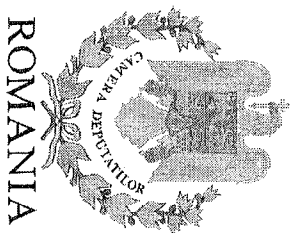


PARLAMENTUL ROMÂNIEI	GRUPUL PARLAMENTAR
CAMERA DEPUTAȚILOR	AL PARTIDULUI NAȚIONAL LIBERAL
NR. 2/103/23.12.2014	3c-151511
	14
	12
	23



Parlamentul României

Camera Deputaților

Grupul Parlamentar al Partidului Național Liberal

telefon: (021) 414 10 70

fax: (021) 414 10 72

email: pnl@cdep.ro

București, 23 decembrie 2014

C ă t r e ,

Secretariatul General al Camerei Deputaților

Domnului Adrian PANCIU

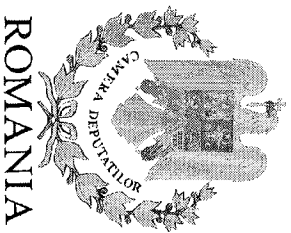
Domnule Secretar General,

În temeiul prevederilor art. 146 lit. a) din Constituție, și în baza art. 15, alin (1) din Legea 47/1992 privind organizarea și funcționarea Curții Constituționale, vă înaintăm *Sesizarea* la Curtea Constituțională cu privire la *Legea privind securitatea cibernetică a României*, adoptată de Senat, în calitate de Cameră decizională, la data de 19.12.2014.

Lider Grup PNL Camera Deputaților,

Deputat Ludovic ORBAN





Parlamentul României

Camera Deputaților

Grupul Parlamentar al Partidului Național Liberal

telefon: (021) 414 10 70

fax: (021) 414 10 72

email: pnl@cdep.ro

Domnului Augustin ZEGREAN
Președintele Curții Constituționale

Stimate domnule Președinte,

În temeiul art. 146 lit. a) din Constituția României, al art. 11 lit. a) raportat la art. 15 alin. (1) din Legea 47/1992 privind organizarea și funcționarea Curții Constituționale, republicată, deputații Partidului Național Liberal, înscriși pe lista anexată, formulează prezenta

SESIZARE DE NECONSTITUȚIONALITATE

prin care vă adresăm solicitarea de a constata neconstituționalitatea *Legii privind securitatea cibernetică a României*, adoptată de Senat, în calitate de Cameră decizională, la data de 19.12.2014.

Ne motivăm această sesizare prin următoarele:

1. Legea privind securitatea cibernetică a României este neconstituțională deoarece încalcă principiul legalității afirmat de Curtea Constituțională ca fiind fundamental pentru buna funcționare a statului de drept, **cu consecința nerespectării dispozițiilor art. 1 alin.(3) din Constituția României, care afirmă că „România este stat de drept..” și ale art.1 alin. (5) din Constituția României, conform căruia „în România respectarea Constituției, a supremației sale și a legilor este obligatorie”.**

Textul legii nu respectă, în opinia noastră, prevederile art. 6 din *Legea 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative*, astfel încât „(1)Proiectul de act normativ trebuie să instituie reguli necesare, suficiente și posibile care să conducă la o cât mai mare stabilitate și eficiență legislativă. Soluțiile pe care le cuprinde trebuie să fie temeinic fundamentate, luându-se în considerare interesul social, politica legislativă a statului român și cerințele corelării cu ansamblul reglementărilor interne și ale armonizării legislației naționale cu legislația comunitară și cu tratatele internaționale la care România este parte, precum și cu jurisprudența Curții Europene a Drepturilor Omului. (la data 18-Mar-2011 Art. 6, alin. (1) din *capitolul I modificat de Art. I, punctul 1. din Legea 29/2011*)”.

Așadar, sunt încălcate prevederile art.1 alin. (5) din Constituție conform căruia „*în România respectarea Constituției, a supremației sale și a legilor este obligatorie*”.

