Proiect de lege al Ministerului Federal de Interne

Proiect de lege de consolidare a securității cibernetice[1]

Din ...

Bundestagul Germaniei, cu aprobarea Bundesratului Germaniei, a adoptat următoarea lege:

[…]

Articolul 4

Modificări aduse Legii privind protecția datelor și a vieții private în telecomunicații și servicii digitale

Legea privind protecția datelor în telecomunicații și servicii digitale din 23 iunie 2021 (Monitorul Oficial Federal I, nr. 1982; 2022 I, nr. 1045), astfel cum a fost modificată ultima dată prin articolul 3 din Legea din 10 martie 2026 (Monitorul Oficial Federal 2026 I, nr. 64), se modifică după cum urmează:

1. după articolul 19 alineatul (4), se adaugă următoarele alineate (5) și (6):

(1) „ În cazul în care un furnizor de servicii digitale ia cunoștință de o perturbare generată de unul dintre serviciile sale în timpul utilizării serviciului de către un utilizator, acesta trebuie să informeze imediat utilizatorul cu privire la acest lucru, cu condiția ca identitatea utilizatorului să fie cunoscută. În măsura în care acest lucru este posibil din punct de vedere tehnic și rezonabil din punct de vedere economic, furnizorul trebuie, în cadrul responsabilității sale privind serviciile digitale furnizate în scop comercial, să informeze utilizatorul cu privire la mijloacele tehnice adecvate, eficiente și accesibile prin care acesta poate detecta și remedia perturbarea. În cazul în care furnizorul a fost informat cu privire la perturbare de către Oficiul Federal pentru Securitatea Informațiilor (BSI), acesta trebuie să transmită utilizatorului toate informațiile incluse în notificarea privind perturbarea, care pot fi utilizate pentru identificarea și remedierea acesteia. Furnizorul poate redirecționa porțiuni din traficul de date către și de la un serviciu utilizat care se confruntă cu o perturbare, în măsura în care acest lucru este necesar pentru a notifica utilizatorul cu privire la perturbare.

(2) În cazul în care un furnizor de servicii digitale este informat de către Oficiul Federal pentru Securitatea Informațiilor (BSI) cu privire la amenințări specifice la adresa securității tehnologiei informației care survin sau afectează utilizarea de către un utilizator a unuia dintre serviciile sale, acesta trebuie să notifice imediat utilizatorul în acest sens, cu condiția ca identitatea utilizatorului să fie cunoscută. În acest sens, furnizorul trebuie, în special, să transmită utilizatorului toate informațiile conținute în notificarea din partea Oficiului Federal pentru Securitatea Informațiilor (BSI) în temeiul primei teze, care permit identificarea și prevenirea amenințărilor. În cazul în care un furnizor de servicii digitale constată existența unor amenințări la adresa securității sistemelor informatice care provin din utilizarea de către utilizator a unuia dintre serviciile sale sau care afectează această utilizare, acesta poate informa utilizatorul cu privire la acest lucru. În măsura în care acest lucru este posibil din punct de vedere tehnic și rezonabil din punct de vedere economic, furnizorul poate recomanda utilizatorului mijloace tehnice adecvate, eficiente și accesibile prin care acesta să poată identifica și preveni aceste amenințări.”

---

[1] Articolul 4 din prezenta lege este notificat în conformitate cu Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului din 9 septembrie 2015 referitoare la procedura de furnizare de informații în domeniul reglementărilor tehnice și a normelor privind serviciile societății informaționale (JO L 241, 17.9.2015, p. 1).

[…]

Justificare

B. Partea specială

Referitor la articolul 4 (Modificări aduse Legii privind protecția datelor și a vieții private în telecomunicații și servicii digitale)

Referitor la punctul 1

Prin noile alineate (5) și (6), furnizorii de servicii digitale au obligația de a-și informa utilizatorii cu privire la perturbările [alineatul (5)] sau amenințările specifice [alineatul (6)] care provin de la unul dintre serviciile lor, precum și de a transmite utilizatorilor informațiile primite de la Oficiul Federal pentru Securitatea Informațiilor (BSI) referitoare la amenințările specifice care afectează clienții furnizorilor, în măsura în care aceste informații sunt cunoscute și notificarea este posibilă.

Obligațiile prevăzute la alineatele (5) și (6) corespund, în esență, celor care le revin deja furnizorilor de servicii de telecomunicații, conform articolului 169 alineatele (5) și (6) din Legea privind telecomunicațiile (TKG). Obligațiile actuale ale furnizorilor de servicii de telecomunicații prevăzute la articolul 169 alineatele (5) și (6) din TKG prezintă lacune în ceea ce privește combaterea amenințărilor respective, întrucât sunt afectate în mod regulat sisteme ale căror operatori nu intră sub incidența TKG. Cu toate acestea, Oficiul Federal pentru Securitatea Informațiilor (BSI) prelucrează zilnic numeroase constatări privind sistemele vulnerabile sau compromise (furnizori de servicii de găzduire, furnizori de servicii de cloud computing, furnizori de servicii de centre de date, operatori de rețele de furnizare de conținut, furnizori de servicii gestionate, furnizori de servicii de securitate gestionate). Deși aceste constatări sunt transmise în prezent furnizorilor, foarte adesea aceștia nu le comunică utilizatorilor vizați, din cauza lipsei unei obligații legale. Prin urmare, amenințarea existentă nu poate fi abordată în mod eficient și regulat.

Alineatele (5) și (6) se referă numai la perturbările sau amenințările generate de un serviciu în timpul utilizării serviciului respectiv de către utilizator. Aceasta se referă la situațiile în care un utilizator, de exemplu, folosește un serviciu de găzduire pentru a administra un site web sau un serviciu de e-mail, iar site-ul web sau serviciul de e-mail de care este responsabil este compromis și utilizat în mod abuziv pentru a distribui programe malware sau e-mailuri de tip phishing. Prin urmare, este vorba despre perturbări și amenințări care afectează un utilizator în timpul utilizării unui serviciu. Printre posibilele exemple de perturbări relevante se numără un cont de e-mail compromis utilizat pentru a trimite mesaje spam, un server compromis utilizat pentru atacuri DDoS sau un site web compromis utilizat pentru a distribui programe malware.

Scopul acestei obligații este de a preveni daunele cauzate de serviciile vulnerabile sau deja compromise. Acest tip de prejudiciu poate afecta atât utilizatorul însuși, cât și alți utilizatori de internet, în cazul în care aceștia sunt vizați de atacuri prin intermediul serviciilor afectate (de exemplu, atacuri cu programe malware, de tip phishing sau DDoS). În plus, furnizorii de servicii digitale au obligația de a-i informa pe utilizatorii a căror utilizare a serviciilor provoacă perturbări sau care sunt expuși unui risc – în măsura în care acest lucru este cunoscut – și de a le transmite acestor utilizatori informațiile comunicate de Oficiul Federal pentru Securitatea Informațiilor (BSI).