

DEPARTAMENTUL PENTRU STUDII PARLAMENTARE ȘI POLITICI U.E.

DIRECȚIA STUDII ȘI DOCUMENTARE LEGISLATIVĂ

**REGLEMENTĂRI PRIVIND INFORMAȚIILE CLASIFICATE
ÎNTR-O SERIE DE STATE MEMBRE ALE UNIUNII EUROPENE**

APRILIE 2016

Documentare și sinteză: Cristina Grecu, consilier parlamentar
Florentina Rădulescu, consilier parlamentar
Dan Alexandreanu, consilier parlamentar

Sinteza documentară poate fi accesată direct pe Intranet la pagina Direcției studii și documentare legislativă

Lucrările elaborate în cadrul Direcției studii și documentare legislativă sunt cu caracter documentar și nu reprezintă punctul de vedere al Camerei Deputaților.

GERMANIA

Cadrul legal:

- Legea cu privire la condițiile și procedura de verificare a securității persoanelor și clasificării documentelor la nivel federal

Legea reglementează condițiile și procedura de verificare a unei persoane care urmează să fie încredințată de către autoritatea competentă cu o sarcină de natură sensibilă, respectiv¹:

1. are acces la informații clasificate sau desfășoară activități care impun utilizarea de informații clasificate: TOP SECRET, SECRET, CONFIDENȚIAL;
2. are acces la informații clasificate privind instituțiile și organisme guvernamentale sau le poate procura;
3. își desfășoară activitatea într-o autoritate sau orice altă entitate publică a Federației, care a fost declarată ca urmare a domeniului de activitate ca deținătoare de informații clasificate de către autoritatea federală supremă competentă, în consultare cu Ministerul Federal de Interne, autoritatea națională pentru protecția și siguranța informațiilor;
4. lucrează cu informații clasificate în temeiul deținerii unui certificat de securitate.

Persoanele care nu au cetățenie germană pot să-și desfășoare activitatea în instituțiile menționate mai sus, în urma semnării de acorduri între statele respective, care fac referire la accesul la informațiile clasificate, doar ulterior verificărilor de siguranță realizate de instituțiile germane de resort.

Activități cu caracter sensibil din punctul de vedere al siguranței naționale sunt efectuate și în zona de activitate a Ministerului Apărării. Potrivit legii, în aceste sectoare de activitate trebuie asigurate măsuri stricte de securitate pentru prevenirea acțiunilor de sabotaj și scurgeri de informații.

În mod vital, în aceste structuri se are în vedere evitarea deteriorării lor din cauza riscurilor operaționale inerente, evitarea punerii în pericol a sănătății sau vieții unor segmente largi ale populației sau personalului care desfășoară activități indispensabile pentru funcționarea comunității și a căror perturbare ar constitui un risc pentru securitatea sau ordinea publică.

Persoanele care urmează să-și desfășoare activitatea cu informații clasificate sunt supuse în prealabil unui control de securitate. Partenerii de viață ai acestor persoane sunt incluse în controlul de securitate în conformitate cu prevederile legale, excepțiile fiind decise de către autoritatea competentă.

Aceste prevederi nu se aplică membrilor organismelor constituționale federale, judecătorilor, în măsura în care își îndeplinesc atribuțiile de drept, cetățenilor străini care urmează să-și exercite profesia în Germania, în interesul organismelor interguvernamentale și a agențiilor care desfășoară activități sensibile din punctul de vedere al siguranței naționale.

Informațiile clasificate reprezintă cerința confidențialității în faptele de interes public, obiecte sau descoperiri, indiferent de forma lor. Ele sunt clasificate în funcție de nevoia lor de protecție pentru un organism oficial:

¹ https://www.gesetze-im-internet.de/s_g/BJNR086700994.html#BJNR086700994BJNG000100307

- informații clasificate *TOP SECRET*, atunci când dezvăluirea acestora pot amenința existența sau interesele vitale ale Germaniei sau ale unui land;
- informații *SECRETE*, atunci când dezvăluirea acestora pot afecta securitatea Germaniei sau ale unui land sau pot provoca vătămări grave ale intereselor lor;
- informații *CONFIDENȚIALE*, atunci când dezvăluirea acestora este dăunătoare pentru interesele Germaniei sau ale unui land.
- informații cu *UTILIZARE RESTRICTIVĂ*, atunci când dezvăluirea acestora este dăunătoare pentru interesele Germaniei sau ale unui land.

Exemple de clasificare:

a) clasificarea ca informații cu indicativul TOP SECRET poate fi avută în vedere, printre altele, pentru

- părți ale planului de alarmă al Forțelor Armate Federale,
- informații generate de Serviciul Federal de Informații,
- alte documente compilații, care au toate elementele pentru a fi clasificate ca SECRETE, dar sunt clasificate TOP SECRET pe ansamblu.

b) clasificarea cu indicativul SECRET poate fi avută în vedere, printre altele, pentru

- informații cu privire la „campania electronică” a Forțelor Armate Federale;
- părți ale planului de alarmare al Forțelor Armate Federale;
- documentația privind infrastructurile critice;
- documente de stat și tratate importante ale Germaniei;
- criptodatele utilizate pentru criptarea documentelor clasificate cu indicativul CONFIDENȚIAL sau superior,
- compilații sau elemente care sunt clasificate cu indicativul CONFIDENȚIAL, dar sunt clasificate SECRET pe ansamblu.

c) clasificarea cu indicativul CONFIDENȚIAL poate fi avută în vedere, printre altele, pentru

- rapoartele de investigare în cazurile de spionaj;
- constatări privind metodele de lucru ale organizațiilor teroriste/extremiste, a căror divulgare ar pune în pericol activitatea viitoare de observare/recunoaștere;
- pozițiile de negociere de politică externă, a căror prezentare prematură ar fi în detrimentul intereselor statului german;
- documentația privind infrastructurile critice;
- documente de stat și tratate ale Germaniei;
- invenții importante, secrete comerciale ale companiilor sau alte fapte cu caracter privat; aspecte sau constatări a căror cunoaștere de către persoane neautorizate pot dăuna interesele statului federal;
- planuri ale rețelelor de calculatoare și a datelor de configurare ale sistemelor folosite de către departamentele care utilizează informații clasificate.

Prin risc de securitate se înțelege:

- punerea sub semnul întrebării a fiabilității unei persoane în exercitarea activităților de natură sensibilă;
- apariția unui pericol particular, de natura tentativelor de publicitate realizate de către serviciile de informații străine, în special privind șantajul
- punerea sub semnul îndoielii a angajamentului persoanei care desfășoară activități de natură sensibilă.

Un risc de securitate poate fi, de asemenea, starea de fapt privind persoana soțului/partenerului persoanei care exercită activități de natură sensibilă.

Structurile responsabile pentru controalele de autorizare de securitate sunt:

a). o autoritate sau o agenție publică aparținând guvernului federal care dorește să atribuie sau să delege atribuții de gestionare a informațiilor clasificate unei persoane angajate;

b). Ministerul de Interne, în ceea ce privește resortisanții germani în legătură cu activitatea desfășurată de aceștia într-o zonă de lucru cu securitate sensibilă;

c). partidele politice, în conformitate cu art. 21 din Legea fundamentală, precum și fundațiile afiliate acestora, pentru propria activitate;

d). o autoritate sau o agenție publică aparținând Guvernului Federal care dorește să transmită informații clasificate către o organizație non-publică.

e). o autoritate sau o agenție publică a Federației care îndeplinește, pe baza unei ordonanțe, sarcini de gestionare a informațiilor clasificate și intenționează să încredințeze unei persoane atribuții în acest domeniu.

Oficiul Federal pentru Protecția Constituției are atribuții în verificarea certificatului de securitate, în conformitate cu prevederile Legii federale pentru protecția Constituției, respectiv, Serviciul militar de contrainformații, în conformitate cu prevederile Legii privind serviciile de contrainformații militare.

În conformitate cu tipul informațiilor clasificate gestionate în activitatea desfășurată, persoana în cauză poate fi supusă următoarelor tipuri de verificări:

1. o verificare de securitate simplă;
2. o verificare de securitate extinsă;
3. un control de securitate extins, inclusiv investigații de securitate.

Verificarea de securitate simplă se efectuează pentru persoanele care urmează să aibă acces la informații confidențiale.

Verificarea de securitate extinsă se efectuează pentru persoanele care au acces la informații clasificate tip SECRET sau informații de tip CONFIDENȚIAL.

O verificare de securitate extinsă, inclusiv investigații de securitate se efectuează pentru persoanele care au acces la informații clasificate TOP SECRET sau informații clasificate tip SECRET, sau care lucrează pentru un serviciu de informații federale, autoritate sau agenție aparținând guvernului federal.

Orice persoană care primește fișiere, modifică, distribuie sau pune la dispoziția terților informații, prin proceduri automatizate, fără autorizație, se pedepsește cu închisoare de până la un an sau amendă.

De asemenea, orice persoană care transmite date protejate cu caracter personal, informații false, sau care sunt utilizate în alte scopuri, cu intenția de a face rău unei alte persoane, se pedepsește cu închisoare de până la doi ani sau amendă.

Urmărirea penală se declanșează numai la cererea persoanei vătămate.

În conformitate cu prevederile art. 4 alin (1) al Legii privind autorizarea accesului de securitate (1994), cu modificările ulterioare, documentele clasificate reprezintă orice fapte, obiecte sau informații care au nevoie să fie păstrate secrete față de interesul public, indiferent de forma lor (de exemplu documente, desene, hărți, fotocopii, materiale fotografice, fișiere electronice și de date, semnale electrice, aparate, echipamente tehnice sau cuvinte vorbite).

În funcție de nevoia lor de protecție, acestora li se atribuie niveluri de clasificare de către un organism oficial.

Orice material intermediar care rezultă în legătură cu materialele clasificate (de exemplu fișiere de calculator, versiuni anterioare, stenograme, înregistrări sonore, folii transparente sau versiuni ale acestora, copii incorect imprimate) trebuie considerate ca fiind materiale clasificate în sensul alineatului anterior. Pentru aceste materiale intermediare pot fi prevăzute excepții doar în ceea ce privește marcarea, înregistrarea și distrugerea lor.

În cazul în care natura materialelor face imposibilă punerea în aplicare a vreunui nivel de protecție, conform clasificării materialelor clasificate, instrucțiunile legale trebuie aplicate *mutatis mutandis*, în măsura posibilului, prin măsuri de securitate echivalente.

Principii generale

1. Materialele clasificate pot fi consultate numai de către persoanele care au nevoie să facă acest lucru pentru îndeplinirea sarcinilor lor de serviciu. Se respectă principiul „*need-to-know*”.

2. Orice persoană însărcinată sau care primește acces la materiale clasificate, indiferent de modul în care materialul a ajuns în posesia lor, este responsabilă pentru păstrarea în siguranță și gestionarea corespunzătoare a acestuia, pentru menținerea securității conținutului său, în conformitate cu instrucțiunile legale aplicabile informațiilor clasificate.

3. Măsurile de tip *state-of-the-art* trebuie luate pentru protejarea materialelor clasificate împotriva oricărui risc de pierdere a confidențialității, disponibilității sau integrității lor.

În cadrul sferei lor de activitate, șefii de departament sunt responsabili pentru buna desfășurare a lucrărilor ce implică utilizarea documentelor clasificate, respectiv activități de consultare, producție, reproducere, gestionare, transmitere electronică, distrugere sau alte utilizări, precum și pentru punerea în aplicare a instrucțiunilor cu aplicabilitate în domeniul materialelor clasificate.

Șefii de departamente majore pot delega sarcinile care le revin în acest domeniu, în totalitate sau în parte, unui membru al personalului care își desfășoară activitatea în departamentele respective.

Autoritățile federale de nivel mediu și instituțiile de drept public echivalente, aflate sub control federal direct, trebuie să desemneze un agent de securitate și un adjunct autorizat atunci când desfășoară activități ce implică utilizarea de documente clasificate.

Departamentele cu specific legat de tehnologia informației trebuie să aibă în componență agenți de securitate. Personalul angajat în structurile respective trebuie să respecte toate măsurile de securitate impuse pentru situațiile de utilizare de documente clasificate.

Orice departament care lucrează ocazional cu materiale clasificate trebuie să se asigure că securitatea documentației este păstrată, în conformitate cu prevederile legale.

Documentația de securitate trebuie actualizată atunci când există modificări relevante, ea trebuind să fie revizuită cel puțin o dată la doi ani.

Documentația poate fi păstrată în format electronic. În cazul în care doar o parte din personal lucrează cu documente clasificate, trebuie luate măsuri tehnice de protecție adecvate, fiabile, care să cuprindă și semnăturile electronice calificate ale persoanelor respective.

Oficiul Federal pentru Securitatea Informației (BSI) trebuie să urmărească punerea în aplicare a instrucțiunilor privind materialele clasificate. Acesta are obligația de a consilia și de a acorda asistență departamentelor care lucrează cu materiale clasificate și pot obține informații privind aplicarea instrucțiunilor în domeniu. BSI poate apela la serviciile altor organisme de sprijin pentru îndeplinirea acestor sarcini, acest lucru necesitând aprobarea prealabilă a Ministerului Federal de Interne pentru fiecare caz în parte.

Oficiul Federal pentru Protecția Constituției, Oficiul pentru Contrainformații Militare și Serviciul Federal de Informații au obligația de a informa BSI, fără întârziere, cu privire la orice informație cu relevanță pentru protecția fizică a materialelor clasificate. În cazul în care o astfel de informație se referă la securitatea comercială și industrie, structura care trebuie informată este Ministerul Federal al Economiei și Tehnologiei.

Organismul emitent sau succesorul său legal trebuie să clasifice sau să declassifice materialele de îndată ce motivele pentru care a fost stabilit un anumit nivel de clasificare încetează să se aplice. Organismul emitent sau succesorul său legal trebuie să notifice schimbarea încadrării documentului tuturor destinatarilor materialului clasificat, în scris sau prin e-mail, utilizând o semnătură electronică calificată sau metode similare sigure.

Materialele clasificate cu indicativul RESTRICȚIONAT nu pot fi reclasificate pe o treaptă superioară, cu excepția cazului în care au fost notificați toți destinatarii materialului clasificat inițial. În cazul în care clasa de clasificare a fost redusă sau nu se mai aplică în aceeași măsură de la o anumită dată, acest lucru trebuie să fie menționat în mod clar pe materialele clasificate sau în documentația de însoțire.

Materialele clasificate trebuie să fie desecretizate după 30 de ani, cu excepția cazului în care, inițial, au fost stabilite perioade mai scurte sau mai lungi. Termenul curge de la data de 1 ianuarie în anul următor de clasificare și nu este afectat de nici o modificare a nivelului de clasificare.

Specificarea unei perioade este supusă următoarelor modificări:

- perioada poate fi prelungită cu până la 30 de ani, cu motive temeinice;
- termenul poate fi prelungit pentru documente individuale sau în întregul lor.

Prelungirea necesită aprobarea autorității federale relevante.

- perioada prelungită trebuie să fie menționată pe prima pagină a proiectului final al materialului clasificat și pe toate exemplarele inițiale. Pentru materialele clasificate în alte forme (de exemplu, aparatele), acest lucru trebuie să se aplice pe documentele de însoțire.

Prelungirea perioadei de la o dată ulterioară, trebuie să fie tratată în modul similar precizat mai sus.

În cazul în care materialele clasificate sunt în custodia Arhivelor Federale, secțiunea secret, notificarea trebuie să fie trimisă către această instituție.

Pentru materialele clasificate secretizate pe o perioadă mai mare de 30 de ani, în momentul intrării în vigoare a instrucțiunilor privind documentele clasificate, organismul emitent sau succesorul său legal poate decide prelungirea perioadei de clasificare. Pentru ca perioadele de prelungire să fie luate în considerare, autoritatea federală supremă competentă poate stabili o perioadă de tranziție de până la cinci ani, pentru care un astfel de material rămâne clasificat conform prevederilor inițiale. Această ultimă prevedere nu se aplică în cazul materialelor clasificate de instituții străine sau internaționale. Un astfel de material poate fi

reclasificat sau declasificat numai de către organismul emitent, cu excepția cazurilor în care există dispoziții contrare prevăzute de acordurile internaționale.

Înainte ca o persoană să aibă acces la materiale clasificate de tip CONFIDENȚIAL sau mai înalt, aceasta trebuie să fie verificată în conformitate cu prevederile Legii privind autorizarea accesului de securitate.

Accesul la materiale clasificate poate fi obținut de către persoane fizice care:

- transportă materiale clasificate în calitate de mesager sau curier;
- asigură paza materialelor clasificate în zonele de păstrare sau de securitate;
- lucrează într-o zonă de securitate;
- instalează sisteme de alarmă sau desfășoară activități de service pentru dispozitivele care protejează materialele clasificate;
- gestionează chei, cifruri sau numere combinate pentru dispozitivele în care se păstrează materialele clasificate (seifuri sau alte sisteme de protecție).

Producerea de materiale clasificate se realizează numai în unități desemnate în acest scop. Numărul de exemplare produse, precum și orice material intermediar clasificat care rezultă, trebuie să fie indicat în proiectul final, înregistrate cu o semnătură electronică calificată.

Pentru materialele clasificate drept TOP SECRET sau SECRET, fiecare copie primară trebuie să aibă un număr de serie, plasat în partea de sus a primei pagini, în cazul documentelor. Pentru alte forme de materiale clasificate, același lucru trebuie să se aplice obligatoriu în fișa de însoțire.

După ce a fost lucrat în format electronic, documentul clasificat drept confidențial trebuie criptat cu ajutorul unui program aprobat de BSI pentru nivelul respectiv de clasificare și stocat în conformitate cu prevederile legale.

Reproducerea materialelor clasificate are o serie de norme specifice:

1. Normele de securitate se aplică tuturor reproducerilor (fotocopii, exemplare tipărite, foi matricole, extracte, replici, etc.);
2. Pentru materialele clasificate TOP SECRET, reproducerile necesită acordul organismului emitent, care urmează să fie afișat pe materialele clasificate. Pentru materiale clasificate cu indicativul SECRET sau CONFIDENȚIAL, destinatarul poate decide dacă reproducerea este permisă, având în vedere respectarea principiului „need-to-know”, cu excepția situației în care organismul emitent decide faptul că materialele nu pot fi reproduse.
3. Numărul de reproduceri de materiale clasificate trebuie să fie menționat pe acestea, iar reproducerile trebuie să fie înregistrate fără întârziere. Același lucru trebuie să-l facă și destinatarul materialelor, în cazul transmiterii electronice.
4. Departamentele în care sunt produse și reproduse materiale clasificate cu indicativul CONFIDENȚIAL sau mai înalt trebuie să desemneze unități specifice cu personal de securitate pentru protejarea acestor operațiuni (control dublu).
5. În cazul utilizării fotocopiatoarelor și echipamentelor multifuncționale cu memorie non-volatilă, se aplică normele BSI.

