AVIZUL BĂNCII CENTRALE EUROPENE

din 11 aprilie 2022

cu privire la o propunere de directivă a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Introducere și temei juridic

La 16 decembrie 2020 Comisia Europeană a adoptat o propunere de directivă a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de abrogare a Directivei (UE) 2016/11481148 ([1]) (denumită în continuare „directiva propusă").. La 3 decembrie 2021, Consiliul Uniunii Europene a convenit asupra abordării sale generale cu privire la propunerea de directivă ([2]). Competența Băncii Centrale Europene (BCE) de a emite un aviz se bazează pe articolul 127 alineatul (4) al doilea paragraf din Tratatul privind funcționarea Uniunii Europene, întrucât directiva propusă conține dispoziții care intră în sfera de competență a BCE, în special promovarea bunei funcționări a sistemelor de plăți, contribuția la buna desfășurare a politicilor promovate de autoritățile competente în ceea ce privește stabilitatea sistemului financiar și atribuțiile BCE privind supravegherea prudențială a instituțiilor de credit în temeiul articolului 127 alineatul (2) a patra liniuță și al articolului 127 alineatele (5) și (6) din tratat. În conformitate cu articolul 17.5 prima teză din Regulamentul de procedură al Băncii Centrale Europene, Consiliul guvernatorilor adoptă prezentul aviz.

Observații generale

BCE sprijină cu fermitate obiectivele directivei propuse de a crește nivelul de reziliență cibernetică în toate sectoarele relevante, de a reduce inconsecvențele din cadrul pieței interne și de a îmbunătăți nivelul de conștientizare a situației și capacitatea colectivă de a se pregăti și de a reacționa prin asigurarea unei cooperări eficiente în Uniune.

BCE recunoaște importanța menținerii unor legături puternice între directiva propusă și sectorul financiar, care ar trebui să rămână parte a ecosistemului rețelelor și sistemelor informatice (NIS) pentru a promova evaluarea consecventă a riscurilor legate de tehnologia informației și comunicațiilor (TIC) în întreaga Uniune și pentru a încuraja schimbul de informații și colaborarea transsectoriale eficace atunci când se combat amenințările cibernetice. În acest scop, ar trebui să fie posibil ca autoritățile competente în temeiul propunerii de regulament al Parlamentului European și al Consiliului privind reziliența operațională digitală a sectorului financiar ([3])(denumită în continuare „DORA") să participe la discuțiile strategice de politică și la lucrările tehnice ale Grupului de cooperare NIS, precum și să facă schimb de informații și să coopereze în continuare cu punctele unice de contact și cu echipele naționale de intervenție în caz de incidente de securitate informatică menționate în directiva propusă ([4]).

1. Sfera de aplicare a directivei propuse

1.1 BCE înțelege că, în ceea ce privește entitățile din sectorul financiar, DORA va fi considerată legislație sectorială care introduce cerințe privind gestionarea riscurilor de securitate cibernetică și notificarea incidentelor care au un efect cel puțin echivalent cu cele prevăzute în propunerea de directivă ([5]). Prin urmare, dispozițiile directivei propuse care se referă la gestionarea riscurilor de securitate cibernetică, la obligațiile de raportare, la schimbul de informații și la supraveghere și asigurarea respectării legislației nu se vor aplica niciunei entități financiare care intră sub incidența DORA ([6]). Astfel cum

([1]) COM(2020) 823 final.
([2]) Disponibil pe website-ul Consiliului European, la adresa www.consilium.europa.eu.
([3]) COM(2020) 595 final.
([4]) A se vedea punctul 1.5 din Avizul CON/2021/20 al Băncii Centrale Europene din 4 iunie 2021 cu privire la o propunere de regulament al Parlamentului European și al Consiliului privind reziliența operațională digitală a sectorului financiar (JO C 343, 26.8.2021, p. 1). Toate avizele BCE se publică pe website-ul BCE. Articolul 17 alineatul (5) și articolul 42 din DORA; articolul 11 din directiva propusă.
([5]) Articolul 2 alineatul (6) din directiva propusă.
([6]) A se vedea considerentul (13) și articolul 2 alineatul (6) din directiva propusă.

s-a clarificat în considerentele directivei propuse, dispozițiile DORA care se referă la măsurile de gestionare a riscurilor TIC, la gestionarea și raportarea incidentelor legate de TIC, la testarea rezilienței operaționale digitale, la acordurile privind schimbul de informații și la riscurile TIC generate de terți ar trebui să se aplice în locul celor din directiva propusă ([7]).

