

# CONTRIBUȚIA OFICIULUI REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT LA PROMOVAREA IMAGINII ROMÂNIEI ÎN PERIOADA POSTADERARE

*Gl. bg.(r) conf. univ. dr. Neculae Năbârjoiu*

## 1. Introducere

Se săvârșește astăzi un real act de curaj din partea organizatorilor, *Centrul Cultural al MAI și Revista Geopolitică*, de a pune în pagină o temă delicată, a cărei finalitate se poate obține doar la nivel strategic.

Gestionarea imaginii de țară în perioada postaderare este și va fi o mare necesitate, o acțiune dificilă, în niciun caz al unui minister, al unei persoane, fie ea de demnitate publică, ci a tuturor românilor, oriunde s-ar afla. Pentru că, cu voia noastră sau nu, contribuim, cu mic cu mare, la conturarea imaginii țării noastre.

Îmi amintesc cu respect afirmația unui general privitoare la gradul militar, că nu este decât un adaos la hainele noastre; el nu-ți îmbunătățește imaginea, nu-ți sporește inteligența și, mai adăuga, „vai de cel ce nu reușește să se comporte la nivelul gradului ce-l poartă”. Tot așa, imaginea României nu poate fi dată doar de unele prezentări protocolare, ci de rezultatele activității din fiecare domeniu.

Voi aborda această comunicare prin prisma preocupărilor mele actuale, în cadrul cărora, alături de un grup inimos de oameni, sub o baghetă magică a unui profesor doctor în management, contribui la realizarea unei imagini reale pe segmentul securității informațiilor clasificate.

*A apăra informația*, a o împiedica să ajungă în mâna inamicului ori a răufăcătorului, a asigura protecția informațiilor nu sunt activități noi. Se poate spune că păstrarea secretului profesional, a secretului militar cu atât mai mult, este o primă condiție a succesului misiunii de îndeplinit.

*Necesitatea securității informațiilor* este determinată de gradul de utilitate al acestora, având în vedere că ele oferă, de cele mai multe ori, atu-ul în jurul căruia se construiesc strategiile câștigătoare, combat cu succes strategiile competitorilor, controlează comportamentele altora (indivizi, grupuri sau organizații) și reprezintă cea mai importantă sursă a puterii sociale.

Prin diseminarea fără control a informațiilor *pot fi afectate interesele și imaginea statului* (securitatea națională), *ale unei organizații* (persoană juridică de drept public sau privat) ori *ale unei persoane fizice*.

N-aș vrea să dau impresia că doresc să găsesc vinovați sau să pregătesc terenul pentru justificarea eventualelor eșecuri dar, am sesizat că există, între noi apărătorii de secrete prin profesie și mass-media, o controversă. Slujitorii mass-media, de altfel buni patrioți și apărători ai intereselor naționale, caută forme de senzațional, mai ales în zona informațiilor cenușii și a unor aspecte negative care, uneori, pot avea caracter confidențial. De aceea, securitatea informațiilor clasificate și prevenirea scurgerii acestora în activitatea de informare publică se află în atenția autorităților publice și militare din toate țările lumii și este considerată una din condițiile asigurării securității naționale. Se veghează ca în mass-media să nu apară informații și date clasificate privitoare la domenii care contribuie la realizarea strategiei naționale de apărare a țării, precum și la măsurile care se preconizează să fie luate în timp de pace sau de război pentru contracararea unei agresiuni.

De obicei, informațiile privind securitatea națională, libere la publicare, sunt în strânsă corelație cu unele interese legate de: conjunctura internațională, tehnica militară achiziționată, aplicații notificate, demonstrații militare, unele operații de redislocare a forțelor de apărare și măsurile de pregătire a acestora, anumite aspecte privind starea morală și coeziunea unităților militare, participarea la acțiuni sociale, sesiuni științifice, simpozioane, activități de protocol, de cinstire sau comemorare a eroilor și alte evenimente.