Nivelul de clasificare trebuie să fie prezentat în mod clar în întregime, cu majuscule, pe materiale clasificate, în așa fel încât să fie diferit de orice altă scriere. În cazul în care un material deține mai mult de un articol de clasificare, acesta trebuie să fie marcat cu cel mai înalt nivel de clasificare.

În cazul în care materialele clasificate sunt reclasificate sau declasificate, marcarea acestora urmează să fie modificată sau ștearsă de către serviciile

emitente sau de către destinatari. Modificarea sau ștergerea marcajelor trebuie să fie evidențiată prin scrierea inițialelor persoanei care a întreprins acțiunea și data la care a fost înregistrată. În cazul în care natura materialelor clasificate nu permite marcarea, de exemplu, în cazul componentelor miniaturizate, aceste dispoziții trebuie să se aplice, *mutatis mutandis*, pe documentele de însoțire.

Materiale clasificate cu indicativul CONFIDENTIAL sau mai înalt, trebuie să fie păstrate în registrele de materiale clasificate. În timpul în care nu este în uz, materiale clasificate cu indicativul CONFIDENTIAL sau mai înalt, trebuie să fie închis într-un spațiu de depozitare adecvat (dulapuri securizate). Pentru materialele clasificate drept TOP SECRET sau SECRET, acest lucru este valabil chiar și în timpul oricăror absențe scurte a persoanelor care lucrează sau gestionează aceste materiale. Materialele clasificate cu indicativul CONFIDENTIAL pot fi lăsate în birou pe perioada unei absențe scurte, cu condiția ca ușa biroului să poată fi blocată cu ajutorul unui dispozitiv de securitate.

În afara perioadei de lucru, un material clasificat trebuie să fie păstrat într-un spațiu corespunzător, care să fie supravegheat printr-un sistem de alarmare. Pentru materialele clasificate cu indicativul CONFIDENTIAL sau SECRET, se poate renunța la supravegherea acestora în situația în care clădirea sau partea clădirii unde sunt depozitate este păzită sau este supravegheată tehnic, sau materialul este stocat doar temporar în imobilul respectiv.

Consultarea și deținerea documentelor clasificate trebuie să fie înregistrată prin intermediul unor registre de materiale clasificate, documente de primire, note de însoțire, formulare, înregistrări de transfer sau de distrugere.

Înregistrările pot fi păstrate în format electronic, în măsura în care este posibil, utilizând sistemele de înregistrare a materialelor clasificate aprobate de BSI.

Înregistrările materialelor clasificate trebuie păstrate timp de cel puțin cinci ani. Pentru registrele în care sunt înscrise documentele clasificate, această perioadă curge din momentul declasării la nivelul RESTRICȚIONAT, declasificării, depunerii sau distrugerii tuturor materialelor clasificate înregistrate în ele. Pentru cărțile clasificate ca materiale clasificate, chitanțe, înregistrări de transfer și înregistrările privind distrugerea, perioada curge de la data eliberării sau data ultimei intrări.

Materialele clasificate drept copii pe suporturi de date trebuie tratate în același fel ca și originalul clasificat, în conformitate cu instrucțiunile BSI, cheile de criptare fiind ținute în mod separat.

Materiale clasificate ca RESTRICȚIONATE trebuie să fie depozitate și gestionate separat de cele neclasificate sau înregistrate cu indicative de securitate superioare.

Furnizarea de materiale clasificate germane către departamentele de specialitate ale unor țări străine sau ale organizațiilor internaționale necesită un acord/convenție de securitate care reglementează un astfel de schimb.

Documentele clasificate ca RESTRICȚIONATE pot fi, de asemenea, furnizate departamentelor țărilor străine fără nici un fel de acord de securitate, cu condiția ca:

- a). aceste materiale să fie necesare în activități oficiale;
- b). beneficiarul a fost informat cu privire la cerința de securitate;
- c). departamentul străin trimite structurii germane o asigurare în scris că va proteja materialele clasificate, în conformitate cu propriile norme naționale.

În situațiile în care nu sunt încheiate acorduri/convenții de securitate, Ministerul Federal de Interne trebuie să fie informat în vederea încheierii unui astfel de acord.

În cazuri excepționale, materiale clasificate cu indicativul CONFIDENTIAL pot fi furnizate departamentelor din țările cu care nu există nici un acord de securitate, cu condiția ca:

- cerințele enumerate la literele a) - c) să fie îndeplinite;
- beneficiarul declară în scris că numai personalul specific, verificat din punctul de vedere al securității, va primi acces la documentele clasificate germane;
- departamentul german va ține evidența informațiilor schimbate;
- departamentul german trimite către Ministerul Federal de Interne o copie a asigurării scrise;
- furnizarea de materiale clasificate cu indicativul TOP SECRET sau SECRET către departamente din țări străine trebuie să fie aprobată de către autoritatea federală cu atribuții în domeniu, în fiecare caz în parte.

Materialele clasificate cu indicativul CONFIDENTIAL sau mai înalt, pot fi scoase dintr-o clădire securizată numai pentru participările la conferințe, întâlniri, discuții, etc.

Materialele clasificate cu indicativul SECRET sau TOP SECRET pot fi scoase din clădirea securizată numai dacă este strict necesar, pentru aceasta fiind necesară aprobarea șefilor de departamente sau autoritățile federale cu atribuții în domeniu. Cheile de criptare se transportă separat. Transportul este permis cu condiția ca materialul clasificat să fie stocat pe un sistem informatic aprobat prin instrucțiunile BSI sau protejat într-un mod similar.

În afara țării, materiale clasificate cu indicativul CONFIDENTIAL sau mai înalt trebuie expediate prin misiunea diplomatică din acel stat, în măsura în care acest lucru este posibil. În caz contrar, Ministerul Afacerilor Externe sau misiunea diplomatică din străinătate trebuie să ambaleze și să sigileze materialele clasificate și să emită un certificat de autorizare pentru transport.

Transportul documentelor clasificate cu indicativul SECRET sau TOP SECRET nu pot fi transportate prin sistemul internațional de curierat.

Orice material clasificat care nu a fost acceptat de către arhivele relevante de profil urmează să fie distrus în așa fel încât conținutul său să fie de nerecunoscut și de nerefăcut.

Materialele clasificate cu indicativul CONFIDENTIAL sau mai înalt, pot fi distruse numai în baza aprobării unei persoane care lucrează cu documente de acest tip. Managerul respectiv trebuie să verifice dacă materialul este clasificat și îl distruge în prezența unui martor.

Registrul de documente clasificate trebuie să conțină informații privind materialul ce a fost distrus: indicativul materialului, părțile care au fost distruse (inclusiv copiile existente), data distrugerii, numărul de pagini, numele persoanei care a dat ordinul de distrugere, numele martorului.

Materialele intermediare pot fi distruse fără prezența unui martor.

Măsurile de protecție a documentelor clasificate vizează următoarele aspecte:

- criptarea materialelor cu indicativul CONFIDENTIAL sau mai înalt, pentru protejarea împotriva accesului autorizat;

- stabilirea de zone de securitate comune pentru unitățile de lucru și persoanele implicate în gestionarea cu materiale clasificate similare;
- stabilirea de zone de securitate adecvate ca volum, modalitate de control și dotare tehnică, potrivit importanței materialelor clasificate.

Mijloacele tehnice de protecție a materialelor clasificate trebuie să îndeplinească următoarele cerințe:

- a) facilitățile de păstrare și seifurile trebuie să fie proiectate în așa fel încât:
 - accesul să poată fi făcut numai după identificarea și autentificarea cu acuratețe a persoanelor respective (date biometrice), celelalte elementele de acces trebuind să fie protejate împotriva copierii neautorizate.
 - accesul neautorizat să fie identificabil imediat;
 - accesul forțat în spațiile respective să nu poată fi făcut prin forță.
- b) sistemele de alarmă trebuie să fie proiectate și instalate în așa fel încât:
 - să detecteze efectiv orice intrus;
 - să nu poată fi dezinstalat de oricine persoană fără atribuții în domeniu, cu excepția cazului în care persoana a fost identificată pentru prima oară în mod efectiv prin intermediul datelor biometrice.
 - alarmarea să se facă la punctul de securitate al spațiului respectiv.
 - să nu poate fi eludat în mod clandestin.
- c) containerele pentru transportul materialelor clasificate și ambalajele pentru scrisori sau colete trebuie să fie proiectate astfel încât orice acces neautorizat la conținutul lor să devină evident.
- d) ușile și încuietorile sau sistemele electronice de control al accesului pentru camere trebuie să prezinte dispozitive anti-bruiere, care să nu permită instalarea nelegală a dispozitivelor de ascultare;
 - cheile, cifrurile sau alte modalități de deschidere trebuie să fie protejate împotriva copierii.

Paza materialelor clasificate impune următoarele elemente:

- cel puțin două persoane care să poată vedea în mod direct sau prin mijloace tehnice zonele de protecție stabilite, pentru a detecta și respinge orice atac, chiar prin forța armelor și care să poată raporta imediat situația de fapt personalului de securitate din clădire;
- patrulare care să fie efectuate la intervale neregulate, în cursul unei perioade stabilite;
- supravegherea tehnică a materialelor clasificate prin intermediul unui sistem de alarmă care să poată alarma în timp real personalul de securitate al clădirii;
- supravegherea prin intermediul unui sistem de monitorizare care să detecteze orice intruziune neautorizată și care să poată alarma în timp real personalul de securitate al clădirii.

Camerele de stocare a materialelor clasificate trebuie să fie echipate cu dispozitive anti-bruiere și trebuie să îndeplinească următoarele cerințe:

- a) să fie protejate împotriva accesului neautorizat;
- b) să posede o atenuare acustică adecvată pentru împiedicarea înregistrărilor exterioare neautorizate;
- c) dacă sunt echipate cu sisteme de telecomunicații, trebuie să nu permită înregistrările exterioare neautorizate;
- d) să fie proiectate astfel încât să permită ascunderea dispozitivelor de supraveghere ale sistemului de securitate al clădirii;

e) să permită luarea măsurilor de precauție, astfel încât dispozitivele anti-bruieră să nu poată fi folosite abuziv în alte scopuri.

Numerele combinate ca mijloc de acces la materialele clasificate (cifruri) se păstrează în plicuri cu indicativul CONFIDENȚIAL, în condiții de siguranță, sub cheie, și trebuie cunoscute doar de utilizatori. Acestea nu trebuie să constea din numere sau grupuri de cifre/litere ușor de găsit, cum ar fi datele personale, numere de telefon sau serii aritmetice.

Numerele combinate ca mijloc de acces la materialele clasificate trebuie să fie modificate astfel:

- după achiziția publică realizată;
- după orice deschidere a porților de acces în absența utilizatorilor;
- în cazul în care se suspectează cunoașterea neautorizată a combinației;
- la intervale regulate, de cel mult 12 luni.

Produce cu funcții de securitate în domeniul tehnologiei informației, care sunt achiziționate pentru a fi utilizate pentru protejarea materialelor clasificate trebuie să îndeplinească următoarele funcții:

- 1) generarea de coduri-cheie;
- 2) criptare;
- 3) ștergerea sau distrugerea suporturilor de date;
- 4) îndeplinirea obiectivelor de securitate;
- 5) protecția liniilor de transport;
- 6) separarea rețelelor cu diferite niveluri maxime de clasificare pentru materialul prelucrat.

Aceste produse trebuie să fie aprobate de către BSI. Omologarea trebuie să includă, de asemenea, specificațiile necesare privind condițiile de utilizare și de funcționare. Punctele 3-6 nu se aplică în cazul materialelor clasificate cu indicativul RESTRICȚIONAT.

- 7) control al accesului la sistem;
- 8) producerea de materiale clasificate;
- 9) conservarea probelor;
- 10) prevenirea tentativelor de modificare a sistemelor informatice;
- 11) înregistrarea și stocarea documentelor.

Transmiterea materialelor clasificate prin sistemul de telecomunicații se realizează astfel:

- materialele clasificate trebuie să fie criptate, prin utilizarea unui sistem de criptare aprobat de către BSI pentru nivelul de clasificare relevant. În cazul în care nu sunt disponibile programe și echipamente omologate de BSI pentru a fi utilizate cu transmiterea de materiale clasificate drept RESTRICȚIONATE, se pot utiliza produse certificate de BSI, în conformitate cu criteriile comune stabilite la nivel național.

- prin derogare de la prima teză a alin. 1, transmiterea necriptată poate fi utilizată în următoarele cazuri:

1) în cazul în care problema este deosebit de urgentă, iar transmiterea prin alte mijloace sigure ar provoca o întârziere nejustificată:

a. pentru convorbiri telefonice cu privire la chestiuni clasificate ca fiind confidențiale, pe o linie aprobată pentru documente RESTRICȚIONATE;

b. pentru apelurile telefonice cu privire la chestiuni clasificate drept confidențiale, pe o linie neprotejată.

2) pentru e-mail-uri, faxuri sau telexuri urgente, clasificate ca RESTRICȚIONATE, în cazul în care expeditorul și destinatarul nu au nici o facilitate de criptare sau alte mijloace de protecție (cum ar fi o parolă) pentru modul corespunzător de transmisie.

3) în cazuri excepționale, cu acordul șefului de departament sau al instituției relevante, pentru transmiterea de materiale clasificate cu indicativul CONFIDENTIAL sau SECRET (cu condiția ca acesta să nu fie marcat pentru aplicarea unui tratament special, cum ar fi criptografia), în cazul în care:

- a. expeditorul și destinatarul nu au nici o facilitate de criptare;
- b. materialele clasificate nu pot fi transmise în timp util prin alte mijloace și orice întârziere ar provoca în mod clar un prejudiciu mai important decât prejudiciul determinat de divulgarea materialului clasificat.

Întreținerea și repararea sistemelor informatice pe care sunt stocate materiale clasificate cu indicativul CONFIDENTIAL sau mai înalt, trebuie să se realizeze după eliminarea acestor materiale din sistemul informatic. În cazul în care acest lucru nu este posibil, activitatea de service trebuie realizată de personal specializat, verificat, în conformitate cu prevederile legale.

Activitatea de service sau de reparare a unui sistem informatic nu poate fi în mod normal efectuată în timp ce se realizează sau se transmite un document clasificat.

Service-ul la distanță este permis numai în cazul în care:

- este efectuat de către personalul autorizat, verificat;
- sistemele criptografice utilizate pot fi întreținute de la distanță;
- se aplică un control în timp real a operațiunilor de service desfășurate la distanță;
- fiecare procedură de service la distanță este lansată separat și terminată, înainte de lansarea alteia.

Fără a aduce atingere prevederilor anterioare, agenții de securitate pot permite unei firme să efectueze service la distanță în cazul în care orientările de securitate au fost verificate de către Ministerul Federal al Economiei și Tehnologiei sau de către o altă autoritate federală.

Ca răspuns la orice situație în care de descoperă o încălcare a normelor de securitate sau se descoperă o vulnerabilitate de securitate, agenții de securitate ai departamentului trebuie să se stabilească faptele existente. Aceștia trebuie să ia toate măsurile necesare pentru a preveni sau de a reduce prejudiciile și pentru a evita repetarea. Dacă investigațiile inițiale evidențiază implicarea unor servicii de informații străine sau un act de trădătoare, trebuie informate imediat Oficiul Federal pentru Protecția Constituției sau Oficiul pentru Contrainformații Militare.

În cazul în care orice material clasificat cu indicativul CONFIDENTIAL sau mai înalt a ajuns la cunoștința unei persoane neautorizate, organismul emitent trebuie să fie informat și să ia măsurile necesare pentru a preveni sau a reduce orice prejudiciu (de exemplu, prin schimbarea planurilor sau intențiilor de notificare a altor structuri).

În cazul în care material german clasificat ajuns la cunoștința unei persoane neautorizate are o importanță considerabilă, Ministerul Federal de Interne, în calitate de autoritate de securitate națională, trebuie să fie informat fără întârziere.

În cazul în care orice mijloc de acces la incintele de depozitare ale materialelor clasificate (cum ar fi parole, chei sau cartele cu cip, etc) este distrus, pierdut sau a intrat în posesia unei persoane neautorizate, acestea trebuie

înlocuite, iar activitatea desfășurată în acel spațiu este restricționată sau suspendată.

SUEDIA

Cadrul legal:

- Legea privind accesul la informații publice și secrete

În Suedia, regimul informațiilor clasificate este reglementat de *Legea privind accesul la informații publice și secrete*², intrată în vigoare la 30 iunie 2009.

Legea conține prevederi referitoare la aplicarea principiului accesului publicului la informațiile deținute de către autoritățile publice și anumite organisme private.

De asemenea, acest act reglementează atât secretul documentelor cât și obligația de confidențialitate. Secretizarea atrage după sine restricții atât asupra dreptului publicului de a obține documente oficiale cât și dreptul funcționarilor publici la liberă exprimare.

Legea conține și prevederi referitoare la cazurile în care o clauză de confidențialitate în conformitate cu dispozițiile privind secretul limitează dreptul la informații publice, în conformitate cu Legea Libertății Presei, respectiv Legea fundamentală privind libertatea de exprimare.

Principii

Toți cetățeni suedezi și străini au dreptul să cunoască documentele deținute de către autoritățile publice, acest drept fiind restricționat în două situații:

- Publicul se bucură numai de dreptul de a cunoaște documentele considerate oficiale. Nu toate documentele unei autorități publice sunt, de fapt, considerate a fi documente oficiale.

- O serie de documente oficiale sunt secrete. Aceasta înseamnă că publicul nu are dreptul să cunoască conținutul acestui tip de documente, iar autorităților publice le este interzisă publicarea lor.

Manipularea documentelor oficiale de către autoritățile publice

- Operațiunea de clasificare

În cazul în care un document oficial conține informații pentru care se poate aplica secretizarea, autoritatea poate marca acest lucru printr-o notă specială, o stampilă de „secret”. În cazul unui document pe hârtie, nota va fi făcută direct pe document. În cazul în care documentul este electronic, nota este introdusă în document sau în sistemul de date în care acesta a fost creat. Marcajul trebuie să conțină informații cu privire la nivelul de secretizare, data când marcajul a fost realizat și, de asemenea, autoritatea care l-a întocmit.

Documentele oficiale considerate de o mare importanță pentru securitatea națională trebuie să conțină marca „secret”. O astfel de notație are caracter de obligativitate pentru autoritatea abilitată să stabilească dacă documentul poate fi divulgat.

² <http://www.regeringen.se/contentassets/2c767a1ae4e8469fbfd0fc044998ab78/public-access-to-information-and-secrecy-act>.

- Obligația autorităților de a oferi acces la informații

La solicitarea unei părți, autoritățile trebuie să furnizeze informații din documentele oficiale deținute care nu au caracter secret. În primă instanță, posibilitatea dezvăluirii unui document este stabilită de către funcționarul responsabil cu documentul, de exemplu, un registrator sau o persoană care răspunde de acest domeniu. În cazuri deosebite, funcționarul trebuie să sesizeze autoritatea de management, fără, însă, a nu produce întârzieri în soluționare.

