Școala Națională de Studii Politice și Administrative
Facultatea de Administrație Publică

PROTEJAREA INTERESEOR ECONOMICE ALE UE ȘI ALE ROMÂNIEI:

STRATEGII DE COMBATERE A CRIMINALITĂȚII INFORMATICE ÎN ADMINISTRAȚIA VAMALĂ

- lucrare de disertație, Drept și guvernare europeană -

Coordonator

Conf. Univ. Dr. Cătălin VRABIE

Absolvent

Pîrlog George Alexandru

București
2025

Instrucțiuni de redactare (A se citi cu atenție!!)

1. Introduceți titlul lucrării în zona aferentă acestuia – nu modificați mărimea sau tipul fontului;
2. Sub titlul lucrării alegeți dacă aceasta este de licență sau de disertație;
3. Introduceți specializarea sau masteratul absolvit în zona aferentă acestuia de pe prima pagină a lucrării;
4. Introduceți numele dvs. complet în zona aferentă acestuia (sub Absolvent (ă));
5. Introduceți anul în care este susținută lucrarea sub București;

NB: Asigurați-vă că ați șters parantezele pătrate din pagina de gardă și cuprins.

6. Trimiteți profesorului coordonator lucrarea doar în format **Microsoft Word** – alte formate nu vor fi procesate;
7. **Nu ștergeți declarația anti-plagiat și nici instrucțiunile** – acestea trebuie să rămână pe lucrare atât în forma tipărită cât și în cea electronică;
8. **Semnați declarația anti-plagiat;**
9. **Cuprinsul este orientativ** – numărul de capitole / subcapitole poate varia de la lucrare la lucrare. **Introducerea, Contextul, Concluziile / Discuțiile și Referințele bibliografice sunt însă obligatorii;**
10. **Este obligatorie folosirea template**-ului. Abaterea de la acesta va cauza întârzieri în depunerea la timp a lucrării.

NB. Lucrările vor fi publicate în extenso pe pagina oficială a hub-ului Smart-EDU, secțiunea Smart Cities and Regional Development: https://scrd.eu/index.php/spr/index.

ATENȚIE: Lucrarea trebuie să fie un produs intelectual propriu. Cazurile de plagiat vor fi analizate în conformitate cu legislația în vigoare.

Declarație anti-plagiat

1. Cunosc că plagiatul este o formă de furt intelectual și declar pe proprie răspundere că această lucrare este rezultatul propriului meu efort intelectual și creativ și că am citat corect și complet toate informațiile preluate din alte surse bibliografice (de ex: cărți, articole, clipuri audio-video, secțiuni de text și sau imagini / grafice).

2. Declar că nu am permis și nu voi permite nimănui să preia secțiuni din prezenta lucrare pretinzând că este rezultatul propriei sale creații.

3. Sunt de acord cu publicarea on-line *in extenso* a acestei lucrări și verificarea conținutului său în vederea prevenirii cazurilor de plagiat.

Numele și prenumele: Pîrlog George Alexandru

Data și semnătura: 21.12.2024

Cuprins

Abstract

Prin prezenta lucrare, îmi propun o analiză elaborată asupra metodelor prin care o administrație vamală modernă face față provocărilor digitalizării și eficientizării domeniilor sale de activitate, atât din perspectiva colectării obligațiilor patrimoniale cuvenite, cât și a monitorizări și combaterii activității infracționale din ramura sa de competență. În cadrul lucrării voi pune accentul pe sisteme informatice aflate deja în uz (sistemul exportatorilor înregistrați Registered Exporter System, sistemul Authorised Economic Operator, sistemul Economic Operators Registration and Identification, sistemul New Computerised Transit System, sistemul de control al importurilor 2 Import Control System 2), în acest scop, cât și pe instrumente digitate folosite de alte administrații vamale în vederea identificării unei soluții optime pentru viitor. Deoarece în momentul de față lucrez în interiorul unei administrații vamale, consider oportun aprofundarea cunoștințelor deja însușite în urma activității profesionale, prin prezenta cercetare. Obiectivele lucrării vor urmării modelele eficiente ale altor administrații vamale, dar și ceea ce s-a implementat cu succes în România, pentru a se identifica o soluție optimă și competitivă, adaptată realităților zilelor noastre. Metodologia se va fundamenta în principal pe stategii implementate de alte administrații vamale din statele membre dar și din spațiul neunional, analize și rapoarte ale organismelor UE și strategii de securitate națională, secundar vor fi analizate articole științifice precum cele publicate în reviste de specialitate precum Smart Cities and Regional Development Journal și în volumele conferințelor Smart Cities International Conference și International Conference on Machine Intelligence & Security for Smart Cities. Cercetarea are ca rezultat identificarea stategiilor celor mai eficiente în combaterea fenomenelor infracționale din sfera de competență vamală și de protejare a intereselor financiare ale României și respectiv UE, utilizând instrumente digitate și sisteme informatice moderne. Prin rezultatele sale, această cercetare poate contribui la îmbunătățirea sistemelor informatice actuale utilizate în administrația vamală română și poate oferi o nouă viziune sau perspectivă în implementarea de noi strategii pe viitor.

Cuvinte cheie: vamă, monitorizare, instrumente, securitate financiară

Introducere

Într-un context global marcat de o accelerare exponențială a procesului de digitalizare, administrațiile publice se confruntă cu o multitudine de provocări emergente, printre care criminalitatea informatică ocupă un loc central. Digitalizarea, deși esențială pentru eficientizarea și transparentizarea proceselor administrative, facilitează în egală măsură apariția unor riscuri cibernetice de amploare, care pot submina integritatea infrastructurilor vamale și securitatea economică a statelor. Dezvoltarea tehnologică rapidă impune un efort concertat din partea instituțiilor responsabile, în vederea implementării unor mecanisme de protecție adecvate și a elaborării unor strategii de prevenire și combatere a criminalității informatice.

Pentru o înțelegere aprofundată a problematicii abordate, se impune clarificarea unor concepte fundamentale: digitalizarea, administrația vamală și criminalitatea informatică. Conceptual, este imperativă distincția dintre „digitizare” și „digitalizare”. Dacă digitizarea se referă exclusiv la conversia informațiilor și proceselor în format digital, digitalizarea presupune o restructurare profundă a fluxurilor operaționale și adoptarea unor tehnologii avansate pentru optimizarea proceselor instituționale. În acest sens, digitalizarea administrației publice și a orașelor inteligente nu se limitează la conversia digitală a sistemelor tradiționale, ci vizează o reconfigurare etapizată a serviciilor publice, accentuând transparența, eficiența și inovarea [1]. În ceea ce privește administrația vamală, Codul vamal al Uniunii Europene (UE) definește atribuțiile esențiale ale autorităților vamale, subliniind importanța acestora în supravegherea fluxurilor comerciale internaționale și în menținerea unui climat economic echitabil.

Aceste autorități sunt responsabile pentru:

- protejarea intereselor financiare ale Uniunii și ale statelor membre ale acesteia;
- protejarea Uniunii de comerțul inechitabil și ilegal și încurajarea activităților economice legitime;
- garantarea securității și siguranței Uniunii și a rezidenților acesteia, protecția mediului, în cooperare strânsă cu alte autorități, dacă este cazul; și

- menținerea unui echilibru adecvat între controalele vamale și facilitarea comerțului legitim [2].

Criminalitatea informatică constituie un domeniu de analiză multidimensional, având un impact profund asupra integrității infrastructurilor digitale. Aceasta include o varietate de infracțiuni, precum atacurile cibernetice asupra sistemelor informatice critice, fraudele electronice, furtul de identitate și acțiunile de spionaj economic. Caracterul dinamic și transnațional al acestui fenomen impune dezvoltarea unor mecanisme legislative și tehnologice adecvate pentru prevenirea și combaterea sa eficientă [3].

Un punct de referință în eforturile de digitalizare a administrației vamale a fost adoptarea Deciziei nr. 70/2008/CE de către Parlamentul European și Consiliu, care a instituit un cadru informatizat pentru gestionarea procedurilor vamale și comerciale. Această inițiativă are ca obiectiv primordial facilitarea comerțului internațional prin sporirea eficienței și securității operațiunilor vamale. În același timp, decizia subliniază importanța interoperabilității sistemelor informatice la nivel european, promovând schimbul de date electronice și reducerea întârzierilor administrative la punctele de frontieră. De asemenea, această reglementare contribuie la intensificarea eforturilor de combatere a fraudelor și contrabandei, prin optimizarea capacităților de monitorizare și analiză a fluxurilor comerciale [4].

Astfel, prezenta lucrare își propune să analizeze strategiile de prevenire și combatere a criminalității informatice în administrația vamală, având ca obiectiv principal protejarea intereselor economice ale Uniunii Europene și ale României. În acest sens, vor fi investigate principalele amenințări informatice cu impact asupra activității vamale, analizându-se implicațiile acestora asupra economiei și soluțiile operaționale aplicabile pentru prevenirea și combaterea fenomenului. În plus, lucrarea va evidenția modele de bune practici implementate la nivel european și internațional, conturând o perspectivă integrată asupra metodelor eficiente de protecție împotriva atacurilor informatice și a obstacolelor care pot afecta procesul de digitalizare a administrației vamale.

Un aspect esențial al studiului îl constituie analiza cadrului legislativ în materie de securitate cibernetică, a măsurilor de protecție implementate și a inițiativelor de cooperare interinstituțională pentru protejarea infrastructurilor digitale vamale. Totodată, studiul va integra perspectivele funcționarilor publici din cadrul Autorității Vamale Române, prin intermediul unor chestionare care vizează evaluarea interacțiunii acestora cu sistemele informatice utilizate în activitatea profesională.

Prin această abordare comprehensivă, lucrarea își propune să contribuie la înțelegerea complexității provocărilor generate de criminalitatea informatică în domeniul vamal, subliniind necesitatea formulării unor politici publice eficiente și coerente, menite să asigure un mediu economic sigur, stabil și competitiv.

Ipotezele de cercetare

În cadrul acestei cercetări, ipotezele formulate urmăresc să ofere un cadru teoretic solid pentru analiza impactului digitalizării asupra securității informatice în administrația vamală, evidențiind relația dintre modernizarea infrastructurilor digitale și măsurile de prevenire și combatere a criminalității informatice.

Prima ipoteză presupune că procesul de digitalizare a administrației vamale va contribui semnificativ la creșterea eficienței mecanismelor de control și supraveghere, determinând o reducere a expunerii la riscurile asociate criminalității informatice. Se consideră că implementarea unor sisteme informatice avansate, bazate pe tehnologii de automatizare, inteligență artificială și criptografie, va facilita monitorizarea tranzacțiilor, detectarea rapidă a activităților frauduloase și

optimizarea fluxurilor de date între instituțiile responsabile, sporind astfel capacitatea autorităților vamale de a preveni și combate infracțiunile informatice.

A doua ipoteză susține că principalele amenințări informatice la adresa administrației vamale sunt într-un proces continuu de diversificare și intensificare, ceea ce impune adoptarea unor măsuri legislative și tehnologice avansate pentru o gestionare eficientă a acestora. Se estimează că atacurile cibernetice asupra infrastructurilor vamale pot include accesul neautorizat la baze de date sensibile, compromiterea sistemelor informatice utilizate pentru procesarea declarațiilor vamale și manipularea fluxurilor de informații esențiale pentru securitatea economică a statelor. În acest context, se presupune că o abordare integrată, care combină reglementări stricte, protocoale de securitate și tehnologii emergente, este necesară pentru a proteja infrastructurile digitale împotriva riscurilor cibernetice în creștere.

Cea de-a treia ipoteză afirmă că integrarea și adaptarea unor strategii și bune practici internaționale în domeniul securității cibernetice vor avea un rol esențial în consolidarea protecției infrastructurilor informatice vamale. Se consideră că adoptarea unor modele de succes utilizate la nivel global, inclusiv standarde internaționale privind securitatea datelor, soluții de autentificare multifactorială și sisteme de detecție și răspuns la incidente cibernetice, vor contribui la reducerea vulnerabilităților specifice administrației vamale. De asemenea, cooperarea interinstituțională la nivel internațional și schimbul de informații între autoritățile vamale din diferite state vor facilita prevenirea și combaterea amenințărilor cibernetice transfrontaliere, sporind astfel reziliența infrastructurilor digitale și asigurând un nivel ridicat de securitate în cadrul proceselor vamale digitalizate.

Obiective

Analiza impactului digitalizării asupra mecanismelor de prevenire și combatere a criminalității informatice în administrația vamală, având în vedere atât implicațiile economice, cât și cele instituționale. Această analiză se va axa pe:

- Identificarea și caracterizarea principalelor vulnerabilități informatice din infrastructura digitală a administrației vamale.
- Evaluarea eficacității măsurilor actuale de securitate informatică în prevenirea și combaterea criminalității informatice în acest domeniu.
- Analiza cadrului legislativ național și european referitor la protecția infrastructurilor digitale vamale.
- Investigarea percepțiilor funcționarilor vamali în raport cu utilizarea sistemelor informatice specifice activității lor.
- Propunerea unor strategii și măsuri de optimizare a securității informatice în administrația vamală, având în vedere modelele de bune practici implementate la nivel internațional.

Metodologia de cercetare

Prezenta cercetare va avea un caracter exploratoriu și descriptiv, având ca obiectiv analiza fenomenului criminalității informatice în contextul procesului de digitalizare a administrației vamale. Studiul va fi fundamentat pe o abordare metodologică complexă, incluzând analiza documentară, prin care se va examina cadrul legislativ, rapoartele internaționale și studiile de specialitate relevante pentru domeniul securității informatice și al administrației vamale. În vederea colectării datelor empirice, va fi administrat un chestionar structurat funcționarilor vamali, utilizând platforma Google Forms pentru eficientizarea procesului de distribuire și centralizare a răspunsurilor, având ca scop evaluarea nivelului de conștientizare, a percepțiilor și a dificultăților întâmpinate în utilizarea infrastructurilor digitale. Datele obținute vor fi supuse unei analize cantitative, prin aplicarea metodelor statistice, în scopul identificării tendințelor și corelațiilor semnificative, precum și unei analize calitative, prin care vor fi interpretate

informațiile rezultate din chestionare și analiza documentară, cu scopul de a evidenția principalele probleme, soluții și recomandări strategice relevante pentru consolidarea securității informatice în domeniul vamal.

Capitolul 1. Rolul administrației vamale în protejarea intereselor economice în e-Guvernare și securitate informatică

Transformările profunde din cadrul administrației publice românești, de la structurile centralizate și birocratice ale secolului trecut până la tendințele moderne ale guvernării digitale, relevă un parcurs evolutiv marcat de reforme administrative, integrare europeană și adaptare la noile provocări tehnologice. În acest cadru, administrația vamală se evidențiază ca o componentă esențială a aparatului de stat, având un rol strategic în protejarea intereselor economice, asigurarea securității frontierelor și facilitarea comerțului internațional.

Odată cu aderarea României la Uniunea Europeană, administrația vamală a fost supusă unui proces amplu de modernizare și armonizare cu normele europene, accentul fiind pus pe digitalizare, eficientizarea procedurilor și consolidarea capacităților instituționale. Înființarea Autorității Vamale Române (AVR) prin Legea nr. 268/2021 a marcat un moment de referință în reconceptualizarea acestei instituții, reflectând nevoia de profesionalizare, autonomie funcțională și răspuns adaptat la complexitatea comerțului global și la noile forme de criminalitate economică.

