?

Confidențialitatea nu mai este doar o chestiune tehnică, ci o dimensiune etică fundamentală în arhitectura sistemelor informaționale strategice. Studiile recente evidențiază că eficiența securității informaționale este influențată de factori instituționali și culturali, iar integrarea acestor aspecte în strategiile de securitate este esențială pentru protejarea datelor sensibile (Metin și alții 2024, 4226). Cercetările subliniază că performanța sistemelor de securitate informațională depinde în mod semnificativ de contextul instituțional și de valorile culturale, iar încorporarea acestor factori în politicile de securitate este crucială pentru asigurarea protecției datelor sensibile (Xu și alții 2025, 6). Loialitatea personalului cu acces la informații clasificate este un alt element critic. Comportamentele deviante, cum ar fi încălcarea politicilor de securitate, pot avea consecințe grave asupra integrității sistemelor informaționale. Analizele comportamentale subliniază importanța unei culturi organizaționale solide și a unei conduceri etice pentru prevenirea acestor riscuri (Metin și alții 2024, 4226). Totodată, loialitatea personalului cu acces la informații clasificate se afirmă ca o verigă esențială în lanțul de securitate. Fenomenele de abatere de la normele etice și riscurile asociate factorului uman rămân printre principalele vulnerabilități ale sistemelor informaționale. Prevenirea acestor riscuri presupune cultivarea unei culturi organizaționale solide, înrădăcinată în valori, precum devotamentul instituțional și disciplina profesională. Responsabilitatea atât la nivel individual, cât și instituțional este esențială în guvernanța sistemelor informaționale. Implementarea unor politici clare și a unor mecanisme de audit eficiente contribuie la asigurarea integrității și disponibilității informațiilor, aspecte cruciale pentru funcționarea optimă a organizațiilor strategice (Almomani și alții 2023, 4467). Pe de altă parte, responsabilitatea în materie de guvernanță informațională implică atât mecanisme formale de control (audit, trasabilitate, reglementări), cât și asumarea conștientă a consecințelor deciziilor luate la toate nivelurile structurale. Implementarea unui cadru de responsabilitate distribuită contribuie la întărirea rezilienței instituționale și la consolidarea încrederii publice (Almomani și alții 2023, 4467).

În acest context, articolul de față își propune să exploreze triada etică, formată din confidențialitate, loialitate și responsabilitate, analizând modul în care aceste valori pot fi integrate în managementul sistemelor informaționale din domeniul

securității naționale. Prin intermediul unei abordări multidisciplinare, vom examina provocările și soluțiile etice care pot contribui la consolidarea securității informaționale în organizațiile strategice.

1. Confidențialitatea în arhitectura sistemelor informaționale strategice

1.1 Definirea conceptului de confidențialitate în contextul securității naționale

Confidențialitatea, alături de integritate și disponibilitate, constituie una dintre cele trei dimensiuni esențiale ale securității informaționale, cunoscută sub denumirea de triada CIA. În sens operațional, confidențialitatea implică protejarea datelor împotriva accesului neautorizat, asigurând că doar persoanele sau entitățile autorizate pot vizualiza, manipula sau distribui informații sensibile. În cadrul organizațiilor de securitate națională, această componentă capătă o importanță critică. Protejarea informațiilor strategice, militare sau diplomatice de compromitere nu este doar o cerință tehnică, ci o obligație instituțională, care susține suveranitatea statului și funcționarea sistemului de apărare. Informațiile clasificate, dacă sunt divulgate sau accesate în mod neautorizat, pot conduce la vulnerabilități operaționale, la afectarea relațiilor internaționale sau chiar la pierderi de vieți omenești în teatrele de operații.

Unul dintre modelele conceptuale fundamentale pentru implementarea confidențialității este modelul Bell–LaPadula. Acesta a fost conceput pentru mediile militare, unde nivelurile de clasificare sunt riguroase. Aceste reguli au drept scop prevenirea accesului la informații de nivel superior de către utilizatori cu autorizații inferioare, respectiv blocarea transferului neautorizat de informații de la niveluri înalte către cele inferioare. Aplicarea acestui model contribuie la menținerea unei ierarhii riguroase de securitate, în care fluxul informațional este strict controlat și documentat. Astfel, confidențialitatea în arhitectura sistemelor informaționale strategice trebuie înțeleasă nu doar ca o măsură tehnologică de protecție, ci și ca o responsabilitate etică și instituțională, ancorată în cadrul normativ național și internațional privind securitatea informației.

1.2. Instrumente tehnologice și procedurale pentru asigurarea confidențialității

Protejarea informațiilor sensibile în cadrul sistemelor informaționale strategice presupune implementarea unui ansamblu de măsuri tehnologice și procedurale, menite să prevină accesul neautorizat, interceptarea sau compromiterea datelor. Aceste măsuri sunt integrate într-o arhitectură de securitate cuprinzătoare, care funcționează atât la nivelul infrastructurii informatice, cât și în cadrul structurilor organizaționale.