- Dreptul de preemțiune al autorităților cu privire la informațiile clasificate

În conformitate cu prevederile Legii privind accesul la informații publice și secrete, clasificarea nu împiedică furnizarea de informații către o altă autoritate, atât timp cât există o prevedere într-un act oficial care relevă faptul că informațiile trebuie furnizate acelei autorități. Un exemplu de o astfel de sarcină e aceea în care furnizarea informațiilor este obligatorie la depunerea mărturiei în conformitate cu prevederile Codului de procedură civilă/penală.

Nu există nicio reglementare care să interzică ca informațiile să fie furnizate unei alte autorități într-un număr de situații stipulate în Legea accesului la informații publice și secrete. Astfel de exemple sunt: informația este necesară pentru un proces al unui funcționar pentru o infracțiune de serviciu, pentru reconsiderarea unei decizii sau a unei măsuri de către autoritatea care deține informația sau pentru supravegherea sau auditarea autorității care deține informațiile.

Legiuitorul nu a fost în măsură să anticipeze toate situațiile în care este necesară divulgarea informațiilor secrete către o altă autoritate, de aceea a fost introdusă o „clauză generală”. Conform acesteia, regimul clasificării nu împiedică furnizarea de informații către o altă autoritate dacă este evident că interesul divulgării acelor informații este mult mai mare decât interesul de a proteja informațiile.

- Dreptul de preemțiune al unei entități private cu privire la informațiile clasificate

O persoană care este suspectată sau acuzată de o infracțiune de serviciu, poate oferi informații clasificate apărătorului său pentru a-i redacta apărarea.

Secretizarea, în conformitate cu anumite dispoziții, nu împiedică o autoritate de la furnizarea de informații către reprezentanții sindicali, angajați ai unor autorități publice, în cazul în care entitatea respectivă are obligația legală de a furniza aceste informații. În cazul în care persoana care primește informații este angajat al unei autorități, el sau ea trebuie să respecte dispoziția de secretizare aplicabilă autorității. În cazul în care reprezentantul sindicatului este angajat acolo, autoritatea îi poate impune o clauză de confidențialitate care prevede anumite rezerve. Un reprezentant sindical poate, în mod independent de clauza de confidențialitate, transmite informații unui membru al consiliului de administrație al organizației sale sindicale. Reprezentantul sindical trebuie să informeze membrul consiliului cu privire la obligația de confidențialitate, acestuia revenindu-i, astfel, aceeași obligativitate de confidențialitate.

- Transferul de informații clasificate

Dispozițiile privind transferul informațiilor clasificate sunt în principal de două tipuri.

- anumite dispoziții privind transferul informațiilor secrete vizează în special organisme sau operațiuni speciale care obțin, în mod normal, informații dintr-un număr de operațiuni diferite. În aceste cazuri, dispozițiile generale privind transferul

informațiilor cu caracter secret au fost introduse acolo unde, în principiu, registrul de clasificare se aplică informațiilor altor autorități și este transferat atunci când informația este dezvăluită structurii speciale sau în cazul unei operațiuni speciale. Exemple de operații la care registrul este transferat sunt operațiunile de supraveghere sau audit. Exemple de organisme la care se transferă registrul sunt autoritățile de arhivare și instanțele.

- cealaltă categorie de dispoziții privind transferul de informații secrete vizează domeniile considerate a fi deosebit de sensibile. În aceste cazuri, nivelul de secretizare este atașat informațiilor indiferent de organismul care le-a obținut.

Regula de bază într-o situație în care concură mai multe dispoziții cu privire la nivelul de clasificare, este aceea că primează nivelul de secretizare cel mai înalt.

- Secretizarea în raport cu o persoană fizică și cu un custode

Clasificarea aplicată în cazul unei persoane fizice se subordonează celei aplicate informațiilor aparținând unei autorități dacă intervine un raport de conexiune între aceste entități. În situații excepționale, persoanei protejate îi este îngăduit dreptul de a controla informațiile secretizate care o privesc. Un astfel de exemplu ar fi documentele de spitalizare, care trebuie păstrate secret în cazul în care starea pacientului s-ar deteriora grav dacă ar lua la cunoștință de conținutul acestora. Aceeași situație se poate aplica și în cazul protejării unui minor în raport cu custodele minorului.

- Răspunderea penală

Dispozițiile care impun sancțiuni pentru infracțiuni la regimul secretului profesional se regăsesc în Codul Penal, cap. 20, secț. 3.

În cazul comiterii cu intenție a unei încălcări a regimului de secretizare, pedeapsa este amendă sau închisoare de maximum un an, iar în cazul unei încălcări comise din neglijență o amendă. Cazurile minore de neglijență nu sunt sancționate.

- Ierarhizarea clasificării

Dispozițiile privind secretizarea conțin adesea mai multe condiții prealabile, cunoscut sub numele de „articole”, care trebuie îndeplinite pentru ca procedura de secretizare să se aplice într-un caz individual. Aceste prevederi sunt introduse cu expresia „Secretul se aplică” în combinație cu sintagma „pentru informații”, iar informațiile sunt totdeauna descrise în detaliu. Informația trebuie să aibă o definiție certă - de exemplu „Relațiile Suediei cu un alt stat”. Clasificarea este, de regulă, stabilită a se aplica acelor informații aflate într-un context special, de exemplu, în problematici certe, în operațiuni certe sau la anumite autorități, care pot fi încadrate în diferite niveluri de clasificare.

O serie de dispoziții privind secretizarea nu prevede condiții speciale pentru aplicabilitatea clasificării la informațiile menționate în context. În orice caz, majoritatea dispozițiilor de confidențialitate sunt supuse unor condiții prealabile în ceea ce privește aplicabilitatea lor, ceea ce impune îndeplinirea anumitor condiții speciale. Condiția este, de regulă, formulată ca o „cerință de daună”. O astfel de cerință se referă la faptul că secretizarea este aplicabilă cu condiția menționării daunelor care pot apărea dacă informația este divulgată. Există două tipuri principale de cerințe de deteriorare: *dreaptă* și *inversă*.

Forma cerinței de deteriorare „dreaptă” este indicată de următorul exemplu: „Secretizarea se aplică aspectelor legate de locul de muncă, asigurare de vătămare sau asigurare de pensie parțială, pentru informații care dacă ar fi divulgate, ar produce daune unei persoane fizice”.

Cerința de deteriorare „inversă” presupune ca secretul să fie principala regulă. Un exemplu de acest tip de cerință a daunelor este următorul: „Secretizarea se aplică în cadrul serviciilor sociale la informațiile referitoare la circumstanțe personale ale unei persoane, doar dacă este evident că informațiile pot fi divulgate fără ca persoana în cauză sau o altă aflată în strânsă legătură cu aceasta să fie lezate”.

Normele privind termenele reprezintă unul dintre modurile posibile prin care, angajând prevederile Legii accesului la informații publice și secrete, este restricționat accesul la informații clasificate. Astfel de norme privind perioadele de păstrare a secretului se referă numai la informațiile din documentele oficiale.

Perioada de secretizare variază de la 2 la 70 de ani, în funcție de interesul protejat. Pentru protecția afacerilor personale ale unei entități private, perioada de păstrare a secretului este de obicei de 50 sau 70 de ani, în timp ce pentru protejarea informațiilor financiare ale unor entități publice sau private, termenul este în cele mai multe cazuri de 20 de ani.

O singură regulă principală se aplică în ceea ce privește punctul de plecare de la care se calculează termenul de păstrare, aceasta fiind data la care documentul a fost realizat. În cazul jurnalelor, registrelor și altor note păstrate în mod continuu, timpul este contabilizat de la momentul în care a fost introdusă informația de clasificat în respectivul document.

- Clasificarea informațiilor guvernamentale, parlamentare și altele

Clasificarea în cadrul Parlamentului se limitează la anumite informații discutate în cadrul Camerei, incluse în înregistrări sau în unele rapoarte ale comisiilor.

Clasificarea este, de asemenea, limitată într-o mare măsură în cazurile Avocatului Parlamentar (JO) și Biroului Ministrului Justiției (JK), aplicându-se, în special, informațiilor furnizate de o persoană particulară.

Există, de asemenea, prevederi speciale cu privire la clasificarea privind informațiile Comisiei pentru apărarea securității și integrității.

ITALIA

Cadrul legal:

- Legea nr.124/2007 privind protejarea informațiilor

Potrivit prevederilor Legii nr.124/2007 privind protejarea informațiilor ce vizează siguranța statului, din categoria informațiilor clasificate fac parte actele secrete de stat: documente, informații, activități, acorduri internaționale, planuri de apărare a instituțiilor stabilite prin Constituție, de protejare a independenței statului italian, în ceea ce privește relațiile cu alte state, pregătirea și apărarea militară a statului, alte date a căror dezvăluire neautorizată ar putea să dăuneze integrității Republicii Italiene.

Informațiile, documentele, înregistrările, activitățile, lucrurile și locurile care intră sub incidența secretului de stat sunt gestionate numai de autoritățile și entitățile chemate să îndeplinească o serie de funcții esențiale, în limitele și competențele stabilite prin lege. Toate actele care se încadrează în categoria secretelor de stat trebuie să fie păstrate într-un mod adecvat pentru a preveni manipularea, furtul sau distrugerea acestora. Obligația care rezultă din apărarea

secretului de stat privește și actele, documentele sau obiectele obținute din străinătate.

Pentru punerea în aplicare a standardelor stabilite de lege, definirea criteriilor de identificare a informațiilor, documentelor, înregistrărilor, activităților, lucrurilor și locurilor care fac obiectul secretului de stat a condus la următoarea clasificare: informații de tip

- SECRET de STAT (SS);
- SECRET (S);
- CONFIDENȚIAL (RR);
- RESTRICȚIONAT (R),

conform prevederilor art. 42 din Legea nr.124/2007 și art. 4 din Decretul Președintelui Consiliului de Miniștri nr. 7/2009.

Declasificarea informațiilor se realizează de către autoritatea care a dispus clasificarea, de o altă entitate autorizată sau de o instituție de nivel superior celei care a produs și secretizat inițial informația.

Emitentul informațiilor clasificate care fac obiectul declasificării, modificării clasificării sau eliminării acesteia trebuie să informeze prompt alți deținători ai materialelor clasificate, supuse schimbărilor administrative.

Pentru accesul la informațiile clasificate, secrete și confidențiale, o persoană trebuie să dețină o autorizație de securitate (NOS). Autorizația de securitate poate să fie superioară tipului de clasificare al documentului de lucru.

Documentele primite din străinătate pot avea următoarele tipuri de clasificare:

- SECRET DE STAT;
- SECRET;
- CONFIDENȚIAL;
- RESTRICȚIONAT.

Aplicarea etichetei de confidențialitate se poate face de către o structură acreditată, conform nivelului de ierarhizare a acesteia.

Declasificarea unui document se realizează în mod automat la un nivel inferior, într-un termen de 5 ani de la operațiunea de clasificare. Declasarea automată nu se aplică în cazul în care, din motive justificate, termenul este prelungit de către autoritatea care a clasificat documentul, perioada de clasificare putând fi extinsă până la 15 ani prin decizie a Președintelui Consiliului de Miniștri.

Acesta are printre atribuții verificarea respectării normelor privind clasificările informațiilor. După caz, prin reglementări interne se determină domeniul de aplicare a nivelurilor individuale de secretizare, entitățile care sunt împuternicite să realizeze acest lucru, precum și serviciile publice care au atribuții de informare în legătură cu documente ce vizează securitatea Republicii, inclusiv cele militare.

În cazul în care o autoritate judiciară dispune verificarea unor documente clasificate, acestea sunt livrate instanței care este obligată să asigure conservarea acestora în moduri care să protejeze confidențialitatea datelor și să asigure dreptul părților în proces de a studia documentele, fără a face copii.

Orice persoană care distruge ilegal documente clasificate sau informații cu relevanță pentru securitatea Republicii, în orice etapă de clasificare sau în perioada de declasificare, se pedepsește cu închisoare de la unu la cinci ani.

În ceea ce privește apărarea secretului de stat, art. 202 din Codul de procedură penală a fost înlocuit cu următorul text³: „Oficialii și funcționarii publici, precum și alte persoane care își desfășoară activitatea într-un serviciu public sunt obligate să refuze să depună mărturie privind fapte care intră sub incidența secretului de stat”.

În cazul în care finalizarea procesului nu se poate realiza decât după cunoașterea unui secret de stat, judecătorul nu poate insista să procedeze în aflarea secretului de stat.

În cazul în care un martor opune părții adverse din proces un secret de stat, instanța trebuie să-l informeze de îndată pe Președintele Consiliului de Miniștri, urmând a suspenda cauza până la clarificarea aspectelor de interes. De asemenea, în cazul în care în termen de treizeci de zile de la notificarea Președintelui Consiliului de Miniștri, acesta nu-și exprimă punctul de vedere privind secretul de stat invocat în proces, instanța poate să stabilească desfășurarea ulterioară a procedurii. Dacă Președintele Consiliului decide că secretul de stat nu trebuie aflat pe parcursul procesului, autoritatea judiciară trebuie să sisteze obținerea și utilizarea acestor date, chiar și în mod indirect.

Sistemul de informații privind securitatea Republicii este format din Președintele Consiliului de Miniștri, Comitetul interministerial pentru securitatea Republicii (CISR), Departamentul pentru securitatea informațiilor (DIS), Agenția de informații externă (AISE) și Agenția de informații internă (AISI).

Potrivit art. 4 al legii, DIS are, printre altele, următoarele atribuții:

a) coordonează întreaga activitate privind securitatea informațiilor, verifică rezultatele activităților întreprinse de AISE și AISI, fără a aduce atingere competenței serviciilor menționate mai sus referitoare la activitatea desfășurată;

b) este informat în mod constant de servicii despre activitatea de informare a Președintelui Consiliului de Miniștri, despre modalitatea de informare și protejarea informațiilor transmise;

c) colectează informații, analize și rapoarte de la serviciile de informații, forțele armate și poliție, de la departamentele guvernamentale și instituțiile private de cercetare; oprește competența exclusivă a AISE și AISI privind pregătirea planurilor de cercetare operaționale relevante, elaborează analize strategice sau pentru situații speciale, evaluări și previziuni, pe baza contribuțiilor sectoriale analitice ale AISE și AISI;

d) elaborează, pe baza informațiilor și a rapoartelor menționate la lit. c), analizele globale care urmează să fie prezentate la CISR, precum și proiecte de cercetare informative, care sunt supuse aprobării Președintelui Consiliului de Miniștri, după consultarea CISR;

d-bis) coordonează activitățile de cercetare a informațiilor destinate consolidării securității cibernetice și a celei naționale;

e) promovează, inclusiv prin reuniuni periodice, schimbul de informații între AISE, AISI și forțele de poliție, notificând rezultatele obținute Președintelui Consiliului de miniștri;

f) furnizează, la ordinul Președintelui Consiliului de Miniștri, după consultarea cu CISR, informații și analize către autoritățile publice sau alte instituții;

g) pregătește, în consultare cu AISE și AISI, planul de achiziție de resurse umane și materiale, precum și toate celelalte resurse necesare serviciilor (...);

³ https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/legge-124-2007.html#Capo_V

i) exercită controlul asupra activității AISE și AISI, verificarea conformității activităților desfășurate de acestea, în contextul regulamentelor, directivelor și ordinelor Președintelui Consiliului de Miniștri. În acest scop, la DIS a fost înființat un birou de inspecție al cărui mod de organizare și funcționare este definit de regulament.

l) asigură punerea în aplicare a instrucțiunilor date de către Președintele Consiliului de Miniștri cu normele speciale, în scopul protecției administrative a secretului de stat și a clasificărilor stabile;

m) desfășoară activități de promovare și difuzare a culturii securității și a comunicării instituționale.

Comitetul interministerial pentru securitatea Republicii (CISR), care are caracter consultativ, elaborează obiectivele generale ale politicii de securitate a informațiilor. Acesta elaborează orientările generale și obiectivele fundamentale care trebuie urmărite în contextul îmbunătățirilor politicilor de securitate a informațiilor, decide cu privire la alocarea resurselor financiare între serviciile DIS și analizează bugetele structurilor, precum și conturile finale.

Comitetul este prezidat de către Președintele Consiliului de Miniștri, din el mai făcând parte: Ministrul afacerilor externe, Ministrul de interne, Ministrul apărării, Ministrul de justiție, Ministrul economiei și finanțelor și Ministrul dezvoltării economice.

Președintele Consiliului de Miniștri poate fi chemat să participe la reuniunile Comitetului, de asemenea, ca urmare a solicitării acestora, fără drept de vot, pot participa și alți membri ai Consiliului de Miniștri, directorii AISE și AISI, precum și alte autorități civile și militare.

UNGARIA

Cadrul legal:

- Legea CLV din 2009 cu privire la protecția informațiilor clasificate

Legea cu privire la protecția informațiilor clasificate reglementează domeniul informațiilor clasificate precum și regimul certificatelor de securitate în baza următoarelor principii:

- ***Principiul necesității și proporționalității:*** dreptul de acces public la date de interes public poate fi limitat prin clasificarea în mod exclusiv pe baza întrunirii termenilor și condițiilor prezentului act, a nivelului de clasificare necesar pentru protecție, precum și a perioadei necesară.

- ***Principiul „need to know”:*** accesul la informații clasificate poate fi acordat numai celor care au absolută nevoie pentru îndeplinirea responsabilităților lor de stat sau publice.

- ***Principiul confidențialității:*** persoanele neautorizate nu au acces la informații clasificate.

- ***Principiul integrității:*** informațiile clasificate pot fi modificate sau șterse exclusiv de către o persoană autorizată.

- ***Principiul disponibilității:*** garantează persoanelor autorizate accesul necesar la/și pentru utilizarea informațiilor clasificate.

