Proiectul de lege privind securitatea si apararea cibernetica a României, adoptat

Senatul a adoptat, miercuri, în calitate de for decizional, proiectul de lege privind securitatea si apararea cibernetica a României, care prevede înfiintarea Sistemului National de Securitate Cibernetica în scopul organizarii si desfasurarii în mod unitar la nivel national a activitatilor specifice.

S-au înregistrat 81 de voturi "pentru", 29 "împotriva" si trei abtineri.

Proiectul de lege, adoptat de Camera Deputatilor, cuprinde cadrul juridic si institutional referitor la organizarea si desfasurarea activitatilor din domeniile securitate cibernetica si aparare cibernetica, a mecanismelor de cooperare si a responsabilitatilor institutiilor cu atributii în aceste domenii. Actul normativ stabileste actiunea autoritatilor si institutiilor publice cu responsabilitati si capabilitati specifice prevenirii si contracararii amenintarilor, vulnerabilitatilor si riscurilor cibernetice.

"Securitatea si apararea cibernetica se realizeaza prin adoptarea si implementarea de politici si masuri în scopul cunoasterii, prevenirii si contracararii vulnerabilitatilor, riscurilor si amenintarilor în spatiul cibernetic", prevede proiectul.

În scopul organizarii si desfasurarii în mod unitar la nivel national a activitatilor specifice securitatii cibernetice, se înfiinteaza Sistemul National de Securitate Cibernetica (SNSC) drept cadru general de cooperare care reuneste autoritatile cu responsabilitati si capabilitati în domeniile de aplicare a legii, în vederea coordonarii actiunilor la nivel national pentru asigurarea securitatii cibernetice.

Actul normativ se aplica în domeniul securitatii cibernetice pentru:

a) retelele si sistemele informatice detinute, organizate, administrate, utilizate sau aflate în competenta autoritatilor si institutiilor publice din domeniul apararii, ordinii publice, securitatii nationale, justitiei, situatiilor de urgenta, Oficiului Registrului National al Informatiilor Secrete de Stat;

b) retelele si sistemele informatice detinute de persoanele fizice si juridice de drept privat si utilizate în vederea furnizarii de servicii de comunicatii electronice catre autoritatile si institutiile administratiei publice centrale si locale;

c) retelele si sistemele informatice detinute, organizate, administrate sau utilizate de autoritati si institutii ale administratiei publice centrale si locale, altele decât cele prevazute anterior la lit. a), precum si de persoane fizice si juridice care desfasoara activitati cu scop lucrativ si nelucrativ de cercetare, dezvoltare, inovare si productie în domeniul tehnologia informatiei si a comunicatiilor sau furnizeaza servicii publice ori de interes public, altele decât cele de la lit. b).

Persoanele care au în responsabilitate aceste retele si sisteme informatice au obligatia de a notifica incidentele de securitate cibernetica prin intermediul Platformei Nationale pentru Raportarea Incidentelor de Securitate Cibernetica (PNRISC), de îndata, dar nu mai târziu de 48 de ore de la constatarea incidentului. Daca incidentele de securitate cibernetica nu pot fi comunicate complet în acest termen, acestea se transmit în cel mult 5 zile calendaristice de la notificarea initiala, informatiile putând fi completate si ulterior cu cele care reies din investigatiile realizate pe baza evenimentului.

Conform proiectului, "furnizorii de servicii tehnice de securitate cibernetica au obligatia de a pune la dispozitia autoritatilor (...), la cererea motivata a acestora, în termen de maximum 48 de ore de la data primirii solicitarii, date si informatii privind incidente, respectiv în maximum 5 zile de la data primirii solicitarii, amenintari, riscuri sau

vulnerabilitati a caror manifestare poate afecta o retea sau un sistem informatic, precum si interconectarea acestora cu tertii si cu utilizatorii finali".

Actul normativ stabileste sanctiuni în cazul nerespectarii de catre aceste persoane a obligatiei de notificare a incidentelor de securitate cibernetica, prin intermediul PNRISC, în termenul prevazut, a obligatiei de comunicare completa a incidentelor de securitate cibernetica, precum si pentru nerespectarea de catre furnizorii de servicii de securitate cibernetica a obligatiei de a pune la dispozitia autoritatilor date si informatii privind incidente, amenintari, riscuri sau vulnerabilitati a caror manifestare poate afecta o retea sau sistem informatic al detinatorului sau al unor terti, în termenul stabilit.

Sunt prevazute amenzi de la 5.000 lei la 50.000 lei, iar în cazul savârsirii unei noi contraventii în termen de sase luni limita maxima este de 200.000 lei.

Pentru operatorii economici cu o cifra de afaceri neta de peste 1.000.000 lei sanctiunea va fi cu amenda în cuantum de pâna la 1% din cifra de afaceri neta, iar, în cazul savârsirii unei noi contraventii, în termen de sase luni limita maxima a amenzii este de 3% din cifra de afaceri neta, potrivit unui amendament admis la comisiile de specialitate din Senat.