Criptarea datelor reprezintă unul dintre cele mai eficiente mijloace tehnologice de protejare a confidențialității. Algoritmii criptografici avansați, precum Advanced Encryption Standard (AES), asigură confidențialitatea informațiilor atât în tranzit, cât și în repaus, împiedicând accesul la conținutul acestora, în absența unei chei valide. În mediile militare, unde datele circulă prin rețele distribuite și adesea vulnerabile,

criptarea este însoțită de protocoale robuste de autentificare și de semnături digitale, care contribuie la validarea identității utilizatorilor și a integrității mesajelor.

O altă modalitate de protejare a confidențialității îl constituie politicile de control al accesului. Acestea sunt reglementate de mecanisme, precum controlul bazat pe roluri (Role-Based Access Control – RBAC) și controlul bazat pe atribute (Attribute-Based Access Control – ABAC), care asigură accesul la informații în funcție de responsabilitățile funcționale și de nivelul de autorizare al fiecărui utilizator. În instituțiile strategice, unde gradul de clasificare al datelor este ridicat, aceste mecanisme sunt completate de politici obligatorii de acces (Mandatory Access Control – MAC), care impun restricții rigide și ierarhizate, în conformitate cu legislația privind informațiile clasificate.

Pe lângă componentele tehnologice, instrumentele procedurale joacă un rol esențial în garantarea confidențialității. Auditarea sistematică a activităților informatice, monitorizarea în timp real a accesului la date și analiza comportamentului utilizatorilor contribuie la identificarea rapidă a posibilelor breșe de securitate (Kent și Souppaya 2006). În paralel, formarea continuă a personalului, derulată prin programe instituționale de conștientizare și de instruire, vizează reducerea riscurilor asociate erorii umane, care rămâne una dintre cele mai frecvente cauze ale compromiterii informațiilor clasificate.

Prin urmare, asigurarea confidențialității nu se limitează la implementarea unor tehnologii performante, ci presupune o guvernanță integrată a riscului informațional, în care procesele, politicile și comportamentele individuale se află într-o relație de interdependență strategică.

1.3. Riscuri asociate divulgării sau pierderii datelor clasificate

Divulgarea neautorizată sau pierderea informațiilor clasificate reprezintă una dintre cele mai grave vulnerabilități în arhitectura sistemelor informaționale strategice, cu implicații directe asupra securității naționale, stabilității geopolitice și capacității operaționale a instituțiilor militare. Aceste incidente pot compromite planuri tactice, pot dezvălui capabilități tehnice sau pot afecta alianțe și parteneriate strategice, generând un efect de domino în lanțurile decizionale și operaționale. În primul rând, compromiterea informațiilor clasificate poate conduce la pierderea avantajului strategic. Cum într-un mediu operațional asimetria informațională este decisivă, accesul adversarilor la date sensibile poate favoriza acțiuni de anticipare, de disuasiune sau de sabotaj, care subminează eficiența și siguranța misiunilor militare. Cazurile documentate în literatura de specialitate relevă faptul că scurgerile de informații din cadrul instituțiilor de apărare au condus în mod repetat la reevaluarea structurilor de comandă, la suspendarea temporară a operațiunilor și la diminuarea încrederii interinstituționale. În al doilea rând, pierderea controlului asupra datelor clasificate afectează sever relațiile internaționale și cooperarea în materie de securitate. Partenerii strategici își bazează schimbul de informații pe premisele confidențialității reciproce și pe existența unor măsuri echivalente de protecție

informațională. O breșă în acest sistem de încredere poate conduce la restrângerea accesului la informații critice, la suspendarea colaborărilor sau la reevaluarea poziției geopolitice a statului afectat.

Din perspectivă instituțională, astfel de incidente generează costuri semnificative atât din punct de vedere logistic, cât și reputațional. Reconfigurarea sistemelor afectate, inițierea anchetelor interne, măsurile de remediere și investițiile suplimentare în securitate implică alocarea unor resurse bugetare considerabile. Mai mult, în rândul opiniei publice, pierderea de informații sensibile poate eroda încrederea cetățenilor în capacitatea statului de a-și proteja interesele fundamentale, alimentând percepția de vulnerabilitate instituțională.

Pentru a limita aceste riscuri, organizațiile strategice trebuie să adopte o abordare proactivă, bazată pe evaluări continue de risc, pe teste de penetrare, pe simulări de incident și pe audituri independente. Aceste mecanisme trebuie susținute de un cadru normativ coerent și de o cultură organizațională orientată spre conformitate, responsabilitate și vigilență informațională. În absența acestor măsuri, protecția datelor clasificate rămâne expusă unor amenințări persistente, sofisticate și cu impact sistemic.

