31 octombrie 2023

Recomandări ale Camerei de Comerț Americane în România (AmCham România) cu privire la transpunerea Directivei NIS2 în legislația națională

RECOMANDĂRI CU CARACTER GENERAL

Ca în multe alte cazuri, directivele UE oferă statelor membre un câmp de reglementare complementară destul de larg, iar *Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148* ***("Directiva NIS2")*** nu face excepție. În acest sens, Directiva NIS2 stabilește mai multe zone în care statele membre pot introduce prevederi suplimentare în procesul de legiferare a transpunerii directivei în dreptul intern. Recomandarea esențială în acest sens este aceea ca autoritățile publice din România să facă uz în mod prudent de această prerogativă conferită prin Directiva NIS2.

- Cu titlu de principiu, orice adăugare la prevederile deja existente în cuprinsul directivei (cu precădere în ceea ce privește aria de obligații ce revin entităților, în special, a celor private) trebuie să fie una prudentă, care să se raporteze la și să fie limitată de prevederile punctelor 81 și 82 din Preambulul Directivei, respectiv:

> *(81) Pentru a se evita impunerea unei sarcini financiare și administrative disproporționate asupra entităților esențiale și entităților importante, măsurile de gestionare a riscurilor în materie de securitate cibernetică ar trebui să fie proporționale cu riscurile la care sunt expuse rețeaua și sistemul informatic în cauză, ținându-se seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri și, după caz, de standardele europene și internaționale relevante, precum și de costul punerii lor în aplicare;*
>
> *(82) Măsurile de gestionare a riscurilor în materie de securitate cibernetică ar trebui să fie proporționale cu gradul de expunere a entității esențiale sau a entității importante la riscuri și cu impactul societal și economic pe care un incident l-ar avea. Atunci când se stabilesc măsuri de gestionare a riscurilor în materie de securitate cibernetică adaptate entităților esențiale și entităților importante, ar trebui să se țină seama în mod corespunzător de expunerea divergentă la risc a entităților esențiale și a entităților importante, cum ar fi importanța critică a entității, riscurile, inclusiv riscurile societale, la care este expusă, dimensiunea entității și probabilitatea producerii incidentelor și gravitatea acestora, inclusiv impactul lor societal și economic.*

- Aceeași prudență și evaluare atentă trebuie să fie exercitată de către autoritățile publice competente în acele cazuri în care Directiva NIS2 le conferă facultatea de a impune anumite obligații – de exemplu, astfel cum prevede Art. 24 alin. 1, statele membre le pot solicita entităților esențiale și entităților importante să utilizeze anumite produse TIC, servicii TIC și procese TIC, dezvoltate de entități esențiale sau de entități importante ori achiziționate de la părți terțe, care sunt certificate în cadrul sistemelor europene de certificare a securității cibernetice. Trebuie avut în vedere faptul că, în funcție de evoluția pe piață a prețurilor acestor produse și servicii, costurile aferente să nu poată fi suportate ușor de entitățile private care nu pot acoperi costurile aferente acestor măsuri decât din venituri proprii, iar nu din resurse de la bugetul de stat;
- În ceea ce privește **domeniul de aplicare**, Art. 5 din Directiva NIS2 permite statelor membre să adopte sau să mențină dispoziții care asigură un nivel mai ridicat de securitate cibernetică, cu condiția ca aceste dispoziții să fie în concordanță cu obligațiile statelor membre prevăzute în dreptul Uniunii. Spre a se evita excese de reglementare, care ar putea îmbrăca inclusiv un caracter abuziv și/sau exagerat de împovărător pentru entitățile private vizate, recomandăm să se țină seama de condiția impusă de Art. 5;
- Totodată, utilizarea serviciilor digitale la nivel transfrontalier este o realitate în contextul dezvoltării accelerate a societății informaționale. Astfel, considerăm important ca, prin transpunerea Directivei NIS2, să nu se restricționeze posibilitatea de a utiliza mijloace de gestionare a informațiilor care să deservească, la nivel transfrontalier, entități din mai multe țări.

CONSIDERAȚII SPECIFICE

1. Securitatea cibernetică a lanțului de aprovizionare

- Una dintre intențiile Directivei NIS2 este de a reglementa securitatea cibernetică în cadrul lanțului de aprovizionare și pentru a oferi asistență entităților esențiale și entitățile importante care își desfășoară activitatea în sectoarele incluse în scopul Directivei NIS2, similar cu acțiunile întreprinse în cazul rețelelor 5G;
- Directiva NIS2 menționează că **analiza riscurilor de securitate** a sistemelor, serviciilor și produselor ICT trebuie să țină cont nu doar de factorii tehnici, ci și de cei non-tehnici. În ceea ce privește factorii non-tehnici care trebuie avuți în vedere în analiza riscului de securitate, aceștia sunt similari cu factorii avuți în vedere de Legea 163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice şi de comunicaţii de interes naţional şi condiţiile implementării reţelelor 5G *(„Legea 5G");*
- În acest sens, pentru a evita suprareglementarea în cazul lanțului de aprovizionare aferent rețelelor 5G, considerăm important ca în procesul de identificare a serviciilor, sistemelor și produselor ICT critice să se țină cont de faptul că, cel puțin în ceea ce privește factorii non-tehnici, sunt incidente prevederile Legii 5G;