Prin aceasta lege se introduc foarte multe confuzii și condiționări pentru cei implicați, în special pentru deținătorii de infrastructuri cibernetică care vor trebui să se supună unor constrângeri generate de unele instituții ale statului, cele mai multe parte ale sistemului național de securitate al țării, aspect care poate genera neplăceri la nivelul relațiilor cu statele democratice europene, în special pe zona de

respectare și apărare a drepturilor și libertăților fundamentale ale cetățeanului protejate prin deciziile Curții Europene a Drepturilor Omului și Constituția României;

La art. 1 al Legii mai sus sesizate se constată că acest act normativ implică doar obligații pentru cei în drept și nu stabilește și drepturile acestora. Deci, se începe cu un dezechilibru fundamental în stabilirea firului logic și teleologic al normei juridice în cauză, prin introducerea de prevederi cu caracter de coerciție pentru persoanele vizate și unele excepții pentru autoritățile implicate în aplicarea acestei legi.

La art. 2 se constată că există o enumerare a entităților/persoanelor cărora li se aplică legea, în esență tuturor deținătorilor de infrastructuri cibernetice, dar fără a se preciza și situațiile în care apar intermediari ce pun la dispoziție astfel de infrastructuri, ce se întâmplă în cazul unor infrastructuri inactice neoperaționale, obligațiile pe care le au acționarii unor persoane juridice, fondatorii unor asociații, fundații sau organizații neguvernamentale care dețin astfel de infrastructuri.

2. Legea privind securitatea cibernetică a României are probleme fundamentale de concepție, propunând o serie de măsuri cu efect limitativ asupra dreptului la viață privată în zona digitală și încalcă în mod evident reglementările europene discutate pe subiectul securității informației. Astfel, sunt încălcate prevederile **articolului 26, alin.(1) din Legea fundamentală: "Autoritățile publice respectă și ocrotesc viața intimă, familială și privată"**.

3. Articolul 23 din Constituție - (1) Libertatea individuală și siguranța persoanei sunt inviolabile și articolul 28 - Secretul scrisorilor, al telegramelor, al altor trimiteri postale, al convorbirilor telefonice și al celorlalte mijloace legale de comunicare este inviolabil sunt încălcate în opinia noastră, prin subminarea gravă

a dreptului la viață privată al cetățenilor și încălcarea secretului corespondenței. Astfel, reținem din textul legii, următoarele articole:

Articolul 17 stipulează că deținătorii de sisteme cibernetice (adică persoanele juridice care au un calculator trebuie să „permită accesul la date” autorităților stipulate în lege (SRI, MAPN, MAI, ORNISS, SIE, STS, SPP, CERTRO și ANCOM). Accesul se face la simpla „solicitare motivată”, în condițiile în care astăzi, conform Codului de procedură penală, **orice acces la sistemele informatice (unde sunt stocate datele informatice) se poate face doar cu autorizarea unui judecător**. Mai mult, accesul la datele de trafic este momentan imposibil pentru organele legal abilitate tocmai deoarece Curtea Constituțională a considerat, prin decizia 440/2014, că un atare acces **nu respectă principiile respectării vieții private**. Cu acest prilej, Curtea a constatat următoarele:

“Legea nr. 82/2012 privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului, precum și pentru modificarea și completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice reprezintă transpunerea în legislația națională a Directivei 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE. Inșă Directiva 2006/24/CE a fost declarată nevalidă prin Hotărârea Curții de Justiție a Uniunii Europene din 8 aprilie 2014, pronunțată în cauzele conexe C-293/12 - Digital Rights Ireland Ltd împotriva Minister for Communications, Marine and Natural Resources și alții - și C-594/12 - Karner Landesregierung și alții. Prin hotărârea menționată instanța europeană a constatat că directiva analizată încalcă dispozițiile art. 7, art. 8 și art. 52 alin. (1)