2. Responsabilitatea instituțională și individuală în guvernanța sistemelor informaționale

2.1 Cadre normative și obligații legale privind protecția informațiilor (legi naționale, tratate internaționale)

Responsabilitatea în materie de guvernanță a informației este strâns corelată cu respectarea unui cadru normativ complex, care reunește reglementări naționale, directive internaționale și tratate multilaterale privind protecția datelor clasificate și a infrastructurilor critice. În România, Legea nr. 182/2002 privind protecția informațiilor clasificate, împreună cu normele metodologice aferente, stabilește obligațiile instituțiilor publice și ale personalului autorizat în ceea ce privește clasificarea, manipularea și stocarea datelor sensibile. Aceste prevederi sunt armonizate cu cerințele NATO și UE privind interoperabilitatea în domeniul informațiilor securizate.

La nivel internațional, instrumente precum Tratatul de Securitate Informațională al NATO și Regulamentul General privind Protecția Datelor (GDPR) – în cazul în care interacțiunea implică și componente civile sau dual-use – impun standarde clare privind confidențialitatea, trasabilitatea și responsabilitatea procesării informațiilor. De asemenea, convenții precum Convenția de la Budapesta privind criminalitatea informatică conturează obligații statale în prevenirea și combaterea accesului ilegal la sisteme și date.

Respectarea acestor norme nu este opțională, ci face parte din responsabilitatea instituțională de a garanta securitatea informațională ca parte integrantă a securității

naționale. Această responsabilitate presupune existența unor structuri funcționale de control intern, audit periodic și actualizare continuă a procedurilor, în conformitate cu evoluțiile tehnologice și cu amenințările emergente (Dragomir-Constantin 2025c, 99-108).

2.2 Mecanisme de responsabilizare: trasabilitate, audit, răspundere penală sau disciplinară

În contextul sistemelor informaționale utilizate de organizațiile strategice, responsabilitatea nu poate fi redusă la un principiu teoretic sau la o valoare abstractă; ea trebuie să fie exprimată concret printr-un ansamblu de mecanisme instituționalizate care să permită atât prevenirea, cât și remedierea incidentelor care afectează confidențialitatea informațiilor clasificate. Această responsabilitate este dublă: individuală, în sensul asumării deciziilor de către fiecare utilizator autorizat, și instituțională, prin existența unor structuri și proceduri care asigură trasabilitatea acțiunilor, auditarea sistemelor și aplicarea de sancțiuni, în caz de abatere.

Trasabilitatea este condiția fundamentală pentru orice formă de responsabilizare. Prin implementarea unor mecanisme tehnice de monitorizare – precum logarea activităților, sistemele de jurnalizare criptografică și platformele de analiză comportamentală –, organizațiile pot asigura o vizibilitate continuă asupra interacțiunilor utilizatorilor cu sistemele critice. Astfel, fiecare accesare, modificare sau transmitere de date este înregistrată și asociată unei identități digitale, eliminând premisele anonimatului și reducând riscul de impunitate (Dignum 2019). Acest sistem de urmărire a acțiunilor individuale este indispensabil pentru identificarea sursei unui incident, dar și pentru stabilirea proporțională a răspunderii.

Auditul, ca instrument formal de verificare a conformității și eficienței, contribuie la menținerea unui climat instituțional transparent și predictibil. Evaluările periodice ale politicilor de securitate informațională, realizate de entități interne sau externe, permit nu doar corectarea abaterilor, ci și anticiparea unor vulnerabilități structurale. În mediile militare, auditul are o dimensiune strategică suplimentară: el validează capacitatea sistemelor informaționale de a susține operațiuni, în condiții de adversitate informațională și cibernetică (Kent și Souppaya 2006).

Sancțiunile disciplinare și juridice completează acest cadru, asigurând un răspuns instituțional proporțional la încălcările normelor de securitate. Fără mecanisme sancționatorii clare, responsabilitatea devine iluzorie, iar organizația se expune riscului ca normele să fie percepute ca pur formale. Aplicarea consecventă a măsurilor – de la retragerea accesului, la suspendarea temporară sau definitivă din funcție, până la urmărirea penală în cazurile grave – contribuie la consolidarea unei culturi instituționale bazate pe respectarea reglementărilor și pe conștientizarea consecințelor individuale ale neglijenței sau intenției malițioase (Metin și alții 2024).

Astfel, responsabilitatea într-un ecosistem informațional de tip strategic nu poate funcționa în absența unui cadru coerent de trasabilitate, audit și sancționare. Această

triadă instituțională asigură nu doar reziliența operațională, ci și legitimitatea internă și externă a organizației în fața provocărilor specifice mediului de securitate contemporan.

