DOI: 10.47743/jss-2021-67-4-21

Directiva NIS: elaborarea unei reglementări-cadru privind securitatea informațiilor din UE

The NIS Directive: Developing the EU Cybersecurity Regulatory Framework

Ștefan Răzvan Tataru¹

Rezumat: Ultimele decenii sunt caracterizate prin digitalizare și inovare tehnologică, evoluție care a determinat atât eficientizarea activităților economice dar și riscuri asupra securității informațiilor de afaceri și a datelor cu caracter personal. Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice – Directiva NIS – vizează protejarea infrastructurilor critice și digitale pentru asigurarea funcționării sistemelor considerate esențiale pentru populație, stabilind în sarcina operatorilor de servicii esențiale și a furnizorilor de servicii digitale obligația de a implementa măsuri minime de protecție corelate cu riscurile la securitatea sistemelor informatice. În prezentul studiu ne propunem să analizăm modul în care Directiva NIS impactează afacerile și, totodată, să evaluăm interacțiunea prevederilor acesteia cu cele ale Regulamentului UE 2016/679 – Regulamentul general privind protecția datelor cu caracter personal (GDPR).

Cuvinte-cheie: Directiva NIS; NIS; GDPR; protecția datelor; securitatea informației; securitate cibernetică

Abstract: The last decades are characterized by digitalization and technological innovation, an evolution that has determined both the efficiency of economic activities and risks on the security of business information and personal data. Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems – the NIS Directive – aims to protect critical and digital infrastructures to ensure the functioning of systems considered essential for the population, laying down essential service operators and digital service providers the obligation to implement minimum protection measures related to the risks to the security of information systems. In this study we aim to analyse how the NIS Directive impacts business and, at the same time, to evaluate the interaction of its provisions with those of EU Regulation 2016/679 – General Regulation on the protection of personal data (GDPR).

Keywords: NIS Directive; NIS; GDPR; data protection; information security; cybersecurity

¹ Doctor în drept, cadru didactic asociat, Facultatea de Economie și Administrarea Afacerilor, Universitatea „Alexandru Ioan Cuza” din Iași, e-mail: razvantataru@gmail.com, Orcid ID 0000-0002-1746-9636.

1. Introducere

Ultimele decenii sunt caracterizate prin digitalizare și inovare tehnologică, evoluție care a determinat atât eficientizarea activităților economice dar și riscuri asupra securității informațiilor de afaceri și a datelor cu caracter personal. Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice² – Directiva NIS - vizează protejarea infrastructurilor critice și digitale pentru asigurarea funcționării sistemelor considerate esențiale pentru populație, stabilind în sarcina operatorilor de servicii esențiale și a furnizorilor de servicii digitale obligația de a implementa măsuri minime de protecție corelate cu riscurile la securitatea sistemelor informatice. Dezideratul Uniunii Europene de a implementa o strategie de securitate cibernetică comună și eficientă la nivelul statelor membre a devenit o necesitate stringentă în contextul celei de-a patra revoluții industriale. Astfel, în contextul în care activitățile productive au fost digitalizate complet, utilizarea inteligenței artificiale și a tehnologiilor cognitive reprezintă o condiție de supraviețuire a întreprinderilor într-o piață internațională competitivă, dispozitivele *Internet of things (IoT)*³ sunt ușor accesibile și de implementat, iar Internetul reprezintă un instrument disponibil pentru eficientizarea tuturor activităților⁴, garanția unor măsuri de securitate asupra informațiilor și sistemelor informatice care permit și, totodată, condiționează desfășurarea în condiții normale a activităților reprezintă o necesitate absolută. Incidentele de securitate cibernetică sunt însoțite adeseori de urmări grave care afectează securitatea datelor și a sistemelor informatice, determinând totodată pierderi financiare și și care determină, în termeni de securitate, de pierderi economice și financiare și de afectare a imaginii organizației⁵.

În lipsa implementării unor măsuri adecvate de securitate a rețelelor și sistemelor informatice, atacurile cibernetice reprezintă o amenințare gravă care poate cauza întreruperi ale serviciilor IT și ale infrastructurilor critice, determinând deopotrivă blocaje în desfășurarea activităților economice, pierderi financiare substanțiale, subminarea încrederii utilizatorilor și pagube majore economiei

² Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, publicată în JO L 194 din data de 19.07.2016.

³ Pentru detalii privind tehnologiile *Artificial Intelligence (AI)* sau *Internet-of-Things (IoT)* a se vedea C.T. Ungureanu, *Drept internațional privat european în raportul de comerț internațional*, Editura Hamangiu, 2021, p. 354 și urm.