1.2 De asemenea, BCE constată că, în abordarea sa generală cu privire la directiva propusă, Consiliul propune o modificare pentru a exclude „entitățile care desfășoară activități în domeniul judiciar, al parlamentelor sau al băncilor centrale" ([8]) din sfera de aplicare al directivei propuse. BCE înțelege că modificarea propusă s-ar extinde la toate misiunile și competențele fundamentale ale Sistemului European al Băncilor Centrale (SEBC), astfel cum sunt prevăzute la articolul 127 alineatul (2) din tratat și la articolul 3.1 din Statutul Sistemului European al Băncilor Centrale și al Băncii Centrale Europene (denumit în continuare „Statutul SEBC"), cum ar fi promovarea bunei funcționări a sistemelor de plăți. În acest sens, se consideră că infrastructurile pieței financiare deținute și operate de Eurosistem, cum ar fi TARGET2 și TARGET2-Securities, se încadrează în propunerea Consiliului de excludere a băncilor centrale din sfera de aplicare a directivei propuse.

2. **Competențele SEBC și ale Eurosistemului în materie de monitorizare**

2.1 Pe lângă obiectivul principal al SEBC de menținere a stabilității prețurilor și în conformitate cu articolul 127 alineatul (2) din tratat, una dintre misiunile fundamentale care trebuie îndeplinite prin intermediul SEBC este promovarea bunei funcționări a sistemelor de plăți ([9]). În îndeplinirea acestei misiuni fundamentale, BCE și băncile centrale naționale pot acorda facilități, iar BCE poate adopta regulamente în vederea asigurării eficienței și solidității sistemelor de compensare și de plăți în cadrul Uniunii și în raporturile cu țările terțe ([10]). În exercitarea rolului său de supraveghere, BCE a adoptat Regulamentul Băncii Centrale Europene (UE) nr. 795/2014 (BCE/2014/28) ([11]) (denumit în continuare „Regulamentul SIPS"), care transpune principiile CPSS-IOSCO pentru infrastructurile pieței financiare ([12]) în legislație direct aplicabilă. Regulamentul SIPS stabilește cerințe atât pentru sistemele de plăți de mare valoare, cât și pentru sistemele de plăți de mică valoare de importanță sistemică, indiferent dacă sunt publice sau private. Cerințele prevăzute în Regulamentul SIPS includ deja, printre altele, gestionarea riscurilor operaționale și instituirea unui cadru de reziliență cibernetică ([13]).

2.2 Pe lângă sistemele de plăți de importanță sistemică, monitorizarea de către Eurosistem acoperă sistemele de plăți care nu sunt importante din punct de vedere sistemic, instrumentele, schemele și mecanismele de plată electronică, precum și alte infrastructuri și prestatori de servicii critice, astfel cum se prevede în cadrul politicii de monitorizare a Eurosistemului ([14]). Sistemele de plăți și alte mecanisme care fac obiectul monitorizării de către Eurosistem nu sunt incluse în mod expres în domeniul de aplicare al directivei propuse ([15]). În același timp, având în vedere că directiva propusă este un instrument de armonizare minimă ([16]), legislația de punere în aplicare adoptată de statele membre s-ar putea suprapune în cele din urmă cu competența de monitorizare a Eurosistemului. Pentru a evita acest lucru, competențele SEBC în temeiul Tratatului și al Statutului SEBC, precum și competențele Eurosistemului în temeiul Regulamentului SIPS și, în general, în temeiul cadrului politicii de monitorizare a Eurosistemului ar trebui să fie recunoscute în mod expres în considerentele directivei propuse.