Trasabilitatea reprezintă o funcționalitate esențială în cadrul arhitecturii de securitate a sistemelor informaționale strategice, definind capacitatea sistemului de a înregistra, urmări și corela toate acțiunile desfășurate asupra resurselor informaționale de către utilizatorii autorizați. Această funcție nu are doar un rol tehnic, ci constituie fundamentul responsabilității individuale și instituționale, oferind suport probatoriu pentru evaluarea comportamentului utilizatorilor și conformității proceselor cu politicile și reglementările în vigoare. În mod operațional, trasabilitatea se realizează printr-un ansamblu de tehnologii și metode, precum loguri de acces detaliate, sisteme de jurnalizare criptografică și module de analiză comportamentală, care permit corelarea fiecărei acțiuni din sistem cu o identitate digitală univocă. În mediile militare și instituționale de înaltă securitate, aceste sisteme sunt configurate pentru a funcționa în regim de nonrepudiere, asigurând că nicio operațiune relevantă nu poate fi contestată ulterior de către actorul care a generat-o (Sulaiman și alții 2022).

Importanța trasabilității nu se limitează la dimensiunea investigativă postincident, deși aceasta este vitală pentru determinarea cauzelor și responsabilităților, în cazul compromiterii informațiilor. Ea joacă un rol preventiv și sistemic în procesul de guvernanță a riscului informațional, permițând instituțiilor să monitorizeze în timp real activitatea utilizatorilor, să detecteze anomalii comportamentale și să reacționeze prompt în fața abaterilor sau a potențialelor atacuri interne. Astfel, trasabilitatea contribuie la consolidarea capacității de reacție operațională și la menținerea unei culturi organizaționale bazate pe transparență și responsabilitate. În plus, trasabilitatea constituie o condiție esențială pentru auditul eficient al sistemelor informatice. În special în organizațiile strategice, logurile trebuie să fie protejate împotriva modificării sau ștergerii, întrucât acestea pot constitui probe juridice în anchete disciplinare sau penale. Din acest motiv, instituțiile militare implementează soluții care asigură integritatea logurilor prin mecanisme de sigilare digitală, de sincronizare temporală cu surse de timp externe și de replicare în sisteme redundante, garantând astfel că orice tentativă de alterare a înregistrărilor este detectabilă și sancționabilă.

Prin urmare, trasabilitatea nu este doar o componentă tehnologică, ci o dimensiune strategică a arhitecturii de securitate, integrată în ansamblul politicilor de conformitate, de control intern și de guvernanță informațională. Fără un mecanism robust de trasabilitate, instituțiile strategice riscă nu doar pierderea controlului asupra resurselor informaționale, ci și diminuarea capacității de a reacționa în mod legitim și eficient în fața abaterilor interne sau a atacurilor externe.

Urmează auditul, una dintre cele mai importante componente ale mecanismului de control instituțional în materie de securitate informațională, acesta având rolul de a evalua conformitatea, eficiența și robustețea proceselor, politicilor și infrastructurilor

informatice. În mediile strategice, auditul transcende dimensiunea pur procedurală, devenind un instrument esențial de guvernanță și anticipare a riscurilor, care contribuie la consolidarea integrității organizaționale și la menținerea capacității operaționale, în condiții de incertitudine sau amenințare.

Auditul de securitate informațională se desfășoară pe două planuri interdependente: cel tehnic și cel procedural. Auditul tehnic presupune examinarea sistemelor informatice din perspectiva configurațiilor de securitate, a nivelurilor de criptare, a sistemelor de detecție a intruziunilor, precum și a politicilor de acces și logare. Obiectivul este identificarea vulnerabilităților care ar putea fi exploatate de actori interni sau externi și evaluarea capacității sistemului de a rezista la atacuri cibernetice, inclusiv cele de tip avansat persistent (APT). În organizațiile militare, acest tip de audit este completat adesea prin simulări de penetrare (”red teaming”), în care echipe specializate încearcă să compromită sistemele în mod controlat pentru a evidenția punctele slabe din apărare.

Pe de altă parte, auditul procedural se concentrează asupra modului în care politicile și regulamentele de securitate sunt aplicate în practică. Acesta analizează compatibilitatea dintre fluxurile operaționale și cerințele normative, gradul de respectare a protocoalelor de acces și de manipulare a informațiilor clasificate, precum și nivelul de instruire al personalului. Discrepanțele dintre prevederile teoretice și comportamentul real al actorilor instituționali pot semnala deficiențe de comunicare, lipsa unei culturi organizaționale axate pe securitate sau chiar riscuri sistemice, generate de toleranța la abateri.

Un audit eficient presupune independența structurilor de control, accesul la date nefiltrate și capacitatea de a formula recomandări operaționale, nu doar constatări tehnice. De asemenea, este esențial ca rezultatele auditului să fie integrate într-un ciclu continuu de îmbunătățire, în care recomandările să fie transpuse în măsuri concrete, iar implementarea acestora să fie urmărită cu aceeași rigoare. În concluzie, auditul nu este doar o practică de verificare retrospectivă, ci și un element activ al sistemului de securitate informațională, menit să detecteze și să corecteze vulnerabilități, să valideze măsuri și să întărească responsabilitatea individuală și instituțională. În absența unei funcții de audit solid ancorate în arhitectura decizională a organizațiilor strategice, controlul riscurilor informaționale rămâne parțial și reactiv, ceea ce poate compromite reziliența întregului sistem.