*Controversa* rezultă, după părerea noastră, din viziuni diferite privind conceptul de presă liberă:

- *în cadrul sistemului de securitate a informațiilor clasificate se acceptă că presa este liberă și datoare să informeze opinia publică, aceasta fiind unica rațiune a existenței sale, dar fără să stânjenească securitatea națională și fără să afecteze imaginea țării, a instituțiilor ori a persoanelor;*

- *poziția presei este că opinia publică trebuie informată despre ce se află în structurile puterii, în cele ale securității naționale, în armată, inclusiv pe timpul desfășurării unor acțiuni militare sau de luptă împotriva terorismului, relatând atât lucrurile bune, cât și pe cele rele, asumându-și prerogativele de a discerne și de a veghea la nepericlitarea securității naționale, implicit a imaginii țării.*

Această controversă, generată de unii factori obiectivi (informații cenușii, necunoașterea întregului ansamblu al intereselor naționale), cât și subiectivi (orgoliile unor specialiști, dorința de a surprinde spectaculosul, de a apăra și ce trebuie și ce nu trebuie) se va menține în permanență. Dacă este păstrată în limite normale, dovedindu-se calm și

înțelegere reciprocă, controversa este benefică, constituind reacția de reglare a sistemului. Dacă orgoliile sunt cele ce guvernează procesul, dacă apar conflicte interumane și mai ales dacă emoțiile sunt cele ce dictează comportamentul, controversa se transformă în conflict, iar din desfășurarea acestuia nu câștigă nici organele care apără secretele, nici presa, nici opinia publică, ci numai adversarii securității naționale și ai apărării țării, artizanii atacurilor la imagine.

Informația, cu atât mai mult cea clasificată, fiind un *factor de putere*, este firesc ca ea să fie protejată. Comunicarea, în aceste condiții, trebuie să-și propună să apere imaginea, iar când este afectată, să sugereze și soluții de refacere a acesteia. În materialele publicate nu trebuie să se folosească drept "condimente" informații clasificate pentru a fi receptate mai bine de auditoriu. România nu-și poate permite, prin atacuri la imagine, diminuarea rolului ei în formare de furnizor de securitate atât în zona de responsabilitate a NATO, cât și a Uniunii Europene.

## **2. Oficiul Registrului Național al Informațiilor Secrete de Stat**

Fiind o instituție relativ nouă, găsesc necesar să prezint câteva date despre instituția pe care o reprezint aici.

Oficiul Registrului Național al Informațiilor Secrete de Stat (ORNISS) reprezintă autoritatea națională de securitate în domeniul protecției informațiilor clasificate naționale, NATO și UE.

ORNISS a apărut în momentul trecerii într-o etapă superioară a politicii de securitate a României în procesul de aderare la NATO, la cererea expresă a Alianței, și funcționează în conformitate cu prevederile stipulate în:

- *Legea nr. 182/2002 privind protecția informațiilor clasificate;*
- *Ordonanța de urgență a Guvernului nr. 153/2002 privind organizarea și funcționarea ORNISS aprobată prin Legea nr. 101/2003;*
- *Hotărârea Guvernului nr. 353/2002 pentru aprobarea Normelor privind protecția informațiilor clasificate ale Organizației Atlanticului de Nord în România;*
- *Hotărârea Guvernului nr.585/2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România.*

ORNISS are misiunea să asigure implementarea unitară a măsurilor de protecție a informațiilor clasificate în România.

ORNISS este o instituție publică aflată *în subordinea Guvernului, în coordonarea directă a primului ministru*, condusă de un director

general cu rang de secretar de stat; acționează în domeniul securității naționale, *cooperând cu serviciile de informații*, fără a desfășura activități specifice acestora; este *organismul național de legătură cu Oficiul de Securitate NATO (NOS)* și cu alte autorități de securitate, din statele membre sau parteneri ale Alianței Nord-Atlantice și ale Uniunii Europene.

### **3. Contribuția ORNISS la promovarea imaginii României în perioada postaderare**

Pentru a scoate în evidență rolul instituției noastre în promovarea imaginii României în perioada postaderare, fac precizarea că, în conformitate cu prevederile *Ordonanței de urgență a Guvernului nr. 153/2002 privind organizarea și funcționarea ORNISS aprobată prin Legea nr. 101/2003*, ORNISS:

- exercită atribuții de reglementare, autorizare, evidență și control, pe baza legislației naționale, a principiilor generale și standardelor minime de securitate ale NATO și ale Uniunii Europene;

- desfășoară activitatea în domeniile: securitatea personalului, securitatea fizică, securitatea documentelor, securitatea industrială (inclusiv emiterea autorizațiilor speciale pentru fotografierea, filmarea, cartografierea și executarea unor lucrări de arte plastice în obiective sau locuri de importanță deosebită pentru protecția informațiilor clasificate) și securitatea informațiilor pe suport electronic (INFOSEC);

- avizează acordurile internaționale departamentale și coordonează activitățile de negociere și de semnare a tratatelor internaționale referitoare la protecția informațiilor clasificate la nivel guvernamental;

- asigură cadrul general de pregătire a persoanelor care au acces la informații clasificate, precum și informarea publicului, ca formă a educației de securitate, parte a culturii de securitate a NATO și a UE.