- De asemenea, în prezent, și Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative *(„Legea Securității Cibernetice")* reglementează măsuri în legătură cu securitatea lanțului de aprovizionare în cazul entităților incluse în scopul legii. Dat fiind că administrația publică a fost inclusă în scopul Directivei NIS2 este important să se asigure o corelare a celor două acte, în speță Legea Securității Cibernetice și actul normativ de transpunere a Directivei NIS2;
- Având în vedere numărul foarte mic de entități care s-au confomat Directivei NIS1 și complexitatea măsurilor de implementare, poate fi luată în considerare crearea unui departament în cadrul Directoratului Național de Securitate Cibernetică (DNSC) care să ofere sprijin societăților cu privire la implementarea măsurilor prevăzute de Directiva NIS2 anterior intrării în vigoare a legii de transpunere. Acest tip de serviciu există în alte state (spre exemplu Franța)[1];
- România va trebui să se asigure că membrii organelor de conducere din cadrul entităților esențiale și al entităților importante au obligația de a urma o formare pentru a dobândi suficiente cunoștințe și competențe pentru a putea identifica riscurile și a evalua practicile de gestionare a riscurilor în materie de securitate cibernetică și impactul acestora asupra serviciilor pe care le furnizează entitatea, și încurajează entitățile esențiale și entitățile importante să ofere o formare similară tuturor angajaților în mod regulat. Acest aspect va trebui destul de bine detaliat cu privire la entitățile care pot furniza aceste servicii, durata sau regularitatea cursurilor care vor trebui urmate, dacă este suficient ca unul dintre membrii organelor de conducere să aibă această formare (director sau administrator) etc;
- Nu în ultimul rând, considerăm că este importantă utilizarea standardelor internaționale, după cum este prevăzut și în Directivă, pentru a facilita implementarea și a crește gradul de conformitate pentru entitățile supuse managementului de risc sau altor obligații prevăzute de legislația de transpunere.

2. Măsuri de gestionare a riscurilor în materie de securitate cibernetică și obligații de raportare

- La Art. 21 alin. 1 paragraful 2, Directiva NIS2 situează un accent special pe **costul punerii în aplicare,** de către entități, a măsurilor tehnice, operaționale și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice pe care entitățile respective le utilizează. Aceste costuri trebuie avute în vedere de autoritățile publice românești, atunci când stabilesc măsuri suplimentare față de cele prevăzute de Art. 21 alin. 2 din Directiva NIS2, în sensul în care ele nu trebuie să ducă la o supra-împovărare a entităților private, care nu pot

[1] https://beta.gouv.fr/startups/NIS2.html

acoperi costurile aferente acestor măsuri decât din venituri proprii, iar nu din resurse de la bugetul de stat;

- Criteriile fundamentale de care autoritățile publice românești trebuie să țină seama, atunci când stabilesc măsuri privind securitatea lanțului de aprovizionare pentru entități, se regăsesc în Art. 21 alin. 3 din Directiva NIS2, și anume: vulnerabilitățile specifice fiecărui prestator și furnizor direct de servicii, precum și calitatea generală a produselor și a practicilor în materie de securitate cibernetică ale prestatorilor și furnizorilor lor de servicii, inclusiv procedurile lor securizate de dezvoltare. Deși un asemenea demers pare extrem de anevoios în materie de timp și resurse, el este important în procesul de determinare exactă a măsurilor aplicabile, și de evitare a stabilirii și impunerii unor măsuri disproporționate.

3. Notificarea incidentelor de securitate

- Legea Securității Cibernetice reglementează un mecanismul de notificare al incidentelor de securitate cibernetică pentru entitățile care intră în scopul legii. Aceste incidente se notifică prin Platforma Națională pentru raportarea incidentelor de securitate cibernetică („PNRISC") către Directoratul Național de Securitate Cibernetică;

- Directiva NIS2 prevede, de asemenea, un mecanism detaliat referitor la notificarea incidentelor de securitate;

- În acest sens, la momentul transpunerii, este necesar ca definirea termenului de "incident semnificativ" să fie dezvoltată prin raportare la definiția oferită de Directiva NIS2 (Art. 23 alin. 3), întrucât există posibilitatea ca un operator economic să aprecieze un incident ca nefiind semnificativ, incident pe care autoritatea l-ar încadra însă în obligația de raportare, și să se expună astfel la o amendă drastică;