Răspunderea juridică și disciplinară reprezintă dimensiunea sancționatorie prin care organizațiile strategice își consolidează mecanismele de control și previn comportamentele neconforme. În mediile cu grad ridicat de secretizare, precum cele militare, responsabilitatea individuală pentru protejarea informațiilor clasificate nu este doar o obligație profesională, ci și o exigență legală, reglementată prin norme interne, legislație națională și tratate internaționale în materie de securitate și apărare.

În cadrul instituțiilor militare, regimul sancționator este completat de regulamente interne care includ, pe lângă suspendarea temporară sau revocarea accesului la informații clasificate, și proceduri de retrogradare sau de excludere din sistem. Responsabilitatea penală se activează atunci când compromiterea informațiilor are loc prin fapte intenționate, din neglijență gravă sau în urma unor omisiuni culpabile. Astfel de fapte includ transferul neautorizat de date, accesul nepermis la sisteme clasificate, pierderea suporturilor fizice de stocare sau nerespectarea procedurilor operaționale. În aceste cazuri, autoritățile competente, inclusiv structurile specializate ale Ministerului Public sau serviciile de contrainformații declanșează anchete care pot conduce la trimiterea în judecată a persoanelor implicate (Metin și alții 2024).

Răspunderea disciplinară, deși distinctă de cea penală, joacă un rol complementar, având ca obiectiv menținerea ordinii interne și a conformității cu normele organizaționale. Aceasta poate fi aplicată inclusiv în situații în care fapta nu întrunește elementele constitutive ale unei infracțiuni, dar reflectă o conduită inacceptabilă din perspectiva obligațiilor de serviciu. Sancțiunile pot varia de la avertismente scrise și scăderea temporară a salariului, până la destituirea din funcție sau excluderea din structurile de securitate, în funcție de gravitatea încălcării și de poziția ocupată de persoana în cauză. În mediile strategice, eficiența acestor forme de răspundere depinde de trei factori: claritatea normelor, consecvența aplicării și transparența procedurilor. Lipsa unui cadru normativ bine definit sau aplicarea selectivă a sancțiunilor poate conduce la erodarea culturii organizaționale bazate pe etică și responsabilitate. Astfel, răspunderea juridică și disciplinară trebuie înțeleasă ca o verigă esențială a ecosistemului de securitate informațională, prin care comportamentul individual este corelat cu normele instituționale, iar protejarea informațiilor sensibile devine un act de conformitate, loialitate și respect față de interesul național.

3. Contribuțiile sistemelor informaționale inteligente la consolidarea responsabilității și eticii organizaționale

În era transformării digitale accelerate și a intensificării amenințărilor hibride, sistemele informaționale inteligente (SII) s-au impus ca elemente esențiale în arhitectura organizațiilor strategice, redefinind paradigmele de guvernanță, de securitate și de luare a deciziilor. Aceste sisteme, fundamentate pe inteligență artificială (IA), pe învățare automată (ML), pe analitică predictivă și pe procese de automatizare cognitivă, extind funcționalitățile infrastructurii informaționale tradiționale, oferind o capacitate crescută de adaptare și anticipare în medii operaționale volatile (Dignum 2019; Xu și alții 2024).

În mod particular, SII permit modernizarea proceselor decizionale prin reducerea incertitudinii și creșterea vitezei de reacție în fața amenințărilor informaționale.

Algoritmii de învățare automată pot analiza volume masive de date în timp real, identificând tipare relevante, anomalii și semnale slabe care ar putea indica o breșă de securitate sau un comportament deviant din partea unui utilizator intern. Această capacitate de detecție precoce, asociată cu mecanisme de răspuns automatizat, contribuie direct la consolidarea rezilienței informaționale și la prevenirea incidentelor cu impact sistemic (Grigaliunas și alții 2024). Mai mult, sistemele inteligente facilitează o guvernanță proactivă a riscurilor informaționale prin generarea de modele predictive și recomandări decizionale, bazate pe evaluarea probabilistică a amenințărilor. Aceste instrumente nu doar susțin procesele tactice de securitate, ci și permit alinierea deciziilor operaționale la standarde etice și juridice prestabilite. Astfel, SII devin instrumente de suport etic în medii în care deciziile rapide trebuie să fie compatibile cu reglementările naționale și internaționale privind protecția datelor și drepturile fundamentale (Dignum 2019; Tounsi și Rais 2018).