⁴ C.T. Ungureanu, *Implicațiile Internetului în viața juridică*, Analele Științifice ale Universității „Alexandru Ioan Cuza” Iași, Tomul LXIII, Științe Juridice, 2017, nr. II, pp. 1-2; Ș.R. Tataru, *Internet Cookies - fișierele cu răvaș juridic*, în Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași, Tomul LXVI, Supliment, Științe Juridice, 2020, p. 33

⁵ Serviciul Român de Informații, *Ghid de bune practice pentru securitatea cibernetică*, [Online] la https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf, accesat 11.11.2021.

Uniunii⁶. Directiva NIS abordează această nevoie prin stabilirea măsurilor necesare „obținerii unui nivel comun ridicat de securitate a rețelelor și a sistemelor de informații în cadrul Uniunii, astfel încât să îmbunătățească funcționarea pieței interne”⁷.

2. „Reglementările” NIS

Uniunea Europeană nu abordează problematica securității cibernetice pentru prima dată în anul 2016, prin intermediul Directivei NIS, preocuparea pentru crearea unui mediu online securizat fiind manifestată încă din anul 2014 când a fost fondată ENISA (Agenția Uniunii Europene pentru Securitatea Rețelelor și Informațiilor)⁸.

Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune stabilește cadrul juridic și instituțional, măsurile și mecanismele necesare în vederea asigurării unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice și a stimulării cooperării în domeniu⁹. Directiva (UE) 2016/1148, cunoscută sub denumirea de Directiva NIS (*Network and Information Security*) reprezintă prima reglementare complexă la nivel comunitar privind securitatea cibernetică și totodată, una dintre cele mai importante componente ale strategiei Uniunii Europene în acest domeniu¹⁰. Prevederile Directivei NIS permit statelor membre să stabilească prin intermediul legislației naționale standarde care să asigure un nivel mai ridicat de securitate. În acest sens, statele membre pot extinde obligațiile de securitate și notificare prevăzute pentru operatorii de servicii esențiale și la entități aparținând altor sectoare și subsectoare nu numai la cele enumerate în anexa la Directiva NIS.

În România, Directiva nr. 2016/1148 a fost transpusă în legislația națională prin intermediul Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, publicată în Monitorul Oficial, Partea I nr. 21 din 9 ianuarie 2019.

⁶ D. Markopoulou, V. Papakonstantinou, P. de Hert, *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*, Computer Law & Security Review 35 (2019) 105336, p. 1.

⁷ Conform art. 1 alin. (1) din Directiva (UE) 2016/1148.

⁸ N. Saqib, V. Germanos, W. Zeng, L. Maglaras, *Mapping of the Security Requirements of GDPR and NIS*, în Preprints, iunie 2020, p. 4, [Online] la <https://www.preprints.org/manuscript/202006.0193/v1>, accesat 11.11.2021; D. Markopoulou, V. Papakonstantinou, P. de Hert, *op. cit.*, p. 2.

⁹ A se vedea și art. 1 din Legea nr. 362/2018.

¹⁰ A se vedea website-ul Agenției Uniunii Europene pentru Securitatea Rețelelor și Informațiilor (ENISA), secțiunea Directiva NIS, [Online] la <https://www.enisa.europa.eu/topics/nis-directive>, accesat 11.11.2021.

2.1. Operatori de Servicii Esențiale vs. Furnizori de Servicii Digitale

Spre deosebire de Regulamentul GDPR care are un domeniu de aplicare material vast, determinând obligații pentru toți operatorii de date cu caracter personal, Directiva NIS vizează doar instituții, autorități sau societăți care au calitatea de Operatori de Servicii Esențiale (OSE) sau de Furnizori de Servicii Digitale (FSD)¹¹.

Conform art. 4 pct. 4 din Directivă, operatorul de servicii esențiale (OSE) desemnează o entitate publică sau privată care activează într-unul dintre sectoarele specifice menționate în Anexa nr. 2 și care îndeplinește cumulativ următoarele condiții¹²: a) furnizează un serviciu esențial pentru susținerea activităților societale și/sau economice de cea mai mare importanță; b) furnizarea serviciului respectiv depinde de rețea și de sistemele informatice; și c) un incident ar avea efecte perturbatoare semnificative asupra furnizării serviciului. Anexa nr. 2 a Directivei prevede șapte sectoare de activitate economică astfel: Energie, Transport, Sectorul bancar, Infrastructuri ale pieței financiare, Sectorul sănătății, Furnizarea și distribuirea de apă potabilă și Infrastructură digitală.

