

□□□□□□□□□□ □ □ □ □ □ □□□□□□□□



□□□□□□ **Comisia de apărare a Senatului precizează, într-un comunicat transmis sâmbătă, că proiectul de lege privind securitatea cibernetică a României nu se adresează persoanelor fizice, utilizatoare de internet, prevederile aplicându-se "persoanelor juridice de drept public sau privat".**

"Proiectul de lege nr 580/2014 privind securitatea cibernetică a României nu se adresează persoanelor fizice, utilizatoare de internet. Prevederile legii se aplică «persoanelor juridice de drept public sau privat, care au calitatea de proprietari, administratori, operatori sau utilizatori de infrastructuri cibernetică». Textul definește infrastructuri cibernetică drept «infrastructuri din domeniul tehnologiei, informației și comunicații, constând în sisteme informatice, aplicații aferente, rețele și servicii de comunicații electronice». Cu alte cuvinte, legea nu face obiectul reglementării activității posesorilor individuali de computere", se arată în comunicat.

Conform sursei citate, acest act normativ "asigură coordonatele generale legislative, necesare gestionării în mod coerent a acțiunilor privind securitatea cibernetică a țării, care este o componentă importantă a securității naționale".

"Articolul 17, care a generat un interes aparte și interpretări eronate, se referă la responsabilitățile pe care le au deținătorii de infrastructuri ciberneticе, persoane juridice de drept public sau privat, pentru asigurarea nivelului de protecție necesar împotriva atacurilor ciberneticе. Acești deținători de infrastructuri ciberneticе operează cu baze de date complexe, unele de interes național, iar aceasta lege îi obliga, practic, să protejeze aceste informații și să asigure sprijinul necesar la solicitarea motivată a structurilor care operează în domeniul securității ciberneticе. Adoptarea proiectului de lege a fost motivată de necesitatea asigurării unui cadru legal în fața amenințărilor ciberneticе, din ce în ce mai complexe și mai dese, și care pot afecta securitatea națională, nicidecum împotriva limitării libertăților individuale și a dreptului la liberă exprimare garantat de Constituție", se mai arată în comunicat.

Comisia de apărare amintește că la forumul industrial al NATO din noiembrie, din Croația, "s-a apreciat ca atacurile ciberneticе au cutremurat industria americană, cu pierderi estimate la peste 300 de mld de dolari".

"Mai mult decât atât, după atacul cibernetic devastator din Estonia, care a paralizat întreaga țară, statele membre NATO au decis înființarea unui Centru de Excelență aliat, dedicat apărării ciberneticе. În acest context, România nu putea rămâne în afara unui cadru legislativ adecvat, care să permită Ministerului Comunicațiilor intervenția în caz de atac cibernetic, în cooperare cu celelalte structuri ale statului de drept", menționează sursa citată.

Senatul a adoptat, vineri, proiectul de lege privind securitatea cibernetică a României, care prevede constituirea Sistemului Național de Securitate Cibernetică, coordonarea unitară a

activităților acestui Sistem fiind făcută de MAE, MAI, MApN, SRI, SIE, STS, SPP, ORNISS și CSAT.

Raportul Comisiei de apărare din Senat, cu amendamente, a fost adoptat cu 95 de voturi "pentru", iar proiectul de lege a fost adoptat cu 92 de voturi "pentru".

Senatul este Cameră decizională, după ce legea a trecut tacit de Camera Deputaților, pe 17 septembrie.

Legea stabilește cadrul general de reglementare în domeniul securității cibernetice și obligațiile ce revin persoanelor juridice de drept public sau privat în scopul protejării infrastructurilor cibernetice, inclusiv furnizorii de servicii de internet, și prevede obligații privind asigurarea securității sistemelor lor și notificarea clienților în situația unor incidente/atacuri cibernetice și luarea de măsuri pentru a restabili condițiile normale de funcționare.

Coordonarea activităților SNSC se realizează de către Consiliul Operativ de Securitate Cibernetică (COSC), format din reprezentanți ai Ministerelor de Externe, de Interne, Apărării, cel pentru Societatea Informațională, SRI, SIE, STS, SPP, ORNISS precum și secretarul CSAT.

Conducerea COCS este asigurată de consilierul prezidențial pe apărare și securitate națională, în calitate de președinte și consilierul premierului pe probleme de securitate, ca vicepreședinte.

SRI este desemnat autoritatea națională în domeniul cibernetic și asigură coordonarea tehnică a COSC. În acest sens, în structura SRI funcționează Centrul Național de Securitate Cibernetică (CNSC).