Un element esențial care diferențiază sistemele informaționale inteligente (SII) de infrastructurile clasice de securitate este capacitatea lor de a facilita o guvernanță proactivă a riscurilor informaționale, bazată pe anticipare, adaptare și conformitate normativă. Această abordare proactivă presupune depășirea paradigmei reactive, în care măsurile de securitate sunt implementate post-factum, și trecerea la un model predictiv, în care amenințările sunt identificate, evaluate și neutralizate înainte de a se materializa.

SII integrează algoritmi de învățare automată și modele de inteligență artificială care procesează volume mari de date din surse heterogene – inclusiv loguri de sistem, fluxuri de comunicație, profiluri comportamentale și indicatori de amenințare – pentru a genera evaluări probabilistice privind riscurile emergente. Prin aceste capabilități, sistemele pot detecta semnale slabe și pot corela evenimente aparent izolate, identificând tipare care indică activități anormale, potențial periculoase, înainte ca acestea să devină manifeste (Tounsi și Rais 2018). Acest tip de analiză predictivă oferă factorilor de decizie un avantaj temporal semnificativ, permițându-le să adopte măsuri de securitate cu caracter preventiv, nu doar corectiv.

Pe lângă dimensiunea tehnică, SII contribuie și la susținerea unui cadru decizional etic și juridic coerent. În organizațiile strategice, unde deciziile trebuie luate adesea în condiții de presiune și incertitudine, instrumentele inteligente oferă sprijin analitic obiectiv, reducând riscul de decizii arbitrare sau nealiniate cu reglementările în vigoare. De exemplu, prin integrarea unor reguli deontologice sau a unor criterii de conformitate cu legislația privind protecția datelor, sistemele pot evalua opțiunile decizionale nu doar din punctul de vedere al eficienței operaționale, ci și al respectării normelor legale și principiilor de drept (Dignum 2019). Această funcție de „asistență etică automatizată" devine crucială în domenii sensibile, precum apărarea națională, securitatea cibernetică sau protecția infrastructurilor critice, unde deciziile pot implica simultan consecințe tehnice, umane și politice. SII pot recomanda opțiuni care minimizează riscurile colaterale, protejează datele personale sau respectă drepturile fundamentale, chiar și în contexte operaționale în care astfel

de dimensiuni sunt ușor de neglijat. Astfel, aceste sisteme nu doar că optimizează răspunsul la amenințări, ci și instituționalizează un cadru de responsabilitate etică distribuită, în care principiile normative sunt încorporate în logica algoritmică a acțiunii. În acest sens, rolul SII transcende funcția de suport tehnologic, devenind parte integrantă a unui mecanism decizional responsabil, capabil să integreze în timp real criterii de securitate, de legalitate și de etică. Într-un ecosistem informațional complex și hiperconectat, în care granițele dintre operațional și normativ sunt din ce în ce mai fluide, această capacitate de a susține decizii compatibile, simultan cu imperativul de eficiență și cu exigențele morale și juridice reprezintă un avantaj strategic major.

Un alt beneficiu esențial al SII constă în sprijinirea culturii organizaționale etice. Prin monitorizarea continuă și imparțială a interacțiunilor utilizatorilor cu sistemele informaționale, aceste tehnologii oferă un cadru de responsabilitate distribuită, în care fiecare actor este conștient că acțiunile sale sunt supuse unui regim obiectiv de evaluare și trasabilitate. În acest sens, tehnologia funcționează nu doar ca un gardian al datelor, ci și ca un mecanism de conformitate morală, reducând spațiul pentru abateri sau comportamente oportuniste (Xu și alții 2024).

Sistemele informaționale inteligente contribuie la modernizarea arhitecturilor de securitate și la profesionalizarea deciziilor strategice, oferind un sprijin tehnologic indispensabil pentru atingerea unui echilibru durabil între eficiență operațională, responsabilitate și etică instituțională. Cum timpul de reacție este critic, iar erorile umane pot avea consecințe ireversibile, integrarea SII nu mai este o opțiune, ci o necesitate strategică pentru organizațiile care gestionează informații clasificate și resurse critice.

Unul dintre cele mai relevante beneficii ale sistemelor informaționale inteligente (SII) în cadrul organizațiilor strategice constă în capacitatea acestora de a susține și de a consolida o cultură organizațională etică, în care normele comportamentale, valorile instituționale și responsabilitatea individuală sunt în mod continuu promovate, verificate și întărite prin mecanisme tehnologice transparente și imparțiale. Spre deosebire de modelele tradiționale de conformitate, care se bazează preponderent pe supraveghere ierarhică și audituri periodice, SII oferă posibilitatea unei monitorizări constante, scalabile și neutre a interacțiunilor dintre utilizatori și resursele informaționale critice. Prin culegerea și analiza automată a datelor privind activitatea utilizatorilor – inclusiv accesarea fișierelor, modificarea configurațiilor, comunicarea prin canale interne sau activitatea în afara orelor de lucru –, aceste sisteme pot construi profiluri comportamentale care permit detectarea devierilor semnificative de la normele instituționale. Această formă de monitorizare nu vizează controlul represiv, ci cultivarea unui mediu în care actorii organizaționali devin conștienți că fiecare acțiune este supusă unei forme de evaluare obiectivă, nemijlocită de percepții sau interese subiective (Xu și alții 2024). În această configurație, tehnologia devine un catalizator al responsabilității individuale, contribuind la internalizarea normelor etice de către utilizatori. Conștientizarea faptului că activitatea profesională este vizibilă și trasabilă