- Clasificarea documentelor

În sensul prezentei legi, următoarele noțiuni sunt definite astfel:

1) *informații clasificate*

a) *informații naționale clasificate*: informații din sfera de interes public care urmează să fie protejate prin clasificare, îndeplinind cerințele formale ale reglementărilor emise în temeiul prezentei legi și marcate pentru clasificare prin prezentul act, în legătură cu care - indiferent de forma sa - orice fel de divulgare, accesul neautorizat, modificarea sau utilizarea acestora, asigurarea accesului persoanelor neautorizate sau blocarea accesului persoanelor autorizate pot afecta în mod direct sau să pună în pericol (denumite în continuare în comun: *daune*) interesele publice care urmează să fie protejate de clasificare și va limita divulgarea și accesul la conținutul său prin intermediul unei clasificări;

b) *informații clasificate străine*: informații furnizate de către toate instituțiile și organizațiile Uniunii Europene, precum și de un stat membru care acționează în numele Uniunii Europene, sau o parte străină sau organizație internațională și transferate printr-un contract internațional sau a unui acord promulgat printr-un act, la accesul cărora există restricții stabilite prin procesul de clasificare de către instituțiile și organizațiile Uniunii Europene, un stat membru care acționează în numele Uniunii Europene, o țară terță sau de partid, precum și de o organizație internațională;

2) *termenul de valabilitate*: anul, luna, ziua, dacă este necesar, ora și minutul până la care clasificatorul de informații limitează dezvoltarea informațiilor naționale clasificate și accesul oricărei persoane, cu excepția persoanelor autorizate;

3) *clasificatorul de informații*: persoana autorizată pentru realizarea clasificării în temeiul sferei sale de competență;

4) *organism de gestionare a informațiilor clasificate*: organismul, instituția, unitatea organizatorică sau o entitate economică de gestionare a informațiilor clasificate pentru a îndeplinirea responsabilităților de stat sau publice;

5) *utilizator*: persoana care, pentru îndeplinirea responsabilităților sale de stat sau publice i se pun la dispoziție informații clasificate în temeiul licenței de utilizare acordată de către un funcționar autorizat să elibereze astfel de licențe de utilizare;

6) *parte intermediară*: persoana fizică care oferă ajutor în legătură cu o chestiune din sfera sa de competența unui organism care îndeplinește responsabilitățile de stat sau publice, și în acest scop utilizarea informațiilor clasificate este necesară;

7) *utilizare*: exercitarea dreptului de a dispune de informații clasificate pentru îndeplinirea responsabilităților de stat sau publice printr-o licență de utilizare emisă de un funcționar autorizat să elibereze astfel de licențe;

8) *licență de utilizator*: o autorizație scrisă, eliberată de către funcționarul autorizat să elibereze astfel de licențe cu definiția specifică a dreptului de dispoziție asupra informațiilor clasificate, persoanei care are dreptul de a utiliza informațiile clasificate pentru îndeplinirea responsabilităților de stat sau publice;

9) *permisul de acces*: o autorizație emisă în formă scrisă de către clasificatorul de informații, conținând afișarea de date personale de identificare ale

persoanei autorizate și temeiul în care persoana are acces la informații naționale clasificate;

10) *declarație de confidențialitate*: o declarație a persoanei care utilizează sau care are acces la informații clasificate, prin care ia la cunoștință de normele și reglementările privind protecția informațiilor clasificate și recunoaște obligațiile de confidențialitate;

11) *certificat personal de securitate*: un certificat pentru a defini cel mai înalt nivel de informații clasificate la care o persoană fizică poate avea acces cu licență de utilizator în termen de valabilitate;

12) *sistem electronic de gestionare a datelor*: echipamentul, metodele și procedurile de manipulare electronică, electromagnetică sau optică a informațiilor clasificate;

13) *certificat de securitate al site-ului*: certificatul care stabilește cel mai înalt nivel de informații clasificate pe care agentul economic este apt să-l gestioneze.

Clasificatorii de informații și reguli privind procedura de clasificare

• Persoane autorizate să realizeze clasificarea în temeiul funcției sau a sferei de competență:

- a) Președintele Republicii;
- b) Președintele Adunării Naționale;
- c) președinții comisiilor parlamentare;
- d) președintele Curții Constituționale;
- e) președintele Curiei;
- f) președintele Tribunalului;
- g) președintele Oficiului Național al Justiției;
- h) Procurorul general;
- i) șeful Parchetului;
- j) comisarul pentru Drepturi Fundamentale;
- k) guvernatorul Băncii Naționale a Ungariei;
- l) membrii Guvernului;
- m) secretari de stat, șeful de cabinet al primului-ministru, secretarul general al Guvernului;
- n) șeful organismului care funcționează în conformitate cu ordinea procedurală a Guvernului;
- o) organismele centrale ale sistemului judiciar, șeful Serviciului Național de Securitate Militară, șeful organismului de prevenire și detectare a criminalității interne, astfel cum sunt definite în Legea poliției, șeful organului anti-terorism astfel cum este definit în Legea poliției, șeful autorității pentru străini și șeful autorității pentru refugiați;
- p) șeful Autorității Naționale de Securitate;
- q) șefii misiunilor externe ale Ungariei și persoanele cu mandat independent de reprezentare, delegate oricărui alt stat, organizație internațională sau centru de cooperare regională pentru îndeplinirea angajamentelor stabilite în acordurile internaționale;
- r) persoane autorizate prin lege să realizeze clasificarea;
- s) șefi de agenții guvernamentale autonome și de organisme independente de reglementare.

• Persoanele fizice/juridice care realizează clasificarea, menționate la art. (1), pot delega competențele lor de clasificare, în scris, după cum urmează :

a) în cazul informațiilor clasificate drept STRICT SECRET adjunctilor lor, iar membrii Guvernului la secretarul de stat pentru administrația publică și subsecretarul de stat;

b) în ceea ce privește informațiile clasificate drept SECRET, CONFIDENTIAL și RESTRICȚIONAT, persoanelor cu mandate de conducere sau numite în funcții de conducere în organisme conduse de către aceștia și învestite cu puteri de autoritate.

• Ministrul apărării naționale, ministrul responsabil cu supravegherea profesională a protecției informațiilor clasificate, ministrul responsabil de politica externă, ministrul responsabil pentru direcția activităților de informații civile, ministrul responsabil pentru direcția serviciilor naționale de securitate civile, precum și cei definiți în art. (1), punctul o) pot delega prerogativele de clasificare pentru orice altă persoană aflată în subordinea lor, având mandat de conducere sau fiind numit într-o poziție de conducere în legătură cu apărarea națională, securitatea națională, externă și relații internaționale, supravegherea profesională a protecției informațiilor clasificate, precum și în domeniul judecătoresc, astfel cum este prevăzut în regulamentul intern.

- *Clasificarea informațiilor*

• Interesele publice eligibile pentru protecția prin clasificare trebuie să includă:

- a) suveranitatea și integritatea teritorială;
- b) ordinea constituțională;
- c) activitățile de apărare, securitatea națională, aplicarea legii și prevenirea criminalității;
- d) justiția, bugetul statului și economia națională;
- e) politica externă și relațiile internaționale;
- f) acțiuni ale organelor de stat maghiare neinfluențate de servicii secrete sau alți factori externi.

• Informațiile sunt protejate numai prin procedura de clasificare, în cazul în care:

- a) informația generată aparține domeniilor de interes public protejat prin clasificare astfel cum este definită mai sus;
- b) dezvăluirea, accesul neautorizat, modificarea sau utilizarea informațiilor, acordarea accesului persoanelor neautorizate sau refuzarea accesului persoanelor autorizate prejudiciază interesele publice protejate de clasificare;
- c) dezvăluirea și accesul la informație, cu excepția persoanelor autorizate, trebuie să fie limitată pentru o anumită perioadă de timp.

• Informațiile pot fi protejate de clasificare în cazul întrunirii tuturor termenilor și condițiilor legale, precum și prin stabilirea unei perioade optime de timp.

• În caz de divulgare, acces neautorizat, modificare sau utilizare a informațiilor, acordarea accesului persoanelor neautorizate sau refuzarea accesului persoanelor autorizate:

- a) vor provoca daune extrem de grave intereselor publice care urmează să fie protejate de clasificare, informațiile vor fi clasificate ca fiind STRICT SECRET;
- b) vor cauza prejudicii grave intereselor publice care urmează să fie protejate de clasificare, informațiile vor fi clasificate cu indicativul SECRET;

c) vor cauza daune intereselor publice care urmează să fie protejate de clasificare, informațiile vor fi clasificate cu indicativul CONFIDENȚIAL;

d) vor afecta interesele publice care urmează a fi protejate de clasificare, vor fi clasificate cu indicativul RESTRICȚIONAT.

- Perioada de clasificare a documentelor este următoarea:

- a) pentru STRICT SECRET și SECRET - nu mai mult de 30 de ani;

- b) pentru CONFIDENȚIAL - nu mai mult de 20 de ani;

- c) pentru RESTRICȚIONAT - nu mai mult de 10 ani.

- Perioada de clasificare a oricăror informații cu indicativul SECRET sau superior poate fi prelungită o dată prin efectuarea unei noi proceduri de clasificare, în cazuri temeinic justificate, și de maxim două ori în situații privind apărarea națională, securitatea națională, aplicarea legii sau a intereselor justiției din Ungaria, în strânsă legătură cu interesele legitime ale persoanelor fizice.

Perioada de clasificare a oricăror informații cu indicativul CONFIDENȚIAL sau RESTRICȚIONAT poate fi prelungită prin efectuarea unei noi proceduri de clasificare, în cazuri extraordinar justificate, o singură dată, cu maxim 5 ani, sau în situații privind apărarea națională, siguranța națională, de aplicare a legii sau a intereselor Ungariei, în strânsă legătură cu interesele legitime ale persoanelor fizice, de maxim două ori.

Noua procedură de clasificare trebuie să fie efectuată înainte de expirarea perioadei anterioare. Caracterul clasificat al oricărei informații încetează să mai existe după expirarea perioadei de valabilitate. Informațiile nu pot fi reclasificate după expirarea perioadei de clasificare.

- Tipul de clasificare a informațiilor trebuie să fie în mod clar vizibil în timpul gestionării informațiilor clasificate. Nivelul de clasificare, termenul de valabilitate, numele clasificatorului și funcția sa (denumite în continuare împreună: marcajul de clasificare) trebuie să fie marcate pe suportul informațiilor clasificate naționale sau - în cazul în care acest lucru nu este posibil - pe o foaie de gardă adiacentă.

- Gestionarea informațiilor care necesită clasificarea națională pe baza unui acord sau tratat internațional se efectuează în conformitate cu prevederile menționate mai sus. Înainte de trimiterea acestor informații către țări străine, nivelul de clasificare trebuie să fie afișat în limba maghiară și în limba stabilită prin acordul sau tratatul internațional - în cazul instituțiilor Uniunii Europene, în limba engleză sau franceză.

- În cazul în care diferite informații clasificate nu pot fi administrate separat, ci numai în comun, acestea vor fi tratate în conformitate cu cel mai înalt nivel de clasificare aplicabil.

- *Entitatea care poate clasifica informațiile*

- 1) instituția care produce informații de responsabilitate publică trebuie să inițieze procedura de clasificare;

- 2) inițiatorul clasificării trebuie să pregătească o propunere de clasificare însoțită de o justificare pentru stabilirea nivelului informațiilor;

- 3) propunerea de clasificare trebuie să includă toate referirile la interesele publice care urmează să fie protejate de clasificare, la nivelul de clasificare, precum și durata clasificării. Justificarea propunerii de clasificare trebuie să includă fapte și condiții care necesită clasificarea;

- 4) în conformitate cu procedura de clasificare, suportul de informație care urmează să fie clasificată se prezintă clasificatorului de informații de către inițiator,

fără întârziere, împreună cu propunerea de clasificare. Clasificatorul de informații decide cu privire la clasificarea informațiilor în termen de 30 de zile de la primirea cererii. În cazul în care clasificatorul de informații nu decide înainte de termenul limită privind clasificarea informațiilor, nu vor fi generate informații clasificate naționale;

5) în cazul în care informațiile astfel cum sunt definite în conformitate cu prevederile legale vor fi generate de către clasificatorul de informații, decizia se ia în formă scrisă, în conformitate cu conținutul propunerii de calificare astfel cum sunt definite în conformitate cu art. (3) al legii, iar informațiile vor fi clasificate în mod corespunzător;

6) până la luarea deciziei de clasificare, în timpul procedurii de clasificare, informațiile sunt gestionate în conformitate cu reglementările personale, fizice, administrative și electronice de securitate, conform cerințelor nivelului de clasificare inițiat;

7) informațiile clasificate naționale sunt create prin procedura de clasificare de către clasificatorul de informații. Crearea informațiilor clasificate naționale trebuie, de asemenea, să respecte cerințele formale ale marcajului de clasificare;

8) la cererea Autorității Naționale pentru Protecția Datelor și Libertatea de Informare, clasificatorul trebuie să justifice clasificarea informațiilor în detaliu, în scris.

- Supravegherea și revizuirea informațiilor clasificate naționale

a) Clasificatorul de informații revizuește informațiile clasificate naționale aflate în sfera sa de competență, clasificate de el însuși sau de către predecesorul său legal, nu mai târziu de o dată la 5 ani - cu excepția cazului în care legea definește un termen mai scurt. Clasificatorul de informații poate implica un expert în supraveghere.

b) Ca rezultat al supravegherii, clasificatorul de informații sau succesorul său legal pot lua următoarele decizii referitoare la informațiile clasificate naționale:

- să păstreze clasificarea dacă termenii și condițiile de clasificare relevante încă prevalează;
- să scadă nivelul de clasificare sau să modifice termenul de clasificare în cazul în care termenii și condițiile de clasificare s-au schimbat;
- să rezilieze clasificarea în cazul în care condițiile de clasificare nu mai sunt întrunite.

c) Toți emitenții sunt informați cu privire la încetarea clasificării, modificarea nivelului de clasificare sau a termenului.

d) Procurorul general poate revizui clasificarea făcută de șeful biroului procurorului, de primul-ministru, de către împuternicitul acestuia, de ministrul responsabil pentru armonizarea activităților guvernamentale, de comisarul guvernamental sau alt membru al Guvernului, de șeful aparatului guvernamental, în conformitate cu normele aplicabile revizuirii clasificării, și, ca urmare, clasificarea poate fi încheiată și nivelul de clasificare sau perioada de clasificare poate fi modificată.

- Informații clasificate străine

3) Termenul de valabilitate a informațiilor clasificate străine este definit în dispozițiile întocmite de către clasificatorul de informații; Fără aceste dispoziții,

informațiile sunt tratate ca informații clasificate până în momentul în care clasificatorul de informații ia o decizie privind supravegherea informațiilor.

4) În cazul în care informațiile clasificate străine sunt generate în colaborare cu organisme care au dreptul de clasificare a informațiilor naționale și gestionarea informațiilor clasificate străine, clasificarea informațiilor trebuie să respecte normele și reglementările organizațiilor internaționale relevante.

5) În cazul în care în masa de informații generată sunt incluse și informații clasificate străine, utilizatorul trebuie să aplice nivelul de clasificare potrivit informațiilor clasificate străine și cel mai lung termen de valabilitate prevăzut.

6) În cazul în care utilizatorul include informații clasificate străine în informațiile naționale care sunt clasificate, informațiile naționale se clasifică în conformitate cu dispozițiile sect. 5-6, iar marcarea informațiilor clasificate străine se realizează în conformitate cu normele și reglementările prevăzute de sect. 7. Ambele niveluri de clasificare sunt consemnate în scris pe informațiile generate, precum și localizarea exactă a celor străine și a informațiilor naționale clasificate.

7) Exceptând următoarele situații: acte legislative ale Uniunii Europene, tratate sau acorduri internaționale care să prevadă altfel; informațiile clasificate străine sunt tratate în conformitate cu normele și reglementările prezentei legi.

- Reguli generale privind securitatea informațiilor clasificate

- Informațiile clasificate sunt utilizate exclusiv pe baza licenței emise de Autoritatea Națională de Securitate, în cazul în care acest fapt este indispensabil îndeplinirii responsabilităților de stat sau publice.

- Accesul la informațiile clasificate se acordă exclusiv persoanelor fizice - cu excepțiile stabilite de lege - cu certificat personal de securitate și declarație de confidențialitate, cu drepturile de utilizare definite în licența de utilizare.

- Pentru emiterea unui certificat de securitate corespunzător accesului la un anumit nivel de clasificare este necesară o inspecție de securitate națională. Certificatul de securitate are o valabilitate de 5 ani. În urma inspecției de securitate se poate stabili imposibilitatea acordării certificatului. În cazul în care deținătorul certificatului de securitate prezintă un risc de securitate, stabilit de o comisie de experți, certificatul poate fi retras.

- Toate organismele responsabile cu gestionarea informațiilor clasificate trebuie să prevadă condițiile de securitate personală, fizică, administrativă și electronică definite de lege, necesare pentru protecția informațiilor clasificate și în conformitate cu nivelul de clasificare a informațiilor.

- Toate spațiile, clădirile și centrele în care sunt gestionate informații clasificate trebuie să fie protejate împotriva accesului persoanelor neautorizate la informații clasificate prin măsuri de securitate fizică.

- Se vor lua măsuri de securitate administrativă pentru a garanta posibilitatea de urmărire și identificare, confidențialitatea, imunitatea și disponibilitatea informațiilor clasificate.

- Se vor lua măsuri electronice de securitate pentru a garanta confidențialitatea, imunitatea și disponibilitatea informațiilor clasificate gestionate prin intermediul sistemului electronic.

- Configurația termenilor și condițiilor de securitate trebuie realizată în funcție de:

- a) nivelul de clasificare a informațiilor clasificate gestionate;
- b) cantitatea și forma de informații clasificate;
- c) nivelul de risc și vulnerabilitate ale amplasamentului, corpului și sistemului electronic;
- d) riscurile de securitate națională.

- Accesul la informații clasificate

1) Orice cetățean, în baza licenței de acces, eliberată de clasificatorul de informații, are dreptul de a avea acces la datele sale cu caracter personal care prezintă și caracter de informații naționale clasificate, fără a fi necesar certificat personal de securitate. Persoana în cauză este obligată, înainte de accesul său la informațiile naționale, să facă o declarație de confidențialitate, în scris, și să respecte prevederile Legii privind protecția informațiilor naționale clasificate.

2) Decizia de eliberare a licenței de acces se ia de către clasificatorul de informații în termen de 15 zile de la solicitarea persoanei în cauză. Clasificatorul de informații va refuza eliberarea unei licențe de acces în cazul în care accesul poate dăuna interesului public. Clasificatorul de informații trebuie să justifice refuzul privind eliberarea licenței de acces.

3) În cazul în care un certificat „*need to know*” este refuzat, persoana în cauză poate contacta Curtea de Apel din Budapesta în termen de 15 zile de la primirea deciziei. În cazul în care Curtea aprobă cererea, clasificatorul trebuie să elibereze certificatul. Unui astfel de proces îi sunt aplicate dispozițiile Codului de procedură civilă, cu condiția ca instanța să se întrunească în ședință închisă, cu celeritate. Procesul poate fi condus doar de un judecător care posedă certificat de securitate cu cel mai înalt nivel de acces. Reclamantul, persoana care intervine în sprijinul reclamantului și reprezentanții acestora pot să nu ia cunoștință de informații clasificate. Alte persoane angrenate în proces sau reprezentanții acestora pot avea cunoștință de informații clasificate doar dacă dețin certificat de securitate prevăzut cu cel mai înalt nivel de acces.