- Având în vedere că există o suprapunere între cele două acte menționate mai sus cu privire la entitățile care sunt în scopul acestora, considerăm important să se asigure că în procesul de transpunere al Directivei NIS2 se va ține cont de obligațiile deja existente, pentru a se evita dubla reglementare a unor entități cu privire la notificarea incidentelor de securitate cibernetică. În acest sens, pentru a se evita paralelismul legislativ, recomandăm analizarea oportunității abrogării Legii Securității Cibernetice, iar elementele distinctive care nu sunt acoperite de Directiva NIS2, să fie preluate în noul act normativ de transpunere (care va abroga deopotrivă Legea 362/2018 de transpunere a Directivei NIS1);
- În special, transpunerea Directivei NIS2 ar trebui să reflecte faptul că numai incidentele care au un impact semnificativ asupra furnizării serviciului ar trebui să facă obiectul cerințelor de notificare și că există o abordare pe niveluri prevăzută în Directiva NIS2 (raportarea necesară după 24 ore/72 ore/1 lună);

- Transpunerea Directivei NIS2 ar trebui să reflecte, de asemenea, faptul că pentru entitățile care furnizează anumite servicii digitale în mai multe state membre, directiva instituie un mecanism de ghișeu unic. Drept urmare, legislația națională care stabilește diverse obligații în temeiul Directivei NIS2, inclusiv notificarea incidentelor, ar trebui să se aplice acelor entități care îndeplinesc criteriile stabilite la Art. 26, adică celor care au România ca autoritate competentă unică.

4. Identificarea entităților esențiale și a entităților importante

- Directiva NIS 2 reclasifică entitățile care sunt în scop în entități esențiale și importante;
- Directiva stabilește atât tipurile de entități considerate a fi esențiale, cât și criteriile în baza cărora statele membre pot identifica și alte tipuri de entități din cele menționate în Anexele I și II la directivă ca esențiale;
- În ceea ce privește entitățile importante, Directiva NIS 2 stabilește că tipurile de entități menționate în Anexele I și II la directivă care nu se califică ca și entități esențiale sunt entități importante, incluzând aici și entitățile identificate de statele membre ca fiind importante. Criteriile în baza cărora se face identificarea entităților importante sunt aceleași cu cele folosite pentru identificarea entităților esențiale;
- În acest context, considerăm important ca actul normativ de transpunere a Directivei NIS 2 să clarifice modul în care vor fi aplicate criteriile de identificare a entităților ca fiind esențiale sau importante, ținând cont de necesitatea implementării consecvente în întreaga Uniune și de sarcinile grupului de cooperare instituit în temeiul directivei (Grupul de Cooperare NIS), și modul în care se va diferenția între cele două tipuri de entități. În acest mod s-ar oferi predictibilitate cu privire la procesul de identificate a entităților fie ca esențiale, fie ca importante.

5. O abordare de tip risk-based pentru entitățile cărora li se aplică Directiva NIS2

- Ca bună practică, considerăm că se poate avea în vedere o abordare etapizată, în funcție de mărimea și industria din care face parte fiecare entitate căreia i se aplică Directiva NIS2, luând în considerare și dacă face sau nu parte dintr-o industrie reglementată. Spre exemplu, luând în considerare și exemplul Belgiei, se pot avea în vedere mai multe tipuri de entități și, implicit, un nivel de evaluare și de implementare a unor măsuri de asigurare a îndeplinirii cerințelor NIS2 diferite, respectiv:
    - Un nivel mic/de pornire al unei entități (destinat întreprinderilor mici și mijlocii sau organizațiilor cu capabilități tehnice limitate);
    - Un nivel de asigurare de bază care să cuprindă măsuri standard de securitate a informațiilor pentru toate companiile (cu tehnologii și procese care sunt, în general, deja disponibile). În cazuri justificate, măsurile sunt adaptate și perfecționate. Pe baza nivelului de bază, măsurile de securitate sunt completate

pentru a proteja organizațiile de riscurile cibernetice crescute pentru a atinge un nivel mai ridicat de securitate;

- Un nivelul important de asigurare conceput pentru a minimiza riscurile atacurilor cibernetice direcționate de către actori cu abilități și resurse comune, pe lângă riscurile cunoscute de securitate cibernetică;
- Un nivelul esențial de asigurare conceput pentru a aborda riscul atacurilor cibernetice avansate din partea actorilor cu competențe și resurse extinse.

6. Implementarea unor măsuri preventive prioritare

- Implementarea unor măsuri prioritare de securitate cibernetică este esențială, iar punerea lor în aplicare pe termen scurt contribuie la limitarea probabilității unui atac cibernetic, precum și a efectelor potențiale ale acestuia. Ca bună practică, luând exemplul Franței, pot fi avute în vedere următoarele măsuri preventive prioritare:
  - consolidarea autentificării în sistemele informatice;
  - creșterea supravegherii securității;
  - asigurarea unui back-up al datelor critice și al aplicațiilor offline.
  - stabilirea unei liste prioritare a serviciilor digitale critice ale entității;
  - asigurarea existenței unui sistem de gestionare a crizelor adaptat unui atac cibernetic.
- Cu toate acestea, pentru a fi pe deplin eficace, acestea trebuie să facă parte dintr-o abordare cuprinzătoare și pe termen lung în materie de securitate cibernetică.