În continuare, voi aborda *domeniile specifice ale activității de protecție a informațiilor clasificate*, respectiv: securitatea personalului, securitatea fizică și a documentelor, securitatea industrială și INFOSEC, subliniind rolul acestora în promovarea unei imagini favorabile a României în această perioadă.

**Securitatea personalului** reprezintă ansamblul măsurilor de protecție legate de accesul persoanelor la informații clasificate. Se asigură astfel, apărarea imaginii fiecăruia dintre noi. Dacă am primi

acces la informații clasificate fără acoperire, ar fi afectată imaginea ORNISS și a autorităților care, în baza legii, fac verificările de rigoare. Dacă accesul incorect ar afecta securitatea națională, iar situația n-ar fi singulară, este evident că putem aprecia că imaginea țării este afectată.

Obiectivele măsurilor de protecție privind accesul persoanelor la informații clasificate urmăresc:

- să *prevină* accesul persoanelor neautorizate la informații clasificate;

- să *permită* identificarea persoanelor care, prin acțiunile lor, pot afecta securitatea informațiilor clasificate;

- să *asigure* accesul persoanelor la informații clasificate numai pe baza unui document special de acces (denumit generic *certificat de securitate*) și a respectării *principiului „nevoia de a cunoaște”*.

Principiul „nevoia de a cunoaște” se referă la necesitatea imperioasă ca o persoană să aibă acces numai la informațiile clasificate exclusiv în scopul realizării atribuțiilor sale de serviciu, numai în momentul și numai pe durata în care accesul este absolut necesar. Nici o persoană nu este îndreptățită, doar prin rang, funcție sau prin deținerea unui certificat de securitate, să aibă acces la o anumită informație clasificată dacă acest lucru nu este absolut necesar pentru îndeplinirea sarcinilor de serviciu.

Aș vrea să fiu lămuritor cu un aspect care ține de imagine și am observat că nu este corect perceput. În presă, chiar în păreri ale unor persoane oficiale, se fac referiri la „certIFICATELE ORNISS”. Este just că, certificatele de securitate sunt eliberate de ORNISS, dar cunoașterea mecanismului acordării ori ridicării este important de știut.

Procedurile privind securitatea personalului urmăresc acordarea accesului la informații clasificate numai persoanelor care se dovedesc loiale, oneste și demne de încredere. Certificatul de securitate, atestând aceste calități, se eliberează în urma unor verificări specifice de securitate, efectuate de autoritățile abilitate prin lege, și reprezintă corolarul muncii acestora pentru gestionarea imaginii celor implicați.

Referitor la obiectul verificărilor, art.7, alin (1) din Legea nr. 182/2002 prevede că „...persoanele care vor avea acces la informații clasificate secrete de stat vor fi verificate, în prealabil, cu privire la onestitatea și profesionalismul lor...”.

*Autoritățile abilitate pentru efectuarea verificărilor de securitate* pentru personalul propriu, precum și pentru personalul altor autorități și instituții publice, agenți economici etc. (stabilit, în condițiile legii, în competența acestora), denumite prin lege *autorități desemnate de*

*securitate*, sunt: Serviciul Român de Informații; Serviciul de Informații Externe; Ministerul Apărării, prin Direcția Generală de Informații a Apărării; Ministerul Administrației și Internelor, prin Direcția Generală de Informații și Protecție Internă; Serviciul de Protecție și Pază; Serviciul de Telecomunicații Speciale.

Legislația prevede că *verificările de securitate* se fac cu aprobarea ORNISS și cu acordul persoanei pentru care se solicită accesul la informații clasificate. Așadar, dacă știu că sunt probleme, nu-mi dau acordul pentru verificări, mi se protejează imaginea, dar nu mai pot lucra cu informații clasificate. Datele privind persoanele sunt clasificate și, ca atare, nu fac obiectul comentariilor.

Din păcate, am întâlnit un caz în care un director, după ce a solicitat ridicarea avizului pentru o persoană pe care n-o dorea în echipă, i-a comunicat acesteia că ORNISS-ul i-a ridicat certificatul, iscând un atac gratuit și incorect la imaginea noastră care, în final, în mod firesc, a ajuns să afecteze imaginea directorului și a instituției respective.