Persoana care gestionează informații clasificate poate refuza să furnizeze informațiile solicitate de un cetățean în baza Legii privind accesul la informații și libertatea de informare, în cazul în care dezvăluirea informațiilor personale ar putea prejudicia statutul de clasificare al acelor informații.

Informațiile clasificate pot fi utilizate exclusiv de către persoana care justifică în mod corespunzător această cerință pentru a-și îndeplini responsabilitățile publice sau de stat, excepțiile fiind reprezentate de biblioteci. Toate persoanele care doresc accesul trebuie să dețină:

- a) un certificat personal de securitate valabil, de nivel egal cu clasificarea informațiilor care urmează să fie utilizate;
- b) o declarație de confidențialitate;
- c) o licență de utilizator.

În legătură cu utilizarea informațiilor clasificate cu indicativul **RESTRICȚIONAT**, pentru a-și îndeplini responsabilitățile de stat sau publice, utilizatorul trebuie să facă o declarație de confidențialitate și să dețină o licență de utilizator.

Persoanele care intră în categoria celor care au nevoie să utilizeze informații clasificate pentru a-și îndeplini responsabilitățile de stat sau publice, sunt:

- a) Președintele Republicii;

- b) Prim-ministrul;
- c) membri ai Curții Constituționale;
- d) Președintele Camerei;
- e) Președinte Curiei, Președinte Oficiului Național al Justiției;
- f) Procurorul General;
- g) Comisarul pentru Drepturi Fundamentale;

h) Președintele Autorității Naționale pentru Protecția Datelor și Libertatea de Informare are dreptul să își exercite drepturile de a dispune - astfel cum sunt definite în secț. 18, art. 2) lit. a) și b) - cu referire la informațiile clasificate din sfera de competență, fără un control național de securitate, certificat de securitate personală, declarație de confidențialitate sau licență de utilizator.

Șeful organismului de gestionare a informațiilor clasificate și șeful de securitate sunt autorizați să-și exercite drepturile de dispoziție referitoare la informațiile clasificate care intră în sfera lor de sarcini și competențe, definite în secț. 18, fără licență de utilizator.

Cu excepția cazului în care legea prevede altfel, judecătorul are dreptul de a-și exercita drepturile sale de dispoziție necesare pentru examinarea cauzelor care îi sunt atribuite, conform ordinului de atribuire fără un control național de securitate, certificat de securitate personală, declarație de confidențialitate sau licență de utilizator.

Nu e necesară nicio licență specială pentru utilizarea informațiilor clasificate în timpul îndeplinirii responsabilităților de stat sau publice pentru cei cu autorizație legală specială.

Atunci când se utilizează informații clasificate pentru îndeplinirea responsabilităților de stat sau publice, șeful organului de gestionare a informațiilor clasificate trebuie să stabilească persoanele din cadrul organizației, care au dreptul să elibereze licențe de utilizator. Licențele de utilizator pentru aceste persoane se eliberează de către conducătorul organului de gestionare a informațiilor clasificate.

Utilizarea informațiilor naționale clasificate în cadrul procedurilor penale sunt reglementate de Codul de procedură penală.

Cu excepția cazului în care se prevede altfel, procurorul care conduce sau participă la procedură, precum și martorul expert desemnat sau implicat în procesul penal au dreptul de a utiliza informațiile clasificate naționale puse la dispoziție într-o procedură penală, fără control de securitate națională, fără a deține certificat personal de securitate, declarație de confidențialitate sau licență de utilizator.

Clasificatorul de informații poate elibera o licență de utilizator pentru utilizarea informațiilor naționale care nu sunt utilizate în cadrul procedurii penale.

Clasificatorul poate oferi acces la informații naționale clasificate pentru structuri ale administrației publice, instanțe de judecată, în scopul documentării unor procese contravenționale sau alte proceduri oficiale, cu excepția proceselor penale. Problema unei licențe de utilizare a informațiilor clasificate nu poate fi refuzată în procedura de control al legalității, condusă de un procuror sau într-un proces civil, putând fi solicitată de către procuror pentru susținerea unui interes public.

În cazul în care persoana care intră sub incidența obligației de confidențialitate trebuie să ofere declarații privind informații clasificate într-un

proces de contencios administrativ, civil sau penal sau alte acțiuni oficiale, persoana care califică informația poate emite o derogare.

- Transferul informațiilor clasificate

1) În cazul în care organismul de gestionare a informațiilor clasificate trebuie să transmită inițial documentele unui terț, acesta trebuie să primească licență de utilizator de la conducătorul organului de gestionare a informațiilor clasificate, dacă nu se prevede altfel de către clasificatorul de informații.

2) Înainte de eliberarea licenței de utilizator, organismul de gestionare a informațiilor clasificate trebuie să verifice dacă partea intermediară îndeplinește toate cerințele de protecție a informațiilor clasificate.

3) Aceleași reglementări de personal, fizice, administrative și electronice de siguranță aplicate organismului de gestionare a informațiilor clasificate sunt obligatorii și pentru terți.

4) Nici o licență de utilizator nu poate fi emisă în cazul în care partea intermediară nu îndeplinește condițiile de securitate a personalului.

5) Terții vor avea acces la informațiile clasificate în mod exclusiv la sediul organismului de administrare a informațiilor clasificate, în cazul în care nu îndeplinește condițiile de securitatea fizică; administrativă sau electronică.

- Mediul de afaceri poate participa numai la procedurile de achiziții publice:

- a) care implică utilizarea de informații *CONFIDENȚIALE* sau cu indicativ superior;

- b) în conformitate cu Legea achizițiilor publice, care vizează și informațiile clasificate, precum și interesele de securitate națională ale Ungariei, sau care necesită măsuri speciale de securitate;

- c) în cazul în care inspecția de securitate industrială a fost efectuată, iar Autoritatea Națională de Securitate a emis certificatul de securitate corespunzător, la nivel de site, pentru organizația în cauză. Inspecția de securitate industrială este inițiată de către organismul de gestionare a informațiilor clasificate sau de Departamentul din cadrul Autorității Naționale de Securitate, care se ocupă de mediul de afaceri.

- Auditul de securitate în companiile industriale cuprind:

- a) auditul entității economice și controlul de securitate națională al persoanelor care utilizează informații clasificate;

- b) auditarea îndeplinirii condițiilor de personal, fizice, administrative și electronice de securitate pentru informații clasificate.

- În cazul în care auditul de securitate nu detectează niciun factor de risc, Autoritatea Națională de Securitate eliberează entității economice un certificat de securitate a site-ului.

- Informațiile clasificate cu indicativul *CONFIDENȚIAL* sau superior pot fi în mod exclusiv prezentate doar agenților economici care au certificat de securitate al site-ului valid.

- Șeful unui organism de gestionare a informațiilor clasificate poate permite furnizarea informațiilor clasificate cu nivel de clasificare *RESTRICTIIONAT*

organizației de afaceri care îndeplinește toate condițiile de personal, fizice, administrative și electronice de securitate.

- Eliberarea certificatelor personale de securitate

1) Certificatul personal de securitate este emis de către Autoritatea Națională de Securitate, în conformitate cu dispozițiile secț. 9, art. 1 pentru utilizatorii de informații clasificate străine și pentru agenții economici care gestionează informații clasificate. În cazul în care nu mai sunt întrunite condițiile de securitate necesare sau acestea încetează să mai existe, Autoritatea Națională de Securitate va refuza eliberarea certificatului personal de securitate sau va retrage certificatul deja eliberat.

2) Organismul de securitate:

a) eliberează certificatul personal de securitate pentru utilizatorii de informații naționale clasificate din cadrul organismului și pentru părțile intermediare;

b) va refuza eliberarea certificatului personal de securitate sau va retrage certificatul emis, în cazul în care condițiile de securitate necesare nu sunt întrunite sau încetează să mai existe.

- Licența de utilizare

1) Licența de utilizator definește drepturile de dispoziție acordate pentru utilizator.

2) Drepturile de dispoziție acoperă următoarele aspecte:

a) administrarea și procesarea documentelor pentru îndeplinirea responsabilităților de stat sau publice;

b) toate activitățile de înregistrare a informațiilor clasificate;

c) deținerea de informații clasificate;

d) repetarea marcării informațiilor clasificate sau încetarea unei astfel de operațiuni;

e) copierea, reproducerea informațiilor clasificate;

f) traducerea informațiilor clasificate;

g) efectuarea de extrase;

h) utilizarea în cadrul organizației;

i) utilizarea în afara organizației;

j) casarea oficială sau anularea;

k) eliberarea licențelor de utilizator;

l) eliberarea licențelor de acces;

m) supravegherea informațiilor clasificate naționale;

n) autorizația de acces la informații clasificate pentru persoanele fizice sau juridice străine;

o) autorizație pentru luarea informațiilor clasificate în afara țării sau de a aduce astfel de informații din străinătate în țară;

p) denunțarea obligativității de confidențialitate;

(3) Utilizatorul are următoarele drepturi:

a) dreptul deplin de a dispune de informațiile pe care le clasifică;

b) drepturi de utilizare, în conformitate cu prevederile art. 2, lit. a) - k) asupra informațiilor clasificate de către alt clasificator de informații.

- Alte obligații privind protecția informațiilor clasificate

1) Orice persoană care deține informații clasificate străine sau naționale din surse necunoscute, ale căror niveluri de clasificare sunt neidentificabile, și nu deține autorizație de utilizare, trebuie să transmită, fără întârziere, aceste informații către Autoritatea Națională de Securitate. Condițiile de depistare și predare a suportului de date trebuie să fie înregistrate în scris.

2) În cazul în care utilizatorul are cunoștință de o încălcare a reglementărilor privind protecția informațiilor clasificate, acesta trebuie să informeze, fără întârziere, șeful de securitate. În cazul în care se constată încălcarea prezentei legi sau a dispozițiilor de punere în aplicare, exprimat printr-un potențial acces al persoanelor neautorizate la informații clasificate *STRICT SECRET*, *SECRET*, *CONFIDENTIAL*, sau un alt pericol, șeful corpului care gestionează informațiile clasificate trebuie să informeze clasificatorul de informații și Autoritatea Națională de Securitate.

- Organisme și persoane implicate în protecția informațiilor clasificate

1) Autoritatea Națională de Securitate este responsabilă cu supravegherea oficială a protecției informațiilor clasificate, gestionarea acestora și cu îndeplinirea funcțiilor securității naționale și industriale. ANS este un organism independent sub îndrumarea ministrului responsabil cu supravegherea profesională a protecției informațiilor clasificate.

2) Autoritatea Națională de Securitate are următoarele atribuții:

a) să autorizeze managementul informațiilor clasificate la organul de gestionare a informațiilor clasificate, având dreptul să modifice sau să retragă autorizația eliberată;

b) să autorizeze utilizarea sistemelor electronice de gestionare a informațiilor clasificate, având dreptul să modifice sau să retragă autorizația eliberată;

c) să păstreze evidența organismelor de gestionare a informațiilor clasificate și a autorizațiilor indicate la punctele a) și b);

d) să formuleze cerințe pentru elementele sistemelor de gestionare a informațiilor clasificate și să elibereze certificate sau recomandări de conformitate a acestora, pe baza examinărilor și a certificatelor de conformitate;

e) să îndeplinească funcția de supraveghere a activităților de codificare;

f) să exercite dreptul de a aviza numirea șefilor de securitate ai organismelor care gestionează informații clasificate;

g) să monitorizeze practicile de clasificare utilizate de clasificatori, context în care, poate emite recomandări individuale sau generale pentru a stabili practici uniforme de clasificare sau poate întocmi analize referitoare la clasificare;

h) să îndeplinească funcția oficială de supraveghere a gestionării informațiilor clasificate la organul de gestionare a informațiilor clasificate, și să inspecteze conformitatea cu legile aplicabile protecției informațiilor clasificate, precum și normele de securitate personală, fizică, administrativă și electronică;

i) să elibereze certificatul de securitate pentru site-ul organizațiilor de afaceri eligibile și să modifice certificatul de securitate al site-ului sau să-l retragă;

j) să investigheze toate rapoartele referitoare la protecția informațiilor clasificate;

k) să cerceteze toate evenimentele legate de pierderea de date clasificate, accesul neautorizat la informații clasificate și încălcarea securității la organul de gestionare a informațiilor clasificate;

l) să întocmească rapoarte privind informațiile clasificate la instituțiile desființate care nu au un succesor legal;

m) să implementeze sarcinile reglementate de autoritățile naționale de securitate în concordanță cu reglementările relevante ale Consiliului Uniunii Europene, Comisiei Europene, EURATOM, EUROPOL, EUROJUST (denumite în continuare în mod colectiv: UE), NATO și UEO și ale acordurilor internaționale privind protecția informațiilor clasificate;

n) să asigure colaborarea cu NATO, UEO, UE și organizațiile competente ale statelor membre și să le furnizeze informații cu privire la activitățile sale în limitele legale;

o) să reprezinte interesele naționale în comitetele internaționale și grupurile de lucru din domeniul protecției informațiilor clasificate;

p) să participe la pregătirea unor acorduri bilaterale sau multilaterale de securitate privind schimbul de informații clasificate, precum și în pregătirea tuturor acordurilor internaționale referitoare la informațiile clasificate;

q) să organizeze cursuri de formare continuă pentru șefii structurilor de securitate;

r) să coopereze cu Autoritatea Națională pentru Protecția Datelor și Libertății de Informare pentru respectarea dreptului constituțional de acces la date de interes public și pentru respectarea libertății de informare.

• Pentru a elibera certificatele personale de securitate, Autoritatea Națională de Securitate gestionează date în legătură cu:

a) persoana în cauză;

aa) datele de identificare personale;

ab) naționalitatea;

ac) documente de identitate, documente de călătorie;

ad) locul de muncă, funcția și responsabilitățile legate de utilizarea informațiilor clasificate;

ae) datele incluse în chestionarul de securitate și avizul experților astfel cum sunt definite de Legea privind serviciile naționale de securitate;

b) numărul, data expirării și nivelul de acces al certificatului personal de securitate eliberat.

• După expirarea termenului sau retragerea ultimului certificat personal de securitate, datele definite la paragraful anterior sunt gestionate de către Autoritatea de Securitate Națională pentru o perioadă de timp egală cu cel mai înalt nivel al sancțiunilor definite de Codul penal pentru fapta penală de abuz de informații clasificate.

- *Responsabilul cu securitatea și comitetul local de supraveghere a securității*

1) Șeful organismului de gestionare a informațiilor clasificate este responsabil pentru stabilirea condițiilor de protecție a informațiilor clasificate.

2) În cazul în care cantitatea de informații clasificate justifică, va fi desemnat un consiliu local de supraveghere ca organism separat, care să desfășoare activități de protecție, situație în care șeful de securitate are drept de control asupra acestuia.

Pentru încălcarea regimului informațiilor clasificate, sancțiunile sunt prevăzute în Codul Penal, la Titlul III:

- *Încălcarea regimului informațiilor clasificate cu indicativul STRICT SECRET și SECRET*

Orice persoană care:

- a) accesează și utilizează în mod neautorizat;
- b) permite accesul persoanelor neautorizate sau blochează accesul persoanelor autorizate la informații clasificate cu indicativul *SECRET* în temeiul Legii privind protecția informațiilor clasificate comite o infracțiune, care se pedepsește cu închisoare de până la 3 ani.

Se sancționează cu închisoare de la 1 la 5 ani, dacă fapta penală este comisă în legătură cu regimul informațiilor clasificate cu indicativul *STRICT SECRET* sau în cazul în care informații clasificate cu indicativul *SECRET* au devenit accesibile pentru persoane străine neautorizate.

Se sancționează cu închisoare de la 2 la 8 ani, dacă fapta penală a avut drept rezultat accesul unei persoane străine neautorizate la informații clasificate cu indicativul *STRICT SECRET*.

Persoana care a întreprins acțiuni pregătitoare prin care a încălcat regimul informațiilor clasificate poate fi pedepsită cu închisoare de până la 2 ani în cazul unei contravenții și cu închisoare de până la 3 ani la săvârșirea unei infracțiuni.

- Încălcarea regimului informațiilor clasificate cu indicativul CONFIDENȚIAL

Orice persoană care:

- a) accesează și utilizează în mod neautorizat;
- b) permite accesul persoanelor neautorizate sau blochează accesul persoanelor autorizate la informații clasificate cu indicativul *CONFIDENȚIAL* în conformitate cu prevederile Legii privind protecția informațiilor clasificate săvârșește o contravenție care se pedepsește cu închisoare de până la 1 an sau muncă în folosul comunității sau plata unei amenzi.

În cazul în care fapta are drept rezultat accesul unei persoane străine neautorizate la informații clasificate confidențiale, pedeapsa este închisoarea de până la 3 ani.

Dacă faptele sunt comise de o persoană autorizată pentru utilizarea informațiilor clasificate, pedeapsa este închisoarea de până la 2 ani, respectiv de la 1 la 5 ani.

- Încălcarea regimului informațiilor clasificate RESTRICȚIONAT

1) Orice persoană care:

- a) accesează și utilizează în mod neautorizat;
- b) permite accesul persoanelor neautorizate sau blochează accesul persoanelor autorizate la informații clasificate cu indicativul *RESTRICȚIONAT*, comite o contravenție care se pedepsește cu muncă în folosul comunității sau amendă.

2) Pedeapsa este închisoarea de până la 1 an, muncă în folosul comunității sau plata unei amenzi în cazul în care fapta incriminată constă în accesul unei persoane străine neautorizate la informații clasificate cu indicativul *RESTRICȚIONAT*.

3) În cazul în care o persoană autorizată pentru utilizarea informațiilor clasificate comite o faptă prevăzută la art. (1), ea va fi pedepsită cu închisoare de până la 1 an, poate primi pedeapsa cu muncă în folosul comunității sau o amendă, iar în cazul art. (2) cu închisoare de până la 3 ani.

FRANȚA

Cadrul legal:

- **Constituția 1958, articolele 15 și 21;**
- **Codul Penal de la articolul 413-9 la articolul 414-9;**
- **Codul apărării, în special articolele R. 1132-2, R. 1132-3, D. 1132-5 și de la R. 2311-1 la R. 2312-2 ;**
- **Codul Muncii ;**
- **Codul piețelor publice;**
- **Codul patrimoniului;**
- **Decizia Curții Constituționale nr. 2011-192 QPC din 10 noiembrie 2011**

Codul Apărării, Partea reglementativă, capitolul referitor la protecția secretului apărării naționale, secțiunea informații și suporturi clasificate⁴, cuprinde modificările introduse prin Decretul nr. 2010-678 din 21 iunie 2010. În articolele R. 2311-2 și R. 2311-3 ale Codului apărării sunt definite cele trei nivele de clasificare. Conform articolului R. 2311-1, procedeele, obiectele, documentele, informațiile, rețelele informatice, datele informatizate sau fișierele care au caracter secret în ceea ce privește apărarea națională sunt denumite în Cod "*informații și suporturi clasificate*".