În prezent, se află în dezbatere propunerea¹³ de Directivă NIS 2.0 care aduce o serie de modificări majore, dintre care menționăm extinderea sectoarelor reglementate pentru entitățile esențiale, de la șapte la zece sectoare. Astfel, Directiva NIS 2.0 lărgeste sfera operatorilor de servicii esențiale prin adăugarea următoarelor sectoare de activitate: Colectarea, eliminarea sau tratarea apei uzate/reziduale, Administrația publică și Spațiul cosmic¹⁴.

Furnizorii de servicii digitale (FSD) reprezintă orice persoană juridică care furnizează un serviciu digital¹⁵, respectiv: piețele online, motoarele de căutare web și serviciile de cloud-computing. Reglementarea națională – Legea nr. 362/2018,

¹¹ Pentru detalii a se vedea M.D. Cole, S. Schmitz, *The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape*, în University of Luxembourg Law Working Paper No. 2019-017, December 31, 2019, [Online] la <http://dx.doi.org/10.2139/ssrn.3512093>, accesat 11.11.2021.

¹² A se vedea art. 5 alin. (2) din Directiva NIS.

¹³ Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final, [Online] la <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN>, accesat 11.11.2021.

¹⁴ A se vedea și website-ul Directoratului Național de Securitate Cibernetică, [Online] la <https://dnsc.ro/citeste/includerea-administratiei-publice-intre-sectoarele-nis-2>, accesat 11.11.2021.

¹⁵ Conform art. 4 alin. (5) din Directiva NIS, „serviciu digital” înseamnă un serviciu în sensul articolului 1 alineatul (1) litera (b) din Directiva (UE) 2015/1535 a Parlamentului European și a Consiliului (17) care este de un tip enumerat în anexa III; Astfel, actul normative la care face trimitere Directiva NIS definește serviciul digital drept „orice serviciu al societății informaționale, adică orice serviciu prestat în mod normal în schimbul unei remunerații, la distanță, prin mijloace electronice și la solicitarea individuală a beneficiarului serviciului”.

definește conceptul de „serviciu digital”¹⁶ prin trimitere la art. 4 alin. (1) pct. 2 din Hotărârea Guvernului nr. 1.016/2004 privind măsurile pentru organizarea și realizarea schimbului de informații în domeniul standardelor și reglementărilor tehnice, precum și al regulilor referitoare la serviciile societății informaționale între România și statele membre ale Uniunii Europene, drept acel „serviciu [...] care se încadrează într-una din categoriile: 1. piață online¹⁷; 2. motor de căutare online¹⁸; 3. serviciu de cloud computing¹⁹”. Definirea limitativă a furnizorilor de servicii digitale prin raportare doar la cele trei tipuri de servicii este justificată prin numărul tot mai mare de persoane care depind fundamental de ele pentru furnizarea propriilor servicii.

2.2. Obligații legale conform NIS

Directiva NIS definește în cadrul articolelor 14-18 cerințele de securitate și notificarea incidentelor pentru operatorii de servicii esențiale și, respectiv, furnizorii de servicii digitale. În cadrul reglementărilor naționale, obligațiile impuse operatorilor de servicii esențiale și furnizorilor de servicii digitale se regăsesc în cadrul art. 10-12 din Legea nr. 362/2018.

În conformitate cu art. 14 alin. (1) din Directiva NIS, statele membre sunt obligate să se asigure că operatorii de servicii esențiale iau măsuri corespunzătoare, tehnice și organizatorice, pentru a gestiona riscurile prezentate pentru securitatea rețelei și a sistemelor informatice pe care le utilizează. În conformitate cu art. 14 alin. (2), măsurile adecvate trebuie să prevină și să reducă la minimum impactul incidentelor care afectează securitatea sistemelor lor, dezideratul urmărit fiind asigurarea continuității serviciilor esențiale.

Din analiza prevederilor Directivei NIS și a Legii nr. 362/2018 putem observa faptul că obligațiile ce revin operatorilor de servicii esențiale pot fi clasificate în a) obligații de a asigura implementarea unor măsuri minime de securitate și b) obligații de notificare a incidentelor de securitate.

¹⁶ A se vedea art. 3 lit. o) din Legea nr. 362/2018.

¹⁷ Directiva NIS definește „piața online” drept „un serviciu digital care permite consumatorilor și/sau comercianților [...], să încheie online vânzări sau contracte de servicii cu comercianți fie pe site-ul internet al pieței online, fie pe site-ul internet al unui comerciant care utilizează servicii informatice furnizate de piața online” – a se vedea art. 4 pct. 17.