Prezentul capitol își propune să analizeze din punct de vedere teoretic rolul și funcționarea administrației vamale ca ramură specializată a administrației publice, cu accent pe procesul de digitalizare și pe mecanismele prin care aceasta contribuie la protejarea intereselor economice ale României și ale Uniunii Europene. În contextul în care amenințările cibernetice, fraudele fiscale și provocările globale devin din ce în ce mai sofisticate, AVR este chemată să își redefinească instrumentele de intervenție, să colaboreze eficient cu alte instituții și să implementeze soluții digitale avansate care să asigure transparență, securitate și eficiență operațională.

Demersul științific va fi structurat astfel încât să reflecte atât fundamentele teoretice ale administrației publice și ale e-guvernării, cât și particularitățile instituționale, juridice și tehnice ale administrației vamale din România.

1.1. Considerații generale privind administrația vamală ca ramură a administrației publice

Administrația publică din România a evoluat semnificativ, de la structurile descentralizate medievale la sistemul modern digitalizat. În perioada fanariotă, birocrația a fost excesivă, iar reformele din secolul XIX, Constituția din 1866, au introdus un model administrativ inspirat de administrația publică franceză [5].

În perioada comunistă administrația publică a fost centralizată și subordonată partidului unic ca mai apoi aderarea la UE (2007) să impună reforme privind transparența și digitalizarea serviciilor publice imprimându-se o tendință către e-Guvernare, modernizând infrastructura digitală și procesele birocratice.

În administrația publică, digitizarea și digitalizarea sunt adesea percepute ca extensii ale e-guvernării. Inițial asociată cu furnizarea de documente și servicii online, e-guvernarea a evoluat profund, incluzând în prezent obiective politice precum reformele instituționale, modernizarea administrației și promovarea unor noi practici democratice [6].

Era digitală în administrația publică românească s-a consolidat începând cu anul 2000, odată cu înființarea Comisiei pentru Administrația Digitală, subordonată Ministerului de Finanțe, având ca obiectiv standardizarea comunicării în sectorul public prin XML[1] și implementarea semnăturii electronice. Prima strategie de e-Guvernare (2002) a urmărit optimizarea serviciilor publice și eficientizarea proceselor administrative. Mai apoi în anul 2003, dezvoltarea infrastructurii digitale a permis schimbul electronic de documente între instituțiile publice. Strategia din 2004 accentuând orientarea administrației către cetățeni și sporirea eficienței. Din 2005, dreptul cetățenilor de a comunica electronic cu autoritățile a fost garantat [7].

Administrația publică din România ca sumă a proceselor prin care guvernul își desfășoară activitatea pentru a implementa politici publice, a oferi servicii cetățenilor și a gestiona resursele publice, include atât instituțiile centrale, cât și cele locale, cu rol de instrumente în îndeplinirea scopurilor și obiectivelor sale, în conformitate cu reglementările naționale și unionale.

Cercetarea mea se va axa pe analiza Autorității Vamale Române, un actor principal al administrației vamale ramură a administrației publice din România. Activitatea Autorității Vamale Române nu trebuie confundată cu cea a Poliției de Frontieră Române, două organisme ale administrației publice centrale distincte.

Prin legea nr. 268/2021, publicată în Monitorul Oficial al României, Partea I, nr. 1077 din 10 noiembrie 2021, ia naștere ca autoritate publică de specialitate, cu personalitate juridică proprie, Autoritatea Vamală Română. Acest act normativ a generat un cadru juridic indispensabil desfășurării activităților vamale armonizate normelor de drept național și unional.

Autoritatea Vamală Română, la care voi face referire folosind acronimul A.V.R, este organizată și funcționează conform H.G. nr. 237/2022, publicată în Monitorul Oficial al României, Partea I, nr. 167 din 18 februarie 2022. Acest act normativ stabilește principiile fundamentale care guvernează activitatea instituției, atribuțiile sale generale și specifice. A.V.R spre deosebire de omologul său american U.S. Customs and Border Protection, se află în directa subordine a Ministerului de Finanțe și nu a Ministerului de Interne. A.V.R este condusă de un președinte cu rang de secretar de stat, numit prin decizia prim-ministrului, care coordonează activitatea celor șapte direcții regionale vamale, împărțite la rândul lor în birouri vamale de interior și birouri vamale de frontieră. În trecut, administrația vamală avea ca principală atribuție perceperea taxelor vamale și a impozitelor indirecte aferente importurilor. Însă, în contextul globalizării, al expansiunii comerțului internațional și al intensificării amenințărilor de securitate, competențele sale au fost semnificativ extinse.

În timp, rolul său de colector de taxe vamale este extins asupra supravegherii și controlului mărfurilor introduse în Uniunea Europeană, asigurând nu doar colectarea taxelor vamale, a TVA-ului și a accizelor, ci și conformitatea produselor cu reglementările europene privind siguranța, sănătatea publică și protecția mediului. De asemenea, are rol în monitorizarea respectării drepturilor de proprietate intelectuală, controlează importurile de precursori de droguri, reglementează comerțul cu bunuri culturale și supraveghează transporturile de deșeuri și specii protejate pentru a preveni activitățile ilegale.

În domeniul combaterii spălării banilor, administrația vamală implementează normele europene privind controlul fluxurilor financiare și colaborează cu autoritățile naționale și internaționale în lupta împotriva fraudei, terorismului și crimei organizate [8].

Implementând mecanisme avansate de control și cooperare interinstituțională, Autoritatea Vamală Română este un actor strategic în protejarea intereselor economice și de securitate ale

[1] Este un limbaj de marcare utilizat pentru stocarea, transportul și structura datelor într-un mod ușor de citit atât pentru oameni, cât și pentru calculatoare. Spre deosebire de HTML, care este destinat prezentării informației, XML definește datele și structura acestora fără a impune un format vizual.

României și Uniunii Europene, asigurând un echilibru între facilitarea comerțului și aplicarea unor măsuri stricte de supraveghere vamală.

1.2. Protejarea intereselor economice prin digitalizarea administrației vamale

Protejarea intereselor economice ale Uniunii Europene și ale României reprezintă un obiectiv fundamental pentru administrația vamală din România. Realizarea acestui obiectiv strategic presupune implementarea unor politici și măsuri care să asigure stabilitatea financiară, competitivitatea pieței și securitatea economică. Administrația vamală intervenind activ pe partea de combatere a fraudei fiscale, asigurarea unui comerț echitabil și prevenirea activităților ilicite care afectează economia.

Pentru realizarea cât mai eficientă a acestui obiectiv este nevoie de o profundă digitalizare a administrației publice, prioritate strategică a Uniunii Europene prin inițiative precum automatizarea completă a guvernării digitale, dezvoltarea platformelor de colaborare între administrațiile publice. Astfel, sprijinind transparența proceselor administrative și îmbunătățind comunicarea dintre administrațiile publice și cetățeni, prin integrarea unor mecanisme digitale avansate, se urmărește reducerea risipei de resurse și creșterea eficienței în furnizarea serviciilor publice. Mai mult, un alt aspect important este promovarea suveranității digitale prin strategii europene precum Digital Single Market, care vizează crearea unui cadru unitar pentru implementarea infrastructurilor digitale și standardizarea proceselor administrative [9].

Creșterea interconectivității și a dependenței de tehnologiile informatice a expus economia globală la riscuri cibernetice semnificative, de la atacuri de tip ransomware la furtul de date financiare și spionaj economic. Aceste amenințări pun în pericol stabilitatea piețelor financiare, încrederea publicului și buna funcționare a administrației publice. Printre cele mai mari provocări în materie de securitate economică se numără criminalitatea informatică, care vizează atât infrastructurile critice, cât și companiile din sectoare esențiale. Atacurile ransomware, de exemplu, blochează accesul la datele unei organizații și solicită plata unei răscumpărări pentru recuperarea acestora. În multe cazuri, victimele nu doar că pierd accesul la date, dar sunt și supuse unor presiuni suplimentare prin amenințarea de a face publice informații sensibile. Mai mult, furtul de date financiare, precum detalii despre conturi bancare sau informații comerciale confidențiale, permite atacatorilor să exploateze aceste resurse pentru fraude sau tranzacții ilegale pe piețele negre. Pentru a preveni astfel de riscuri, instituțiile publice și companiile trebuie să adopte măsuri stricte de securitate informatică. Utilizarea autentificării în doi factori (2FA), criptarea datelor și monitorizarea continuă a sistemelor sunt doar câteva dintre metodele esențiale de protecție. De asemenea, instruirea constantă a personalului și dezvoltarea unor politici de securitate bine definite contribuie la reducerea vulnerabilităților [10].

Aplicat direct asupra administrației vamale protejarea intereselor economice ale Uniunii Europene se realizează prin controlul regimurilor vamale, asigurând perceperea corectă a taxelor și prevenirea evaziunii fiscale. Declararea și vămuirea electronică a mărfurilor permit trasabilitatea și reduc riscurile de fraudă, iar analiza riscurilor și controalele vamale contribuie la prevenirea contrabandei. Simplificarea și digitalizarea proceselor vamale, inclusiv vămuirea centralizată și înscrierea în evidențele declarantului, optimizează fluxurile comerciale și reduc costurile administrative. În cazul nerespectării reglementărilor, operatorii economici sunt sancționați cu datorii vamale, amenzi sau retragerea autorizației, asigurând conformitatea și securizarea schimburilor comerciale [11].

1.3. Provocări ale securității informatice

O primă provocare ar fi însăși digitalizarea proceselor vamale. Aceasta expune sistemele informatice la riscuri semnificative, printre care se numără spionajul cibernetic, ce poate facilita contrabanda și frauda fiscală prin acces neautorizat la date comerciale sensibile. Atacurile de tip malware au potențialul de a perturba sistemele electronice de declarare, afectând desfășurarea operațiunilor vamale și generând blocaje în fluxurile comerciale internaționale. De asemenea, tehnicile de inginerie socială și phishing exploatează vulnerabilitățile umane, compromițând accesul securizat la bazele de date vamale și expunând informații sensibile. Hacking-ul sponsorizat de state reprezintă o amenințare strategică suplimentară, demonstrând posibilitatea infiltrării în rețele vamale și manipulării datelor privind importurile și exporturile. Pentru a preveni astfel de riscuri, este esențială implementarea unor soluții avansate de protecție, precum rețelele false de tip „shadow networks", care pot detecta și neutraliza atacurile înainte de compromiterea infrastructurii vamale. În acest context, dezvoltarea unor strategii solide de securitate cibernetică și intensificarea cooperării internaționale sunt necesare pentru menținerea integrității și eficienței administrației vamale în fața amenințărilor digitale emergente [12].

Raportul din 2022 al Curții de Conturi Europene subliniază o intensificare semnificativă a amenințărilor cibernetice, accentuată de contextul pandemic și manifestată printr-o creștere a atacurilor de tip phishing . În acest cadru, instituția a adoptat un plan strategic pentru perioada 2022–2024, care integrează principiul „Zero Trust" și prevede implementarea unui sistem avansat de acces de la distanță, menit să înlocuiască soluția VPN existentă. În plus, se remarcă implicarea activă în elaborarea normelor interinstituționale de securitate cibernetică, parțial aplicate, cu scopul de a consolida reziliența infrastructurii IT [13].

O altă provocare importantă de menționat este migrarea tehnologiilor de securitate cibernetică din mediile interne către soluții cloud sau hibride având în vedere reticența organizațiilor atât publice cât și private. Astfel, adoptarea soluțiilor cloud este limitată de temeri privind vulnerabilitățile de securitate, de dificultățile de conformitate cu reglementările specifice și de pregătirea insuficientă a instituțiilor, în special a celor cu resurse restrânse. Mai mult, încrederea în securitatea mediilor cloud este compromisă de riscurile inerente integrării tehnologiilor noi și de impactul potențial asupra relațiilor comerciale în cadrul tranziției către modele hibride sau de software prin intermediul internetului, eliminând necesitatea instalării și gestionării locale a acestora. Furnizorul de servicii se ocupă de întreținerea, actualizarea și securizarea aplicației, iar utilizatorii accesează software-ul pe baza unui abonament, ceea ce permite flexibilitate, scalabilitate și costuri operaționale reduse [14].

Mai mult, resursa financiară joacă un rol esențial în cadrul securității informatice uneori devenind chiar una din provocări. Administrațiile publice germane, de exemplu, se confruntă cu provocări semnificative în domeniul securității IT, generate de insuficiența fondurilor, deficiențe strategice și un know-how tehnic limitat. Deși există cadre teoretice și sisteme de management al securității, complexitatea acestora conduce la implementări defectuase, sporind vulnerabilitățile infrastructurii IT. Astfel, este imperativă dezvoltarea unei culturi organizaționale centrate pe securitate, care să implice atât liderii, cât și angajații în adoptarea unei abordări proactive în alocarea resurselor și implementarea măsurilor preventive [15].

O altă provocare identificată este manipularea sistemelor biometrice, cum ar fi amprentele digitale sau recunoașterea facială în administrația vamală. Aceasta generează vulnerabilități privind confidențialitatea datelor, expunerea la atacuri cibernetice și posibilitatea manipulării informațiilor digitale. În contextul digitalizării datelor biometrice, sistemele vamale devin susceptibile la acces neautorizat, modificări frauduloase sau inserarea de cod malițios în fluxurile de date, ceea ce poate compromite integritatea proceselor de verificare a identității și securitatea frontierelor. Prin urmare, este imperativ ca aceste sisteme să fie protejate prin măsuri suplimentare

de securitate, în vederea asigurării unui nivel ridicat de reziliență în fața amenințărilor cibernetice [16].
Având în vedere provocările identificate, în cadrul capitolului al doilea voi realiza o analiză detaliată a strategiilor și sistemelor implementate de Autoritatea Vamală Română pentru a răspunde noilor cerințe impuse de digitalizare și de criminalitatea informatică, în vederea protejării intereselor economice ale României și ale Uniunii Europene.

Capitolul 2. Sisteme și strategii implementate în prezent de Autoritatea Vamală Română

2.1. Cadrul normativ european de reglementare al sistemelor

În urma cercetării am identificat un nucleu al reglementărilor unionale cu privire la sistemele informatice vamale și îl voi prezenta pentru a putea urmării pe parcursul capitolului modul în care acestea au fost transpuse în sistemele folosite la nivel național.

Acestea contribuie în mod activ la E-guvernare, folosirea tehnologiei de către administrația publică pentru a îmbunătăți serviciile și a eficientiza procesele. Astfel, se permite o comunicare mai rapidă și accesibilă între autorități, cetățeni, oferind acces simplu la informații și servicii publice [17].

Regulamentul (UE) nr. 952/2013, Codul Vamal al Uniunii Europene, constituie fundamentul legal esențial pentru digitalizarea operațiunilor vamale. Acesta stabilește un cadru general pentru funcționarea administrațiilor vamale, impunând obligația utilizării sistemelor informatice în toate aspectele proceselor vamale. Astfel, regimul electronic de declarare a mărfurilor este consolidat, facilitând procesarea rapidă și eficientă a declarațiilor vamale și a documentelor aferente, ceea ce conduce la o reducere semnificativă a timpului de așteptare și la simplificarea interacțiunilor cu operatorii economici [18].