nu doar descurajează comportamentele oportuniste, dar și încurajează adoptarea unor practici conforme, în care respectarea politicilor nu mai este percepută ca o obligație externă, ci ca o normă integrată în identitatea profesională a individului. Această responsabilitate distribuită – susținută de sisteme imparțiale și automate – are avantajul de a reduce spațiul de manevră pentru acțiuni distructive, consolidând, în același timp, încrederea în mecanismele instituționale de control.

Mai mult, SII pot contribui la dezvoltarea unui climat organizațional în care conformitatea morală nu este doar un rezultat al fricii de sancțiune, ci al înțelegerii și asimilării valorilor instituționale. Prin analiza comportamentelor colective și individuale, sistemele pot genera informații utile referitoare la tiparele dominante, vulnerabilitățile etice ale organizației și necesitatea unor intervenții de formare sau ajustare culturală. Acest tip de feedback analitic permite decidenților să adopte politici proactive de etică organizațională, fundamentate pe date, nu doar pe presupuneri sau incidente reactive (Tounsi și Rais 2018).

Prin capacitățile avansate de analiză predictivă, de detectare a anomaliilor, de automatizare a reacțiilor și de asistare a deciziilor, SII asigură un sprijin operațional care depășește sfera tehnică și care pătrunde în dimensiunile normative și organizaționale ale securității. Astfel, deciziile nu mai sunt adoptate exclusiv în baza intuiției sau experienței individuale, ci sunt susținute de date, corelate cu scenarii, evaluate în funcție de riscuri și filtrate prin constrângeri etice și juridice. Această recalibrare a procesului decizional permite nu doar minimizarea erorilor umane, ci și consolidarea legitimității și transparenței în interiorul instituțiilor strategice (Dignum 2019). În contextul operațional contemporan, în care timpul de reacție este comprimat, iar presiunea asupra liderilor instituționali este constantă, deciziile rapide, dar conforme devin un imperativ. În această ecuație, SII oferă un avantaj competitiv prin capacitatea lor de a furniza informații în timp real, de a învăța din incidente anterioare și de a genera soluții adaptive în fața unor amenințări dinamice (Tounsi și Rais 2018).

Mai mult, prin promovarea unei culturi organizaționale bazate pe transparență, trasabilitate și etică distribuită, aceste sisteme sprijină dezvoltarea unei instituții agile, capabile să funcționeze în medii volatile, fără a-și compromite valorile fundamentale. În acest sens, rolul SII nu este limitat la un instrument de securitate, ci se extinde către statutul de infrastructură critică pentru decizia responsabilă, guvernanța strategică și reziliența organizațională. Așadar, în mediile instituționale care gestionează informații clasificate, infrastructuri critice sau mize strategice naționale, implementarea sistemelor informaționale inteligente nu mai poate fi considerată un lux sau o alegere opțională. Ea reprezintă o necesitate pentru consolidarea securității, optimizarea deciziilor și asigurarea unei conduite instituționale conforme cu standardele internaționale de etică, legalitate și performanță.

Concluzii

În condițiile creșterii volumului de date strategice și accentuării amenințărilor hibride, protejarea informațiilor sensibile nu mai poate fi realizată eficient prin mecanisme tradiționale de securitate și de control instituțional. Articolul de față a argumentat că triada etică, formată din confidențialitate, loialitate și responsabilitate, nu poate fi susținută fără integrarea tehnologiilor emergente, în special a sistemelor informaționale inteligente (SII).

Aceste sisteme nu doar extind capabilitățile tehnice ale organizațiilor strategice, ci și transformă fundamental modul în care este înțeleasă și aplicată guvernanța informațională. Prin capacitatea de a monitoriza în timp real comportamentul utilizatorilor, de a genera evaluări predictive ale riscurilor și de a susține deciziile strategice prin recomandări conforme cu standardele etice și juridice, SII devin infrastructuri de responsabilitate distribuită. Ele oferă garanții suplimentare pentru integritatea proceselor și reduc semnificativ riscul de eroare umană, de abuz sau de neglijență instituțională.