Art. R2311-2 precizează că informațiile și suporturile clasificate sunt împărțite pe trei nivele: 1. *FOARTE SECRET-APĂRARE*; 2. *SECRET-APĂRARE*; 3. *CONFIDENTIAL-APĂRARE*.

Conform art. R2311-3, nivelul *FOARTE SECRET-APĂRARE* este acordat informațiilor și suporturilor care se referă la prioritățile guvernamentale în domeniul apărării și la securitatea națională și a căror divulgare este de natură să afecteze foarte grav apărarea națională.

Nivelul *SECRET-APĂRARE* este rezervat informațiilor și suporturilor a căror divulgare afectează grav apărarea națională.

Nivelul *CONFIDENTIAL-APĂRARE* este rezervat informațiilor și suporturilor a căror divulgare este de natură a afecta apărarea națională sau ar putea conduce la descoperirea unui secret de apărare națională clasificat cu nivelul *FOARTE SECRET-APĂRARE* sau *SECRET-APĂRARE*.

Art. R2311-4 precizează că informațiile și suporturile clasificate poartă mențiunea nivelului lor de clasificare. Informațiile și suporturile clasificate care nu trebuie comunicate, total sau parțial, în funcție de conținutul lor, decât anumitor organizații internaționale sau anumitor state sau cetățenilor lor, au mențiunea specială care precizează statele, cetățenii sau organizațiile internaționale care ar putea avea acces la ele. Informațiile și suporturile clasificate care nu ar trebui comunicate în niciun caz total sau parțial organizațiilor internaționale, statelor străine sau cetățenilor lor, poartă, din punctul de vedere al nivelului de clasificare, mențiunea *SPECIAL FRANCE*.

În Codul apărării se precizează că modificările nivelului de clasificare și declasificarea, precum și modificările și ștergerea mențiunilor speciale sunt decise de autoritățile care au decis clasificarea.

În articolul R2311-5 al Codului apărării se menționează că Primul-ministru stabilește criteriile și modalitățile de organizare ale protecției informației și suporturilor clasificate la nivelul *FOARTE SECRET-APĂRARE*, definește

⁴ <https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000020411220&dateTexte=&categorieLien=cid>

clasificările speciale care corespund priorităților guvernamentale. În condițiile stabilite de Primul-ministru, fiecare ministru, pentru ceea ce intră în atribuțiile sale, stabilește informațiile și suporturile care vor fi stabilite la acest nivel.

În articolul R 2311-6 se precizează că, în condițiile stabilite de Primul-ministru, informațiile și suporturile clasificate ca nivel *SECRET-APĂRARE* sau *CONFIDENȚIAL-APĂRARE*, precum și modalitățile de organizare ale protecției lor, sunt stabilite de fiecare ministru în parte, pentru administrațiile și organismele care aparțin departamentului său ministerial.

În articolul R 2311-6-1 se menționează că sistemele de informație care conțin informații clasificate fac obiectul, înaintea de folosirea lor, unei omologări a nivelului lor de clasificare. Protecția acestor sisteme de informații, în condițiile fixate prin decret al Primului-ministru, în funcție de amenințările cu care acestea se confruntă în ceea ce privește disponibilitatea și integritatea informațiilor pe care le conțin, trebuie asigurată prin dispozitive, materiale sau logistice, agreeate de Agenția națională de securitate a sistemelor de informație. Autoritatea responsabilă de folosirea sistemului de informație atestă aptitudinea sistemului de a asigura, la nivelul solicitat, disponibilitatea și integritatea sistemului, precum și confidențialitatea și integritatea informațiilor pe care acesta le conține. Această atestare impune omologarea de securitate. Aplicarea acestor dispoziții se face prin decret al Primului-ministru.

În articolul R 2311-7 se menționează că nimeni nu este calificat a cunoaște aceste informații și suporturile clasificate dacă nu posedă o decizie de abilitare și nu are nevoie de ele, conform aprecierii autorității de folosire a sistemului sub controlul căreia se află. Abilitările se acordă atât persoanelor fizice cât și celor juridice. În articolul R 2311-8 se subliniază că decizia de abilitare precizează nivelul de clasificare al informațiilor și suporturilor clasificate pe care titularul le poate cunoaște precum și utilizarea lor. Acestea se stabilesc conform unor proceduri stabilite de către Primul-ministru.

Pentru nivelul "*Foarte secret-apărare*" decizia este luată de Primul-ministru și indică categoria sau categoriile speciale la care persoana abilitată are acces.

Pentru nivelul de clasificare "*Secret-apărare*" sau "*Confidențial-apărare*", decizia de abilitare este luată de fiecare ministru, pentru departamentul său ministerial. Conform articolului R2311-8-1, fiecare ministru poate delega, prin hotărâre a prefectului teritorial competent, semnarea deciziilor de abilitare a agenților plasați sub autoritatea prefectului și a persoanelor angajate în organismele care exercită aceste atribuții.

Conform prevederilor Codului Apărării, ministrul apărării poate delega, printr-un decret ministerial, puterile în materie de luarea deciziilor, pentru următoarele autorități din departamentul său ministerial:

- 1) șefii de stat major;
- 2) secretarul-general pentru administrație, directorii generali, directorii și șefii de serviciu ai administrației centrale;
- 3) șeful controlului general al armatelor și membri corpurilor inspecției, atașați direct ministerului;
- 4) comandanții formațiilor, comandanții organizatorici și operaționali al forțelor și interarme, comandanții formațiunilor administrative sau organismelor administrate, precum și directorii sau șefii de organisme care nu aparțin administrației centrale a ministerului apărării.

Cei delegați la punctele 1 și 4 pot delega semnarea subordonaților lor.

În articolul R2311-9 se menționează că ministrul apărării sau comandamentul este abilitat a restrânge utilizarea mijloacelor de comunicare și

informare, oricare ar fi ele, pentru a asigura protecția militarilor în operațiuni, pentru executarea misiunii sau securitatea activităților militare. Deținerea sau folosirea aparatelor fotografice, cinematografice, telefonice, telematice sau a celor care înregistrează sau posturilor de emisie sau recepție radiodifuziune sau televiziune în incinte și stabilimente militare sau în campanie, în cantonamente și vehiculele, limitele flotei și aeronavelor, pot fi supuse unei autorizări prealabile.

Conform Codului Penal: prin articolul 413-9, introdus prin Legea nr. 2009-928 din 29 iulie 2009, se precizează că: prezintă caracter secret al apărării în sensul prezentului articol procedeele, obiectele, documentele, informațiile, rețelele informatice, datele informatizate sau fișierele de interes pentru apărarea națională care au făcut obiectul clasificării destinate a restrânge difuzarea sau accesul lor. Pot face obiectul unor astfel de măsuri procedeele, obiectele, documentele, informațiile, rețelele informatice, datele informatizate sau fișierele a căror divulgare sau al cărui acces este de natură a prejudicia apărarea națională sau ar putea duce la descoperirea unui secret de apărare națională. Nivelele clasificării procedeele, obiectelor, documentelor, informațiilor, rețelelor informatice, datelor informatizate sau fișierelor care prezintă un caracter secret legat de apărarea națională și autoritățile cu responsabilități în definirea modalităților în care este organizată protecția sunt stabilite prin decret în Consiliul de Stat.

Prin art. 413-10 se precizează că se pedepsește cu 7 ani închisoare și 100.000 euro amendă fapta oricărei persoane care deține, prin stat sau profesie, fie prin funcție sau printr-o misiune temporară sau permanentă, un procedeu, obiect, document, informație, rețea informatică, dată informatizată, sau fișier care are un caracter secret legat de apărarea națională, sau distruge, deturneză, sustrage sau reproduce sau dă acces unei alte persoane non-calificate sau aduce la cunoștința publicului sau a unei persoane noncalificate. Se pedepsește cu aceleași pedepse fapta, oricărei persoane depozitare, de a fi lasat să acceadă la acestea, de a distruge deturna, sustrage, reproduce sau divulga procedeu, obiectul, documentul, informația, rețeaua informatică, data informatizată sau fișierul vizat de aliniatul precedent. Dacă persoana depozitară a acționat prin imprudență sau neglijență, infracțiunea este pedepsită cu 3 ani închisoare și 45.000 euro amendă.

Art. 413-11 precizează că se pedepsește cu 5 ani închisoare și 75.000 euro amendă fapta oricărei persoane neautorizate conform art. 413-10 care:

1. asigură posesia, accederea sau luarea în cunoștiință a unui procedeu, obiect, document, informație, a unei rețele informatice, date informatizate, sau unui fișier care prezintă caracterul unui secret legat de apărarea națională;
2. distruge, sustrage sau reproduce, în orice manieră, un astfel de procedeu, obiect, document, informație, rețea informatică, dată informatizată sau fișier;
3. aduce la cunoștința publicului sau a unei persoane neautorizate un asemenea procedeu, obiect, document, informație, rețea informatică, dată informatizată sau fișier.

În articolul 413-12 se menționează că tentativa se pedepsește.

Hotărârea din 30 noiembrie 2011 referitoare la aprobarea Instrucțiunilor generale interministeriale nr. 1300 asupra protecției secretului apărării naționale⁵,

⁵ Arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la Défense nationale, sursa:

versiunea consolidată din 15 martie 2015, incluzând ultimele modificări făcute prin aplicarea Decretului nr. 2014-445 din 30 aprilie 2014, art. 10, conține la Anexe, *Instrucțiunea generală* elaborată de guvernul francez pentru acest domeniu.

Noua reglementare a fost impusă de adoptarea Legii nr. 2009-928 din 31 iulie 2009 referitoare la programarea militară pe perioada 2009-2014 și a Decretului nr. 2010-678 din 21 iunie 2010 referitor la protecția secretului de apărare națională. În continuarea Cărții Albe a apărării naționale din iunie 2008 și conform deciziei Consiliului Constituțional din 10 noiembrie 2011, s-a urmărit consolidarea securității juridice a protecției secretului apărării naționale.

În introducerea Instrucțiunii generale se menționează că una din problemele juridice importante a fost cea legată de clivajul tradițional dintre apărare și securitate în ceea ce privește informația. În caz de divulgare, anumite informații prezintă un risc la adresa apărării și securității naționale, astfel încât numai anumite persoane trebuie să aibă drept de acces la ele. În acest context, anumite informații și suporturi dobândesc un anumit caracter secret, beneficiază de o protecție strictă juridică și materială. Instrucțiunile generale prezintă organizarea generală a protecției secretului legat de apărarea națională, clarificând obligațiile juridice și materiale inerente acestei protecții, condițiile în care fiecare ministru le va aplica, asigurând cea mai mare eficiență dispozitivului.

Instrucțiunea generală prezintă procedurile de abilitare și control ale persoanelor care pot avea acces la secret, tratamentul, schimbul, conservarea sau transportul documentelor clasificate și protecția lor. Procedura îmbină respectarea drepturilor constituționale legate de salvagardarea intereselor naționale și prevederile referitoare la infracțiunile penale. Conform acestora, orice persoană a cărei acțiune contravine dispozițiilor, compromițând secretul, se expune la sancțiuni administrative și penale.

Instrucțiunea generală stabilește criteriile, nivelele și condițiile clasificării informațiilor. Ea se referă, de asemenea, la schimburile de informații clasificate la nivel național, european și internațional. Ținând cont de faptul că toate statele își protejează informațiile clasificate, Franța, conform acordurilor de securitate semnate, garantează în timpul schimburilor reciproce de informații, protecția informațiilor clasificate transmise de alte state partenere.

În document se precizează că protecția nu se referă numai la informațiile clasificate transmise pe hârtie ci și prin mijloace informatice și electronice, la elaborarea, tratarea, stocarea și transmiterea lor. Sistemele de informare și comunicare specifice infrastructurilor vitale ale vieții economico-sociale, ale instituțiilor publice, prezintă vulnerabilități specifice. Amenințarea unor atacuri informatice multiforme și posibilitatea compromiterii utilizării acestora, impun reguli de securitate a sistemelor de informații adaptate evoluției rapide a tehnicilor și un nivel de expertiză ridicat, difuzat către toți actorii publici sau privați.

Instrucțiunea generală este structurată astfel:

- Titlul I - principiile și organizarea protecției; autoritățile competente;
- Titlul II - măsurile de securitate referitoare la persoane; referiri la accesul la secrete legate de apărarea națională, la acreditare, la anumite cazuri particulare;
- Titlul III - măsurile de securitate referitoare la suportii și informațiile clasificate.

În Titlul I sunt prezentate principiile generale și organizarea protecției. În document se menționează că protecția secretului se referă la toate domeniile de

activitate legate de apărare și securitate națională: politic, militar, diplomatic, științific, economic, industrial. Se precizează că sunt clasificate informațiile a căror divulgare este de natură a atinge apărarea și securitatea națională. Franța poate proteja informațiile pe care le schimbă cu organizațiile internaționale și alte state străine. Protecția secretului este asigurată prin asumarea responsabilității care se aplică domeniului public și privat.

Secretariatul general al apărării și securității naționale (SGDSN)⁶ este autoritatea națională referitoare la securitate care poate delega responsabilități către autoritățile de securitate din domenii particulare. Secretariatul aplică reglementările în domeniul protecției secretului⁷, respectiv art. 413-9 - 413-12 Cod Penal; art. D1132-8, art. L2311-1 și art. de la R2311-1 la R2311-12 ale Codului Apărării; Hotărârea din 30 noiembrie 2011 și Instrucțiunile generale interministeriale referitoare la protecția secretului apărării naționale anexate.

În capitolul I sunt prezentate principiile generale ale protecției secretului. În art. 1 sunt prezentate fundamentele protecției, menționându-se că secretul de apărare națională constituie un element important al apărării și asigurării securității naționale în domenii care au legătură cu acestea: politic, militar, diplomatic, științific, economic, industrial. Anumite informații referitoare la apărare și securitatea națională necesită o anumită protecție particulară care asigură limitarea difuzării, în condițiile definite de prezenta Instrucțiune. Atingerea securității și apărării naționale poate fi făcută prin divulgarea unor informații sau a unor suporti care au fost clasificate. Acordarea mărcii de clasificare se face așa cum a fost definită în articolele R. 2311-2, R. 2311-3 și R. 2311-4 ale Codului Apărării.

În art. 2 se definesc termenii utilizați, cu referire și la termenii de „informație sau suporturi clasificate” care desemnează procedeele, obiectele, documentele, informațiile, rețelele informatice, datele informatizate sau fișierele care prezintă un caracter secret al apărării naționale.

Articolul 3 precizează că Instrucțiunea generală se aplică tuturor administrațiilor centrale, serviciilor deconcentrate ale statului și instituțiilor publice naționale plasate sub autoritatea unui ministru, în toate entitățile, publice sau private, vizate de secretul apărării naționale, tuturor persoanelor deținătoare, chiar și cu titlu provizoriu, unui astfel de secret, inclusiv în cadrul achiziționării și executării unui contract.

În art. 3 se fac mențiuni referitoare la clasificare, amintindu-se prevederile din Codul Apărării referitoare la cele trei nivele de clasificare: **FOARTE SECRET-APĂRARE**; **SECRET-APĂRARE**; **CONFIDENTIAL-APĂRARE**.

În Instrucțiunea generală se precizează că decizia de clasificare cu titlu de secret de apărare națională a unei informații sau a unui suport are drept urmare plasarea sub protecția dispozițiilor specifice Codului Penal.

Aplicarea marcatului de clasificare constituie singurul mijloc de a-i conferi această protecție specială.

Publicarea sau cesionarea unor filme, fotografii sau înregistrări făcute în incinte, stabilimente militare construcții ale flotei sau aeronavelor, sau cu ocazia unor manevre sau oricăror operațiuni militare trebuie să aibă autorizarea prealabilă a comandantului formațiunii administrative.

O informație clasificată este compromisă când este adusă la cunoștința publicului sau nei persoane neabilitate sau care nu avea nevoie de o cunoaște.

⁶ <http://www.sgdsn.gouv.fr/>

⁷ http://www.sgdsn.gouv.fr/site_rubrique124.html

Evaluarea riscului de compromitere a informațiilor și suporturilor clasificate și a vulnerabilităților persoanelor sau sistemelor, din perspectiva atingerii intereselor fundamentale ale națiunii, are scopul de a garanta protecția secretului. Stricta aplicare a măsurilor de securitate definite prin Instrucțiunea prezentă, completată de difuzarea lor și sensibilizarea personalului, contribuie la eficacitatea dispozitivului și permite combaterea acțiunilor rău intenționate, adesea facilitate de ignoranță, imprudență, neatenție sau neglijență. Protecția secretului, când este vorba de informație sau de un suport, trebuie asigurată de persoanele fizice sau juridice, prin dreptul public sau privat. În caz contrar, chiar involuntar, aceste persoane se fac vinovate de compromiterea lor și suferă aplicarea sancțiunilor prevăzute la art. 413-10 și următoarele din Codul Penal.

Art. 5 face referiri la mențiunile speciale de confidențialitate făcute pentru anumite informații care nu sunt clasificate, dar care pot primi totuși, din partea celui care le emite, o marcă de confidențialitate, cu scopul de a restrânge difuzarea lor la un domeniu specific sau pentru a garanta protecția lor, cu mențiunea *difuzare restrânsă*. Aceste mențiuni, care nu corespund unor clasificări, nu atrag protecția penală proprie secretului de apărare națională. Scopul lor este de a sensibiliza utilizatorul la discreție, atunci când folosește documente pe care se află o astfel de mențiune. Cel care divulgă se expune la sancțiuni disciplinare sau profesionale. Mențiunea *difuzare restrânsă* atrage atenția că aceste informații nu trebuie difuzate decât acelor persoane care au atribuții în domeniu.

În art. 6 al Instrucțiunii generale se face referire la accesul la secretele legate de apărarea națională. Doar persoanele calificate pot avea acces la secretele legate de apărarea națională. Calificarea implică reunirea a două condiții cumulative:

- nevoia de a cunoaște sau de a accede la o informație clasificată, atestată de autoritatea care le utilizează: aprecierea nevoii de a cunoaște se bazează pe principiul conform căruia o persoană nu poate lua cunoștință de informații clasificate decât în măsură în care exercitarea funcției sau îndeplinirea misiunii sale o cere. Aceasta se face conform art. 20 al Instrucțiunii.

- emiterea autorizației corespunzătoare gradului de clasificare a informațiilor luate în considerare: decizia care permite o autorizație expresă, eliberată la sfârșitul unei proceduri specifice, definite în această Instrucțiune, care să permită unei persoane, sub rezerva nevoii de a cunoaște, de a avea acces la informații clasificate sau suporturi clasificate cu un nivel precizat în decizie, ca și de nivel sau nivele inferioare. Decizia care permite accesul este însoțită de un angajament de a respecta, în mod corespunzător, obligațiile și responsabilitățile legate de protecția informațiilor clasificate.