Pornind de la fundamentul oferit de Codul Vamal al Uniunii Europene, Regulamentul (CE) nr. 515/97, cu modificările și completările ulterioare, implementează Sistemul de Informații Vamale (SIV). Acest sistem facilitează schimbul de informații între autoritățile vamale din statele membre, contribuind semnificativ la îmbunătățirea controlului vamal și la gestionarea riscurilor asociate comerțului internațional. Acesta integrează datele provenite din diverse surse, permițând o analiză cuprinzătoare a riscurilor și o reacție promptă în cazul identificării neregulilor sau a activităților suspecte, ceea ce asigură un răspuns eficient la provocările contemporane [19].

În contextul securității frontierelor, Sistemul de Informații Schengen (SIS), reglementat prin Regulamentul (UE) nr. 2016/399, permite schimbul rapid de informații între autoritățile vamale și agențiile de securitate. SIS facilitează o coordonare eficientă între statele membre în ceea ce privește controlul la frontieră și combaterea criminalității transfrontaliere, având un rol esențial în asigurarea securității frontierelor externe ale Uniunii Europene. Acest sistem joacă un rol crucial în identificarea rapidă a persoanelor și bunurilor care prezintă un risc, consolidând astfel măsurile de securitate [20].

Regulamentul de punere în aplicare (UE) 2023/1070 din 1 iunie 2023 reglementează sistemele esențiale pentru gestionarea operațiunilor vamale. Sistemul de Decizii Vamale (SDV) facilitează luarea deciziilor privind regimul vamal al bunurilor, asigurând conformitatea cu Codul Vamal al Uniunii. Sistemul de Gestionare Uniformă a Utilizatorilor și Semnătură Digitală (GUU&SD) permite autentificarea utilizatorilor și semnarea electronică a documentelor, sporind securitatea proceselor vamale.

Sistemul de Informații Tarifare Obligatorii Europene (ITOE) asigură accesul la informații tarifare actualizate, facilitând declararea corectă a bunurilor. Sistemul de Înregistrare și Identificare a Operatorilor Economici (EORI) permite înregistrarea operatorilor economici, facilitând gestionarea relațiilor comerciale în Uniunea Europeană. Sistemul Operatorilor Economici Autorizați (AEO) recunoaște statusul operatorilor economici de încredere, oferindu-le beneficii în procesele vamale.

Sistemul de Control al Importurilor 2 (ICS2) îmbunătățește controlul asupra importurilor prin gestionarea riscurilor, iar sistemul privind Fișele de Informații pentru Regimuri Speciale (INF SP) gestionează informațiile pentru regimurile vamale speciale, asigurând conformitatea cu reglementările specifice. Sistemul Exportatorilor Înregistrați (REX) facilitează înregistrarea exportatorilor care beneficiază de preferințe tarifare în cadrul acordurilor comerciale, în timp ce sistemul privind Dovada Statutului Unional (PoUS) certifică statutul unional al bunurilor, facilitând circulația acestora în cadrul Uniunii Europene. În cele din urmă, sistemul de Supraveghere (SURV3) monitorizează conformitatea operațiunilor vamale, contribuind la prevenirea fraudelor și asigurarea respectării normelor [21].

Pe lângă elementele de reglementare și uniformizare a sistemelor informatice vamale la nivel european, normele U.E. contribuie la prioritizarea implementării acestora, cum s-a întâmplat în cazul celor 22 de sisteme electronice cu termen finalul anului 2025, conform Deciziei de punere în aplicare (UE) 2019/2151 a Comisiei de stabilire a Programului de lucru referitor la dezvoltarea și instalarea sistemelor electronice prevăzute în Codul Vamal al Uniunii [22].

La momentul realizării cercetării nu am identificat norme U.E. care să prevadă implementarea de sisteme informatice bazate pe inteligență artificială în domeniul vamal. Cu toate acestea poziționarea U.E. este îndreptată către reglementarea inteligenței artificiale (IA) pentru maximizarea beneficiilor și prevenirea impactului negativ asupra drepturilor fundamentale. Lipsa unui cadru juridic clar poate duce la utilizări inadecvate și la riscuri în materie de protecție a datelor. Astfel, elaborarea unor norme care să asigure echilibrul între inovație și protecția drepturilor omului devine o prioritate. Mai mult, UE promovează o abordare coordonată prin strategii și grupuri de experți, punând accent pe siguranță, etică și respectarea valorilor fundamentale [23].

2.2. Sisteme informatice publice implementate de Autoritatea Vamală Română

A.V.R grupează aceste sisteme în vămuirea electronică sau E-Customs [24]. Dintre acestea am ales să prezint în cadrul cercetării sistemele EORI-RO, ICS-RO, ECS-RO, și RO e-Sigiliu, deoarece le consider relevante pentru cercetare.

Primul sistem pe care îl voi prezenta este sistemul EORI-RO. Numărul EORI (Economic Operators Registration and Identification) este un identificator unic atribuit de autoritățile vamale operatorilor economici și altor persoane implicate în operațiuni vamale pe teritoriul Uniunii Europene [25]. Acesta permite identificarea clară a entităților în relația cu autoritățile vamale și facilitează schimbul de informații între instituțiile relevante, contribuind la eficientizarea proceselor vamale.

Obținerea unui număr EORI este obligatorie pentru operatorii economici care desfășoară activități reglementate de legislația vamală, precum importul, exportul, tranzitul sau depozitarea mărfurilor, precum și pentru persoanele fizice sau juridice care introduc sau scot mărfuri din Uniunea Europeană.

În România, atribuirea numerelor EORI este realizată de Autoritatea Vamală Română. Cererea de înregistrare se depune prin intermediul aplicației electronice EORI-RO și trebuie să fie însoțită de documente justificative. După verificare, autoritatea competentă atribuie numărul EORI, care devine obligatoriu în toate comunicările cu autoritățile vamale.

Structura numărului EORI include un cod de țară, urmat de un identificator unic, care poate fi codul unic de identificare (CUI) pentru persoanele juridice sau codul numeric personal pentru persoanele fizice. Acest număr poate fi invalidat la solicitarea titularului sau în cazul încetării activităților care necesită înregistrare [26].

Sistemul de Control al Importului, (ICS-RO) reglementează procesul de introducere a mărfurilor pe teritoriul vamal al Uniunii Europene, asigurând conformitatea acestora cu normele vamale și de securitate. Declarația sumară de intrare trebuie depusă la primul birou vamal înainte de sosirea mărfurilor. Operatorii economici transmit declarațiile sumare prin intermediul sistemului informatic ICS-RO, care verifică datele furnizate. În urma acestei verificări, declarația este fie acceptată și înregistrată prin alocarea unui număr de referință unic (MRN – Master Reference Number), fie respinsă în cazul în care nu respectă cerințele impuse. Numărul MRN, alcătuit din 18 caractere alfanumerice, este atribuit de primul birou vamal de intrare sau, dacă declarația este depusă într-o altă locație, de biroul vamal respectiv. Pe baza informațiilor conținute în declarația sumară de intrare, autoritatea vamală competentă efectuează analiza de risc, având ca obiectiv prevenirea riscurilor asociate fluxului de mărfuri și asigurarea respectării reglementărilor vamale în vigoare [27].

Sistemul de Control al Exportului (ECS-RO) constituie o platformă informatică dezvoltată de Comisia Europeană începând cu anul 2007, având drept scop facilitarea schimbului de informații și mesaje între autoritățile vamale naționale, operatorii economici și Comisia Europeană, cu privire la mărfurile declarate la export.

Implementarea și utilizarea sistemului ECS-RO permite autorităților vamale să monitorizeze procesul de ieșire a mărfurilor de pe teritoriul vamal al Uniunii Europene și reprezintă principalul instrument pentru certificarea exportului în scopuri fiscale, inclusiv în ceea ce privește aplicarea taxei pe valoarea adăugată (TVA) și a altor taxe. Totodată, acest sistem asigură un nivel uniform de protecție în cadrul controalelor vamale aplicate mărfurilor exportate, facilitează distribuirea rezultatelor analizei de risc între autoritățile vamale implicate și gestionează declarațiile sumare de ieșire (EXS) [28].

Prin cel mai nou sistem implementat, Sistemului Național RO e-Sigiliu, A.V.R. realizează monitorizare în timp real a mijloacelor de transport prin sigilii inteligente. Această inițiativă vizează reducerea semnificativă a transportului ilegal de mărfuri și a descărcărilor frauduloase, contribuind la diminuarea fraudei vamale și fiscale prin creșterea transparenței procesului de transport.
Sistemul utilizează sigilii electronice cu tehnologie GPS, permițând urmărirea detaliată a traseului transporturilor și intervenția rapidă a echipelor mobile pentru constatarea și sancționarea fraudelor. De asemenea, sistemul optimizează resursele și reduce costurile asociate supravegherii și controlului vamal, asigurând controale mai precise bazate pe date în timp real [29].

Aceste sisteme informatice contribuie semnificativ la combaterea criminalității informatice în domeniul vamal prin mecanisme avansate de verificare, monitorizare și analiză a riscurilor. Prin intermediul sistemului EORI-RO, se asigură identificarea unică a operatorilor economici, prevenind utilizarea identităților false și reducând riscul fraudelor asociate manipulării datelor de înregistrare. Totodată, integrarea acestui sistem cu alte baze de date instituționale facilitează depistarea inconsecvențelor și a tentativelor de înregistrare frauduloasă.

Sistemul ICS-RO joacă un rol esențial în analiza automată a riscurilor prin impunerea depunerii electronice a declarațiilor sumare de intrare înainte de sosirea mărfurilor. Acesta permite

verificarea automată a informațiilor furnizate de operatorii economici și identificarea anomaliilor, reducând posibilitatea manipulării frauduloase a datelor vamale. Utilizarea algoritmilor avansați pentru analiza riscurilor contribuie la creșterea eficienței în detectarea tentativelor de fraudă și la consolidarea securității schimburilor comerciale.

În ceea ce privește exporturile, ECS-RO facilitează schimbul de date între autoritățile vamale naționale și europene, prevenind raportările fictive destinate evitării obligațiilor fiscale. Prin gestionarea electronică a declarațiilor de export și analiza comparativă a fluxurilor de mărfuri, acest sistem ajută la detectarea schemelor frauduloase și a incongruențelor în declarațiile vamale. Digitalizarea procesului de certificare fiscală permite un nivel ridicat de transparență și elimină vulnerabilitățile asociate documentelor fizice.

Sistemul RO e-Sigiliu aduce un plus de securitate prin monitorizarea în timp real a transporturilor, utilizând sigilii electronice inteligente echipate cu tehnologie GPS. Acest mecanism previne alterarea sau substituirea mărfurilor pe parcursul tranzitului, iar generarea alertelor automate în cazul unor deviații neautorizate contribuie la diminuarea fraudelor informatice legate de transportul ilegal de bunuri. Prin aceste măsuri, resursele vamale sunt optimizate, iar capacitatea de intervenție a autorităților este semnificativ îmbunătățită.

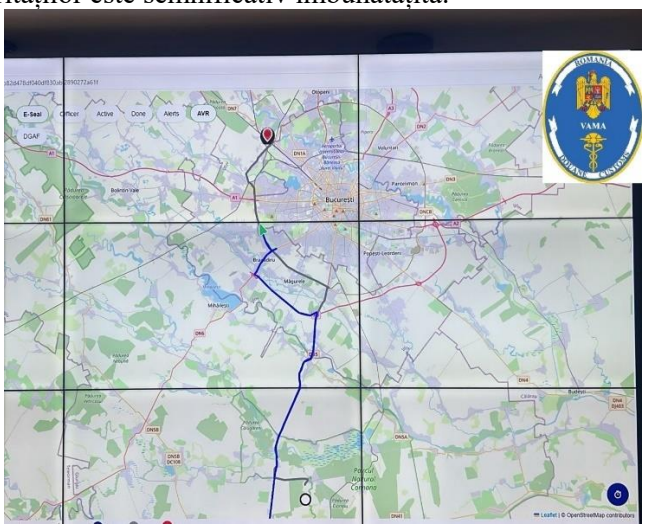

Figura 1. Monitorizare GPS a sistemului RO e-Sigiliu
Sursa: Facebook Autoritatea Vamală Română https://shorturl.at/PqpyI

Integrarea acestor sisteme informatice avansate permite detectarea și prevenirea eficientă a criminalității informatice în domeniul vamal, reducând fraudele documentare, manipularea ilicită a datelor și utilizarea mijloacelor digitale pentru eludarea obligațiilor vamale și fiscale. Aceste instrumente tehnologice contribuie la creșterea transparenței proceselor vamale și la consolidarea securității economice printr-un control strict și automatizat al fluxurilor comerciale.

Pe lângă eficacitatea în combaterea amenințărilor informatice la adresa infrastructurii vamale, aceste sisteme reușesc să distrugă un mit sau o preconcepție în ceea ce privește E-Guvernarea, mitul disponibilizării personalului [30] o dată cu introducerea acestor sisteme. Pe lângă eficientizare, acestea generează nevoia de personal ancorat în realitățile moderne și o pregătire avansată în infrastructurile digitale, elemente ce beneficiază cetățeanului.

2.3. Potențiale amenințări asupra sistemelor informatice din administrația vamală din România

Conform unui raport al Comisiei Europene, interoperabilitatea între sistemele de informații, precum Sistemul de Informații Schengen (SIS) și Sistemul Vamal de Control al Importurilor

(ICS2), poate îmbunătăți gestionarea riscurilor la adresa securității. Totuși, această interoperabilitate poate introduce și vulnerabilități exploatabile de către actori ostili [31].

În plus, Serviciul Român de Informații (SRI) subliniază că principalele amenințări cibernetice la adresa securității naționale provin de la actori statali rău intenționați, grupări de criminalitate cibernetică, grupări extremiste (hacktiviste) și grupări teroriste. Aceste categorii de agresori pot viza infrastructura informatică a organizațiilor internaționale, inclusiv a celor din domeniul vamal [32].

De asemenea, Parlamentul European evidențiază că trăim într-o economie bazată pe date, ceea ce le face o țintă majoră pentru infractorii cibernetici. Amenințările la adresa datelor pot fi clasificate în principal ca accesări neautorizate și scurgeri de date, ambele reprezentând riscuri semnificative pentru organizațiile care gestionează informații sensibile [33].

Autoritatea Vamală Română se confruntă cu mai multe amenințări la securitatea informatică, identificate în Planul Strategic Instituțional 2025-2028. Printre acestea se numără atacurile cibernetice și fraudele informatice, care pot afecta atât datele, cât și continuitatea operațiunilor. Sistemele vamale sunt expuse atacurilor de tip phishing – unde infractorii informatici se prezintă drept organizații de încredere și folosind mail-uri automate au scopul de a fura date sensibile [34] - , DdoS - atacurile DDoS (Distributed Denial of Service) inundă platformele web cu un număr mare de cereri, cauzând funcționarea intermitentă sau oprirea completă a acestora [35] - , ransomware - Ransomware-ul este un software periculos care criptează fișierele și sistemele unei organizații, făcându-le inaccesibile, țintește servere și baze de date, iar victimele sunt obligate să plătească o răscumpărare, de obicei în criptomonede, pentru a-și recupera fișierele. Denumirea provine din cuvântul englezesc "ransom" (răscumpărare) combinat cu sufixul "-ware" pentru software, ceea ce poate duce la pierderea sau compromiterea informațiilor sensibile - [36].

O altă vulnerabilitate majoră este infrastructura IT învechită, care crește riscul de exploatare a breșelor de securitate. Lipsa interoperabilității între sistemele vamale și alte entități guvernamentale poate duce la pierderi de date sau la acces neautorizat. Modernizarea sistemului informatic este esențială pentru a asigura siguranța și eficiența proceselor de vămuire.