¹⁸ Motorul de căutare online este „un serviciu digital care permite utilizatorilor să caute, în principiu, în toate site-urile internet sau site-urile internet într-o anumită limbă pe baza unei interogații privind orice subiect sub forma unui cuvânt, a unei fraze sau a unei alte informații-cheie și care revine cu linkuri în care se pot găsi informații legate de conținutul căutat” – a se vedea art. 4 pct. 18.

¹⁹ Conform art. 4 pct. 19 din Directiva NIS, „serviciu de cloud-computing” înseamnă un serviciu digital care permite accesul la un bazin redimensionabil și elastic de resurse informatice care pot fi puse în comun. Pentru detalii privind conceptul de cloud-computing a se vedea C.T. Ungureanu, *Contractul Cloud Computing în comerțul internațional*, Revista Moldovenească de Drept Internațional și Relații Internaționale Nr. 3 (37), 2015, pp. 26-27.

2.2.1. Obligații pentru Operatorii de servicii esențiale

Operatorii de servicii esențiale, spre deosebire de furnizorii de servicii digitale, se identifică și se înscriu în Registrul operatorilor de servicii esențiale²⁰. Astfel, conform art. 8 din Legea nr. 362/2018, entitățile care îndeplinesc condițiile și criteriile stabilite pentru a se califica drept operator de servicii esențiale au obligația de a notifica CERT-RO²¹ (Centrul Național de Răspuns la Incidente de Securitate Cibernetică) în vederea înscrierii în Registrul operatorilor de servicii esențiale în termen de 30 de zile de la data îndeplinirii acestora.

Dintre principalele obligațiile ce revin operatorilor de servicii esențiale în conformitate cu prevederile art. 10 din Legea nr. 362/2018, amintim: „a) implementează măsurile tehnice și organizatorice adecvate și proporționale pentru îndeplinirea cerințelor minime de securitate [...]; b) implementează măsuri adecvate pentru a preveni și minimiza impactul incidentelor care afectează securitatea rețelelor și a sistemelor informatice utilizate pentru furnizarea acestor servicii esențiale, cu scopul de a asigura continuitatea serviciilor respective [...]; c) notifică de îndată CERT-RO în calitate de CSIRT național incidentele care au un impact semnificativ asupra continuității serviciilor esențiale [...]; d) pun la dispoziția CERT-RO informații care să permită stabilirea impactului transfrontalier al incidentului [...]; h) se interconectează [...] la serviciul de alertare și cooperare al CERT-RO, asigură monitorizarea permanentă a alertelor și solicitărilor primite prin acest serviciu ori prin celelalte modalități de contact și ia în cel mai scurt timp măsurile adecvate de răspuns la nivelul rețelelor și sistemelor informatice proprii; i) asigură de îndată răspunsul la incidentele survenite, restabilesc în cel mai scurt timp funcționarea serviciului la parametrii dinaintea incidentului și realizează auditul de securitate [...]”.

Conform celor anterior precizate, cerințele de securitate care trebuie adoptate de operatorii de servicii esențiale sunt însoțite de obligația de a notifica autoritățile competente cu privire la orice incident care are un impact asupra continuității serviciilor esențiale pe care le oferă un operator. În conformitate cu art. 14 alin. (3) din Directiva NIS, statele membre trebuie să se asigure că operatorii de servicii esențiale notifică „orice incident care are un impact semnificativ asupra continuității serviciilor esențiale pe care le furnizează”. În stabilirea impactului unui incident de securitate, operatorul de servicii esențiale va avea în vedere prevederile art. 14 alin. (4) din Directivă care furnizează o listă a parametrilor care trebuie luați în considerare, și anume: numărul de utilizatori afectați, durata incidentului și răspândirea geografică în raport cu zona afectată de incident. Mai mult decât atât,

²⁰ Conform art. 5 din Legea nr. 362/2018. A se vedea și N. Saqib, V. Germanos, W. Zeng, L. Maglaras, *op. cit.*, p. 7.

²¹ În România, Centrul Național de Răspuns la Incidente de Securitate Cibernetică CERT-RO reprezintă autoritatea competentă la nivel național sau echipa de răspuns la incidente de securitate informatică (CSIRT). Începând din 24 septembrie 2021, CERT-RO a fost desființat iar atribuțiile acestuia au fost preluate de către Directoratul Național de Securitate Cibernetică (DNSC). Pe parcursul prezentului articol au fost utilizate ambele denumiri, respectiv CERT-RO și DNSC, în funcție de actul normativ indicat, ambele desemnând aceeași entitate – CSIRT național din România.

conform art. 10 alin. (3) din Legea nr. 362/2018, operatorii de servicii esențiale trebuie să notifice de îndată echipa națională de intervenție în caz de incidente de securitate informatică (*Computer Security Incident Response Team – CSIRT*²²) și în situația în care afectarea serviciilor esențiale se datorează unor incidente care afectează un furnizor de servicii digitale de care depinde furnizarea serviciilor esențiale.