În art. 7 al instrucțiunii se face referire la locurile care adăpostesc informațiile clasificate, de orice nivel, precizându-se că acestea sunt spații deținute de persoane abilitate, conform exigențelor cerute. Accesul în aceste locuri, pe motiv de serviciu, este asigurat pe baza dispozițiilor din dreptul muncii, din contractele de prestare de servicii, din dreptul penal, conform procedurii penale sau celor din convențiile internaționale.

În art. 8 se face referire la controalele și inspecțiile organizate periodic pentru a verifica aplicarea dispozițiilor, de către organismele care emit, primesc, prelucrează sau conservă informații clasificate, conform instrucțiunilor și directivelor referitoare la protecția secretului.

Pentru organismele care prelucrează, tratează informații sau suporturi clasificate de nivelul **FOARTE SECRET-APĂRARE**, inspecțiile și controalele sunt asigurate de Secretariatul general al apărării și securității naționale (SGDSN).

Acesta propune toate măsurile necesare îmbunătățirii condițiilor generale de securitate. Acestea sunt efectuate în legătură cu departamentele ministeriale. Rapoartele de sinteză includ eventualele anomalii sesizate, măsurile de corectare a deficiențelor. La cererea ministrului de resort, controalele și inspecțiile periodice vizează organismele care prelucrează informații și suporturi clasificate de nivelul *SECRET-APĂRARE* și *CONFIDENȚIAL-APĂRARE*. Secretariatul general al apărării și securității naționale (SGDSN) poate inspecta aceste organisme.

În capitolul II se face referire la organizarea protecției secretului care trebuie să fie precisă, trebuie să asigure buna aplicare a măsurilor definite de Instrucțiunea generală.

Art. 9 precizează că Primul-ministru, conform art. 21 din Constituție, este responsabil cu apărarea națională. Conform articolelor R. 2311-5, R. 2311-6 și R. 2311-7 al Codului Apărării sunt menționate competențele Primului-ministru care:

- pentru nivelul *FOARTE SECRET-APĂRARE* stabilește criteriile și modalitățile de organizare a protecției și definește clasificările speciale care corespund diferitelor priorități guvernamentale; stabilește condițiile în care fiecare ministru, pentru departamentul de care răspunde, stabilește informațiile și suporturile clasificate la acest nivel;

- pentru nivelul *SECRET-APĂRARE* și *CONFIDENȚIAL-APĂRARE* stabilește condițiile în care fiecare ministru, pentru departamentul de care răspunde, indică informațiile și suporturile clasificate și modalitățile de protecție;

- în ceea ce privește abilitarea: definește procedura prealabilă luării deciziei de abilitare; ia decizia de de abilitare pentru nivelul *FOARTE SECRET-APĂRARE* și indică clasificările speciale la care persoana abilitată are acces. Pentru exercitarea acestor competențe, Primul-ministru este asistat de Secretarul general al apărării și securității naționale.

În art. 10 se face referire la Secretarul general al apărării și securității naționale (SGDSN) care, sub autoritatea Primului-ministru, definește și coordonează, pe plan interministerial, politica de securitate în domeniul protecției secretului de apărare națională. În această calitate, el propune, difuzează, aplică și controlează măsurile necesare protecției secretului. Competențele SGDSN se exercită în cadru național și internațional.

La nivel național, pentru toate nivelele de clasificare, SGDSN este responsabil de difuzarea și controlul aplicării măsurilor de protecție a secretului. În această calitate, el se asigură, pe baza unui raport care îi este furnizat anual, că acestea sunt respectate în fiecare departament ministerial. Pentru nivelul *FOARTE SECRET-APĂRARE*, el ia decizia de abilitare, prin delegarea Primului-ministru. Pentru supravegherea aplicării măsurilor și pentru asigurarea controlului el efectuează inspecții. El definește și organizează rețelele de securitate corespunzătoare și desemnează, pentru fiecare din clasificările speciale, un agent central de securitate ale cărui misiuni sunt definite prin instrucțiuni speciale. În secțiunea V sunt definite atribuțiile SGDSN în domeniul securității sistemelor de informații.

La nivel internațional, SGDSN, autoritatea națională de securitate (ANS) pentru secretul de apărare națională, pentru aplicarea acordurilor și tratatelor internaționale, este interlocutorul cu autoritățile de securitate străine. El negociază acordurile generale de securitate cu statele străine, organizațiile internaționale, instituțiile și organismele Uniunii Europene și este consultat în legătură cu un acord de interes, în ansamblu sau parțial, cu protecția reciprocă și schimbul de informații clasificate. SGDSN este informat, de către ministere, în legătură cu negocierile

dintr-un domeniu particular, cu acordurile referitoare la protecția reciprocă și schimbul de informații clasificate.

SGDSN participă, cu partenerii săi străini, la elaborarea reglementărilor în cadrul comitetelor de securitate ale organizațiilor și instituțiilor și organelor Uniunii Europene. El stabilește procedurile de abilitare cerute și organizează, dirijează și controlează rețelele de securitate corespunzătoare. SGDSN pune în practică acordurile internaționale referitoare la abilitarea cetățenilor francezi care merg în străinătate și pentru cetățenii străini aflați în Franța. SGDSN asigură, aplicând acordurile internaționale, securitatea informațiilor clasificate încredințate Franței. SGDSN stabilește toate măsurile de protecție a informațiilor și suporturilor pe care le deține Franța, care au fost clasificate de către un stat străin sau o organizație internațională.

Art. 11 definește responsabilitățile miniștrilor, fiecare ministru, în departamentul său, trebuind să aplice dispozițiile referitoare la securitatea informațiilor sau suporturilor clasificate deținute de orice serviciu sau entitate publică sau privată de sub autoritatea sa. În acest cadru vor fi efectuate inspecții periodice de verificare a aplicării acestora.

Ministrul ia decizia de abilitare pentru nivelele *SECRET-APĂRARE* și *CONFIDENTIAL-APĂRARE*. El identifică, în condițiile stabilite de Primul-ministru, informațiile și suporturile care urmează a fi clasificate pe unul din cele trei nivele și modalitățile de organizare a protecției pentru nivelele *SECRET-APĂRARE* și *CONFIDENTIAL-APĂRARE*.

Pentru ceea ce intră în atribuțiile sale, fiecare ministru stabilește prin instrucțiuni specifice, condițiile de folosire a nivelelor *SECRET-APĂRARE* și *CONFIDENTIAL-APĂRARE* și informațiile care ar trebui clasificate la nivel *FOARTE SECRET-APĂRARE*.

În art. 12 se face referire la înalții funcționari din apărare și securitate (HFDS), care, conform Codului apărării naționale, asistă fiecare ministru și care dispun de un serviciu specializat. Ei au autoritate asupra ansamblului direcțiilor și serviciilor departamentului ministerial. În cadrul acestora, ei sunt responsabili de difuzarea și aplicarea dispozițiilor referitoare la securitatea apărării și de protecția secretului. Ei supraveghează buna funcționare a serviciilor care gestionează informații și suporturi clasificate, verifică exactitatea inventarelor, procedează la controlarea și efectuează inspecțiile necesare, propun măsuri a consolidarea eficacității măsurilor de protecție aplicate. Ei iau, prin delegarea ministrului, deciziile de abilitare pentru nivelele *SECRET-APĂRARE* și *CONFIDENTIAL-APĂRARE*. Ei asigură legăturile necesare cu SGDSN pentru abilitările *FOARTE SECRET-APĂRARE* și pentru cele naționale și cele internaționale *SECRET-APĂRARE* și *CONFIDENTIAL-APĂRARE*.

Înalții funcționari din apărare și securitate au legătură cu omologii din alte ministere și cu secretarul general al apărării și securității naționale (SGDSN) căruia îi prezintă un raport anual cu: numele, numărul persoanelor abilitate, numărul abilitărilor în curs de validare, locurile care adăpostesc elemente aflate sub acoperirea secretului de apărare, volumul documentelor clasificate, catalogul utilizării și inventarelor, numărul controalelor și inspecțiilor efectuate, deficiențele relevate în dispozitivele de protecție a secretului, măsurile de corectare, cazurile de compromitere și acțiunile de formare. Acest raport este clasificat la nivel *CONFIDENTIAL-APĂRARE* și are marca *Special France*.

Pentru departamentele ministeriale care utilizează sisteme de informații este nevoie de asigurarea protecției printr-un funcționar de securitate a sistemelor de informații (FSSI), desemnat de HFDS și plasat sub autoritatea sa. În funcție de

propriile sisteme ale fiecărui minister, poate fi desemnat cel puțin un HFDS în organismele, întreprinderile, instituțiile publice aflate sub tutelă.

În Secțiunea 2 se face referire la organizarea funcțională, în art. 13, precizându-se modalitățile de delegare a semnăturii și stabilirea competenței, pentru fiecare nivel. În art. 14 se face referire la rolul autorităților ierarhice care au delegare de la ministru în acest domeniu.

În cadrul întreprinderilor publice sau private autorizate a trata sau a deține informații și suporturi clasificate, autoritatea ierarhică își asumă răspunderea aplicării măsurilor de securitate referitoare la protecția secretului. Dacă informațiile și suporturile clasificate ca *FOARTE SECRET-APĂRARE* trebuie utilizate în cadrul organismului, autoritatea ierarhică trebuie să ceară, prin instrucțiune specială a Primului-ministru, crearea unei antene de utilizare.

Pentru gestionarea, înregistrarea și conservarea informațiilor și suporturilor clasificate de nivel *SECRET-APĂRARE* sunt create birouri de protecție a secretului, în zone în care sunt respectate normele de securitate din respectiva instrucțiune. Autoritățile ierarhice se ocupă de abilitarea persoanelor aflate sub responsabilitatea lor.

În art. 15, se face referire la ofițerul de securitate, numit de șeful serviciului de angajări, care este corespondentul unui înalt funcționar din apărare și securitate/HFDS, în funcție de modalitățile proprii fiecărei structuri. Ofițerul de securitate stabilește regulile și consemnele de securitate referitoare la persoanele și informațiile sau suporturile de informații și controlează aplicarea lor. El participă la instrucția și sensibilizarea personalului în ceea ce privește protecția secretului. Ofițerul de securitate răspunde de abilitarea persoanelor și de legătura cu serviciile de anchetare, de controlul accesului în zone protejate. El poate conduce și biroul protecției secretului. Întreprinderilor publice sau private depozitare ale unor secrete de apărare națională sau titulare de piață care implică tratarea sau deținerea unor informații și suporturi clasificate trebuie să desemneze un ofițer de securitate.

În articolul 17 se face referire la rețelele de securitate *FOARTE SECRET-APĂRARE* în care protecția informațiilor și suporturilor clasificate de acest nivel este organizată prin reglementări speciale care completează dispozițiile cu caracter general din prezenta Instrucțiune. Conform acestora, nici un serviciu sau organism nu poate elabora, prelucra, stoca, pune în circulație informații și suporturi de acest nivel, fără să aibă în prealabil autorizarea din partea SGDSN. Circulația acestor informații pe cale electronică este interzisă. Serviciul sau organismul trebuie să dispună în mod imperativ de o antenă de utilizare, cu clasificarea corespunzătoare. Aceste antene de utilizare sunt create prin decizie a SGDSN, la propunerea ministrului. Circulația informațiilor și suporturilor clasificate implică obligatoriu o rețea de securitate pentru garantarea protecției fiecărei clasificări speciale. Un agent central de securitate, desemnat de SGDSN, exercită controlul centralizat al acestei circulații, prin diferite antene de utilizare. Responsabilul fiecărei antene este ales din personalul admis pentru clasificare specială și este asistat de un agent de securitate care veghează la respectarea regulilor referitoare la protecția secretului.

În Titlul III sunt prezentate măsurile de securitate referitoare la persoane, precizându-se că nu pot accede la informații clasificate decât persoanele abilitate și care au nevoie să le cunoască. Abilitarea este o procedură dificilă care nu trebuie angajată decât dacă ea este strict necesară și conformă catalogului de locuri de muncă. Controlul elementar permite verificarea acordului dat unei persoane, dacă aceasta prezintă un grad de încredere suficient pentru a i se autoriza accesul în locul care adăpostește secrete de apărare națională sau i se

poate încredința o misiune specială. Deciziile de abilitare sunt notificate celor interesați.

În capitolul I se face referire la accesul la secretul de apărare națională, în articolul 19 fiind enunțat principiul aplicat, în virtutea articolului R. 2311-7 al Codului Apărării, conform căruia nimeni nu este calificat să cunoască informații sau suporturi clasificate dacă nu este abilitat la nivelul cerut și dacă nu are nevoie să le cunoască.

În articolul 20 se face referire la *cataloagele locurilor de muncă*, făcându-se mențiunea că înalții funcționari de apărare și securitate elaborează instrucțiunile necesare pentru a se stabili, de către fiecare autoritate competentă, în cadrul serviciului de stat și organismului public sau privat, și pentru fiecare nivel de clasificare, lista locurilor de muncă sau funcțiilor care necesită accesul la informații sau suporturi clasificate. Aceste liste sunt denumite *cataloage ale locurilor de muncă*. Cei care verifică aceste cataloage, pe toate cele trei nivele, sunt HFDS. Cererile de abilitare se fac în funcție de aceste liste, acordându-se în mod excepțional și bine întemeiat, abilitarea pentru cei care nu sunt înscrși în cataloage. Cataloagele pot fi elaborate pe direcții, serviciu, pe nivel de servicii deconcentrate ale statului. Ele sunt actualizate anual. Autoritatea ierarhică apreciază posturile și funcțiile care pot cere acces la informații sau suporturi clasificate, evitând acordarea facilă a abilitărilor. În unele situații repertoarul persoanelor abilitate poate înlocui cataloagele.

În articolul 21 este abordată pe larg nevoia de a cunoaște, menționându-se că abilitarea nu trebuie să permită accesul fără limită la orice fel de informație sau la orice suport clasificat decât dacă autoritatea ierarhică apreciază că acest acces este necesar pentru exercitarea funcției sau pentru îndeplinirea misiunii. Autoritatea ierarhică apreciază în mod riguros și măsurat nevoia de a cunoaște informații clasificate.

Conform art. 22, candidații la abilitare sunt informați, prin menționări pe notițe individuale, ceea ce li se cere, obligațiile induse de abilitare, precum și dispozițiile referitoare la responsabilitatea penală în caz de compromitere. După notificarea deciziei de abilitare, informarea inițială se completează cu o ședință de sensibilizare a persoanei în cauză față de riscurile de compromitere, amintindu-se reglementările în vigoare.

În capitolul II se face referire pe larg la procedura de abilitare, în articolul 23 facându-se precizări legate de obiectul abilitării. Autoritatea ierarhică supraveghează abilitarea personalului aflat sub responsabilitatea sa. Abilitarea începe prin constituirea unui dosar, apoi prin aplicarea unei proceduri de abilitare, conforme cu nivelul corespunzător catalogului. Cererea de abilitare declanșează o procedură care verifică dacă o persoană poate, fără risc pentru apărarea și securitatea națională sau pentru propria securitate, să cunoască informații sau suporturi clasificate în exercițiul funcțiilor sale. Procedura cuprinde desfășurarea unei anchete de securitate care să permită autorității de abilitare să ia decizia în cunoștință de cauză. Informațiile sau suporturile clasificate nu pot fi aduse la cunoștința unei persoane neabilitate. Orice persoană care are nevoie de o abilitare, dar nu se supune procedurii de abilitare este îndepărtată din postul respectiv.

În articolul 24 se face referire la procedura de abilitare, menționându-se că procedura prealabilă deciziei de abilitare este o operațiune de lungă durată și care implică personal numeros. Astfel, dacă un post necesită o abilitare de nivel *SECRET-APĂRARE* sau *CONFIDENTIAL-APĂRARE*, procedura nu este angajată decât pentru persoana efectiv numită, cu excepția unor cazuri speciale. Pentru

abilitarea cerută de nivelul *FOARTE SECRET-APĂRARE*, autoritatea de angajare apreciază oportunitatea desfășurării unei anchete în legătură cu fiecare candidat.

1. Constituirea dosarului are ca obiect identificarea elementelor care vor fi verificate prin ancheta de securitate. Pentru simplificare, se poate conveni dematerializarea procedurilor. Astfel, cererea de abilitare și nota individuală pot fi încărcate și completate pe cale electronică. Transmiterea serviciului de anchetă poate să se facă pe cale electronică, cu condiția ca sistemul de informare folosit să garanteze identificare și autentificarea emitentului ca și a destinatarului, să asigure confidențialitatea și integritatea datelor și să permită urmărirea acțiunilor efectuate. Dacă recursul la forma dematerializată nu este posibil, dosarul de abilitare se constituie la cererea formulată de șeful serviciului angajări care atestă nevoia cunoașterii informațiilor sau suporturilor clasificate, la un anume nivel, de către o persoană nominalizată. Cererea este însoțită de o notă individuală de securitate, completată de cel interesat și verificată de ofițerul de securitate al serviciului sau de organismul căruia îi aparține. Acesta este întocmit în trei exemplare (un original și două copii, datate și purtând semnătura originală a solicitantului) și trei fotografii tip pașaport originale, recente și identice. Dosarul de abilitare este trimis de către șeful de serviciu pentru angajări la autoritatea de abilitare (SGDSN, HFDS, ASD, prefect) care verifică caracterul complet și transmite instrucțiunea: pentru nivelul *FOARTE SECRET-APĂRARE*, la SGDSN, care investighează prin serviciile de anchetă competente; pentru nivelul *SECRET-APĂRARE* și *CONFIDENȚIAL-APĂRARE*, direct la serviciul de anchetă competent.

2. Investigarea cazului include ancheta de securitate care este un studiu administrativ realizat cu scopul de a detecta posibilele vulnerabilități ale candidatului.

Aceasta este realizată de: serviciul de anchetă al Ministerului de interne pentru personalul civil (inclusiv cei care lucrează pentru jandarmerie) sau organizațiile care lucrează în sectorul civil; serviciile de anchetă ale Ministerului Apărării pentru civilii sau militarii Ministerului Apărării, personalul militar al Jandarmeriei, personalul angajat în organizații sau companii care lucrează pentru Ministerul Apărării.

Ancheta administrativă se bazează pe criterii obiective, aplicate pentru a stabili dacă persoana în cauză, prin comportamentul său sau prin mediul său imediat, are o vulnerabilitate, fie pentru că ea însăși este o amenințare la adresa secretului, fie pentru că ea este în pericol de șantaj sau sub presiuni exercitate de un serviciu de informații externe, de un grup terorist, de o organizație sau persoană care desfășoară activități subversive și care ar putea pune în pericol interesele statului.