În plus, schimbul de date transfrontalier cu state precum Ucraina, Republica Moldova și Serbia expune AVR la riscul de interceptare și compromitere a informațiilor. Consolidarea mecanismelor de protecție a schimbului de date prin criptare avansată și autentificare multifactor este necesară pentru protejarea integrității și confidențialității informațiilor vamale.

O altă problemă este utilizarea insuficientă a analizei de risc și a inteligenței artificiale în detectarea și prevenirea fraudelor vamale. Lipsa unor algoritmi avansați pentru analiza volumelor mari de date limitează capacitatea de identificare a comportamentelor suspecte în tranzacțiile vamale. Dezvoltarea unor sisteme bazate pe inteligență artificială ar putea îmbunătăți capacitatea AVR de a combate frauda și evaziunea vamală. De asemenea, lipsa unei pregătiri adecvate în domeniul securității cibernetice a personalului reprezintă un risc major.

Un alt aspect problematic este dependența de echipamente tehnologice învechite, inclusiv scannerele de control și laboratoarele vamale, care sunt susceptibile la atacuri informatice și pot afecta precizia detectării contrabandei. În concluzie, pentru îmbunătățirea securității informatice a Autorității Vamale Române, se recomandă modernizarea infrastructurii IT, dezvoltarea unui sistem avansat de analiză de risc, îmbunătățirea protecției schimbului de date internațional, instruirea constantă a personalului și achiziția de echipamente moderne. Implementarea acestor măsuri ar putea reduce semnificativ riscurile cibernetice și asigura protecția fluxului de date vamale, contribuind astfel la securizarea frontierelor și a economiei naționale [37].

2.4. Strategii în implementare în cadrul Autorității Vamale Române, Hub-ul Vamal European de Date și A.I.

În ceea ce privește strategiile în implementare trebuie avut în vedere că administrația vamală din România trebuie analizată din perspectiva interconctării si interdependenței acestea cu structurile Uniunii Europene.

În acest context, se remarcă tot mai clar o tendință de instituționalizare a unei Agenții Vamale a Uniunii Europene, idee care capătă consistență în cadrul dezbaterilor comunitare recente. Propunerea privind înființarea unei astfel de entități a fost formulată pentru prima dată la 31 martie 2022, de către Grupul de Experți privind Provocările Uniunii Vamale, organism constituit la nivelul Uniunii Europene [38]. Ulterior, în cadrul celei de-a 62-a reuniuni a Trade Contact Group, organizată sub egida Comisiei Europene la data de 28 februarie 2023, această inițiativă a fost reluată, fiind discutate totodată propuneri referitoare la instituirea unui Hub Vamal European de Date și la simplificarea procedurilor vamale [39].

Potrivit poziției exprimate de Comisia Europeană, una dintre atribuțiile fundamentale ale viitoarei agenții ar urma să vizeze coordonarea analizei de risc la nivelul Uniunii și sprijinirea mecanismelor de răspuns în situații de criză, fără a implica atribuții operative directe sau interacțiuni nemijlocite cu mediul de afaceri. În paralel, a fost avansată ideea consolidării colaborării între autoritățile vamale naționale, prin dezvoltarea unui cadru normativ și operațional menit să faciliteze supravegherea unitară a pieței și aplicarea coerentă a legislației vamale în ansamblul spațiului comunitar. În ceea ce privește propunerea de instituire a unui Hub Vamal European de Date, acesta ar avea ca obiectiv centralizarea, într-o platformă digitală integrată, a datelor comerciale transmise de operatorii economici din toate statele membre, oferind astfel autorităților vamale un instrument unificat pentru gestionarea riscurilor, efectuarea formalităților vamale și combaterea fraudelor [40].

Prin valorificarea tehnologiilor de analiză avansată a datelor, se urmărește identificarea timpurie a vulnerabilităților sistemice, monitorizarea evoluțiilor tranzacționale și optimizarea activităților de control. Pe termen mediu și lung, această infrastructură digitală ar putea deveni interfața unică pentru gestionarea tranzacțiilor comerciale în interiorul Uniunii Europene, contribuind astfel la consolidarea protejării intereselor economice și la creșterea eficienței în materie vamală.

O altă strategie în implementare este cea a inteligenței artificiale ca element tehnic de eficientizare a administrației vamale la nivel european. Un pas semnificativ în procesul de transformare digitală a administrației vamale este realizat de către Germania prin înființarea Biroului pentru Inteligență Artificială (AI Office). Această structură nou creată are rolul de a gestiona, coordona și consilia în toate aspectele referitoare la utilizarea tehnologiilor bazate pe inteligență artificială în cadrul administrației vamale. Utilizarea acesteia implică, însă, respectarea unor standarde juridice și etice stricte. În acest context, Biroul pentru Inteligență Artificială (AI Office) funcționează ca structură centrală de coordonare și expertiză, având rolul de a asigura dezvoltarea și implementarea responsabilă a aplicațiilor de inteligență artificială. Biroul garantează respectarea cadrului normativ aplicabil, inclusiv Regulamentul privind Inteligența Artificială (AI Act) al Uniunii Europene, adoptat în august 2024 și intrat în vigoare în februarie 2025. Acest act legislativ interzice utilizările cu grad ridicat de risc, precum sistemele de scoring social sau identificarea biometrică în timp real în spațiile publice, cu excepții clar reglementate. Inițial, personalul AI Office a fost selectat din cadrul administrației vamale germane, însă viitoarele recrutări vor include și candidați externi. Activitățile curente vizează formarea profesională în domeniul AI, cu accent pe securitatea informațională, protecția datelor și responsabilitatea utilizării tehnologiilor emergente. În perspectivă, se urmărește dezvoltarea unui portofoliu instituțional de proiecte AI, care să integreze toate inițiativele tehnologice relevante desfășurate în cadrul administrației vamale [41].

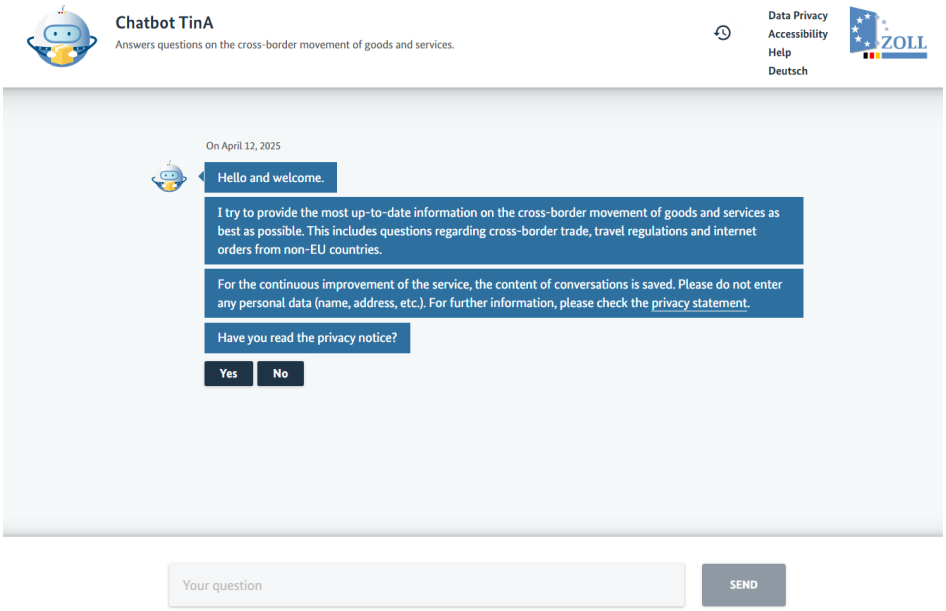

Figura 2. Asistent AI pentru asistență în chestiuni vamale în Germania
Sursa: https://tina-zoll.bundesbots.de/?lang=en

Integrarea AI în administrația publică presupune automatizarea unor procese repetitive, optimizarea fluxurilor de lucru și dezvoltarea unor soluții inteligente de interacțiune, precum asistenții virtuali, sistemele de recunoaștere facială sau traducerea automată. Aceste tehnologii pot contribui semnificativ la consolidarea capacității instituționale și la sprijinirea procesului decizional bazat pe date, dar vine la pachet cu riscuri semnificative, între care se remarcă adâncirea inegalităților digitale, în special între instituțiile cu resurse tehnologice limitate și cele mai bine echipate. Automatizarea excesivă a proceselor decizionale fără intervenție umană poate conduce la pierderea responsabilității instituționale și la afectarea drepturilor fundamentale ale cetățenilor [42].

Pentru a contracara aceste riscuri, este esențială dezvoltarea competențelor digitale în rândul funcționarilor publici. Formarea profesională continuă în domeniul AI, însoțită de o cultură organizațională deschisă spre inovație, contribuie la asigurarea unei utilizări etice și eficiente a tehnologiilor emergente în sectorul public. Astfel, inteligența artificială poate deveni nu doar un mijloc de modernizare administrativă, ci și un factor de consolidare a încrederii cetățenilor în instituțiile statului [42].

Strategia Uniunii Europene privind implementarea inteligenței artificiale în administrația vamală se înscrie în direcția consolidării unei administrații digitale proactive, eficiente și centrate pe cetățean, prin valorificarea tehnologiilor emergente.

În cadrul unui proiect-pilot desfășurat sub egida Direcției Generale pentru Sprijin în Reforme Structurale (DG REFORM), în colaborare cu autoritățile vamale estoniene, a fost elaborată o strategie care vizează integrarea treptată a AI în procesele vamale. Aceasta include elaborarea unui cadru strategic, identificarea unor cazuri de utilizare relevante, precum analiza automată a imaginilor cu raze X și detecția rețelelor de fraudă, precum și formularea unui plan de acțiune operațional. Uniunea europeană doreste dezvoltarea unei arhitecturi digitale moderne capabile să gestioneze volume mari de date nestructurate și instituirea unui cadru instituțional dedicat A.I. pentru aceasta este necesar, însă, unui mecanism flexibil de implementare, monitorizare și evaluare a modelelor AI, într-un mediu controlat și sigur. Pe termen lung, obiectivul strategic este integrarea extensivă a AI în toate dimensiunile administrației vamale, de la analiza de risc și alocarea resurselor, până la sporirea capacității de combatere a fraudei și facilitarea cooperării transfrontaliere între autoritățile vamale din statele membre ale Uniunii Europene [43].

Implementarea inteligenței artificiale (AI) în cadrul administrației vamale din România reprezintă un instrument esențial pentru optimizarea controlului asupra fluxurilor comerciale și modernizarea activităților instituționale. Algoritmilor de învățare automată ar putea fi concentrați pe identificarea eficientă a riscurilor și alocarea prioritară a resurselor către transporturile cu potențial de fraudă, reducând totodată timpii de procesare pentru transporturile cu risc scăzut, precum cele efectuate de operatorii economici autorizați (AEO). Beneficiile integrării AI în sistemul vamal includ: automatizarea proceselor și detectarea tiparelor de fraudă, consolidarea securității la frontieră prin tehnologii de recunoaștere vizuală, creșterea acurateței în colectarea taxelor vamale și facilitarea interacțiunii cu operatorii economici prin asistență digitalizată continuă. Aceste direcții susțin tranziția către o administrație vamală eficientă, predictibilă și centrată pe utilizarea tehnologiilor avansate.

2.5. Importanța securității informatice în protejarea intereselor economice naționale și unionale

Securitatea informatică reprezintă un factor strategic în protejarea stabilității economice atât la nivel național, cât și unional. Conform raportului ENISA privind starea securității cibernetice în Uniune, nivelul actual al amenințărilor este considerat „substanțial", cu un impact direct asupra funcționării entităților esențiale, inclusiv a infrastructurilor publice și economice. Atacurile cibernetice pot perturba lanțurile comerciale și pot genera pierderi semnificative la nivel bugetar, subliniind importanța implementării eficiente a cadrului normativ european în domeniu, precum Directiva NIS2, Cyber Resilience Act și Cyber Solidarity Act. Totodată, raportul evidențiază necesitatea consolidării capacității de reacție prin politici coordonate, exerciții naționale și implicarea întregului ecosistem instituțional. Nivelul scăzut de maturitate cibernetică în unele sectoare critice și lipsa mecanismelor unitare de gestionare a riscurilor afectează capacitatea statelor membre de a proteja interesele economice. În acest context, securitatea cibernetică nu mai este doar o chestiune tehnologică, ci devine o componentă fundamentală a rezilienței economice și a funcționării coerente a pieței interne europene [44].

Sistemele informatice utilizate de Autoritatea Vamală Română gestionează zilnic fluxuri considerabile de date sensibile privind operațiunile de import, export și tranzit, cu un impact direct asupra veniturilor colectate din taxe vamale, accize și TVA, având în vedere că autoritățile vamale sunt responsabile pentru o parte importantă din veniturile bugetare ale Uniunii și contribuie la protejarea economiei împotriva fraudei și evaziunii fiscale în conformitate așa cum prevede Codul Vamal Unional, orice compromitere a acestor sisteme – fie prin acces neautorizat, alterarea datelor sau blocarea infrastructurii – poate produce nu doar pierderi financiare la bugetul național, ci și la disfuncționalități majore în lanțurile comerciale și logistice [44].

Pentru exercițiul bugetar aferent anului 2025, Comisia Europeană a înaintat propunerea unui buget anual în valoare de 199,7 miliarde de euro, căruia i se adaugă aproximativ 72 miliarde de euro din alocările instrumentului NextGenerationEU. Acesta este distribuit după cum urmează: 53,8 miliarde de euro pentru Politica Agricolă Comună, 49,2 miliarde pentru politica de coeziune economică, socială și teritorială, 16,3 miliarde pentru acțiuni externe, 13,5 miliarde pentru cercetare și inovare – în special prin intermediul programului Horizon Europe – și fonduri semnificative pentru infrastructură, mediu, securitate, migrație, sănătate, apărare și educație. Un sprijin deosebit este acordat Ucrainei, sub forma a 4,3 miliarde de euro în granturi și 10,9 miliarde de euro sub formă de împrumuturi [45].

Este important de înțeles modul în care aceast buget este realizat și modul de distribuire, pentru a avea reprezentarea efectelor negative generate de o colectare defectuasă a taxelor vamale, sau mai periculos, cum manipularea malițioasă a sistemelor informatice vamale de către actori ostili,

prin generarea de breșe de securitate ar zadărnici finanțarea proiectelor de interes aflate sub umbrela UE.

Mai mult, dincolo de funcția lor fiscală, taxele vamale constituie un instrument de politică comercială și economică, contribuind la protejarea pieței interne, la reglementarea schimburilor comerciale internaționale și la atingerea obiectivelor strategice ale Uniunii, în special în domeniul durabilității și al competitivității economice.

În acest sens, aplicarea unui cadru integrat de securitate informatică, fundamentat pe principiile evaluării continue a riscurilor și pe adaptarea măsurilor tehnico-organizatorice la specificul operațional al AVR, devine o condiție indispensabilă pentru asigurarea rezilienței digitale instituționale. Potrivit ghidului DNSC destinat IMM-urilor, practici precum definirea clară a politicilor interne de securitate, desfășurarea de audituri periodice, instruirea personalului în domeniul cibernetic și un control strict al accesului la date sunt măsuri aplicabile nu doar mediului privat, ci și entităților publice cu rol strategic precum AVR [46].