Un alt aport esențial al acestor tehnologii constă în sprijinirea unei culturi organizaționale etice. Prin trasabilitate, imparțialitate în evaluare și capacitate de adaptare, SII contribuie la întărirea conștiinței profesionale a personalului și la internalizarea valorilor instituționale. Astfel, tehnologia funcționează nu doar ca un instrument de control, ci și ca un mecanism de cultivare a eticii instituționale, în care responsabilitatea nu este impusă extern, ci susținută prin infrastructură și proces decizional.

Integrarea sistemelor informaționale inteligente în arhitectura organizațiilor strategice trebuie să fie privită nu ca o opțiune tehnologică, ci ca o necesitate strategică. Sistemele informaționale inteligente oferă premisele unei guvernanțe robuste, conforme, proactive și orientate spre valori. Mediul informațional tot mai instabil, unde timpul de reacție este critic, iar costurile greșelilor sunt ireversibile, vizează SII, care se constituie într-un suport indispensabil pentru asigurarea securității, legitimității și rezilienței instituționale.

Referințe

Almomani, Iman, Aala Alkhayer și Walid El-Shafai. 2023. "E2E-RDS: Efficient End-to-End Ransomware Detection System Based on Static-Based ML and Vision-Based DL Approaches". *Sensors 23* (9): 4467. https://doi.org/10.3390/s23094467.

Bell, David Elliott și Leonard LaPadula. 1973. "Secure Computer Systems: Mathematical Foundations. Technical Report MTR-2547", Vol. I. https://websites.umich.edu/~cja/LPS12b/refs/belllapadula1.pdf

Dignum, Virginia. 2019. "Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way". Springer. https://link.springer.com/book/10.1007/978-3-030-30371-6

Dragomir, Florentina-Loredana și Gelu Alexandrescu. 2017a. "Applications of Artificial Intelligence in Decision-Making Process". *Bulletin of "Carol I" National Defense University* 4(2): 56-61. https://cssas.unap.ro/en/pdf_periodicals/si63.pdf.

___. 2017b. "The Axiomatic Character of Decision". *Bulletin of "Carol I" National Defense University* 6 (1): 16-22. https://www.ceeol.com/search/article-detail?id=548274.

Dragomir, Florentina-Loredana, Gelu Alexandrescu și Florin Postolache. 2018. "Tools for hierarchical security ". *The 14 the International Scientific Conference "eLearning and Software for Education"*, Bucharest, Carol I" National Defence University, April 19 - 20, Advanced Distributed Learning Association, vol. 4, pp. 34-38.

Dragomir-Constantin, Florentina-Loredana. 2025a. "Information System for Macroprudential Policies." *Acta Universitatis Danubius. Œconomica* 21 (1): 48-57. https://dj.univ-danubius.ro/index.php/AUDOE/article/view/3254.

___. 2025b. "Thinking Patterns in Decision-Making in Information Systems". *New Trends in Psychology* 7 (1): 89-98. https://dj.univ-danubius.ro/index.php/NTP/article/view/3255.

___. 2025c. "Thinking Traps: How High-Performance Information Systems Correct Cognitive Biases in Decision-Making". *New Trends in Psychology 7* (1) 99-108. https://dj.univ-danubius.ro/index.php/NTP/article/view/3257.

Grigaliūnas, Šarūnas, Michael Schmidt, Rita Brūzgienė și Smyrli Panagiota. 2024. "Holistic Information Security Management and Compliance Framework". https://epubl.ktu.edu/object/elaba:209322117/.

Kent, Karen și Murugiah Souppaya. 2006. "Guide to Computer Security Log Management. NIST Special Publication 800-92. National Institute of Standards and Technology". https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf

Metin, Bilgin, Fatma Gözde Özhan și Martin Wynn. 2024. "Digitalisation and Cybersecurity: Towards an Operational Framework." *Electronics* 13 (21): 4226. https://www.mdpi.com/2079-9292/13/21/4226.

Sulaiman, Nur Shafinas, Mohd Azlan Fauzi, Wendy Wider și Jasmine Rajadurai. 2022. "Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review." *Social Sciences* 11 (9): 386. https://www.mdpi.com/2076-0760/11/9/386.

Tache, Florentina-Loredana, Postolache Florin, Nachila Cătălin și Ivan Maria Alexandra. 2010." Consulting in Electronic Commerce." *Acta Universitatis Danubius. Œconomica* 6 (3): 162-169. https://journals.univ-danubius.ro/index.php/oeconomica/article/view/707.

Tounsi, Wassim și Hassen Rais. 2018. "A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attack". *Computers & Security* 72. https://www.sciencedirect.com/science/article/abs/pii/S0167404817301839?via%3Dihub.

Xu, Yao, Jixin Wei, Ting Mi și Zhihua Chen. 2024 "Data Security in Autonomous Driving: Multifaceted Challenges of Technology, Law, and Social Ethics." *World Electric Vehicle Journal* 16 (1): 6. https://doi.org/10.3390/wevj16010006.