*Conținutul verificărilor* este stabilit prin standardele naționale de protecție a informațiilor clasificate. Criteriile principale relevante în acordarea avizului de securitate au în vedere aspectele ce pot genera riscuri de securitate.

*În urma verificărilor*, autoritatea abilitată eliberează un *aviz de securitate*.

ORNISS, pe baza analizei concluziilor prezentate în avizul de securitate, decide cu privire la eliberarea *certificatului de securitate*.

O *procedură de reverificare* se impune ori de câte ori este necesar să se garanteze menținerea condițiilor în baza cărora s-a eliberat certificatul de securitate pentru acces la informații clasificate.

Reverificarea este obligatorie de fiecare dată când apar indicii că menținerea certificatului nu mai este compatibilă cu interesele de securitate.

*Neacordarea certificatului de securitate sau retragerea* motivată a acestuia determină interdicția de acces la informații clasificate.

***Securitatea fizică*** reprezintă un domeniu expresiv, greu de eludat, privind promovarea imaginii. Ansamblul măsurilor de protecție aplicate în spațiile în care sunt gestionate informații clasificate ce trebuie protejate împotriva accesului neautorizat, deteriorării, distrugerii, pierderii sau compromiterii, se află, de regulă, la vedere.

Măsurile de securitate fizică, aplicate în cadrul programelor de protecție fizică, urmăresc:

- să prevină pătrunderea neautorizată a persoanelor în spațiile protejate;
- să prevină, să descopere și să împiedice acțiunile ostile, de natură să afecteze securitatea informațiilor clasificate;
- să asigure condiții ca persoanele autorizate să intre în contact numai cu acele informații la care au dreptul pe baza certificatului de securitate și a principiului „nevoia de a cunoaște”

Programele vizând securitatea fizică cuprind măsurile active și pasive de protecție a informațiilor clasificate, care se referă la:

- stabilirea și delimitarea zonelor speciale de securitate;
- reglementarea și controlul accesului în zonele de securitate;
- paza și supravegherea zonelor de securitate.

**Securitatea documentelor** reprezintă aplicarea măsurilor și procedurilor de protecție pentru prevenirea sau detectarea acțiunilor ce pot conduce la pierderea sau compromiterea informațiilor clasificate, precum și pentru recuperarea informațiilor care au făcut obiectul unor asemenea acțiuni.

Domeniul „securitatea documentelor” stabilește măsurile ce trebuie aplicate de către toți cei ce utilizează informații clasificate, pe întreaga durată a ciclului de viață al acestora, corespunzător cu nivelul lor de clasificare, cu privire la aspectele presupuse de gestionarea informațiilor clasificate.

**Securitatea industrială** se referă la ansamblul măsurilor de protecție a informațiilor clasificate vehiculate în domeniul industrial, în legătură cu licitarea, negocierea și derularea unor contracte clasificate.

Asigurarea unei calități superioare a managementului informațiilor clasificate din domeniul industrial nu este doar un accesoriu obligatoriu, ci constituie o problemă de imagine națională, una din căile de acces în clubul select al națiunilor industrializate.

Reprezintă un *contract clasificat*, orice contract, încheiat în condiții legale, în cadrul căruia se cuprind și se vehiculează informații clasificate.

Participarea la negocieri în vederea încheierii unui contract clasificat este permisă în baza unei *autorizații de securitate industrială*, eliberată în urma unor verificări specifice, care confirmă aplicarea măsurilor minime de securitate prevăzute în standarde.

*Derularea unui contract clasificat* de către un agent economic se realizează în baza unui *certificat de securitate industrială*, eliberat în urma verificărilor specifice, care confirmă aplicarea măsurilor minime de

securitate prevăzute în standarde. Să ne imaginăm ce ar însemna să primească certificat pentru un contract NATO o firmă de apartament, fără bonitate, în imposibilitate să se achite de minime obligații. Imaginea României, a Guvernului, a ORNISS și a autorității care a făcut verificarea ar fi compromisă.

Verificările de securitate urmăresc ca:

- angajații, managerii sau proprietarii să dețină certificat de securitate corespunzător nivelului de clasificare al informațiilor la care vor avea acces;
- spațiile în care se vor gestiona informații clasificate să fie protejate corespunzător standardelor specifice;
- obiectivul industrial să fie stabil din punct de vedere economic, să nu fie implicat în litigii care îi pot afecta stabilitatea economică, să-și plătească obligațiile financiare și să nu prezinte riscuri de securitate.