Prin urmare, integrarea acestor principii în strategia instituțională a Autorității Vamale Române contribuie la consolidarea capacității României de a proteja interesele financiare ale Uniunii, în deplină conformitate cu exigențele europene în materie de securitate cibernetică. Aceasta presupune o schimbare de paradigmă, de la un model reactiv la unul proactiv, orientat spre anticiparea amenințărilor, diminuarea riscurilor și întărirea controlului asupra infrastructurilor critice informatice din domeniul vamal [47].

Capitolul 3. Analiză comparativă și modele de bune practici asupra strategiilor de combatere a criminalității informatice în administrația vamală

Acest capitol își propune să realizeze o analiză comparativă între strategiile de securitate informatică aplicate în cadrul administrației vamale române și modelele de bune practici existente la nivelul altor administrații vamale din Uniunea Europeană și din spațiul extra-unional. Plecând de la premisa că securitatea cibernetică reprezintă o dimensiune strategică a protejării intereselor economice naționale și unionale, analiza vizează identificarea acelor mecanisme și abordări care s-au dovedit eficiente în prevenirea și combaterea criminalității informatice ce vizează infrastructurile digitale vamale.

În primă fază, vor fi prezentate rezultatele unui chestionar aplicat funcționarilor din cadrul Autorității Vamale Române, cu scopul de a evalua percepțiile acestora asupra interacțiunii cu sistemele informatice, analizate în capitolul precedent și a gradului de conștientizare privind riscurile cibernetice. Ulterior, vor fi analizate modele funcționale de securitate informatică implementate în alte administrații vamale, urmărind în special aplicabilitatea acestora în contextul românesc.

3.1. Prezentarea chestionarului aplicat și a eșantionului relevant raportat la studiul de caz

În cadrul cercetării, am elaborat și aplicat, un chestionar structurat, destinat evaluării interacțiunii funcționarilor vamali din cadrul Autorității Vamale Române (AVR) cu sistemele informatice operaționale, precum și a percepției acestora asupra nivelului de securitate informatică instituțională. Chestionarul a fost aplicat unui eșantion de 36 de inspectori vamali atât dintre cei care ocupă funcții de conducere cât și de execuție, din cadrul direcțiilor de specialitate ale structurii centrale ale autorității. Instrumentul a fost construit în conformitate cu obiectivele generale ale cercetării, vizând nu doar identificarea unor eventuale vulnerabilități tehnice sau

organizaționale, ci și înțelegerea nivelului de pregătire digitală al personalului, alături de deschiderea acestuia față de integrarea de tehnologii emergente în activitatea vamală.

Chestionarul a fost structurat pe patru mari categorii de întrebări, pentru a permite o analiză tematică riguroasă:

- Întrebări demografice și instituționale: această secțiune urmărește profilarea generală a respondenților, prin variabile precum: vârsta, genul, funcția ocupată și vechimea în cadrul instituției. Aceste date permit corelarea ulterioară a răspunsurilor cu caracteristicile socio-profesionale ale eșantionului.
- Întrebări privind utilizarea sistemelor informatice: întrebările din această secțiune investighează frecvența, tipologia și complexitatea interacțiunii cu principalele sisteme digitale utilizate în cadrul AVR (EORI-RO, ICS-RO, ECS-RO, RO e-Sigiliu etc.). De asemenea, se evaluează gradul de familiaritate al funcționarilor cu funcționalitățile acestora și eventualele dificultăți tehnice întâlnite.
- Întrebări referitoare la securitatea informatică: această categorie urmărește percepțiile privind nivelul actual de protecție informatică din instituție, experiențele personale legate de incidente informatice, măsura în care sunt respectate politicile interne de securitate și gradul de încredere în sistemele informatice. Totodată, sunt evaluate nevoile percepute privind formarea profesională în domeniul securității informatice.
- Întrebări privind inovația digitală și perspectivele de dezvoltare: această secțiune include itemi privind deschiderea față de implementarea de soluții bazate pe inteligență artificială, automatizare sau analiză avansată a datelor. Se investighează nivelul de acceptare instituțională față de noile tehnologii și gradul de încredere al respondenților în capacitatea acestora de a contribui la eficientizarea și securizarea activităților vamale.

Chestionarul a fost aplicat online, prin intermediul platformei Google Forms, iar răspunsurile au fost colectate anonim, cu respectarea confidențialității datelor.

Datele astfel obținute vor fi supuse unei analize atât din punct de vedere cantitativ prin interpretări descriptive cât și din punct de vedere calitativ prin identificarea temelor emergente și a percepțiilor dominante, în subcapitolul următor (3.2). Această etapă va permite evaluarea capacității reale a administrației vamale de a răspunde provocărilor criminalității informatice, precum și identificarea unor direcții concrete de intervenție strategică în vederea consolidării securității informatice instituționale.

3.2. Analiză asupra interacțiunii inspectorilor vamali cu sistemele informatice prin procesarea datelor colectate în cadrul chestionarului

În ceea ce privește profilul respondenților, aceștia aparțin în majoritate categoriilor de vârstă 41 - 50 de ani și peste 50 ani, ceea ce indică o populație activă profesional, cu experiență consolidată în administrația vamală.

Putem observa de asemenea că procentul celor din categoria între 30 - 40 și sub 30 de ani însumat reprezintă 31,4% din respondenți ceea ce poate indica o tendință considerabilă de absorbție a funcționarilor publici în faza incipientă a carierei în administrația vamală.

Analizând categoriile de vârstă ale respondenților putem observa că din punct de vedere al resursei umane există un echilibru între cei în formare și cei cu vastă experiență.

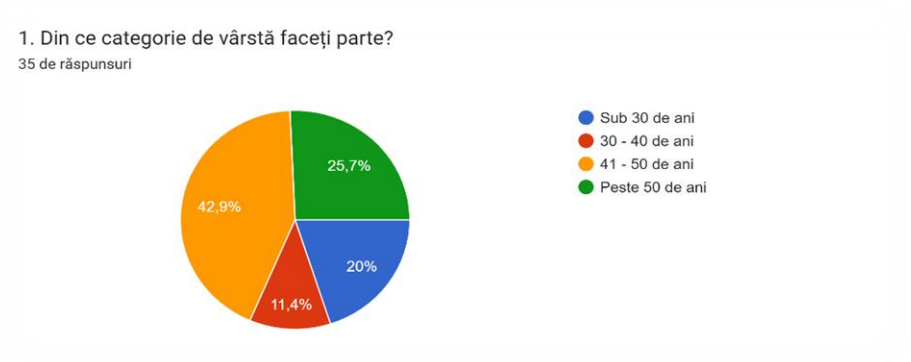

Figura 3. Întrebarea numărul 1 din cadrul chestionarului
Sursa: Chestionar privind interacțiunea inspectorilor vamali cu sistemele informatice publice din cadrul Autorității Vamale Române https://forms.gle/FmfR3k2r1nXeqkxF9

Cu privire la genul respondenților am observat că majoritatea acestora este alcatuită din funcționari publici de gen feminin.

Respondenții chestionați ocupă atât funcții de conducere cât și funcții de execuție opiniile exprimate nefiind unidirecționale acestea expun atât punctul de vedere al celor direct implicați în activitatea vamală cât și opiniile celor în poziții de management.

În privința vechimii în cadrul instituție, cei mai mulți respondenți declară o activitate de peste 10 ani, aspect care conferă robustețe opiniilor exprimate, întrucât sunt formulate de persoane cu o expunere îndelungată la dinamica tehnologică din mediul vamal.

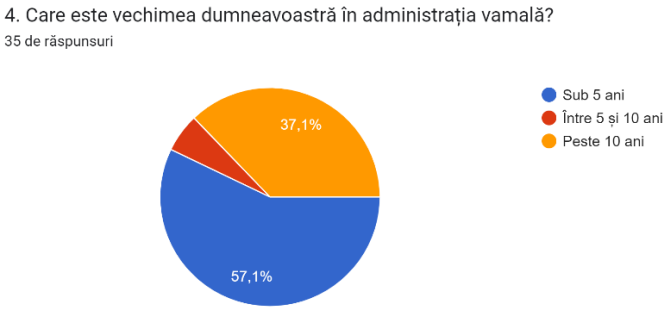

Figura 4. Întrebarea numărul 4 din cadrul chestionarului
Sursa: Chestionar privind interacțiunea inspectorilor vamali cu sistemele informatice publice din cadrul Autorității Vamale Române https://forms.gle/FmfR3k2r1nXeqkxF9

Un rezultat notabil îl constituie frecvența ridicată a utilizării sistemelor informatice, cei mai mulți respondenți declarând că le utilizează zilnic, ceea ce atestă o digitalizare avansată a proceselor vamale.

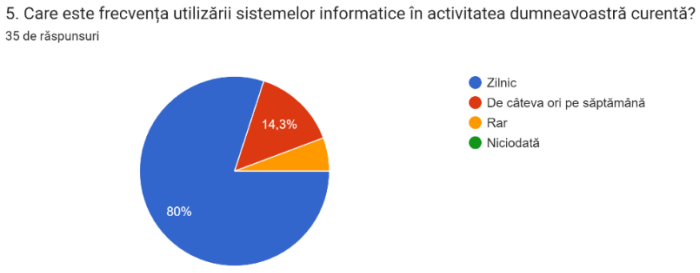

Figura 5. Întrebarea numărul 5 din cadrul chestionarului
Sursa: Chestionar privind interacțiunea inspectorilor vamali cu sistemele informatice publice din cadrul Autorității Vamale Române https://forms.gle/FmfR3k2r1nXeqkxF9

Cu toate acestea, gradul de accesibilitate și ușurință în utilizare este apreciat doar ca fiind „acceptabil” de către majoritatea respondenților, ceea ce semnalează existența unor posibile neconcordanțe între funcționalitățile sistemelor și nevoile operaționale ale utilizatorilor finali.

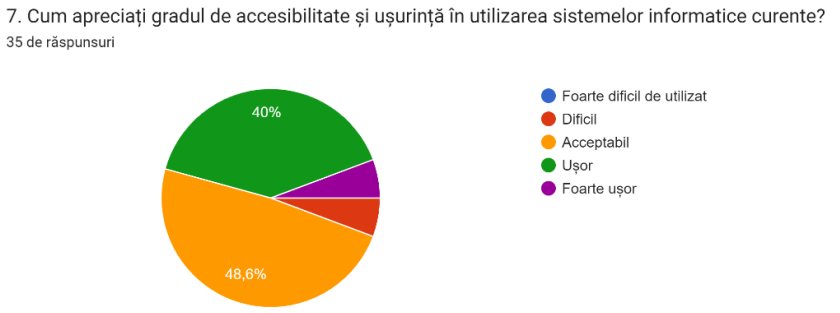

Figura 6. Întrebarea numărul 7 din cadrul chestionarului
Sursa: Chestionar privind interacțiunea inspectorilor vamali cu sistemele informatice publice din cadrul Autorității Vamale Române *https://forms.gle/FmfR3k2r1nXeqkxF9*

Principala dificultate percepută de funcționarii vamali în utilizarea sistemelor informatice este timpul îndelungat de răspuns și procesare al sistemelor informatice (15 mențiuni), urmată de probleme tehnice recurente, precum erori sau întreruperi de sistem (14 mențiuni). Aceste aspecte sugerează deficiențe în performanța tehnică și în stabilitatea infrastructurii digitale utilizate.

De asemenea, infrastructura IT învechită (11 mențiuni) și lipsa instruirii adecvate (10 mențiuni) reprezintă factori semnificativi care afectează eficiența operațională și utilizarea optimă a resurselor informatice. Interfețele dificile (8 mențiuni) accentuează problemele de accesibilitate, influențând negativ fluiditatea activităților curente.

Aceste constatări evidențiază faptul că provocările tehnice sunt strâns corelate cu aspectele organizaționale, precum formarea profesională și designul centrat pe utilizator. Aceste situații ar trebui abordate coroborat prin modernizare tehnologică, optimizare funcțională și investiții în instruirea personalului. Elemente esențiale pentru consolidarea rezilienței cibernetice a administrației vamale.

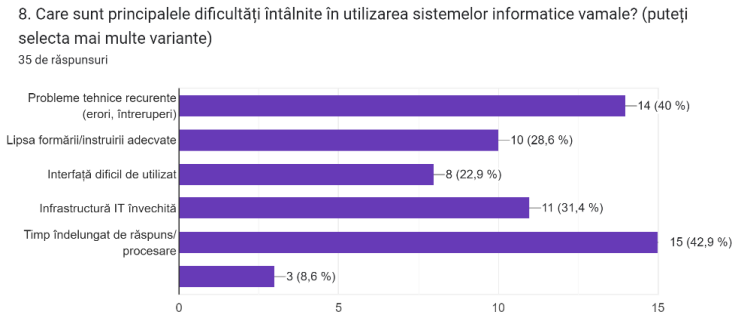

Figura 7. Întrebarea numărul 8 din cadrul chestionarului
Sursa: Chestionar privind interacțiunea inspectorilor vamali cu sistemele informatice publice din cadrul Autorității Vamale Române *https://forms.gle/FmfR3k2r1nXeqkxF9*

În ceea ce privește percepția asupra impactului sistemelor informatice asupra eficienței activității vamale, rezultatele chestionarului indică o opinie predominant favorabilă. Majoritatea covârșitoare a respondenților (29 din 35) consideră că utilizarea acestor sisteme contribuie „în mare măsură” la creșterea eficienței operaționale, în timp ce 5 respondenți au optat pentru răspunsul „într-o oarecare măsură”, iar un singur participant a apreciat că sistemele informatice nu aduc niciun beneficiu în acest sens.

Această distribuție a răspunsurilor evidențiază un nivel ridicat de acceptare și valorizare a digitalizării în activitatea vamală. Chiar dacă au fost identificate în alte secțiuni dificultăți tehnice și nevoi de îmbunătățire, percepția generală este că informatizarea proceselor a dus la o optimizare a fluxurilor de lucru, la reducerea birocrației și la sporirea capacității de control asupra operațiunilor de import, export și tranzit.

Rezultatul susține ipoteza conform căreia funcționarii vamali recunosc beneficiile sistemelor informatice și sunt receptivi la extinderea utilizării acestora, cu condiția unei modernizări continue și a unei mai bune adaptări la nevoile operaționale curente.

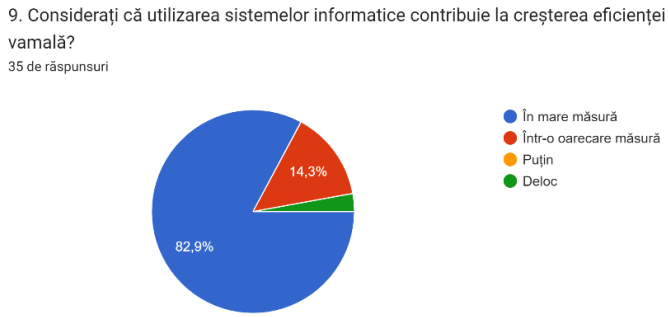

Figura 8. Întrebarea numărul 9 din cadrul chestionarului
Sursa: Chestionar privind interacțiunea inspectorilor vamali cu sistemele informatice publice din cadrul Autorității Vamale Române https://forms.gle/FmfR3k2r1nXeqkxF9

Întrebarea 10 a urmărit percepția funcționarilor vamali asupra nivelului de securitate al sistemelor informatice, utilizând o scală de la 1 la 5. Majoritatea respondenților au oferit scoruri ridicate: 19 au indicat nivelul 4, iar 8 nivelul 5, în timp ce doar 7 respondenți au optat pentru valori mai scăzute (2 sau 3). Media generală este de 3,94, reflectând o percepție predominant pozitivă, dar nu lipsită de rezerve.
Această apreciere evidențiază un nivel moderat spre ridicat de încredere în securitatea actuală a sistemelor, dar și nevoia de îmbunătățire continuă, având în vedere sensibilitatea datelor gestionate și importanța respectării standardelor europene de securitate cibernetică.