din Carta drepturilor fundamentale a Uniunii Europene.” Totodată, amintim că în Decizia nr. 461 din 16 septembrie 2014 asupra obiecției de neconstituționalitate a dispozițiilor Legii pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice și Curtea a reținut faptul că, “deși nici Constituția și nici jurisprudența Curții Constituționale nu interzic stocarea preventivă, fără o ocazie anume, a datelor de trafic și de localizare, modalitatea prin care sunt obținute și stocate datele necesare pentru identificarea utilizatorilor serviciilor de comunicații electronice pentru care plata se face în avans, respectiv a utilizatorilor conectați la puncte de acces la internet nu respectă condițiile impuse de principiul proporționalității, nu oferă garanții care să asigure confidențialitatea datelor cu caracter personal, aducând atingere însăși esenței drepturilor fundamentale referitoare la viață intimă, familială și privată și la secretul corespondenței, precum și libertății de exprimare.”

Prin aceasta lege în mod mascat se restrâng drepturi și libertăți ale cetățeanului prin permiterea accesului la infrastructura cibernetică și la datele conținute în baza unei simple motivări comunicate de instituțiile abilitate și nominalizate prin lege fara existenta unei aprobari judecatoresti conform Codului de procedura penala si conform cerintelor adoptate de Curtea Constitutionala prin Deciziile 440/2014 si 461/2014, deci lege nu este armonizata la cerintele Curtii Constitutionale a României.

Articolul 10 stipulează că Serviciul Român de Informații este desemnat autoritate națională în domeniul securității cibernetice, calitate în care asigură coordonarea tehnică, organizarea și executarea activităților ce privesc securitatea cibernetică a României. În vreme ce Uniunea Europeană propune în directiva NIS ca instituțiile care se ocupă de domeniul securității cibernetice să fie „organisme civile, care să funcționeze integral pe baza controlului democratic, și nu ar trebui să

desfășoare activități în domeniul informațiilor”, Parlamentul României acordă acces nelimitat și nesupravegheat la toate datele informatice deținute de persoane de drept public și privat unor instituții care nu îndeplinesc niciuna din condițiile de mai sus.

Amintim faptul că, în 2014, Curtea Constituțională a României a mai constatat neconstituționalitatea Legii “Big Brother” și a Legii cartelelor prepay și a Wi-Fi-ului cu buletinul. Acestea erau acte normative în ton cu recent adoptata *Lege a securității cibernetice* și care încălcau grav dreptul la viață privată și protecția datelor personale, instituirea unui regim de supraveghere informatică total nedemocratic, sub pretextul protecției securității naționale. Mai mult, textul de lege care face obiectul prezentei sesizări nu prevede care sunt modalitățile de control asupra celor care utilizează informațiile obținute, precum și faptul că nu există garanția că datele nu pot fi folosite și în alte scopuri.

Faptul că în această vară Curtea Constituțională a declarat neconstituționale două legi care, în esență, încălcau aceleași drepturi ca și Legea la care ne referim, constituie un motiv suplimentar, serios pentru o dezbateră reală a implicațiilor Legii securității cibernetice și, într-un cadru mai larg, a echilibrului dintre **drepturile individuale** și securitatea națională pe care România trebuie să îl asigure prin sistemul său de legi.

4. Legea încalcă dispozițiile art. 148, alin (2) și următoarele, din Constituția României, prin netranspunerea corectă reglementărilor comunitare în materie. Totodată, considerăm că art. 17 alin. 1 lit. a) nu este conform cu jurisprudența Curții Europene de Justiție. În primul rând nu se precizează exact ce date necesită a fi deținute, iar cadrul în care se solicită aceste date nu prezintă suficiente garanții procesuale. A se vedea în acest sens cauzele reunite C-293/12 și C-594/12.

Totodată, considerăm că Legislația românească trebuie să țină seama de legislația europeană în materie și trebuie să fie în concordanță cu următoarele directive europene: 2006/24/EG, 2002/58/EG, sancționate de CJUE C-301/06.

CEDO a invalidat în aprilie 2014 directiva deoarece încălca drepturile fundamentale ale omului.