Cerințele minime de securitate sunt stabilite de către CERT-RO prin normele tehnice, operatorii de servicii esențiale având obligația de a le respecta în vederea asigurării unui nivel comun de securitate a rețelelor și sistemelor informatice. *„Normele tehnice aplicabile operatorilor de servicii esențiale se stabilesc în baza cel puțin a următoarelor categorii de activități de asigurare a securității rețelelor și sistemelor informatice: a) managementul drepturilor de acces; b) conștientizarea și instruirea utilizatorilor; c) jurnalizarea și asigurarea trasabilității activităților în cadrul rețelelor și sistemelor informatice; d) testarea și evaluarea securității rețelelor și sistemelor informatice; e) managementul configurațiilor rețelelor și sistemelor informatice; f) asigurarea disponibilității serviciului esențial și a funcționării rețelelor și sistemelor informatice; g) managementul continuității funcționării serviciului esențial; h) managementul identificării și autentificării utilizatorilor; i) răspunsul la incidente; j) mentenanța rețelelor și sistemelor informatice; k) managementul suporturilor de memorie externă; l) asigurarea protecției fizice a rețelelor și sistemelor informatice; m) realizarea planurilor de securitate; n) asigurarea securității personalului; o) analizarea și evaluarea riscurilor; p) asigurarea protecției produselor și serviciilor aferente rețelelor și sistemelor informatice; q) managementul vulnerabilităților și alertelor de securitate”*²³.

Conform prevederilor art. 5 alin (5) în implementarea măsurilor de securitate, *„operatorii de servicii esențiale: a) identifică rețelele și sistemele informatice care susțin furnizarea de servicii esențiale; b) elaborează și implementează politici și planuri proprii de securitate a rețelelor și sistemelor informatice; c) asigură managementul incidentelor care afectează securitatea rețelelor și sistemelor informatice; d) previn accesul neautorizat la rețelele și sistemele informatice; e) previn diseminarea datelor deținute la nivelul rețelelor și sistemelor informatice către alte persoane decât cele autorizate să cunoască conținutul acestora; f) implementează un sistem de management al riscului; g) implementează planuri de acțiune pe niveluri de alertă de securitate a rețelelor și sistemelor informatice; h) asigură continuitatea serviciilor”*.

2.2.2. Obligații pentru Furnizorii de servicii digitale

Furnizorii de servicii digitale, spre deosebire de operatorii de servicii esențiale, sunt liberi să ia măsuri tehnice și organizaționale pe care le consideră adecvate și proporționale pentru a gestiona riscul prezentat pentru securitatea

²² Pentru mai multe detalii a se vedea art. 9 din Directiva NIS.

²³ Conform art. 25 alin. (3) din Legea nr. 362/2018.

sistemelor lor²⁴. Art.16 alin. (1) din Directivă enumeră elementele care trebuie să fie luate în considerare de un furnizor de servicii digitale atunci când identifică și adoptă măsuri de securitate pentru rețeaua informatică, și anume: (a) securitatea sistemelor și instalațiilor, (b) gestionarea incidentelor, (c) managementul continuității activității, (d) monitorizarea, auditul și testarea și (e) conformitatea cu standardele internaționale.

Adițional cerințelor de securitate menționate, pentru ca furnizorii de servicii digitale să asigure un nivel ridicat de securitate a rețelei și a sistemului său informatic, aceștia au obligația de a notifica orice incident cu impact substanțial asupra prestării serviciului lor²⁵.

Notificarea incidentelor de securitate va cuprinde, în mod obligatoriu, următoarele informații: a) elementele de identificare ale infrastructurii și operatorului sau furnizorului în cauză; b) descrierea incidentului; c) perioada de desfășurare a incidentului; d) impactul estimat al incidentului; e) măsuri preliminare adoptate; f) lista de autorități ale statului afectate de incident; g) întinderea geografică potențială a incidentului; h) date despre efecte potențial transfrontaliere ale incidentului²⁶.

2.3. Sancțiuni conform NIS

Conform art. 36 din Legea nr. 362/2018, la nivel național, controlul respectării prevederilor Directivei NIS este exercitat de Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), instituție publică cu personalitate juridică, aflată în coordonarea Ministerului Comunicațiilor și Societății Informaționale²⁷. Începând cu data de 27 septembrie 2021, CERT-RO a fost desființat, atribuțiile acestuia fiind preluate de către Directoratul Național de Securitate Cibernetică²⁸.