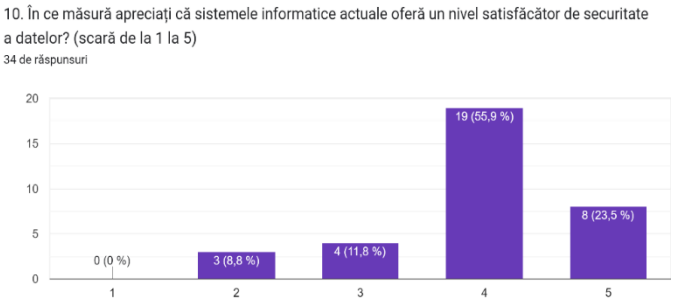

Figura 9. Întrebarea numărul 10 din cadrul chestionarului
Sursa: Chestionar privind interacțiunea inspectorilor vamali cu sistemele informatice publice din cadrul Autorității Vamale Române https://forms.gle/FmfR3k2r1nXeqkxF9

Întrebarea 11 a explorat experiența funcționarilor vamali cu incidente de securitate informatică. Majoritatea respondenților (23) au declarat că nu au întâmpinat astfel de incidente, în timp ce 4 au confirmat existența acestora. Un număr de 8 respondenți au ales opțiunea „Nu știu / Nu răspund”, sugerând o posibilă lipsă de informare sau o delimitare neclară între probleme tehnice și incidente de securitate propriu-zise.

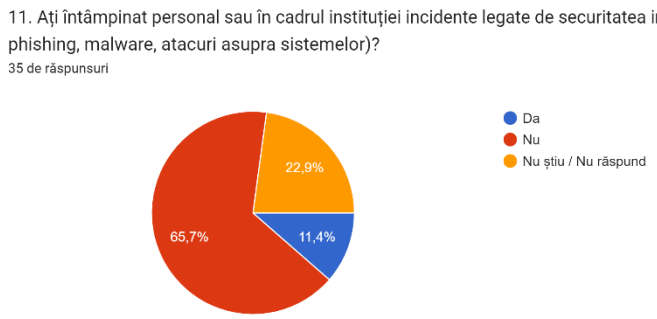

Figura 10. Întrebarea numărul 11 din cadrul chestionarului
Sursa: Chestionar privind interacțiunea inspectorilor vamali cu sistemele informatice publice din cadrul Autorității Vamale Române https://forms.gle/FmfR3k2r1nXeqkxF9

Majoritatea participanților (17 din 35) afirmă că au beneficiat de instruiri, însă doar „destul de rar", ceea ce sugerează o lipsă de constanță sau o frecvență insuficientă a programelor de formare. Doar un număr redus (6 respondenți) declară că au parte de instruiri constante, ceea ce poate indica fie o lipsă de resurse, fie o distribuție inegală a oportunităților de instruire.

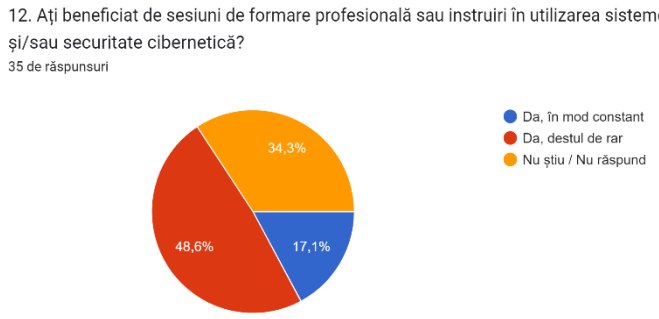

Figura 11. Întrebarea numărul 12 din cadrul chestionarului
Sursa: Chestionar privind interacțiunea inspectorilor vamali cu sistemele informatice publice din cadrul Autorității Vamale Române https://forms.gle/FmfR3k2r1nXeqkxF9

Răspunsurile pentru întrebarea deschisa „13. Care considerați că este cel mai vulnerabil punct în infrastructura informatică a administrației vamale?" sunt diverse, evidențiind atât aspecte tehnice, cât și organizaționale. Deși unii respondenți (8) nu s-au putut pronunța, ceilalți indică zone precum echipamentele învechite, interconectarea insuficientă a bazelor de date și aplicațiile interne ca posibile puncte slabe. Totodată, sunt semnalate nevoia de instruire continuă și consolidarea competențelor în securitate cibernetică. Această varietate de perspective reflectă un interes real pentru îmbunătățire și oferă un punct de plecare valoros pentru dezvoltarea unei strategii integrate de securizare a infrastructurii informatice.

La întrebarea 14. „Care sunt cele mai eficiente măsuri care ar putea contribui la îmbunătățirea securității informatice în cadrul AVR?" , întrebare deschisă, cele mai frecvent menționate măsuri privesc instruirea personalului, cu 2 respondenți care subliniază importanța formării continue în domeniul securității informatice.

La întrebarea 15 – „Credeți că implementarea unor tehnologii avansate, precum inteligența artificială, ar putea contribui la eficientizarea activității vamale și combaterea criminalității informatice?", aproape jumătate dintre respondenți manifestă deschidere față de utilizarea tehnologiilor avansate, inclusiv inteligența artificială, în activitatea vamală. Un număr egal exprimă incertitudine, ceea ce poate indica fie o lipsă de informare suficientă privind beneficiile acestor tehnologii, fie o rezervă justificată. Proporția celor care resping ideea este redusă (3 din 35), ceea ce sugerează o atitudine general favorabilă explorării inovației, dar cu necesitatea unor clarificări și exemple aplicate pentru a crește gradul de încredere.

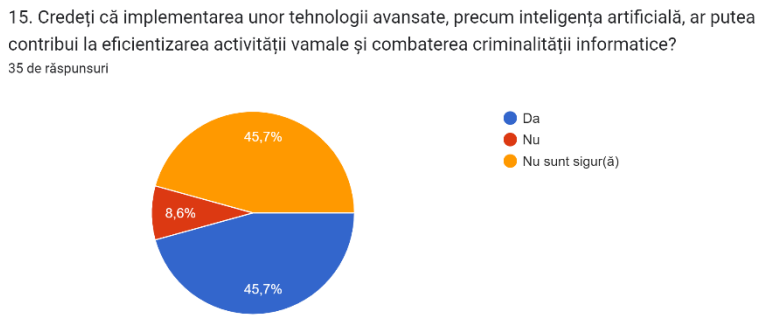

Figura 12. Întrebarea numărul 15 din cadrul chestionarului
Sursa: Chestionar privind interacțiunea inspectorilor vamali cu sistemele informatice publice din cadrul Autorității Vamale Române https://forms.gle/FmfR3k2r1nXeqkxF9

Răspunsurile la întrebarea 16 – „Aveți alte sugestii sau observații referitoare la sistemele informatice utilizate în cadrul administrației vamale?", evidențiază nevoia de îmbunătățire a vitezei sistemelor, simplificarea proceselor, integrarea bazelor de date, digitalizarea extinsă și ghiduri clare pentru utilizatori. Propunerile indică direcții clare pentru optimizarea sistemelor informatice vamale.

În urma analizei tuturor răspunsurilor se evidențiază o interacțiune continuă între inspectorii vamali și sistemele informatice utilizate în cadrul Autorității Vamale Române, reflectând un grad ridicat de integrare digitală în activitatea instituției. Răspunsurile colectate prin intermediul chestionarului indică faptul că digitalizarea nu mai reprezintă o simplă componentă auxiliară, ci un element structural indispensabil în derularea procedurilor vamale moderne.

Majoritatea respondenților declară utilizarea zilnică a sistemelor informatice, ceea ce confirmă o dependență operațională directă de infrastructura digitală actuală. În același timp, percepția generală este una favorabilă în ceea ce privește contribuția tehnologiei la creșterea eficienței și transparenței în activitatea vamală. Cu toate acestea, analiza calitativă a răspunsurilor evidențiază și o serie de disfuncționalități, precum dificultăți tehnice recurente, lipsa unor interfețe prietenoase și, mai ales, nevoia acută de instruire periodică a personalului.

Un aspect remarcabil este dat de componența eșantionului analizat, care include preponderent funcționari vamali cu o vechime considerabilă în sistem. Această caracteristică conferă validitate și profunzime evaluărilor exprimate, demonstrând că provocările semnalate nu sunt rezultatul unei lipse de familiaritate cu instrumentele digitale, ci reflectă realități instituționale persistente. În mod semnificativ, și personalul cu vechime redusă manifestă un interes sporit față de tehnologii emergente, precum inteligența artificială, ceea ce subliniază deschiderea generațiilor noi către inovație și adaptabilitate.

În concluzie, datele analizate susțin ideea unui cadru instituțional aflat într-un proces accelerat de digitalizare, dar care necesită ajustări strategice pentru a-și valorifica pe deplin potențialul. Consolidarea capacității instituționale ar trebui să includă, cu prioritate, modernizarea infrastructurii IT, dezvoltarea continuă a competențelor digitale ale personalului și implementarea unor soluții tehnologice orientate spre prevenirea riscurilor informatice. Aceste direcții sunt esențiale pentru consolidarea rolului Autorității Vamale Române ca actor cheie în protejarea intereselor economice naționale și europene într-un mediu digital dinamic și tot mai complex.

3.3. Modele de bune practici la nivelul spațiului unional și extra-unional

Luând în considerare contextul internațional caracterizat de o creștere exponențială a criminalității informatice și de o interdependență economică globală tot mai accentuată, modelele

de bune practici adoptate la nivelul administrațiilor vamale capătă o importanță strategică în consolidarea rezilienței instituționale și a securității infrastructurilor digitale. Analiza acestor modele, atât din cadrul Uniunii Europene, cât și din spațiul extra-unional, oferă un reper startegic pentru formularea unor politici naționale adaptate cerințelor actuale, în cadrul unui proces complex de digitalizare și optimizare a activității vamale.

Subcapitolul de față are ca obiectiv prezentarea unor inițiative relevante implementate în diferite jurisdicții, care au demonstrat eficiență în contracararea riscurilor informatice și în consolidarea capacității instituționale de răspuns la provocările digitale contemporane. Demersul analitic va fi orientat către identificarea acelor abordări care pot fi transferate, cu adaptările necesare, în contextul românesc, contribuind astfel la perfecționarea cadrului normativ și operațional în materie de securitate informatică vamală.

Prin această abordare comparativă se urmărește nu doar reliefarea rezultatelor pozitive obținute de alte administrații vamale, ci și o înțelegere aprofundată a contextelor legislative, instituționale și tehnologice în care aceste practici au fost implementate, în vederea susținerii unui proces coerent de armonizare și modernizare la nivel național.

Pentru început, voi analiza modelele unionale, deorece acestea au o transpunere mult mai omogenă dată fiind tendința de uniformizare atât normativă, cât și procedurală și de infrastructură la nivelul statelor UE.

Complexificarea comerțului internațional este determinată de o serie de factori structurali și conjuncturali, precum avansul accelerat al tehnologiilor digitale, reconfigurările geopolitice, evenimentele globale cu impact sistemic și evoluția continuă a comportamentului și așteptărilor consumatorilor. În acest context, o gestionare eficientă a fluxurilor comerciale internaționale presupune o capacitate crescută de adaptare instituțională, integrarea progresivă a soluțiilor digitale și orientarea către principii de sustenabilitate economică și operațională.

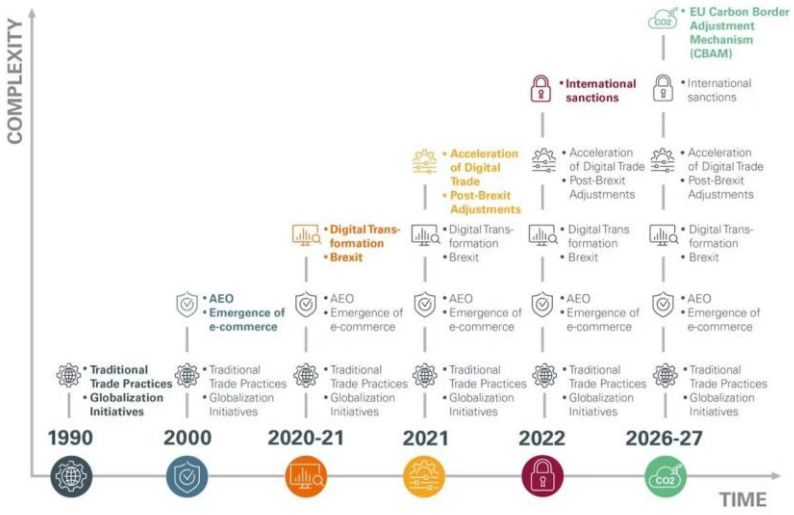

Figura 13. Evoluția complexității comerțului global în timp
Sursa: https://shorturl.at/txQne

Pentru a evidenția rolul digitalizării în protejarea intereselor economice, se impune analiza unor bune practici relevante. Exemplele din Uniunea Europeană și Statele Unite oferă repere concrete privind eficientizarea controlului vamal prin instrumente informatice și cooperare interinstituțională.

O bună practică esențială în domeniul vamal o constituie utilizarea analizei de risc în baza datelor transmise înainte de sosirea mărfurilor. Uniunea Europeană implementează în acest sens sistemul

Import Control System 2 (ICS2), care colectează declarații sumare de intrare (ENS) pentru toate modurile de transport, facilitând evaluarea riscurilor înainte de sosire. Acest mecanism contribuie semnificativ la prevenirea fraudei prin subevaluare și contrabandă, asigurând o degajare rapidă a mărfurilor cu risc scăzut [48]. Practica este similară cu abordarea americană Air Cargo Advance Screening (ACAS), care implică trimiterea anticipată a datelor de încărcare și utilizarea inteligenței artificiale pentru detectarea amenințărilor în transportul aerian expres [49].

Un alt exemplu de eficiență este interoperabilitatea prin model de date unificat. UE utilizează EU Customs Data Model (EUCDM) pentru a integra datele între diferitele sisteme informatice vamale. Un caz concret este transformarea automată a certificatelor veterinare TRACES în date de declarație în cadrul sistemului CSWCERTEX. Această automatizare reduce semnificativ erorile și accelerează controlul cantitativ [50]. Pe plan american, sistemul Automated Commercial Environment (ACE) joacă un rol similar, oferind un portal unic pentru importatori și exportatori, prin care se realizează schimbul de date și analiza de risc în timp real [51].

Implementarea unui sistem Single Window guvernamental este un alt pilon al eficientizării vamale. În SUA, platforma International Trade Data System (ITDS) conectează 47 de agenții la ACE, reducând birocrația și timpul de procesare [52]. În UE, inițiativa similară este EU Single Window Environment for Customs, care urmărește verificarea automată a licențelor și cotelor la import, prevenind astfel pierderile bugetare și practicile de dumping [52].

Parteneriatul public-privat în domeniul securității este de asemenea vital. În SUA, programul Customs-Trade Partnership Against Terrorism (CTPAT) presupune audituri riguroase și recompense pentru operatorii cu lanțuri logistice sigure [54]. UE reflectă această abordare prin programul AEO (Authorised Economic Operator), care oferă beneficii similare, inclusiv recunoaștere mutuală și integrare cu sisteme de informare anticipată [55].

