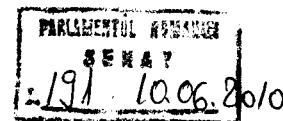
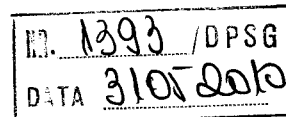




GUVERNUL ROMÂNIEI
PRIMUL – MINISTRU



Domnule președinte,

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 și 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 științifică și standardele naționale și internaționale de securitate abordează problematica securității sistemelor informatice și de comunicații din perspectiva mult mai generală și acoperitoare a sistemelor de protecție proiectate corespunzător tipului și valorii informațiilor, având componente organizatorice, tehnice și procedurale dimensionate în funcție de rezultatele analizei de risc, care vizează în esență sistemele de management al securității informațiilor la nivelul organizațiilor.

2. Propunerea legislativă nu are definită o arie clară, fiind stabilită doar o excepție de la aplicare, la art. 1 alin. (3) și 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 excepția anterior menționată, există norme prin care este reglementată foarte clar securitatea acestora.

Sistemul de clasificare de securitate care se intenționează a fi instituit este, din punctul nostru de vedere, mai complex și mai complicat decât sistemul de clasificare a informațiilor instituit prin *Legea nr. 182/2002 privind protecția informațiilor clasificate*, în sensul în care, potrivit acestui din urmă act normativ, sistemul de clasificare are la bază importanța și impactul consecințelor divulgării informațiilor în cauză, iar sistemul de clasificare ce se dorește a fi reglementat este definit prin trei indicatori (F- fiabilitate, I - integritate și C - confidențialitate), doi dintre aceștia, respectiv integritate și confidențialitate, fiind detaliați deficitar, cel de-al treilea nefiind deloc explicitat).

De asemenea, menționăm că există standarde internaționale larg acceptate și 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, menționăm că la nivelul Uniunii Europene și NATO au fost emise acte normative care reglementează protecția informațiilor neclasificate care pot fi implementate în cadrul sistemelor informatice. În plus, structurile INFOSEC de la nivelul Uniunii Europene și NATO devin structuri de asigurare a informațiilor (Information Assurance) prin includerea în sfera de competență și a

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

3. Deși denumirea și 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 și de informații le sunt aplicabile (publice, neclasificate dar nedestinate publicității, confidentiale, etc.);

- dacă aceste criterii se aplică numai sistemelor de protecție a informațiilor (așa cum se deduce din art. 4) și/sau sistemelor informatice care le vehiculează;

- dacă există și care sunt elementele legate de rolul și destinația sistemului la încadrarea acestuia într-o clasă de securitate;

- dacă există și care sunt relațiile dintre stabilirea clasei de securitate a unui sistem și procesul de management al riscurilor de securitate din sistemul respectiv.

4. Conform prevederilor **art. 1 alin. (1) și alin. (3)** din propunerea legislativă, se dorește instituirea unor măsuri minime de securitate aplicabile sistemelor informatice, precum și 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 și 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 și ale art. 42 lit. h), respectiv art. 6 alin. (1), art. 24 alin. (2), art. 30 și ale art. 42 din *Legea nr. 182/2002 privind protecția informațiilor clasificate*, și prevăd că informațiile secrete de serviciu se stabilesc de conducătorul persoanei juridice, pe baza normelor prevăzute prin hotărâre a Guvernului. În același 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 și informațiilor secrete de serviciu în ceea ce privește: a) clasificarea, declasificarea și măsurile minime de protecție”.

Având în vedere cele menționate, semnalăm că deși nu există niciun impediment din punct de vedere constituțional pentru o astfel de abordare, potrivit normelor de tehnică legislativă și a practicii constante în elaborarea actelor normative, inițiativa de a modifica și completa o hotărâre a Guvernului, aparține, de regulă, tot Guvernului. De aceea, pentru simplificarea procedurii de emitere a actului normativ, și, totodată, pentru respectarea ierarhiei actelor normative, sugerăm analizarea posibilității introducerii modificărilor propuse pe calea unei hotărâri a Guvernului.

Pentru celelalte categorii de informații prelucrate pe sistemele informatice ale instituțiilor publice, sunt aplicabile prevederile *Legii nr. 544/2001 privind liberul acces la informațiile de interes public*, care dispun, conform art. 5 și art. 6 din lege, în sarcina autorităților sau instituțiilor publice, obligația publicării unor liste privind informațiile de interes public comunicate din oficiu, respectiv comunicate la cerere.

Prin urmare, normele de securitate a sistemelor informatice din instituțiile 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 și protecția vieții private în sectorul comunicațiilor electronice*, cu modificările și completările ulterioare, *Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date* și cu *Legea nr. 544/2001*.

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

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

- controlul accesului la serviciile rețelei (conexiunile la serviciile rețelei trebuie controlate, iar pentru obținerea 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 restricționare 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 și integrității comunicațiilor, a datelor recepționate, transmise și stocate; menținerea unei arhive electronice locale, menținerea unui registru automatizat de audit care cuprinde evenimentele legate de utilizarea și administrarea sistemului informatic; aceste informații vor fi păstrate pentru o anumită perioadă și 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 ieșire, utilizarea tehnicilor de criptare, utilizarea mecanismelor de semnare electronică și protejarea codului aplicațiilor și a fișierelor 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 și integritatea comunicațiilor, confidențialitatea și nonrepudierea comunicațiilor; autenticitatea părților care participă la transferurile de date; protecția datelor cu caracter personal; păstrarea secretului bancar; trasabilitatea transferurilor de date; împiedicarea, detectarea și monitorizarea accesului neautorizat în sistem; restaurarea informațiilor gestionate de sistem în cazul unor calamități naturale și evenimente imprevizibile).

7. Cu privire la soluția de la **art. 5**, apreciem că la determinarea clasei de securitate aceasta ar trebui să facă referire și 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 desfășurarea 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 și 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 și îmbunătățirea continuă. Politicile și 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) și *integritatea* apar ca obiective de securitate ale clasei de securitate, contrar faptului că acestea constituie obiective de securitate ale informațiilor și 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 aceștia să fie explicați 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 și Societății Informaționale de a aproba și 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 și înlăturare a riscurilor, precum și 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 același 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 micșorarea veniturilor sau majorarea cheltuielilor aprobate prin buget, trebuie să se prevadă și mijloacele necesare pentru acoperirea minusului de venituri sau creșterea cheltuielilor"*.

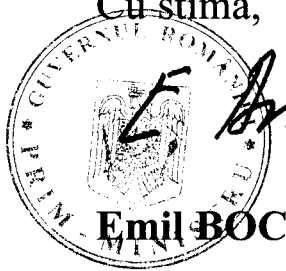
Totodată, potrivit art. 30 din *Legea nr. 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative, republicată, cu modificările și completările ulterioare*, instrumentul de prezentare și motivare trebuie să cuprindă mențiuni privind impactul financiar asupra bugetului general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

Prin urmare, modificarea legislativă propusă nu îndeplinește cerințele constituționale și legale privind motivarea și 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**

Președintele Senatului