Legea nr. 362/2018 prezintă în cuprinsul art. 38 faptele care constituie încălcări ale cerințelor NIS și care, după caz, pot atrage răspunderea contravențională sau penală. Sancțiunile prevăzute de Legea nr. 362/2018 pentru încălcarea dispozițiilor privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice constau în aplicarea de amenzi cuprinse între 3.000 lei și 50.000 lei, iar în cazul constatării unor încălcări repetate limita maximă a amenzii este plafonată la 100.000 lei. Întrucât valoarea pragurilor maxime ale amenzii ar putea fi considerată un risc de afaceri asumat de către marile companii, Legea nr. 362/2018 instituie pentru persoanele cu o cifră de afaceri de peste 2.000.000 lei,

²⁴ Conform art. 16 alin. (1) din Directiva NIS. A se vedea și D. Markopoulou, V. Papakonstantinou, P. de Hert, *op. cit.*, p 5.

²⁵ A se vedea art. 16 alin. (3) și 4) din Directiva NIS.

²⁶ Conform art. 26, alin. (3) din Legea nr. 362/2018.

²⁷ Hotărârea de Guvern nr. 494/2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO.

²⁸ Ordonanța de urgență nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, publicată în Monitorul Oficial, Partea I, nr. 918 din 24 septembrie 2021.

sancțiunea amenzii în cuantum de la 0,5% la 2% din cifra de afaceri, iar, în cazul unor încălcări repetate, amendă de până la 5% din cifra de afaceri.

3. Analiză comparativă: NIS vs. GDPR

Interacțiunea inevitabilă a prevederilor Directivei NIS cu cele ale Regulamentului GDPR este prezentată expres în cadrul capitolului 7 al Directivei.

Intrarea în vigoare a Regulamentului GDPR și a Directivei NIS, au coincis în mare măsură, respectiv luna aprilie și luna iulie a anului 2016. Procesele de legiferare s-au desfășurat independent și în paralel, neexistând o coordonare în vederea armonizării celor două reglementări. Dovadă a acestui aspect este și art. 2 al Directivei NIS care face trimitere la Directiva 95/46/CE pentru prelucrarea datelor cu caracter personal, în loc de Regulamentul GDPR care era în vigoare la data respectivă.

În același timp, GDPR nu face nicio trimitere directă către prevederile Directivei NIS, clarificând însă, în textul considerentului nr. 49, faptul că *„prelucrarea datelor cu caracter personal în măsura strict necesară și proporțională în scopul asigurării securității rețelelor și a informațiilor, și anume capacitatea unei rețele sau a unui sistem de informații de a face față, la un anumit nivel de încredere, evenimentelor accidentale sau acțiunilor ilegale sau rău intenționate care compromit disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor cu caracter personal stocate sau transmise, precum și securitatea serviciilor conexe oferite de aceste rețele și sisteme, sau accesibile prin intermediul acestora, de către autoritățile publice, echipele de intervenție în caz de urgență informatică, echipele de intervenție în cazul producerii unor incidente care afectează securitatea informatică, furnizorii de rețele și servicii de comunicații electronice, precum și de către furnizorii de servicii și tehnologii de securitate, constituie un interes legitim al operatorului de date în cauză”*.

Cu toate acestea, lipsa recunoașterii explicite nu înseamnă că Directiva NIS și GDPR nu au legătură. Dimpotrivă, atâta timp cât rețelele și sistemele informaționale sunt utilizate pentru prelucrarea datelor cu caracter personal, ambele instrumente juridice își găsesc aplicare concomitent²⁹.

Interacțiunile între GDPR și Directiva NIS pot apărea ori de câte ori se găsesc date cu caracter personal în sistemele furnizorilor de servicii digitale și/sau ale operatorilor de servicii esențiale. Un prim punct de intersecție a celor două reglementări este reprezentat de securitatea informațiilor, inclusiv a celor cu caracter personal. Principiul securității datelor cu caracter personal este unul dintre principiile de bază ale GDPR și include principiul integrității și cel al confidențialității datelor, fiind menționat în art. 5 alin. (1) lit. f) din GDPR faptul că datele trebuie *„prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate)”*.

²⁹ D. Markopoulou, V. Papakonstantinou, P. de Hert, *op. cit.*, p. 10.