Un exemplu de excelență în domeniul securității informatice este strategia de tip security-by-design. Estonia, stat membru UE, a implementat o arhitectură informatică bazată pe microservicii, fără permisiune de modificare retroactivă a datelor și audituri anuale, în conformitate cu standardele ISO 27001 și Directiva NIS2 [56]. În mod echivalent, SUA aplică cadrul NIST CSF 2.0 în cadrul CBP (Customs and Border Protection), adoptând principii precum Zero Trust și autentificare multifactor (MFA), cu responsabilitate clară la nivel de CISO [57].

Modelul american se remarcă printr-o structură centralizată, în care agențiile federale precum Department of Homeland Security (DHS) și U.S. Customs and Border Protection (CBP) coordonează politicile vamale și de securitate cibernetică într-un cadru integrat. Potrivit lui Ravich și Cancelmo, această integrare vizează în special protejarea lanțurilor de aprovizionare și a infrastructurii digitale critice, în vederea menținerii funcționalității sistemului economic în fața atacurilor informatice [58]. Pierderile estimate de Consiliul Consultativ Economic al Casei Albe ca urmare a activităților cibernetice malițioase, între 57 și 109 miliarde USD anual, evidențiază impactul sever asupra economiei și justifică măsurile adoptate [59].

În 2023, U.S. Customs and Border Protection (CBP) a publicat Cyber Incident Guidance for Customs Brokers, un ghid operațional dedicat comisionarilor vamali, ce oferă un exemplu relevant de bună practică în integrarea securității cibernetice în infrastructura vamală. Documentul propune o abordare structurată pe trei etape – prevenție, răspuns și recuperare – reflectând întregul ciclu de gestionare a riscurilor informatice. Pentru prevenție, sunt recomandate măsuri tehnice avansate, precum segmentarea rețelelor, autentificarea multifactorială, actualizarea sistemelor, testele de penetrare și auditurile IT, completate de formarea continuă a personalului. Etapa de răspuns prevede existența unui plan clar documentat, care include identificarea sursei atacului, izolarea sistemelor afectate, notificarea autorităților și conservarea probelor digitale. În faza de recuperare, accentul este pus pe elaborarea și testarea Planului de Continuitate a Activității (BCP) și a Planului de Recuperare în caz de Dezastru (DRP), adaptate specificului fiecărei organizații [60].

Documentul se remarcă prin aplicabilitate practică și claritate, promovând o abordare tactică și parteneriatul public-privat în gestionarea riscurilor cibernetice, responsabilitatea fiind împărțită între autorități și actorii economici implicați.

Dintr-o perspectivă critică, documentul CBP se remarcă prin claritate, aplicabilitate practică și caracter preventiv, aspecte adesea absente din documentele similare emise de alte administrații vamale. Spre deosebire de abordările normative sau strategice generale, acest ghid are o orientare tactică și este construit pe baza principiilor de gestionare a riscurilor operaționale. În plus, el reflectă filozofia americană a parteneriatului public-privat în materie de securitate, unde responsabilitatea nu este atribuită exclusiv statului, ci este împărțită între toți actorii implicați în ecosistemul vamal.

Cu toate acestea, aplicabilitatea ghidului în alte jurisdicții - precum Uniunea Europeană - ar necesita ajustări semnificative, având în vedere diferențele de reglementare, resurse și organizare administrativă. Totuși, principiile de bază rămân universal valabile: proactivitatea în fața riscurilor, transparența în gestionarea incidentelor și consolidarea rezilienței digitale prin măsuri operaționale coerente. În Uniunea Europeană, protejarea securității economice și informatice se desfășoară într-un cadru multinațional complex, în care Comisia Europeană, Parlamentul European, ENISA și autoritățile naționale colaborează pentru formularea și aplicarea politicilor. Spre deosebire de abordarea centralizată din SUA, UE funcționează pe baza subsidiarității, ceea ce implică o diversitate de strategii naționale. Van der Meulen subliniază că, în absența unei arhitecturi instituționale unitare în domeniul cibernetic vamal, este nevoie de o mai bună coordonare între statele membre pentru a preveni fragmentarea și vulnerabilitățile transfrontaliere [61]. Politicile de control al exporturilor de produse cu dublă utilizare, cum sunt tehnologiile de supraveghere cibernetică, devin instrumente de echilibru între comerț și valori democratice, dar ridică și probleme de aplicare uniformă [62].

Comparativ, SUA oferă un model de intervenție rapidă și parteneriat public-privat solid, sprijinit de standarde tehnice și operaționale clare. Uniunea Europeană adoptă o abordare normativă și multidimensională, punând accent pe valori, transparență și echilibru geopolitic, dar întâmpină dificultăți în implementarea unitară a acestor politici în teritoriu.

Ambele modele au puncte tari: SUA în execuție și coordonare, UE în reglementare și viziune strategică. Într-un context global tot mai interconectat și instabil, schimbul de bune practici și convergența standardelor ar putea contribui la crearea unui cadru vamal internațional mai sigur, mai rezilient și mai eficient.

Capitolul 4. Strategii de implementat

Pornind de la premisele analizate în capitolele anterioare, devine evident că reforma digitală a administrației vamale nu poate fi desprinsă de dezvoltarea unei arhitecturi robuste de securitate informatică. În condițiile în care volumul tranzacțiilor internaționale crește exponențial, iar digitalizarea sistemelor vamale devine o condiție sine qua non pentru eficiență, România trebuie să își consolideze capacitatea instituțională și tehnologică de prevenire și gestionare a riscurilor informatice. Experiența acumulată de alte entități statale, în special de către U.S. Customs and Border Protection (CBP), oferă un cadru valoros de bune practici care pot fi adaptate și integrate în arhitectura operațională a autorității vamale române.

Documentul Cyber Incident Guidance for Customs Brokers, publicat de CBP în 2023, reprezintă un model operațional concret de abordare sistemică a securității cibernetice în domeniul vamal. Acest ghid, destinat comisionarilor vamali, propune o structură funcțională stucturată în trei etape esențiale: prevenție, răspuns la incident și recuperare post-incident. Adaptarea acestui model la contextul românesc ar putea contribui semnificativ la profesionalizarea managementului

riscurilor cibernetice în sfera activităților vamale și la reducerea vulnerabilităților critice ale sistemelor informatice gestionate de Autoritatea Vamală Română (AVR).

În prima etapă, prevenția, România ar trebui să instituie un cadru normativ și tehnic care să oblige toate structurile vamale și operatorii economici autorizați (AEO) să adopte măsuri minimale de securitate IT, în conformitate cu bunele practici internaționale. Printre acestea se numără: segmentarea logică a rețelelor, implementarea autentificării multifactoriale, actualizarea periodică a sistemelor software, efectuarea regulată de teste de penetrare și audituri de securitate IT. Suplimentar, este necesară instituționalizarea unui program de formare profesională continuă în domeniul securității cibernetice, adresat nu doar personalului IT, ci și funcționarilor vamali de execuție, având în vedere că factorul uman reprezintă în continuare una dintre cele mai mari surse de risc.

Etapa de răspuns la incident, așa cum este structurată în ghidul CBP, presupune existența unui plan operațional documentat, aplicabil la nivelul fiecărei structuri vamale regionale, care să includă: identificarea rapidă a sursei atacului, izolarea sistemelor compromise, notificarea autorităților competente (DNSC, CERT-RO, SRI) și colectarea probelor digitale în vederea investigării. În acest scop, se recomandă dezvoltarea unei platforme digitale securizate de raportare a incidentelor, care să permită transmiterea în timp real a alertelor și comunicarea bidirecțională între structurile locale și cele centrale ale AVR. Această abordare ar contribui la standardizarea procedurilor de reacție și la reducerea timpului de răspuns în caz de atacuri cibernetice.

În etapa de recuperare, accentul trebuie pus pe dezvoltarea și testarea a două instrumente esențiale pentru continuitatea operațională: Planul de Continuitate a Activității (BCP) și Planul de Recuperare în caz de Dezastru (DRP). Aceste documente trebuie adaptate la specificul fiecărui birou vamal – în funcție de volumul operațiunilor, infrastructura IT existentă și riscurile regionale și testate periodic prin exerciții simulate (ex. tabletop cyber drills[2]), în colaborare cu instituțiile de securitate cibernetică. Totodată, este recomandat ca aceste planuri să fie aliniate cu cerințele Regulamentului (UE) 881/ 2019 privind ENISA și cu cadrul de referință al NIST Cybersecurity Framework, într-o versiune armonizată la nivelul administrației publice românești.

În completare, o altă direcție strategică de implementat este instituționalizarea unui parteneriat public-privat în domeniul vamal și cibernetic, inspirat de modelul colaborativ american. Acest parteneriat ar putea lua forma unui program voluntar de conformitate în securitate informatică, similar statutului AEO, care să ofere facilități administrative operatorilor economici ce respectă un set extins de standarde cibernetice. Acești operatori ar deveni parteneri strategici ai AVR, beneficiind de tratament preferențial în procesul de vămuire, dar și asumându-și responsabilitatea de a contribui activ la securitatea întregului lanț de aprovizionare. În acest sens, se poate propune dezvoltarea unui certificat național de conformitate cibernetică vamală, acordat în urma unui audit extern acreditat, care să garanteze alinierea la bunele practici internaționale.

Pentru a atinge un grad ridicat de maturitate instituțională, România trebuie să urmărească integrarea graduală a acestor măsuri în cadrul digital al Sistemului Informatic Vamal Integrat (SIVI), în paralel cu implementarea sistemelor AES-RO și NCTS5-RO. În acest context, ar fi oportună înființarea unei unități de securitate cibernetică specializată la nivelul AVR, care să funcționeze ca nod de legătură între instituțiile de securitate naționale și cele europene, să coordoneze implementarea acestor strategii și să asigure monitorizarea continuă a riscurilor informatice din domeniul vamal.

[2] Exerciții strategice simulate, desfășurate într-un mediu controlat, în care participanții își testează capacitatea de răspuns la incidente cibernetice prin scenarii ipotetice și decizii operative, fără utilizarea infrastructurii IT reale.

În completarea direcțiilor strategice anterior prezentate, se impune o extindere substanțială a cadrului de acțiune prin integrarea unor măsuri sistemice și tehnologice avansate, care să consolideze poziția Autorității Vamale Române (AVR) în cadrul arhitecturii de securitate economică și digitală a Uniunii Europene. Dat fiind contextul marcat de digitalizarea accelerată a proceselor vamale și de diversificarea formelor de criminalitate transfrontalieră, este imperativă trecerea de la o abordare reactivă la una anticipativă, bazată pe instrumente de analiză inteligentă a datelor.

O direcție strategică fundamentală vizează implementarea unui sistem avansat de analiză predictivă, care să utilizeze inteligența artificială (AI) și tehnologiile big data în evaluarea în timp real a riscurilor comerciale. Un astfel de sistem ar permite nu doar identificarea timpurie a tiparelor de fraudă vamală, ci și alocarea optimizată a resurselor de control. Prin valorificarea datelor generate de sistemele informatice vamale existente - cum ar fi PoUS (Proof of Union Status), ICS2 (Import Control System 2) sau RO e-Sigiliu - AVR ar putea dezvolta un mecanism analitic de supraveghere bazat pe modele comportamentale și indicatori de risc, consolidând astfel capacitatea sa operațională de prevenire a pierderilor bugetare și de protejare a intereselor financiare ale Uniunii.

Complementar, se recomandă înființarea unei Unități Naționale de Reacție Cibernetică Vamală (UNRCV), care să funcționeze ca un centru de coordonare și intervenție rapidă în caz de incidente informatice care afectează infrastructura vamală. Această structură ar avea rolul de a asigura interoperabilitatea operațională între entitățile IT ale AVR, Direcția Națională pentru Securitate Cibernetică (DNSC), Ministerul Finanțelor și actorii internaționali relevanți, precum OLAF și EUROPOL. Printre atribuțiile sale principale s-ar număra elaborarea și actualizarea continuă a protocoalelor comune de securitate, organizarea de exerciții anuale de simulare ale amenințărilor și dezvoltarea de scenarii strategice de intervenție, menite să testeze și să îmbunătățească reziliența instituțională în fața amenințărilor informatice.

Pentru a garanta alinierea la standardele internaționale și pentru a asigura un mecanism transparent de monitorizare, se impune instituționalizarea unui sistem de audit extern independent în domeniul securității cibernetice vamale, realizat anual de către organisme de certificare acreditate. Acest audit ar avea rolul de a evalua nivelul de maturitate cibernetică al AVR, de a identifica vulnerabilitățile critice ale infrastructurii informatice și de a emite recomandări strategice de conformare la standardele de referință, precum ISO/IEC 27001 și NIST Cybersecurity Framework. În plus, raportările rezultate ar trebui integrate în rapoartele anuale de performanță instituțională și corelate cu obiectivele naționale de transformare digitală.

În perspectiva integrării României într-un spațiu vamal european pe deplin digitalizat, este esențială armonizarea arhitecturii informatice naționale cu viitorul Hub Vamal European de Date, care urmează a deveni un pilon fundamental al politicii vamale comune. Pentru atingerea acestui obiectiv, se recomandă demararea unor proiecte-pilot de interoperabilitate între sistemele AES-RO și NCTS5-RO și platformele comune ale Comisiei Europene, urmărind testarea schimbului securizat de date, sincronizarea terminologică și adaptarea cadrului juridic intern la cerințele UE privind protecția datelor, standardele de securitate și fluxurile logistice digitale.

Nu în ultimul rând, România trebuie să elaboreze și să adopte o strategie națională de protejare a intereselor financiare ale Uniunii Europene în domeniul vamal, ca parte integrantă a Planului Național de Redresare și Reziliență (PNRR). Această strategie ar trebui să includă obiective clare privind accelerarea digitalizării proceselor vamale, întărirea capacității instituționale de prevenire a fraudei, extinderea parteneriatelor public-private în domeniul securității informatice și profesionalizarea continuă a personalului vamal. În acest context, se propune și înființarea unui Centru Național de Excelență în Securitate Cibernetică Vamală, dezvoltat în parteneriat cu mediul academic, sectorul privat și instituțiile europene, care să funcționeze ca un hub de formare, cercetare și inovare în domeniul protecției informatice aplicate mediului vamal.

În concluzie, aplicarea coerentă a acestor direcții strategice în contextul administrației vamale românești ar marca tranziția de la o abordare reactivă la una proactivă și anticipativă, aliniată la cele mai înalte standarde internaționale de securitate economică și informatică. Aceasta ar contribui nu doar la protejarea veniturilor bugetare și la asigurarea fluxului comercial legal, ci și la consolidarea poziției României ca actor european responsabil în arhitectura de securitate digitală a Uniunii Europene.

Discuții / Concluzii

Lucrarea a pornit de la premisa că o administrație vamală modernă nu poate răspunde exigențelor actuale fără o infrastructură digitală avansată și fără o cultură organizațională care să integreze în mod sistematic și proactiv dimensiunea securității informatice. Într-un mediu global dinamic, marcat de intensificarea digitalizării, de reconfigurări geopolitice și de proliferarea amenințărilor informatice, Autoritatea Vamală Română (AVR) se află în fața unei provocări strategice: aceea de a-și consolida rolul instituțional ca garant al stabilității economice naționale și europene.