([7]) Considerentul 13 din directiva propusă.
([8]) Articolul 2 alineatul (3a) primul paragraf litera (b) din abordarea generală a Consiliului privind directiva propusă.
([9]) Articolul 127 alineatul (2) din TFUE, astfel cum este reflectat în articolul 3.1 din Statutul SEBC.
([10]) Articolul 22 din Statutul SEBC.
([11]) Regulamentul (UE) nr. 795/2014 al Băncii Centrale Europene din 3 iulie 2014 privind cerințele de monitorizare pentru sistemele de plăți de importanță sistemică (BCE/2014/28) (OJ L 217, 23.7.2014, p. 16).
([12]) A se vedea Principles for Financial Market Infrastructures (Principii privind infrastructurile pieței financiare) ale Comitetului pentru sisteme de plăți și decontare (CPSS) și al Comitetului tehnic al Organizației internaționale a comisiilor de valori mobiliare (IOSCO), disponibile pe website-ul Băncii Reglementelor Internaționale, la adresa www.bis.org. Responsabilitatea D inclusă în aceste principii prevede că „toți membrii CPSS și IOSCO trebuie să aplice principiile în ceea ce privește IPF-urile relevante din jurisdicțiile lor în cea mai mare măsură permisă de cadrul juridic din jurisdicția lor.
([13]) Articolul 15 din Regulamentul (UE) nr. 795/2014 (BCE/2014/28);
([14]) Eurosystem oversight policy framework (Cadrul politicii de monitorizare a Eurosistemului), versiunea revizuită (iulie 2016) disponibilă pe website-ul BCE la adresa www.ecb.europa.eu.
([15]) Articolul 2 din directiva propusă și anexele I și II la directiva propusă.
([16]) Articolul 3 din directiva propusă.

3. **Riscurile TIC generate de terți, gestionarea incidentelor și crizelor de mare amploare, schimbul de informații și strategia națională de securitate cibernetică**

3.1 *Gestionarea riscurilor TIC generate de terți*

3.1.1 Directiva propusă împuternicește autoritățile competente, atunci când își exercită competențele de asigurare a respectării legislației în ceea ce privește entitățile esențiale, să emită instrucțiuni obligatorii sau un ordin prin care să le solicite entităților respective să remedieze deficiențele identificate sau încălcările obligațiilor prevăzute de directiva propusă ([17]). În același timp, „supraveghetorul principal" desemnat în cadrul DORA poate adresa recomandări furnizorilor terți esențiali de servicii TIC pentru a gestiona riscurile sistemice potențiale pe care le implică practicile de externalizare și concentrarea TIC de către terți ([18]).

3.1.2 Având în vedere că o entitate esențială în temeiul directivei propuse poate fi, de asemenea, desemnată drept un furnizor terț esențial de servicii TIC în temeiul DORA, BCE reiterează ([19]) faptul că ar trebui evitată emiterea de recomandări contradictorii și de instrucțiuni obligatorii. În acest sens, BCE salută abordarea generală a Consiliului cu privire la directiva propusă. Potrivit acestei abordări, autoritățile competente trebuie să informeze „Forumul de monitorizare", instituit în temeiul DORA, atunci când își exercită competențele de supraveghere și de punere în aplicare în legătură cu o entitate esențială desemnată drept furnizor terț esențial de servicii TIC în temeiul DORA ([20]).

3.2 *Gestionarea incidentelor și crizelor de mare amploare*

3.2.1 În conformitate cu directiva propusă ([21]), statele membre trebuie să desemneze una sau mai multe autorități competente responsabile cu gestionarea incidentelor și crizelor de mare amploare. Astfel cum se clarifică în considerentele directivei propuse, un incident de mare amploare ar trebui să însemne un incident cu un impact semnificativ asupra a cel puțin două state membre sau a cărui perturbare depășește capacitatea unui stat membru de a răspunde la acesta. Incidentele de mare amploare se pot transforma în crize de sine stătătoare, perturbând buna funcționare a pieței interne ([22]).

3.2.2 Deși autoritățile competente desemnate în temeiul DORA rămân responsabile de gestionarea incidentelor de securitate cibernetică legate de entitățile financiare, cooperarea cu structurile și autoritățile instituite în temeiul directivei propuse va fi esențială pentru asigurarea unui răspuns coordonat în întreaga Uniune. În acest scop, BCE ar considera binevenită participarea autorităților competente desemnate în temeiul DORA, inclusiv a BCE, la Rețeaua europeană a Organizației de legătură în caz de crize cibernetice (EU-CyCLONe) ([23]), atunci când sectorul financiar este afectat de incidente și crize de securitate cibernetică de mare amploare.

