Nr. 1393 /DPSG
DATA 31.05.2010

PARLAMENTUL ROMÂNIEI
SENAT
Nr. 191 10.06.2010

GUVERNUL ROMÂNIEI
PRIMUL – MINISTRU

**Domnule preşedinte,**

În conformitate cu prevederile art. 111 alin. (1) din Constituție, Guvernul României formulează următorul

**PUNCT DE VEDERE**

referitor la propunerea legislativă intitulată *„Lege privind măsurile de securitate ale sistemelor informatice”*, inițiată de 13 deputați – PD-L, PNL, PSD, UDMR, Minorități Naționale (Bp. 631/2009).

## I. Principalele reglementări

Propunerea legislativă are ca obiect de reglementare stabilirea *„sistemului de măsuri minime de securitate aplicabile sistemelor informatice din administrația publică”*, deoarece, conform *Expunerii de motive, „în acest moment nu există o reglementare a măsurilor de securitate pentru sistemele informatice din administrația publică, acest lucru conducând la o nepotrivire între informația care este vehiculată în cadrul administrației publice şi nivelul de securitate ce trebuie asigurat”.*

## II. Observații

1. Apreciem că denumirea actului normativ este improprie scopului declarat în *Expunerea de motive* în contextul în care teoria ştiinţifică şi standardele naţionale şi internaţionale de securitate abordează problematica securităţii sistemelor informatice şi de comunicaţii din perspectiva mult mai generală şi acoperitoare a sistemelor de protecţie proiectate corespunzător tipului şi valorii informaţiilor, având componente organizatorice, tehnice şi procedurale dimensionate în funcţie de rezultatele analizei de risc, care vizează în esenţă sistemele de management al securităţii informaţiilor la nivelul organizaţiilor.

2. Propunerea legislativă nu are definită o arie clară, fiind stabilită doar o excepţie de la aplicare, la art. 1 alin. (3) şi anume sistemele care prelucrează date cu caracter secret de stat. Semnalăm, în acest sens că pentru alte categorii de sisteme informatice, care nu se încadrează în excepţia anterior menţionată, există norme prin care este reglementată foarte clar securitatea acestora.

Sistemul de clasificare de securitate care se intenţionează a fi instituit este, din punctul nostru de vedere, mai complex şi mai complicat decât sistemul de clasificare a informaţiilor instituit prin *Legea nr. 182/2002 privind protecţia informaţiilor clasificate*, în sensul în care, potrivit acestui din urmă act normativ, sistemul de clasificare are la bază importanţa şi impactul consecinţelor divulgării informaţiilor în cauză, iar sistemul de clasificare ce se doreşte a fi reglementat este definit prin trei indicatori (F- fiabilitate, I - integritate şi C - confidenţialitate), doi dintre aceştia, respectiv integritate şi confidenţialitate, fiind detaliaţi deficitar, cel de-al treilea nefiind deloc explicitat).

De asemenea, menţionăm că există standarde internaţionale larg acceptate şi utilizate cu privire la aspectele care fac obiectul propunerii legislative în cauză din care o mare parte au fost acceptate ca Standard Românesc (ex. SR ISO 27001), acestea putând fi implementate în sistemele informatice. Totodată, menţionăm că la nivelul Uniunii Europene şi NATO au fost emise acte normative care reglementează protecţia informaţiilor neclasificate care pot fi implementate în cadrul sistemelor informatice. În plus, structurile INFOSEC de la nivelul Uniunii Europene şi NATO devin structuri de asigurare a informaţiilor (Information Assurance) prin includerea în sfera de competenţă şi a

informațiilor neclasificate, urmând ca această modificare să se aplice şi organizării şi modului de lucru al structurilor INFOSEC naționale.

3. Deşi denumirea şi primul articol fac trimitere către un sistem de măsuri de securitate, conținutul inițiativei legislative se limitează doar la încercarea de a prezenta un sistem de clasificare în funcție de obiectivele securității informațiilor vehiculate, fără a prezenta clar următoarele aspecte:

- căror categorii de sisteme informatice şi de informații le sunt aplicabile (publice, neclasificate dar nedestinate publicității, confidențiale, etc.);
- dacă aceste criterii se aplică numai sistemelor de protecție a informațiilor (aşa cum se deduce din art. 4) şi/sau sistemelor informatice care le vehiculează;
- dacă există şi care sunt elementele legate de rolul şi destinația sistemului la încadrarea acestuia într-o clasă de securitate;
- dacă există şi care sunt relațiile dintre stabilirea clasei de securitate a unui sistem şi procesul de management al riscurilor de securitate din sistemul respectiv.

4. Conform prevederilor **art. 1 alin. (1) şi alin. (3)** din propunerea legislativă, se doreşte instituirea unor măsuri minime de securitate aplicabile sistemelor informatice, precum şi stabilirea unor clase de securitate, care sunt aplicabile tuturor sistemelor informatice din instituțiile publice, cu excepția sistemelor informatice de prelucrare a datelor secrete de stat. *Per a contrario*, rezultă că nu sunt excluse de la aplicarea acestei propuneri sistemele informatice care prelucrează date – secrete de serviciu.