**INFOSEC** reprezintă totalitatea măsurilor de securitate destinate protecției informației procesate, stocate ori transmise prin sisteme informatice și de comunicații sau alte sisteme electronice, împotriva pierderii confidențialității, integrității, disponibilității, autenticității și non-repudierii în mod accidental sau intenționat, precum și destinate prevenirii pierderii integrității ori disponibilității sistemelor, a serviciilor și resurselor acestora.

Domeniile de activitate specifice activității INFOSEC sunt: COMSEC (securitatea comunicațiilor), COMPUSEC (securitatea calculatoarelor), CRIPTO (securitatea criptografică) și TEMPEST (protecția împotriva radiațiilor ce pot compromite informația clasificată).

Am prezentat activitatea structurilor ORNISS cu unele realizări și limite insistând pe aspectele care influențează imaginea. S-au realizat unele rezultate și este bine să le scoatem în evidență. Prezint, spre edificare, aprecierile Comisiei NOS de inspecție (iunie 2005): *„sistemul românesc de protecție a informațiilor NATO se situează, la toate elementele din componența sa, deasupra standardelor obligatorii (over the top)”* iar, în final, să concluzioneze: *„nu a fost doar o inspecție, ci cunoașterea unei experiențe pozitive, ale cărei elemente vor fi aplicate și în alte țări membre ale Alianței”*.

De asemenea, Comisia de inspecție a Consiliului UE și a Comisiei Europene, constituită din experți ai structurilor de securitate (Oficiul de Securitate și Oficiul INFOSEC), a evidențiat *„conformitatea activităților desfășurate în cadrul ORNISS și ADS-uri cu prevederile Regulamentului*

*de Securitate al UE”, si a apreciat că „este asigurat un înalt grad de securitate” și „sunt create condiții pentru gestionarea informațiilor UE clasificate”*

Este evident că aceste aprecieri ale structurilor de profil din cele două organizații reprezintă contribuții la promovarea imaginii României, ele fiind aduse la cunoștința tuturor statelor membre ale acestora.

Doresc să mă refer în continuare, pe scurt, la alte aspecte importante ale activității ORNISS în procesul de implementare a reformei în domeniul protecției informațiilor clasificate, aspecte care evidențiază rolul important al instituției noastre în promovarea imaginii României.

#### **Negocierea acordurilor internaționale:**

ORNISS coordonează, la dispoziția primului-ministru, activitățile de negociere și încheiere a acordurilor internaționale de protecție a informațiilor clasificate cu statele membre ale NATO și UE, precum și cu alte state, avizează acordurile privind protecția informațiilor clasificate din domeniul apărării, inițiază sau avizează actele normative cuprinzând prevederi în materie.

Au fost semnate deja 5 acorduri, se află în procedura de semnare 2 acordurile bilaterale pentru protecția reciprocă a informațiilor clasificate, sunt în curs de negociere acorduri de securitate cu 8 state și cu alte 3 au fost întreprinse acțiuni pentru demararea negocierilor.

**Activitatea de relații internaționale** constituie o componentă importantă a activității desfășurate de ORNISS. Aceasta implică participarea la acțiuni organizate de NATO și UE, în scopul dezbaterii și clarificării unor aspecte de securitate relevante pentru perfecționarea sistemului național de protecție a informațiilor clasificate.

ORNISS asigură participarea specialiștilor săi în cadrul comitetelor, comisiilor și grupurilor de lucru organizate de Alianță și de UE pe problematica securității informațiilor clasificate, cu o prestație respectabilă și o contribuție esențială la imaginea țării.

#### **Cooperarea interinstituțională:**

În exercitarea atribuțiilor ce i-au fost conferite prin lege, ORNISS colaborează cu instituțiile cu responsabilități în domeniul protecției informațiilor clasificate.

Astfel, procesul de evaluare și verificare în vederea autorizării accesului la informații clasificate este coordonat de către ORNISS, ca

autoritate națională de securitate și este realizat împreună cu autoritățile desemnate de securitate. De asemenea, unele sarcini specifice din domeniile de competență ale ORNISS sunt realizate în colaborare cu alte instituții publice, în funcție de profilul activității acestora, cum ar fi: Ministerul Afacerilor Externe, Ministerul Economiei și Comerțului, Ministerul Comunicațiilor și Tehnologiei Informațiilor.

În vederea creării cadrului legal în materie, ORNISS a încheiat protocoale speciale cu autoritățile desemnate de securitate, care reglementează condițiile de cooperare pe domeniile specifice fiecărei activități.