Analiza întreprinsă a arătat că, există progrese notabile - materializate prin platforme precum AES-RO, ICS2, RO e-Sigiliu și NCTS5-RO – totuși, România se află încă în etapa de tranziție de la digitalizarea procedurală la transformarea digitală reală. Aceste inițiative tehnice, oricât de promițătoare, își ating potențialul doar în măsura în care sunt acompaniate de o strategie coerentă privind securitatea informatică, de formarea continuă a resurselor umane, și de o deschidere activă spre parteneriate interinstituționale și colaborări internaționale. Din această perspectivă, tehnologia devine un mijloc, nu un scop, iar cheia succesului constă în modul în care este integrată în viziunea instituțională de ansamblu.

Un punct de sprijin important în cadrul cercetării l-a reprezentat analiza modelelor de bune practici, și în special a documentului Cyber Incident Guidance for Customs Brokers, elaborat de U.S. Customs and Border Protection (CBP). Acest ghid oferă nu doar un exemplu funcțional de bună practică, ci și un cadru operațional care poate fi adaptat realităților românești. În acest sens, transpunerea sa la nivelul AVR poate constitui nu doar o sursă de indrumare, ci un instrument de acțiune strategică.

Lucrarea propune un ansamblu coerent de măsuri cu aplicabilitate practică directă. Printre acestea se evidențiază: crearea unei Unități Naționale de Reacție Cibernetică Vamală, instituționalizarea unui certificat de conformitate cibernetică pentru operatorii economici, utilizarea inteligenței artificiale în analiza de risc vamală, precum și armonizarea arhitecturii IT a AVR cu viitorul Hub Vamal European de Date. Aceste propuneri sunt concepute ca răspunsuri realiste și fezabile la provocările identificate, iar implementarea lor poate genera un impact instituțional semnificativ, cu beneficii directe asupra eficienței administrative, competitivității economice și rezilienței digitale.

Din punct de vedere academic, această cercetare contribuie la dezvoltarea unui domeniu actual în România – securitatea cibernetică aplicată administrației vamale – oferind o perspectivă integratoare, care îmbină analiza politicilor publice, bunele practici internaționale și instrumente aplicate de guvernanță digitală. Lucrarea își propune să umple un gol în literatura de specialitate autohtonă, oferind nu doar un cadru conceptual, ci și o metodologie aplicabilă, capabilă să susțină viitoare cercetări în domeniul digitalizării administrației publice vamale.

În plan instituțional, utilitatea lucrării este deosebit de concretă. Propunerile formulate pot sta la baza unor reforme structurale în cadrul AVR și pot servi drept puncte de referință în elaborarea de politici publice, strategii de securitate sau programe de investiții digitale. Mai mult, ele pot fi utilizate în procesul de atragere și justificare a finanțărilor europene nerambursabile, în special prin mecanismele PNRR și CEF Digital, oferind o viziune coerentă și aliniată la standardele Uniunii Europene. În acest sens, lucrarea se constituie ca un instrument de lucru pentru decidenți,

un ghid strategic pentru implementatori și o resursă tehnică pentru formatori și dezvoltatori instituționali.

În concluzie, România dispune de toate condițiile necesare pentru a-și transforma administrația vamală într-o instituție digitală, sigură, predictibilă și interoperabilă. Mai mult decât o simplă conformare la cerințele europene, această transformare ar reprezenta o afirmare a capacității statului român de a furniza soluții, nu doar de a implementa directive. Autoritatea Vamală Română are potențialul de a deveni un exemplu regional de bune practici în materie de securitate economică și digitală, iar această lucrare își propune să ofere o direcție clară și argumentată pentru atingerea acestui obiectiv.

Astfel, rezultatele cercetării nu doar că subliniază urgența unor intervenții strategice, dar oferă și mijloacele prin care acestea pot fi realizate. Într-o perioadă în care încrederea în capacitatea statului de a proteja interesele economice este esențială, o administrație vamală eficientă și securizată devine un element-cheie al stabilității și prosperității naționale.

References

[1] Catalin Vrabie, „"Promisiunile Inteligenței Artificiale (AI) Administrației Publice și Orașelor Inteligente"," *Proceedings of the 11th Smart Cities International Conference (SCIC) - December 2023,* 2023.

[2] *Regulamentul (UE) nr. 952/2013 al Parlamentului European și al Consiliului din 9 octombrie 2013 de stabilire a Codului vamal al Uniunii,,* 2013.

[3] „United Nations Office on Drugs and Crime (UNODC),COMPREHENSIVE STUDY ON CYBERCRIME - Draft February 2013," 2013.

[4] *DECIZIA NR. 70/2008/CE A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 15 ianuarie 2008 privind crearea unui mediu informatizat pentru vamă și comerț,* 2008.

[5] Florin Negoiță, Istoria administrației publice din România, București: Universul juridic, 2011.

[6] Cezar Corneliu MANDA, Digitalizarea administrației publice din România –între nevoile și aspirațiile unei societăți moderne a secolului XXI, Bucuresti: Smart Cities International Conference (SCIC) Proceedings. 9, 2023, p. 42.

[7] Corneliu Cezar MANDA , Digitalizarea administrației publice din România –între nevoile și aspirațiile unei societăți moderne a secolului XXI., București: Smart Cities International Conference (SCIC) Proceedings. 9,, 2023, p. 48.

[8] Guvernul României, *HOTĂRÂRE nr. 237 din 16 februarie 2022 privind organizarea și funcționarea Autorității Vamale Române,* București, 2022.

[9] Vlad Stoicescu, Teodora Ioana Bițoiu, Cătălin Vrabie, „The Smart Community: Strategy Layers for a New Sustainable Continental Framework," *Smart Cities,* vol. 6, nr. 1, 2023.

[10] Cătălin Vrabie, „MACHINE INTELLIGENCE SECURITY FOR SMART CITIES," în *PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON MACHINE INTELLIGENCE & SECURITY FOR SMART CITIES (TRUST)*, 2024.

[11] DG TAXUD, „TAXUD_UCC_Customs Procedures and Customs , Programul de e-learning Regimuri vamale și declarații vamale," 2024.

[12] Cătălin Vrabie, „Convergența securității digitale," *Smart Cities International Conference (SCIC) Proceedings. 3,* 2023.

[13] Curtea de Conturi UE, „Activitățile Curții în 2022 Raportul anual de activitate al Curții de Conturi Europene," 2022.

[14] Guy WAIZEL, „Marketing insights when shifting cybersecuritytechnologies to the cloud or hybrid cloud in the context ofsmart cities," *Smart Cities International Conference (SCIC) Proceedings. 11,* 2024.

[15] Christian SCHACHTNER, „Creation of a distinct culture for the overall system"Compliance, IT security and Data protection" inmunicipalities in Germany," *Smart Cities International Conference (SCIC) Proceedings. 10,,* 2023.

[16] Caterina TOMULESCU, „Cyberbiosecurity. A short review," *Smart Cities International Conference (SCIC) Proceedings. 8,,* 2023.

[17] M. G. MIHĂILĂ, , „E-guvernarea, Romania 2000-2030. Orase inteligente si dezvoltare urbana," *SCRD,* pp. 267-268, 2023.

[18] Parlamentul European și Consiliul, *Regulamentul (UE) nr. 952/2013 de stabilire a Codului vamal al Uniunii..*

[19] *Regulamentul (CE) nr. 515/97 al Consiliului din 13 martie 1997 privind asistența reciprocă între autoritățile administrative ale statelor membre și cooperarea dintre acestea și Comisie în vederea asigurării aplicării corespunzătoare a legislației din dome.*

[20] *Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului din 9 martie 2016 cu privire la Codul Uniunii privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen).*

[21] *Regulamentul de punere în aplicare (UE) 2023/1070 al Comisiei din 1 iunie 2023 privind modalitățile tehnice pentru dezvoltarea, întreținerea și utilizarea sistemelor electronice destinate schimbului și stocării de informații în temeiul Regulamentului (UE).*

[22] „Autoritatea Vamală Română," Strategie privind reforma autorității vamale din România 2022 - 2024, 2022. [Interactiv]. Available: https://www.customs.ro/assets/pdf/comunicate/delia/Strategie_AVR_2022-2024.pdf. [Accesat 13 03 2025].

[23] G. M. MIHĂILĂ, „Integrated European –level measures regarding artificial intelligence in relation to human rights," *SCRD,* p. p.389, 2024.

[24] Autoritatea Vamală Română, „Autoritatea Vamală Română," [Interactiv]. Available: https://www.customs.ro/. [Accesat 14 03 2025].

[25] *Regulamentul delegat (UE) nr. 2015/2446 al Comisiei,* 2015.

[26] *Regulamentul de punere în aplicare (UE) nr. 2015/2447 al Comisiei,* 2015.

[27] ANAF, *ORDIN Nr. 1195/2016 din 13 aprilie 2016 pentru aprobarea Normelor tehnice de utilizare a Sistemului de control al importului,* București, 2016.

[28] ANAF, *Ordinul președintelui ANAF nr. 1194/13.04.2016,* București, 2016.

[29] „Autoritatea Vamală Română," Autoritatea Vamală Română a demarat aplicarea sigiliilor inteligente în cadrul Sistemul Național RO e-Sigiliu, 2025. [Interactiv]. Available: https://www.customs.ro/noutati/-autoritatea-vamala-romana-a-demarat-aplicarea-sigiliilor-inteligente-in-cadrul-sistemul-national-ro-e-sigiliu-. [Accesat 16 03 2025].

[30] Cătălin Vrabie, ELEMENTE DE E-GUVERNARE, 2016, p. 9.

[31] Comisia Europeană, „COMUNICARE A COMISIEI CĂTRE PARLAMENTUL EUROPEAN, CONSILIU ȘI COMITETUL ECONOMIC ȘI SOCIAL EUROPEAN Trecerea uniunii vamale la o etapă superioară: un plan de acțiune," Bruxelles, 2020.

[32] SRI, „Serviciul Român de Informații," [Interactiv]. Available: https://www.sri.ro/cyberint?. [Accesat 16 03 2025].

[33] Parlamentul European, „Securitate cibernetică: principalele amenințări," 2022.

[34] Bitdefender, „Bitdefender," [Interactiv]. Available: https://www.bitdefender.com/ro-ro/business/infozone/what-is-phishing. [Accesat 15 03 2025].

[35] Directoratul Național de Securitate Cibernetică, „Directoratul Național de Securitate Cibernetică," [Interactiv]. Available: https://dnsc.ro/citeste/comunicat-atacuri-ddos-grupari-rusia-site-uri-romania. [Accesat 16 03 2025].

[36] Bitdefender, „Bitdefender," [Interactiv]. Available: https://www.bitdefender.com/ro-ro/business/infozone/what-is-ransomware. [Accesat 16 03 2025].

[37] Ministerul Finanțelor, „Planului strategic al Ministerului Finanțelor 2025-2028," Bucuresti, 2025.

[38] Comisia Europeană, „Comisia Europeană. Report by the Wise Persons Group on the Challenges Facing the Customs Union," 2022.

[39] Comisia Europeană, „Comisia Europeană. Trade Contact Group – 62nd Plenary Meeting – Summary Report," 2023.

[40] Comisia Europeană, „Comisia Europeană. Customs Reform – Towards a Stronger and More Modern Customs Union," 2023.

[41] „World Customs Organisation News," German Customs puts AI front and centre, 6 03 2025. [Interactiv]. Available: https://mag.wcoomd.org/magazine/wco-news-106-issue-1-2025/german-customs-ai/. [Accesat 05 03 2025].

[42] Cătălin Vrabie, „AI de la idee la implementare. Traseul sinuos al Inteligenței Artificiale către maturitate," *The Smart Cities and Regional Development (SCRD) Book Series,* 2024.

[43] EU Commission Directorate-General for Structural Reform Support, „Revenue Administration's Strategy on Artificial Intelligence Estonia," 2023.

[44] European Union Agency for Cybersecurity (ENISA), „Report on the State of Cybersecurity in the Union," 2024.

[45] Comisia Europeană, „Eurpean Commission," EU Budget 2025 aims to reinforce funding for Europe's priorities, 19 06 2024. [Interactiv]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3247. [Accesat 10 04 2025].

[46] ENISA, *Ghid privind securitatea cibernetică pentru IMM,* Directoratul Național de Securitate Cibernetică.

[47] Guvernul României, *NOTĂ DE FUNDAMENTARE OUG privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din.*

[48] European Commission, „Taxation and Customs Union," Import Control System 2 (ICS2), [Interactiv]. Available: https://taxation-customs.ec.europa.eu/customs-4/customs-security/ics2_en. [Accesat 14 04 2025].

[49] U.S. Customs and Border Protection, Air Cargo Advance Screening (ACAS), 29 08 2024. [Interactiv]. Available: https://www.cbp.gov/border-security/ports-entry/cargo-security/acas. [Accesat 16 04 2025].

[50] European Commission, „Taxation and Customs Union," EU Customs Data Model (EUCDM), [Interactiv]. Available: https://taxation-customs.ec.europa.eu/online-services/online-services-and-databases-customs/eu-customs-data-model-eucdm_en. [Accesat 17 04 2025].

[51] U.S. Customs and Border Protection, ACE and Automated Systems, [Interactiv]. Available: https://www.cbp.gov/trade/automated. [Accesat 17 04 2025].

[52] U.S. Departament of Agriculture, International Trade Data System (ITDS): Helping Boost Trade, [Interactiv]. Available: https://www.ams.usda.gov/content/international-trade-data-system-itds-helping-boost-trade?utm. [Accesat 17 04 2025].

[53] European Commission, „Taxation and Customs Union," The EU Single Window Environment for Customs, [Interactiv]. Available: https://taxation-customs.ec.europa.eu/eu-single-window-environment-customs_en. [Accesat 17 04 2025].

[54] U.S. Customs and Border Protection, CTPAT Best Practices, [Interactiv]. Available: https://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism/bestpractices?. [Accesat 17 04 2025].

[55] World customs organisation, WCO SAFE Package WCO tools to secure and facilitate global trade, [Interactiv]. Available: https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/frameworks-of-standards/safe_package.aspx. [Accesat 17 04 2025].

[56] Marika Rand , „Grant Thornton," What is the Estonian information security standard, E-ITS and what approach to take?, 27 03 2025. [Interactiv]. Available:

https://www.grantthornton.ee/en/insights1/what-is-the-estonian-information-security-standard-e-its-and-what-approach-to-take/. [Accesat 17 04 2025].

[57] U.S. Customs and Border Protection, U.S. Customs and Border Protection Cybersecurity Strategy, [Interactiv]. Available: https://www.cbp.gov/document/publications/us-customs-and-border-protection-cybersecurity-strategy. [Accesat 18 04 2025].

[58] DANIEL M. GERSTEIN, DOUGLAS C. LIGOR, „Economic Security and the U.S. Department of Homeland Security, RAND Corporation," 2023. [Interactiv]. Available: https://www.rand.org/pubs/perspectives/PEA2210-1.html. [Accesat 17 04 2025].

[59] Council of Economic Advisers, „The Cost of Malicious Cyber Activity to the U.S. Economy," 2018.

[60] U.S. Customs and Border Protection, „Cyber Incident Guidance for Customs Brokers," 2023.

[61] Dr Nicole van der Meulen, Eun A Jo, Stefan Soesanto, *Cybersecurity in the European Union and Beyond,* Brussels: European Parliament, 2015.

[62] Rudi Du Bois, Alexandre Tapia Reyes, *Dual-use and cyber-surveillance: EU policies and current practices,* European Parlament, 2023.