3. Închiderea investigației și avizul de securitate este ultima etapă a procedurii de abilitare. Ancheta administrativă realizată ca parte a abilitării este completată prin emiterea unui aviz de securitate, prin care departamentul de investigare trimite concluziile autorității competente care este singura în măsură să ia decizia de abilitare. Acest aviz este o evaluare a vulnerabilităților eventuale, detectate în timpul anchetei și permite autorității decizionale să aprecieze oportunitatea abilitării individului, având în vedere probele furnizate și garanțiile pentru nivelul de securitate cerut. Concluziile referitoare la securitate pot fi de trei tipuri:

- aviz fără obiecție, când investigația nu a relevat nici o vulnerabilitate de natură a reprezenta un risc pentru securitatea informațiilor sau suporturilor clasificate, nici pentru persoana în cauză;

- aviz restrictiv, când persoana în cauză prezintă anumite vulnerabilități care constituie riscuri directe sau indirecte pentru securitatea informațiilor sau suporturilor clasificate la care ar avea acces, dar și măsurile specifice luate de ofițerul de securitate pentru a le lua sub control;

- aviz defavorabil, când au apărut informații precise că persoana în cauză are vulnerabilități care reprezintă riscuri pentru secret, astfel încât nicio măsură nu pare a fi suficientă pentru a le neutraliza.

Avizul de securitate este emis pentru un nivel anume de abilitare.

Avizul fără obiecție este valabil pentru un nivel precizat ca și pentru nivelele inferioare. Pentru avizul restrictiv sau defavorabil serviciile de anchetă se pronunță, caz cu caz, asupra oportunității acordării abilitării pentru nivelele inferioare. Avizele restrictiv sau defavorabil pot fi clasificate conform aprecierii serviciului de anchetă. Avizele acordate sunt însoțite de o fișă confidențială în care se indică motivarea avizului. Această fișă este compusă din două părți: una în care se indică elementele non-clasificate care pot fi comunicate candidatului, celalaltă care este destinată doar autorității de abilitare. Fișa confidențială se returnează după comunicare și se păstrează la serviciul de anchetă respectiv. Durata valabilității avizului de securitate este stabilită în funcție de nivelul de abilitare solicitat, neputând să depășească 5 ani pentru nivelul *FOARTE SECRET-APĂRARE*; 7 ani pentru nivelul *SECRET-APĂRARE* și 10 ani pentru nivelul *CONFIDENȚIAL-APĂRARE*. Avizul de securitate nu constituie, în sine, nici autorizarea nici respingerea ei și nu înlocuiește autoritatea de abilitare care ia decizia, după ce a luat în considerare diferitele elemente instrumentate la dosar.

Art. 25 precizează că decizia de abilitare sau refuzul ei sunt în legătură cu concluziile serviciului de anchetă. Oricare ar fi sensul rezultatelor anchetei de securitate, în decizie nu se face nici o referire la avizul de securitate, autoritatea putând accepta sau respinge o cerere de abilitare. Autoritatea de abilitare poate decide, dacă ancheta a evidențiat vulnerabilitatea elementelor, să acorde abilitarea, numai după luarea unor precauții speciale. Astfel, pentru a asigura în modul cel mai eficient protecția informațiilor clasificate, se atrage atenția angajatorului, printr-o procedură de avertizare, sau printr-o procedură de alertă în legătură cu persoana respectivă, cu riscurile la care aceasta ar fi expusă. Procedurile de avertizare și vigilență pot fi combinate.

1. Decizia de abilitare este decizia care acordă abilitarea unei persoane, în funcție de nevoia de a fi informat, pentru a avea acces la informații clasificate la nivelul specificat în decizie, precum și la nivelele inferioare. Pentru nivelul *FOARTE SECRET-APĂRARE*, decizia precizează clasificarea specială. Dacă o persoană trebuie să aibă acces în mod regulat la informații cu mai multe clasificări speciale, va fi emisă o decizie de abilitare pentru fiecare dintre ele.

2. *Avertizarea* se lansează atunci când avizul de securitate este restrictiv sau defavorabil, autoritatea de abilitare putând să acorde abilitarea, punând în gardă ofițerul de securitate competent. Această procedură permite acestuia să aplice măsuri de securitate sau să aplice precauții suplimentare în raport cu persoana în cauză, dacă este necesar, cu consultarea HFDS sau a serviciului de anchetă. Acestea decid dacă elementele relevate de anchetă pot fi comunicate ofițerului sau angajatorului. Pentru nivelul *FOARTE SECRET-APĂRARE* procedura de avertizare este acordată de către SGDSN care păstrează abilitarea acordată.

3. *Alerta* se instituie când autoritatea de abilitare decide să acorde abilitarea pe baza unui aviz de securitate restrictiv sau defavorabil, alegând să solicite starea de alertă în legătura cu persoana în cauză. Aceasta constă în a sensibiliza pe cel în cauză în legătură cu elemente de vulnerabilitate relevate de anchetă, acest

dialog purtându-se în prezența ofițerului de securitate din serviciul respectiv. Autoritatea de abilitare definește modalitățile de alertă în legătură cu serviciul de anchetă, pentru fiecare caz în parte, solicitând prezența unui reprezentant al acestuia la întrevvedere cu persoana în cauză. În funcție de situație, ofițerul de securitate studiază cu acest serviciu măsurile de securitate complementare care trebuie luate. Cu această ocazie se elaborează o atestare specifică, semnată de ofițerul de securitate al serviciului de angajări, de persoana în cauză, de reprezentantul autorității de abilitare. Atestarea specifică este păstrată de autoritatea de abilitare. Pentru nivelul **FOARTE SECRET-APĂRARE**, aplicarea alertei este făcută de către SGDSN care păstrează atestarea.

4. Respingerea abilitării este adusă la cunoștință persoanei în cauză, nefiind nevoie să fie motivată.

În art. 26 se face referire la notificarea deciziei luate de autoritatea de abilitare care este transmisă ofițerului de securitate. La primirea ei, acesta o notifică candidatului la abilitare, indiferent dacă este favorabilă sau nu. Dacă decizia este favorabilă, persoana în cauză semnează un angajament de responsabilitate prin care sunt luate la cunoștință obligațiile speciale impuse de accesul la informațiile sau la suporturile clasificate, precum și sancțiunile prevăzute de Codul penal, aplicate în caz de neatenție deliberată, precum și reglementările referitoare la secretul de apărare națională. Se notifică de asemenea celui interesat perioada abilitării, precum și obligația de a comunica ofițerului de securitate orice schimbare referitoare la viața lui personală (căsătorie, divorț, PACS, ruptura unei vieți în comun, etc), la activitatea profesională sau la locul de reședință. Persoanei în cauză i se semnalează că trebuie să informeze în legătură cu orice relație existentă cu unul sau mai mulți cetățeni străini, stabilită în afara cadrului profesional. Ofițerul le va notifica autorității de abilitare care ar putea decide o reexaminare a dosarului de abilitare de către serviciul de anchetă care, la rândul său, va studia emiterea unui nou aviz și reluarea procedurilor. În cazul refuzului abilitării, decizia este notificată persoanei în cauză de către ofițerul de securitate care informează în legătură cu căile de recurs aflate la dispoziție pentru a contesta această decizie. Dacă candidatul solicită autorității de abilitare explicarea respingerii, candidatului i se comunică motivele, numai dacă acestea nu sunt clasificate.

În art. 27 se face referire la durata validității abilitării, menționându-se că aceasta este în legătură cu durata ocupării postului și că încetează atunci când acesta părăsește locul de muncă. În decizia de abilitare se precizează, de obicei, durata abilitării.

În art. 30 se precizează că abilitările, dosarele în curs de abilitare sunt înscrise de fiecare departament ministerial, într-un *repertor al abilitărilor*, acordate pe toate cele trei nivele de clasificare. SGDSN deține repertoriul central al abilitărilor **FOARTE SECRET-APĂRARE**, inclusiv cele din domeniul internațional.

În articolul 31 se face referire la încetarea abilitării care se poate realiza odată cu încetarea funcțiilor, cu expirarea abilitării în legătură cu ocuparea postului. Aceasta poate fi reînnoită, în termen de șase luni de la data expirării. Retragera abilitării în cursul validității mandatului de abilitare se efectuează dacă persoana în cauză nu mai îndeplinește condițiile inițiale de abilitare sau dacă au apărut elemente noi de vulnerabilitate sesizate de serviciul de anchetă, de superiorul ierarhic, de ofițerul de securitate. Decizia de retragere este notificată persoanei în cauză și în ea sunt menționate căile de recurs.

În capitolul III, art. 32 face referire la cazurile particulare legate situații speciale: aplicarea unei proceduri de control simplificate, solicitată de autoritatea de abilitare, prin acord; procedura de urgență care este o procedură excepțională acordată în termen foarte scurt, pe o durată de maximum 6 luni. Pentru informațiile *FOARTE SECRET-APĂRARE* acestea sunt acordate de SGDSN.

În articolul 37 se face referire la abilitarea cetățenilor străini care se poate face numai pentru nivelul *CONFIDENTIAL-APĂRARE* sau *SECRET-APĂRARE*, de către ministrul respectiv sau autoritatea de securitate delegată (ASD).

În articolul 38 se precizează că abilitarea în domeniul internațional pentru acces la informații și suporturi clasificate se face prin aplicarea acordurilor internaționale pe care Franța le-a semnat cu statele membre ale NATO, a dispozițiilor juridice aplicabile în cadrul Uniunii Europene, a acordurilor de securitate semnate de Franța. Decizia de abilitare la nivel internațional nu dă acces la informații și suporturi clasificate de la nivel național.

În Titlul III se face referire la măsurile de securitate luate în legătură cu informațiile și suporturile clasificate. În preambul se menționează că decizia de a clasifica o informație sau un suport legat de un secret de apărare națională se ia pentru a restrânge accesul la acestea la persoanele abilitate și care justifică nevoia de a le cunoaște.

Informațiile și suporturile sunt clasificate conform criteriilor precizate în Instrucțiunea generală și se aplică după o apreciere riguroasă a oportunității ei, conform dispozițiilor penale corespunzătoare.

În capitolul I sunt prezentate pe larg principiile generale ale clasificării.

În secțiunea 1, în art. 38-41, se face referire la regulile clasificării, reamintindu-se că pentru nivelul *FOARTE SECRET-APĂRARE* responsabilitatea deciziei de clasificare aparține Primului-ministru, iar pentru nivele *SECRET-APĂRARE* și *CONFIDENTIAL-APĂRARE* ministrului de resort, cu respectarea regulilor stabilite de Primul-ministru.

În articolul 40 se precizează că aceste criterii de clasificare sunt stabilite prin Instrucțiune ministerială, de fiecare minister în parte, nivelul de clasificare fiind stabilit în funcție de natura informației sau suportului. Dacă este cazul, este clasificată și sursa informațiilor și suporturilor clasificate.

În art. 42 se face referire la marcajul aplicat informațiilor și suporturilor clasificate, la principiile acestui proces și la elementele sale constitutive: timbrul, identificarea și paginarea (inclusiv marcarea paragrafelor alineatelor, anexelor). Acestea permit verificarea autenticității și integrității informației sau suportului. În Instrucțiunea generală sunt menționate prescurtările utilizate pentru marcaj și sunt analizate tipurile de marcaje.

Marcajul pentru suport hârtie are 3 elemente constitutive: timbrul, identificarea (care începe de la prima pagină) și paginarea.

Marcajul pentru suportul non-hârtie este adaptat fiecărui tip de suport, aplicându-se timbrul și identificarea. Când este imposibil de realizat această operațiune se aplică numărul de înregistrare. La paginarea documentelor electronice în josul primei pagini se menționează numărul total de pagini ale documentului. Paginile goale poartă mențiunea *Fără text*.

În secțiunea 3 se fac precizări în legătură cu înregistrarea informațiilor și suporturilor clasificate, în articolul 45 menționându-se că ele sunt înregistrate în ordine cronologică, prin sistem de înregistrare manual sau informatizat, prin metode care să permită identificarea destinatarului. Cel care face înregistrarea are răspunderea protecției datelor, alături de biroul de protecție a secretului.

În secțiunea 4 se fac precizări referitoare la durata clasificării, în articolul 46 menționându-se că sensibilitatea unei informații sau a unui suport clasificat poate evolua în funcție de timp și circumstanțe, autoritatea emitentă apreciind durata utilă a clasificării și menționând data declasificării.

În capitolul II se face referire la gestionarea informațiilor sau suporturilor clasificate. În secțiunea 1 se detaliază elementele legate de conservarea acestora, iar în articolul 47 se menționează condițiile materiale de conservare, mijloacele de securizare, păstrarea cifrurilor, procedurile de utilizare.

În secțiunea 2 sunt menționate regulile de reproducere, în articolul 48 făcându-se observația că generalizarea și diversitatea mijloacelor de reproducere cresc riscurile de difuzare necontrolată a informațiilor sau suporturilor clasificate. Pentru fiecare nivel de clasificare sunt desemnate procedurile de desemnare a celor responsabili de autorizarea reproducerii, procedurile de control al reproducerii, sistemul de înregistrare a numărului reproducerilor, protecția reproducerilor în funcție de fiecare material în parte.

În articolul 49 sunt făcute mențiuni speciale pentru reproducerea totală a unor informații și suporturi

În secțiunea 3 se face referire la inventarierea informațiilor sau suporturilor clasificate, în articolul 51 precizându-se că este nevoie a identifica permanent traseul documentelor clasificate și deținerea lor de către anumite persoane. Cu acest scop, fiecare minister va stabili metodele de inventariere și urmărire, de obicei anuală, a documentelor clasificate *SECRET-APĂRARE* și *CONFIDENȚIAL-APĂRARE*. Procesele verbale de inventar vor fi deținute de HFDS care le transmite la SGDSN, cel târziu până la data de 31 martie a fiecărui an.

În secțiunea 4 se fac referiri la protecția materialelor clasificate, în articolul 52 fiind menționate dispozițiile generale legate de toate stadiile trecerii lor (programarea, studiul, planul, fabricarea sau construcția, testarea, etc.), legate de utilizarea, întreținerea, repararea și transportul lor. Autoritatea responsabilă de acest proces, de la faza de program la livrare, deținere și utilizare, stabilește materialele de protecție, în funcție de nivelul de clasificare. Ele trebuie să elimine orice posibilități de identificare și detectare, terestre sau aeriene și utilizarea oricăror mijloace tehnice folosite în acest scop.

În articolul 53 se face referire la protecția în timpul transportului, iar în articolul 54 la difuzarea și arhivarea lor. În capitolele III și IV se prezintă în detaliu aceste măsuri de protecție. În secțiunea 1 se fac precizări în legătură cu protecția în procesul de difuzare, iar în secțiune 2 de cea din timpul procesului de arhivare.

În legătură cu difuzarea și expedierea se face precizarea că autoritatea de expediere stabilește lista destinatarilor și se asigură că aceștia sunt abilitați să le primească, notând numele și numărul lor. Pentru informațiile clasificate de nivelul *SECRET-APĂRARE* autoritatea de expediere este biroul de protecție a secretului; pentru nivelul *CONFIDENȚIAL-APĂRARE* expedierea este făcută de personalul abilitat în acest sens. Pentru expediere, autoritatea emitentă procedează la marcajul, înregistrarea fiecărui suport, prin operațiuni precise de anvelopare interioară și exterioară. Supravegherea expedierii se face prin intermediul borderoului de primire, urmărind păstrarea numărului de înregistrare. Formalitățile de recepție sunt îndeplinite de biroul de protecție a secretului al organismului destinatar. Acesta verifică integritatea ambalajului, înregistrează documentul, semnează de primire și trimite foaia B din borderou emitentului.

Art. 57 face referire la transportul informațiilor sau suporturilor clasificate, făcându-se precizări în legătură cu transportul în interiorul aceleiași imobil, de către deținător sau de o persoană abilitată sau curier intern; în legătură cu

schimbarea clădirii sau zonei geografice, printr-un transportator autorizat, pe cale militară, pe cale civilă, în funcție de nivelul de clasificare.

În art. 58 se face referire la transportul informațiilor sau suporturilor clasificate către străinătate, subliniindu-se că pentru acesta sunt autorizate mijloacele prin curier militar, valiză diplomatică, certificat de curier. Pentru transportul informațiilor sau suporturilor clasificate în cadrul NATO și UE se utilizează serviciul *recomandat internațional*.

În capitolul IV se face referire la distrugerea și arhivarea informațiilor sau suporturilor clasificate. În articolul 59 este descrisă procedura ordinară de distrugere pentru informațiile sau suporturile perimate sau inutile, menționându-se că ea este realizată de persoane abilitate, urmărindu-se a fi imposibilă refacerea lor. Tehnicile de distrugere sunt adaptate numărului și tipului suportului documentelor. În urma efectuării acestui proces se întocmește un proces verbal de distrugere care poartă semnătura autorității de distrugere, corespunzătoare fiecărui nivel. Aceasta informează autoritatea de clasificare în legătură cu efectuarea acestui proces.

În articolul 60 se face referire la evacuarea și distrugerea de urgență care se desfășoară în condiții excepționale și în caz de amenințare imediată, ea realizându-se conform unor planuri de evacuare și distrugere anterior elaborate.

În articolul 61 se face referire la principiile generale ale arhivării informațiilor sau suporturilor clasificate, precizându-se că orice autoritate care deține informații sau suporturilor clasificate, care produce sau primește astfel de documente are obligația de a asigura conservarea și protecția lor, conform dispozițiilor legislative sau regulamentelor de funcționare a serviciilor de arhivare atașate.

Codul patrimoniului definește arhivele conform anumitor elemente distinctive și instituie un regim specific de arhivare. În Instrucțiunea generală se precizează că serviciul istoric al apărării, arhivele ministerului afacerilor externe, direcția națională de patrimoniu au responsabilități în ceea ce privește arhivarea informațiilor sau suporturilor clasificate din domeniul apărării.

În articolul 63 se face referire la comunicarea către public a informațiilor sau suporturilor declassificate, arhivate. Aceasta se face respectând prevederile Codului penal, ale Codului patrimoniului și legii din 17 iulie 1978 referitoare la îmbunătățirea relației dintre administrație și public, cu modificările ulterioare. În acest demers se respectă condițiile de comunicabilitate impuse de lege.

BIBLIOGRAFIE

GERMANIA

- *Legea cu privire la condițiile și procedura de verificare a securității persoanelor și clasificării documentelor la nivel federal*

https://www.gesetze-im-internet.de/s_g/BJNR086700994.html#BJNR086700994BJNG000100307

SUEDIA

- *Legea privind accesul la informații publice și secrete*

<http://www.regeringen.se/contentassets/2c767a1ae4e8469bfd0fc044998ab78/public-access-to-information-and-secrecy-act>

ITALIA

- *Legea nr.124/2007 privind protejarea informațiilor*

https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/legge-124-2007.html#Capo_V

UNGARIA

- *Legea CLV din 2009 cu privire la protecția informațiilor clasificate*

<http://www.nbf.hu/aboutus.html>

FRANȚA

- *Codul Apărării*

<https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071307&idArticle=LEGIARTI000020411220&dateTexte=&categorieLien=cid>