Implementarea consecventă a reformei în domeniu, precum și stabilitatea și credibilitatea instituției, profesionalismul și experiența personalului, acumulate în decursul activității desfășurate, au contribuit la transformarea ORNISS într-un garant al eficienței sistemului de protecție a informațiilor NATO și naționale clasificate, precum și într-un partener al structurilor comunitare specializate în protecția informațiilor U.E. clasificate.

În ceea ce privește proiectele de viitor apropiat, ORNISS are în vedere continuarea reformei vizând: încheierea acordurilor de securitate cu fiecare din statele membre NATO; perfecționarea cadrului pentru protecția informațiilor UE clasificate; extinderea Sistemului Național de Registre și adaptarea acestuia la exigențele protejării, în perspectivă, a informațiilor UE; dezvoltarea cooperării cu autoritățile desemnate de securitate; consolidarea cooperării cu autoritățile naționale de securitate din țările membre NATO și UE.

Ca o recunoaștere a profesionalismului și seriozității cu care este abordată problema promovării imaginii tuturor structurilor implicate, inclusiv a țării, *nici unul din certificatele de securitate emise până în prezent de către ORNISS pentru acces la informațiile NATO sau UE clasificate nu a fost invalidat de Oficiul de Securitate al NATO (NOS) ori de Oficiul de Securitate al Consiliului UE.*

Un domeniu de activitate la fel de important îl constituie acreditarea de către ORNISS a sistemelor informatice și de comunicații (SIC) prin intermediul cărora sunt transmise informații ale Alianței Nord – Atlantice și ale Uniunii Europene. Faptul este deosebit de relevant ținând cont de participarea României la operațiuni de menținere a păcii inițiate de NATO, precum și la acțiuni similare desfășurate sub egida Uniunii Europene.

Sub aspectul perfecționării instrumentarului internațional, ORNISS participă la negocierea și încheierea de acorduri bilaterale și

internaționale privind protecția informațiilor clasificate, absolut indispensabile pentru realizarea schimbului de informații în cadrul activităților de cooperare la care va participa România.

Întrucât securitatea nu este un domeniul abstract, ci se realizează pentru oameni împreună cu oamenii, ORNISS își gestionează propria imagine printr-o contribuție substanțială la realizarea *educației de securitate*, prin organizarea de stagii de pregătire, seminarii și mese rotunde pe teme specifice pentru personalul din instituțiile publice care dețin și gestionează informații clasificate. Oficiul contribuie determinant la realizarea unei imagini favorabile României, prin realizarea unei *culturi de securitate* la nivelul societății, în primul rând al structurilor care utilizează informații clasificate, ca parte a culturii de securitate a Alianței și a Uniunii Europene.

**În concluzie**, se poate aprecia că România dispune în prezent de un sistem de protecție a informațiilor clasificate modern, deplin operațional, obiectiv, eficace și credibil, dezvoltat în jurul ORNISS, ca autoritate națională de securitate, edificat pe baza standardelor Alianței Nord-atlantice, îndeplinind integral cerințele de securitate ale acesteia și standardele de securitate ale Uniunii Europene. În acest mod, ORNISS contribuie în mod esențial la consolidarea rolului prefigurat pentru România, de furnizor de securitate și de imagine pozitivă.

### **Bibliografie:**

- Legea nr. 182/2002 privind protecția informațiilor clasificate;
- Hotărârea de Guvern nr. 353/2002 pentru aprobarea Normelor privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România.
- Hotărârea de Guvern nr. 781/2002 privind protecția informațiilor secrete de serviciu;
- Hotărârea de Guvern nr.585/2002 pentru aprobarea standardelor naționale de protecție a informațiilor clasificate în România;
- Ordonanța de urgență a Guvernului nr.153/2002 privind organizarea și funcționarea Oficiului Registrului Național al Informațiilor Secrete de Stat (ORNISS), aprobată prin Legea nr. 101/2003;
- Marius Petrescu, prof. univ. dr., Neculae Năbârjoiu, conf. univ. dr., *Managementul informațiilor*, Editura Bibliotheca, 2006;
- Marius Petrescu, prof. univ. dr., Constantin Romanoschi, prof. univ. dr., *"Contribuția Oficiului Registrului Național al Informațiilor Secrete de Stat la consolidarea rolului României ca furnizor de securitate"*, A XI-a sesiune de comunicări științifice, ANI, 08 aprilie 2005, vol.I;
- Stan Petrescu, gl. bg.(r), dr., *"Informațiile – a patra armă"*, Editura militară, 1999.