Precizăm că *Hotărârea Guvernului nr. 781/2002 privind protecția informațiilor secrete de serviciu* şi *Hotărârea Guvernului nr. 585/2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate* au fost adoptate în temeiul expres al dispozițiilor art. 31 alin. (1), art. 32 şi ale art. 42 lit. h), respectiv art. 6 alin. (1), art. 24 alin. (2), art. 30 şi ale art. 42 din *Legea nr. 182/2002 privind protecția informațiilor clasificate,* şi prevăd că informațiile secrete de serviciu se stabilesc de conducătorul persoanei juridice, pe baza normelor prevăzute prin hotărâre a Guvernului. În acelaşi sens, art. 1 lit. a) din Hotărârea Guvernului nr. 781/2002 prevede că „*Standardele naționale de protecție a informațiilor clasificate în România, aprobate prin Hotărârea*

*Guvernului nr. 585/2002, se aplică în mod corespunzător şi informaţiilor secrete de serviciu în ceea ce priveşte: a) clasificarea, declasificarea şi măsurile minime de protecţie".*

Având în vedere cele menţionate, semnalăm că deşi nu există niciun impediment din punct de vedere constituţional pentru o astfel de abordare, potrivit normelor de tehnică legislativă şi a practicii constante în elaborarea actelor normative, iniţiativa de a modifica şi completa o hotărâre a Guvernului, aparţine, de regulă, tot Guvernului. De aceea, pentru simplificarea procedurii de emitere a actului normativ, şi, totodată, pentru respectarea ierarhiei actelor normative, sugerăm analizarea posibilităţii introducerii modificărilor propuse pe calea unei hotărâri a Guvernului.

Pentru celelalte categorii de informaţii prelucrate pe sistemele informatice ale instituţiilor publice, sunt aplicabile prevederile *Legii nr. 544/2001 privind liberul acces la informaţiile de interes public,* care dispun, conform art. 5 şi art. 6 din lege, în sarcina autorităţilor sau instituţiilor publice, obligaţia publicării unor liste privind informaţiile de interes public comunicate din oficiu, respectiv comunicate la cerere.

Prin urmare, normele de securitate a sistemelor informatice din instituţiile publice vor fi elaborate în conformitate cu Legea nr. 182/2002, Hotărârea Guvernului nr. 585/2002, Hotărârea Guvernului nr. 781/2002, *Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, cu modificările şi completările ulterioare, Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date* şi cu *Legea nr. 544/2001.*

5. Referitor la definiţiile prevăzute la **art. 3**, apreciem că acestea trebuie completate/reformulate datorită caracterului incomplet şi ambiguu al acestora.

Totodată, **art. 3 lit. b)** ar trebui să nuanţeze dacă *„măsurile de securitate de bază"* se referă la:

- controlul accesului la serviciile reţelei (conexiunile la serviciile reţelei trebuie controlate, iar pentru obţinerea accesului la astfel de servicii este recomandată implementarea unei proceduri formale),
- controlul accesului la nivelul sistemului de operare (sistemul de operare trebuie să prevadă măsuri de restricţionare a accesului la date existente pe calculatoare),

- controlul accesului la aplicații (prevenirea accesului neautorizat la informațiile gestionate de aplicațiile software).

La **art. 3 lit. c)**, apreciem că definiția referitoare la *„securitatea de bază”* trebuie să facă referire la diferitele măsuri de securitate informatice (de ex. asigurarea securității fizice a sistemelor informatice, protecția antivirus; asigurarea unui mecanism de autentificare a utilizatorilor; asigurarea confidențialității şi integrității comunicațiilor, a datelor recepționate, transmise şi stocate; menținerea unei arhive electronice locale, menținerea unui registru automatizat de audit care cuprinde evenimentele legate de utilizarea şi administrarea sistemului informatic; aceste informații vor fi păstrate pentru o anumită perioadă şi în arhiva de siguranță).

**Art. 3 lit. i)** face referire la *„integritatea claselor de securitate”*, dar din conținutul definiției ar rezulta că se referă la *integritatea datelor* din sistemele informatice. Dacă se are în vedere integritatea datelor din sistemele informatice, atunci definiția ar trebui să cuprindă referiri la: validarea datelor de intrare, controlul procesării interne, autentificarea mesajelor transmise electronic, validarea datelor de ieşire, utilizarea tehnicilor de criptare, utilizarea mecanismelor de semnare electronică şi protejarea codului aplicațiilor şi a fişierelor sistemului de operare.