În contextul expus, ne întrebăm dacă măsurile tehnice și organizatorice pentru securitatea datelor implementate în vederea conformării la prevederile NIS sunt la nivelul „adecvat” pentru conformitatea cu prevederile GDPR și vice-versa³⁰. Considerăm că fiecare sistem informatic și fiecare prelucrare de date trebuie analizată particular, iar în urma identificării și evaluării riscurilor de securitate să fie implementate măsurile tehnice și organizatorice corespunzătoare situației faptice. Așadar, nu există o garanție asupra faptului că măsurile de securitate implementate în temeiul GDPR sunt suficiente pentru îndeplinirea obligațiilor prevăzute de reglementările NIS și nici vice-versa³¹.

Un alt punct de interacțiune a reglementărilor NIS și GDPR apare în situația unui incident de securitate care ar trebui notificat autorității competente din domeniul protecției datelor cu caracter personal, dar și autorității competente din domeniul securității cibernetice. Având în vedere obiectul diferit al GDPR și NIS, entitățile aflate în scenariul anterior prezentat ar trebui să notifice autoritățile competente în mod independent, respectând procedurile și cerințele impuse de fiecare reglementare³².

În ceea ce privește termenul de notificare a incidentului de securitate, art. 33 GDPR prevede obligația operatorului de a notifica incidentul autorității de supraveghere competente fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta. Pe de altă parte, Directiva NIS nu prevede un termen pentru îndeplinirea obligației de notificare a incidentelor, lăsând statelor membre posibilitatea de a stabili un asemenea termen. Astfel, legiuitorul român a prevăzut în cuprinsul Legii nr. 362/2018 obligația operatorilor de servicii esențiale și a furnizorilor de servicii digitale de a notifica de îndată CSIRT național incidentele care au un impact semnificativ asupra continuității serviciilor esențiale/furnizării serviciilor digitale³³.

Asemeni prevederilor GDPR care obligă operatorii de date cu caracter personal să desemneze un Responsabil cu protecția datelor (*Data Protection Officer* - DPO)³⁴, art. 10 alin. (1) lit. f) din Legea nr. 362/2018 impune operatorilor de servicii

³⁰ A se vedea și N. Saqib, V. Germanos, W. Zeng, L. Maglaras, *op. cit.*, pp. 17-18.

³¹ Pentru similitudine a se vedea și M.D. Cole, S. Schmitz, *op. cit.*; C. Burton, *Security of personal data*, în C. Kuner, L.A. Bygrave, C. Docksey, *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020, p. 633.

³² Punct de vedere susținut și de autoritatea de supraveghere a datelor cu caracter personal din Regatul Unit al Marii Britanii - Information Commissioner's Office, [Online] la <https://ico.org.uk/for-organisations/the-guide-to-nis/nis-and-the-uk-gdpr/>, accesat 11.11.2021. Mai mult decât atât, propunerea de Directivă NIS 2.0 prevede în art. 32 posibilitatea autorităților competente (NIS) să informeze autoritățile de supraveghere (GDPR) cu privire la încălcările obligațiilor de securitate cibernetică care implică o încălcare a securității datelor cu caracter personal. A se vedea și S. Schmitz-Berndt, S. Schiffner, *Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR*, în *International Review of Law, Computers & Technology*, 2021, 35:2, 101-115, DOI: <https://doi.org/10.1080/13600869.2021.1885103>, p. 106. C. Burton, *op. cit.*, p. 643.

³³ Conform art. 10 și art. 12 din Legea nr. 362/2018.

³⁴ Conform art. 37 din GDPR.

esențiale obligația de a stabili mijloace permanente de contact și de a desemna responsabilul cu securitatea rețelelor și sistemelor informatice cu obligația monitorizării mijloacelor de contact.

În ceea ce privește regimul sancționator, fapta prin care sunt încălcate simultan dispozițiile GDPR și cele NIS poate atrage amenzi administrative sau alte sancțiuni prevăzute în cele două reglementări, în mod cumulativ, acestea neexcluzându-se reciproc³⁵.

Este necesar a se avea în atenție și analizată posibilitatea unui conflict între Directiva NIS și Regulamentul GDPR, scenariu puțin probabil, dar posibil. Doctrina de specialitate oferă în acest sens un posibil scenariu în care prevederile GDPR ar intra în conflict cu cele ale Directivei NIS³⁶. Scenariul menționat prevede situația în care un stat membru UE ar decide să permită operațiuni de prelucrare a datelor cu caracter personal interzise sau strict reglementate de GDPR, ca parte a strategiei naționale de securitate cibernetică, precum operațiunile de profilare pe baza unor categorii speciale de date (adrese IP care provin din regiuni cu concentrație mare de populații etnice sau religioase) fără asigurarea garanțiilor prevăzute de art. 22 din GDPR.