De asemenea, proiectul prevede că la nivel național se constituie Sistemul Național de Alertă Cibernetic, care reprezintă un ansamblu de măsuri și proceduri destinat prevenirii și contracarării atacurilor cibernetice.

Instituirea nivelurilor de alertă cibernetică precum și trecerea de la un nivel la altul de alertă se stabilește de către CSAT.

La articolul 17 al proiectului de lege se prevede că "(1) Pentru realizarea securității cibernetică, deținătorii de infrastructuri cibernetică au următoarele responsabilități: "a) să acorde sprijinul necesar, la solicitarea motivată a SRI, MAPN, MAI, ORNISS, SIE, STS, SPP, CERT-RO și ANCOM, în îndeplinirea atribuțiilor ce le revin acestora și să permită reprezentanților desemnați în acest scop la datele deținute, relevante în contextul solicitării; b) să informeze, de îndată, autoritățile și instituțiile publice prevăzute la lit. a) cu privire la incidentele cibernetică identificate, conform procedurilor stabilite prin normele metodologice la prezenta lege. (2) Deținătorii de infrastructuri cibernetică pot solicita asistență de specialitate autorităților și instituțiilor publice cu atribuții în domeniul securității cibernetică, pentru asigurarea securității cibernetică în domeniul lor de activitate".

Conform articolului 18 din lege, deținătorii de infrastructuri cibernetică, furnizorii de servicii de internet, au obligația de a-și notifica, de îndată, clienții, persoane de drept public și privat, în situațiile în care sistemele informatice utilizate de aceștia au fost implicate în incidente sau atacuri cibernetică și de a dispune măsurile necesare în vederea restabilirii condițiilor normale de funcționare dar nu mai târziu de 24 de ore din momentul în care au fost sesizați de autoritățile competente.

Monitorizarea și controlul aplicării legii se asigură de către Camera Deputaților și Senat, Administrația Prezidențială, Guvern, CSAT precum și instituțiile și autoritățile publice prevăzute la articolul 10, și anume Ministerelor de Externe, de Interne, Apărării, cel pentru Societatea Informațională, SRI, SIE, STS, SPP, ORNISS.

Legea prevede că în vederea exercitării atribuțiilor, conducătorii autorităților desemnează persoane abilitate să desfășoare activități de control, care, în baza și limitele împuternicirii au dreptul de a solicita declarații sau orice documente necesare pentru efectuarea controlului, să facă inspecții, inclusive inopinate, la orice instalație, incintă sau infrastructură, cu respectarea prevederilor legale în vigoare și să primească, la cerere sau la fața locului, informații sau justificări.

Contravențiunile includ amenzi de la 500 la 5.000 de lei, pentru nerespectarea de către deținătorii de infrastructură cibernetică a obligației privind punerea în aplicare a politicii de securitate cibernetică și amenzi de la 1.000 la 10.000 de lei, pentru nerespectarea obligației de a permite

autorităților să intervină, precum și a obligației de a reține și asigura integritatea datelor referitoare la incidentele ciberneticе.

Guvernul a adoptat, în aprilie, proiectul de lege privind securitatea cibernetică, ceea ce va permite operaționalizarea Sistemului Național de Securitate Cibernetică.

Proiectul a fost prezentat în dezbaterе publică de către Ministerul pentru Societate Informațională.

"Proiectul de lege adoptat de Guvern va permite operaționalizarea Sistemului Național de Securitate Cibernetică – SNSC, care va facilita adoptarea de măsuri proactive și reactive privind informarea, monitorizarea, diseminarea, analizarea, avertizarea, coordonarea, decizia, reacția, refacerea și conștientizarea. De asemenea, actul normativ definește o terminologie unitară în domeniul securității ciberneticе și a unui cadru armonizat de acțiune a autorităților și instituțiilor publice", se arată în comunicat.

La începutul lunii aprilie, Consiliul Suprem de Apărare a Țării a decis luarea unor măsuri care să permită contracararea amenințărilor ciberneticе la adresa României, în condițiile în care în ultima perioadă acestea s-au diversificat.

"S-a apreciat că în ultima perioadă aceste amenințări s-au diversificat, devenind o opțiune tot mai atractivă pentru actorii statali sau nonstatali întrucât nu implică resurse foarte mari. Membrii CSAT au decis luarea unor măsuri care să permită urgentarea adoptării cadrului normativ și operaționalizării Agendei Digitale 2020 ca parte integrantă a efortului european de dezvoltare a societății informaționale și implicit a acțiunilor subsecvente ce sunt dedicate securității ciberneticе", informa un comunicat al Administrației Prezidențiale.

** sursa - MEDIAFAX