De asemenea, **Art. 17 alin. 1 lit. b)** nu e conform cu jurisprudența Curții Europene de Justiție. Pentru o astfel de informare este necesară o monitorizare perpetuă a tuturor persoanelor, aspect ce creează o obligație disproporționată pentru subiecții vizati și implică totodată încălcarea drepturilor persoanelor monitorizate fără să existe în legătură cu acestea o suspiciune în legătură cu eventualitatea comiterii vreunei infracțiuni. A se vedea în acest sens cauza **Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL** (C-70/10).

Legea contravine din multe puncte de vedere și propunerii de Directivă NIS (Network & Information Security) care pornește de la scopul protecției datelor personale ale cetățenilor și nu de la crearea de noi atribuții pentru serviciile secrete. În timp ce Directiva NIS are drept scop protejarea sistemelor informatice și a datelor informatice ale cetățenilor, Legea, în forma adoptată, reprezintă un cec în alb care poate fi folosit de serviciile de informații pentru a controla orice persoană de drept privat (SRL, SA, PFA, ONG) care deține un sistem informatic (adică orice calculator sau smart-phone). Potențialul pentru abuzuri este, astfel, enorm. Acesta decurge din nenumăratele ambiguități prezente în lege, începând de la definirea vagă a „deținătorilor de sisteme informatice” și continuând cu obligațiile ce le revin celor care cad sub incidența legii.

Întreaga arhitectura a actului normativ este de natura a permite încălcarea drepturilor fundamentale ale omului, fara a exista un remediu eficient impotriva unor astfel de incalcarari.

Așa cum a aratat constant in jurisprudenta sa, Curtea Europeana a Drepturilor Omului considera că „un sistem de supraveghere secretă destinat apărării siguranței naționale implică riscul de a submina, ba chiar de a distruge, democrația sub pretextul apărării ei” (*Klass și alții împotriva Germaniei*).

În cazul nostru, posibilitatea accesării fără mandat a datelor electronice provenind de la orice computer, indiferent de proprietarul său (pentru că datele trec prin serverele societăților ce oferă accesul la internet) este o ingerință nejustificată în dreptul la protecția corespondenței, adică în dreptul la viață privată, drept garantat de art. 26 și 28 din Constituție.

O astfel de ingerință nu numai că nu este necesară într-o societate democratică, dar ea are tocmai efectul contrar: subminează esența societății democratice.

Astfel, sub pretextul protecției împotriva atacurilor cibernetice, orice fel de date pot fi accesate la bunul plac al puterii executive, fără existența vreunui control al societății civile.

Mai mult, așa cum arată CEDO, deși într-o societate democratică limitele protecției drepturilor fundamentale pot fi reduce în cazul unor pericole deosebite (terorism, infracțiuni transfrontaliere) probele obținute prin aceste proceduri nu pot fi folosite în cazurile de drept comun (cele care nu implică protecția siguranței naționale, așa cum este ea definită prin lege), acolo unde garanțiile procedurale trebuie să fie strict respectate. Or, legea atacată nu instituie nicio interdicție de utilizare a datelor în orice alt mod decât cel necesar pentru protecția în fața atacurilor cibernetice, situație ce poate submina garanția unui proces echitabil.

Mai mult, legea nu prevede nicio interdicție cu privire la interceptarea comunicațiilor protejate prin legi speciale. Astfel, dreptul la apărare este încălcat, orice comunicații legale și legitime între avocat și acuzat putând fi interceptate fără

mandat și în secret, situație incompatibilă cu dispozițiile art. 24 alin. 1 din Constituție.

Pe cale de consecință vă rugăm, onorată Curte, să constatați că *Legea privind securitatea cibernetică a României* este neconformă cu prevederile art. 1, alin. (3) și (5), art. 23, 24, 26 și 28 din Constituție, fiind astfel neconstituțională.

În drept, ne motivăm sesizarea pe dispozițiile art. 55 alin.(1) din *Regulamentul activităților comune ale Camerei Deputaților și Senatului* și ale art. 15 alin.(1) și (2) din *Legea 47/1992 privind organizarea și funcționarea Curții Constituționale*.