3.3 *Schimbul de informații*

3.3.1 După cum s-a arătat mai sus, BCE sprijină ferm cooperarea dintre autoritățile competente desemnate în temeiul DORA și structurile și autoritățile instituite în temeiul directivei propuse. În special, schimbul de informații între autorități poate permite dezvoltarea transsectorială a cunoștințelor, poate contribui la prevenirea și gestionarea eficace a atacurilor cibernetice și poate promova evaluarea consecventă a riscurilor legate de TIC în întreaga Uniune. Cu toate acestea, BCE subliniază că schimbul de informații ar trebui să aibă loc acolo unde există mecanisme de clasificare și de schimb de informații clar stabilite, însoțite de garanții adecvate pentru a asigura confidențialitatea ([24]). BCE salută abordarea generală a Consiliului cu privire la directiva propusă, care propune schimbul regulat de

([17]) Articolul 29 alineatul (4) litera (b) din directiva propusă.
([18]) A se vedea articolul 31 din DORA.
([19]) A se vedea punctul 1.2 din Avizul CON/2021/20.
([20]) Articolul 29 alineatul (10) din abordarea generală a Consiliului cu privire la directiva propusă.
([21]) Articolul 7 alineatul (1) din directiva propusă.
([22]) Considerentul 27 din directiva propusă.
([23]) Articolul 14 din directiva propusă.
([24]) A se vedea punctul 1.5 din Avizul CON/2021/20.

informații relevante între autorități ([25]), instituirea unor acorduri de cooperare care să specifice un mecanism pentru schimbul de informații ([26]) și transmiterea automată și directă a notificărilor privind incidentele ([27]). În acest sens, ar trebui să se asigure faptul că informațiile care sunt confidențiale în temeiul dispozițiilor privind secretul profesional din DORA ([28]) sau ale legislației sectoriale relevante ([29]) pot face obiectul schimbului cu autoritățile competente menționate în directiva propusă numai în cazul în care schimbul respectiv este necesar pentru ca autoritățile competente să aplice dispozițiile directivei propuse ([30]).

3.4 *Strategia națională de securitate cibernetică*

3.4.1 În temeiul directivei propuse, statele membre trebuie să adopte strategii naționale de securitate cibernetică pentru a defini obiectivele strategice și măsurile adecvate de politică și de reglementare în vederea atingerii și menținerii unui nivel ridicat de securitate cibernetică ([31]). Astfel cum s-a clarificat în considerentele directivei propuse, statele membre ar trebui să continue să includă sectorul financiar în strategiile lor de securitate cibernetică ([32]). Cu titlu indicativ, ca parte a strategiilor lor naționale de securitate cibernetică, statele membre ar trebui să adopte politici care să abordeze securitatea cibernetică în lanțul de aprovizionare pentru produsele și serviciile TIC utilizate de entități pentru furnizarea serviciilor lor. În ceea ce privește sectorul financiar, strategiile naționale de securitate cibernetică ar trebui să fie consecvente cu cadrul de reglementare care decurge din DORA. În acest sens, BCE consideră că sunt necesare clarificări suplimentare pentru a se asigura că strategiile naționale de securitate cibernetică sunt consecvente cu legislația specifică sectorului.

În cazul în care BCE recomandă modificarea directivei propuse, propunerile de redactare specifice însoțite de o explicație în acest sens se regăsesc într-un document tehnic de lucru. Documentul tehnic de lucru este disponibil în limba engleză pe EUR-Lex.

Adoptat la Frankfurt pe Main, 11 aprilie 2022.

Președinta BCE
Christine LAGARDE

([25]) Articolul 11 alineatul (5) din abordarea generală a Consiliului cu privire la directiva propusă.
([26]) Considerentul 23a din abordarea generală a Consiliului cu privire la directiva propusă.
([27]) Considerentul 13 din abordarea generală a Consiliului cu privire la directiva propusă.
([28]) A se vedea articolul 49 din DORA.
([29]) Articolele 53-62 din Directiva 2013/36/UE a Parlamentului European și a Consiliului din 26 iunie 2013 cu privire la accesul la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit, de modificare a Directivei 2002/87/CE și de abrogare a Directivelor 2006/48/CE și 2006/49/CE (JO L 176, 27.6.2013, p. 338).
([30]) Articolul 2 alineatul (5) și articolul 11 alineatul (4) din directiva propusă.
([31]) Articolul 5 din directiva propusă.
([32]) Considerentul 13 din directiva propusă.