6. **Art. 4** ar trebui să conțină cerințe minime de securitate pe care un sistem informatic al instituției publice ar trebui să le îndeplinească (de ex. confidențialitatea şi integritatea comunicațiilor, confidențialitatea şi nonrepudierea comunicațiilor; autenticitatea părților care participă la transferurile de date; protecția datelor cu caracter personal; păstrarea secretului bancar; trasabilitatea transferurilor de date; împiedicarea, detectarea şi monitorizarea accesului neautorizat în sistem; restaurarea informațiilor gestionate de sistem în cazul unor calamități naturale şi evenimente imprevizibile).

7. Cu privire la soluția de la **art. 5**, apreciem că la determinarea clasei de securitate aceasta ar trebui să facă referire şi la următoarele aspecte: identificarea obiectivelor care trebuie protejate, identificarea riscurilor/amenințărilor specifice fiecărui obiectiv, ierarhizarea riscurilor, identificarea controalelor prin care vor fi eliminate/diminuate riscurile. Nu trebuie omis nici faptul că acest proces nu este unul static, ci, din contră unul dinamic, astfel spus trebuie avute în vedere schimbările care intervin în desfăşurarea activității instituției publice, pentru a fi reflectate

corespunzător în politica de securitate informatică. Dacă spre exemplu, apare o modificare legislativă cu impact asupra instituției, trebuie avut în vedere din nou modelul folosit pentru evaluarea riscurilor pentru a vedea dacă acesta reflectă riscurile apărute ca urmare a acestei modificări.

De asemenea, apreciem că propunerea legislativă ar trebui să menționeze şi modalitățile de rezolvare a incidentelor, având în vedere că raportarea incidentelor de securitate are ca obiectiv minimizarea efectelor negative sau a incorectei funcționări a sistemelor/echipamentelor.

Monitorizarea unor astfel de incidente permite determinarea performanței sistemelor de securitate şi îmbunătățirea continuă. Politicile şi procedurile de securitate trebuie implementate astfel încât să asigure un răspuns consistent la astfel de incidente.

Totodată, textul art. 5 este confuz în sensul că nu rezultă că *fiabilitatea* (în realitate, disponibilitatea) şi *integritatea* apar ca obiective de securitate ale clasei de securitate, contrar faptului că acestea constituie obiective de securitate ale informațiilor şi sistemelor informatice. De asemenea, sunt utilizați o serie de termeni în baza cărora ar trebui să se stabilească o anumită clasă de securitate, fără ca aceştia să fie explicitați sau definiți (de ex. performanța, viteza de răspuns în timpul de sarcină maximă, timpul de sarcină maximă la orele de vârf, sursă de informații, informații pentru uz intern, informații confidențiale, etc. ).

8. Semnalăm faptul că textul propunerii legislative nu cuprinde norme privind responsabilitatea implementării măsurilor de securitate sau tragerea la răspundere juridică în cazul nerespectării dispozițiilor acesteia, în contextul propus regăsindu-se, cu privire la acest aspect, doar instituirea obligației Ministerului Comunicațiilor şi Societății Informaționale de a aproba şi de a publica, pe pagina proprie pe Internet, un document privind implementarea măsurilor minime de securitate pentru sistemele informatice.

Apreciem că, în vederea reglementării domeniului securității sistemelor informatice în administrația publică, este necesară o evaluare corespunzătoare a riscurilor potențiale, a măsurilor de prevenire şi înlăturare a riscurilor, precum şi a costurilor pe care le-ar presupune implementarea măsurilor stabilite printr-un asemenea act normativ.

9. Din perspectiva motivării corespunzătoare a soluției legislative propuse, apreciem că în *Expunerea de motive* nu se formulează argumente suficiente în raport de art. 138 alin. (5) din Constituția

României, republicată, potrivit căruia *„Nici o cheltuială bugetară nu poate fi aprobată fără stabilirea sursei de finanțare”.*

În acelaşi sens, art. 15 alin. (1) din *Legea nr. 500/2002 privind finanțele publice*, prevede că *"În cazurile în care se fac propuneri de elaborare a unor proiecte de acte normative a căror aplicare atrage micşorarea veniturilor sau majorarea cheltuielilor aprobate prin buget, trebuie să se prevadă si mijloacele necesare pentru acoperirea minusului de venituri sau creşterea cheltuielilor".*

Totodată, potrivit art. 30 din *Legea nr. 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative, republicată, cu modificările şi completările ulterioare*, instrumentul de prezentare şi motivare trebuie să cuprindă mențiuni privind impactul financiar asupra bugetului general consolidat atât pe termen scurt, pentru anul curent, cât şi pe termen lung (5 ani), inclusiv informații cu privire la cheltuieli şi venituri.

Prin urmare, modificarea legislativă propusă nu îndeplineşte cerințele constituționale şi legale privind motivarea şi indicarea precisă a sursei financiare din care se vor asigura cheltuielile ocazionate de aplicarea acestui program.

## III. Punctul de vedere al Guvernului

Având în vedere considerentele menționate, **Guvernul nu susține adoptarea acestei propuneri legislative.**

Cu stimă,

**Emil BOC**

Domnului senator **Mircea Dan GEOANĂ**

Preşedintele Senatului