Astfel, orice suprapunere a domeniului de aplicare ar trebui rezolvată printr-o relație *lex specialis - lex generalis*, GDPR prevalând în cazul unui conflict cu prevederile Directivei NIS. În sprijinul acestei opinii evidențiem faptul că atât GDPR³⁷ cât și Tratatul de funcționare a Uniunii Europene³⁸ includ dreptul la protecția datelor cu caracter personal în categoria drepturilor fundamentale. Mai mult decât atât, analizând valorile sociale ocrotite de GDPR și Directiva NIS este indubitabil faptul că protecția datelor cu caracter personal trebuie să prevaleze securității cibernetice. Totodată, opinia poate fi argumentată și prin ierarhia instrumentelor juridice potențial conflictuale. Așadar, Directiva NIS fiind transpusă în legislația națională a fiecărui stat membru, un potențial conflict ar

³⁵ Punct de vedere susținut și de autoritatea de supraveghere a datelor cu caracter personal din Regatul Unit al Marii Britanii - Information Commissioner's Office, [Online] la <https://ico.org.uk/for-organisations/the-guide-to-nis/nis-and-the-uk-gdpr/>, accesat 11.11.2021.

³⁶ D. Markopoulou, V. Papakonstantinou, P. de Hert, *op. cit.*, p. 10-11.

³⁷ Considerentul (1) din GDPR prevede faptul că: „Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este un drept fundamental. Articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene („carta”) și articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE) prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc”.

³⁸ Art. 16 TFUE prevede faptul că: „(1) Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc. (2) Parlamentul European și Consiliul, hotărând în conformitate cu procedura legislativă ordinară, stabilesc normele privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii, precum și de către statele membre în exercitarea activităților care fac parte din domeniul de aplicare a dreptului Uniunii, precum și normele privind libera circulație a acestor date”.

avea loc între un Regulament UE și o normă de drept națională, reglementarea europeană având în mod normal prioritate.

Concluzii

Directiva NIS reprezintă un prim pas spre standardizarea nivelului minim de securitate cibernetică la nivelul operatorilor de servicii esențiale și a furnizorilor de servicii digitale care activează în statele membre UE. Totuși, această etapă necesară a fost implementată cu întârziere în contextul evoluției tehnologiei, a răspândirii și accesibilității dispozitivelor IoT și a prelucrărilor automatizate de date.

Întrucât măsurile tehnice necesar a fi implementate de persoanele vizate de Directiva NIS pot reprezenta pentru operatorii de date cu caracter personal un model de urmat în misiunea de conformare la prevederile GDPR și de asigurare a securității datelor confidențiale, conformarea la standardele de securitate cibernetică cât mai înalte devine un deziderat pentru orice entitate care prelucrează informații.

Având în vedere complexitatea și amploarea elementelor tehnice din reglementările NIS subliniem faptul că, spre deosebire de procesul de conformare la prevederile Regulamentului GDPR în care juristul avea nevoie de sprijinul unui specialist IT, implementarea standardelor de securitate impuse de Directiva NIS devine și mai anevoioasă în lipsa unei cooperări active între echipa de specialiști IT și juriști.

Referințe

- Cole M.D., Schmitz S., *The Interplay Between the NIS Directive and the GDPR in a Cybersecurity Threat Landscape* (December 31, 2019), în University of Luxembourg Law Working Paper No. 2019-017, <http://dx.doi.org/10.2139/ssrn.3512093>
- Kuner C., Bygrave L.A., Docksey C., *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, 2020
- Saqib N., Germanos V., Zeng W., Maglaras L., *Mapping of the Security Requirements of GDPR and NIS*, în Preprints, iunie 2020
- Schmitz-Berndt S., Schiffner S., *Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR*, în International Review of Law, Computers & Technology, 2021, 35:2, pp. 101-115, <https://doi.org/10.1080/13600869.2021.1885103>
- Tataru Ș.R., *Internet Cookies - fișierele cu răvaș juridic*, în Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași, Tomul LXVI, Supliment, Științe Juridice, 2020
- Ungureanu C.T., *Contractul Cloud Computing în comerțul internațional*, în Revista Moldovenească de Drept Internațional și Relații Internaționale, Nr. 3 (37), 2015
- Ungureanu C.T., *Drept internațional privat european în raportul de comerț internațional*, Editura Hamangiu, București, 2021
- Ungureanu C.T., *Implicațiile Internetului în viața juridică*, în Analele Științifice ale Universității „Alexandru Ioan Cuza” Iași, Tomul LXIII, Științe Juridice, nr. II, 2017