



COMISIA EUROPEANĂ

Bruxelles, 4.6.2012
SWD(2012) 136 final

DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI

REZUMAT AL EVALUĂRII IMPACTULUI

Care însoțește documentul

**Propunere de
REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI
privind identificarea electronică și serviciile de asigurare a încrederii pentru tranzacțiile
electronice pe piața internă**

{COM(2012) 238 final}
{SWD(2012) 135 final}

DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI

REZUMAT AL EVALUĂRII IMPACTULUI

Care însoțește documentul

Propunere de REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind identificarea electronică și serviciile de asigurare a încrederii pentru tranzacțiile electronice pe piața internă

1. CONTEXTUL POLITIC, ASPECTE PROCEDURALE ȘI CONSULTAREA PĂRȚILOR INTERESATE

Instaurarea încrederii în mediul online este esențială pentru dezvoltarea economică. Lipsa de încredere determină consumatorii, întreprinderile și administrațiile să ezite să efectueze tranzacții pe cale electronică și să adopte noi servicii. Cadrul de reglementare propus urmărește să asigure tranzacții electronice sigure și fără întreruperi între întreprinderi, cetățeni și administrații, îmbunătățind astfel eficiența serviciilor electronice publice și private, precum și a activităților economice electronice și a comerțului electronic.

Există obstacole în calea serviciilor electronice transfrontaliere și ele trebuie să fie eliminate. Pentru a constitui stimulente și nu obstacole, **identificarea și autentificarea electronică și semnăturile electronice, precum și serviciile conexe de asigurare a încrederii (eIAS)** trebuie, prin urmare, să fie recunoscute și acceptate reciproc pe întreg teritoriul UE.

Nu există un cadru transfrontalier și transsectorial cuprinzător, la nivelul UE, pentru serviciile eIAS. La nivelul UE, există un cadru juridic doar pentru semnăturile electronice, nu și pentru identificarea și autentificarea electronică și nici pentru serviciile conexe de asigurare a încrederii. În *Agenda digitală pentru Europa*, Comisia a anunțat că va propune măsuri juridice privind semnăturile electronice pentru a asigura recunoașterea reciprocă a identificării și a autentificării electronice, pentru a elimina fragmentarea și lipsa de interoperabilitate, pentru a consolida cetățenia digitală și a preveni criminalitatea informatică.

În vederea efectuării prezentei evaluări a impactului, Comisia a colectat informații oferite de statele membre, Parlamentul European și părțile interesate în cadrul unor discuții, ateliere și conferințe. Au fost lansate o serie de studii privind eIAS și s-a studiat literatura de specialitate din domeniu. O consultare publică a fost lansată în 2011 pentru a colecta informații privind modul în care identificarea și autentificarea electronică și semnăturile electronice pot contribui la piața unică. Consultarea a fost completată de o anchetă specifică menită să înregistreze punctele de vedere și nevoile specifice ale IMM-urilor.

2. DEFINIREA PROBLEMEI

Utilizatorii se pot confrunta cu dificultăți în ceea ce privește utilizarea transfrontalieră a serviciilor eIAS. Principalele obstacole care împiedică funcționarea sigură și fără întreruperi a serviciilor eIAS transfrontaliere sunt:

1 — fragmentarea pieței: prestatorii de servicii sunt supuși unor reguli diferite, în funcție de statele membre pe care le deservesc.

În ceea ce privește semnăturile electronice, armonizarea introdusă de Directiva 1999/93/CE privind semnăturile electronice este insuficientă. Au fost identificate patru probleme: divergențe privind punerea în aplicare la nivel național, ca urmare a interpretărilor diferite ale directivei de către statele membre, invocarea în fapt a unei derogări pentru aplicațiile în sectorul public, standarde neactualizate și obligații de supraveghere lipsite de claritate care duc la probleme de interoperabilitate transfrontalieră, la o situație fragmentată la nivelul UE și la denaturări pe piața internă.

În ceea ce privește identificarea electronică, soluțiile tehnologice diferite pentru identificarea personală în diferitele state membre, lipsa de certitudine juridică în ceea ce privește utilizarea transfrontalieră a identificării electronice și lipsa de claritate privind răspunderea pentru corectitudinea datelor de identitate generează probleme de interoperabilitate.

În ceea ce privește serviciile conexe de asigurare a încrederii, dat fiind că nu există un cadru juridic la nivelul UE, unele state membre au adoptat legislații naționale pentru unele dintre aceste servicii, iar prestatorii care doresc să își ofere serviciile în mai multe state membre se confruntă cu costuri ridicate. Ambele situații duc la obstacole pe piața internă și la fragmentare.

2 — lipsa de încredere: lipsa de încredere în sistemele electronice, în instrumentele furnizate și în cadrul juridic poate da impresia că există mai puține garanții juridice decât în cazul interacțiunilor din viața reală.

În cazul semnăturilor electronice, cerințele naționale de supraveghere sunt diferite din punct de vedere calitativ de la un stat membru la altul. Prin urmare, părțile care se bazează pe semnătura electronică au dificultăți în a evalua modul în care este supravegheat un prestator de servicii.

În cazul identificării electronice și a serviciilor conexe de asigurare a încrederii, legislațiile naționale diferite nu oferă utilizatorilor siguranță atunci când interacționează online în diferite situații transfrontaliere.

Principalele patru cauze ale acestor probleme sunt:

A: Un cadru juridic actual insuficient dezvoltat

Serviciile eIAS sunt esențiale pentru o gamă largă de interacțiuni electronice, cum ar fi serviciile bancare electronice, serviciile e-guvernare sau e-sănătate. La nivelul UE, există un cadru de reglementare limitat și imperfect care se concentrează în special asupra semnăturilor electronice. Nu există un cadru specific pentru recunoașterea și acceptarea reciprocă a identificării electronice sau pentru serviciile conexe de asigurare a încrederii, precum marcarea temporală sau sigiliile electronice.

B: Lipsa coordonării între dezvoltarea semnăturii electronice și a identificării electronice

Infrastructurile eIAS naționale au fost dezvoltate separat, fără coordonare la nivelul UE. Ca urmare a acestui fapt, nu există o interoperabilitate transfrontalieră a soluțiilor tehnice, ceea ce reprezintă un obstacol în calea tranzacțiilor electronice. Lipsa recunoașterii și acceptării reciproce este unul dintre motivele scepticismului utilizatorilor și prestatorilor de servicii electronice cu privire la dezvoltarea eIAS.

C: Lipsa transparenței privind garanțiile referitoare la securitate

Adoptarea unor măsuri de securitate stricte și armonizate este esențială pentru crearea unor soluții demne de încredere. Acest lucru este deosebit de important pentru accesul la serviciile în care sunt implicate date cu caracter personal, cum ar fi serviciile de e-sănătate. Directiva 99/93/CE a recunoscut că pot fi considerate ca având securitate juridică doar semnăturile electronice care garantează siguranța și care sunt astfel suficient de protejate împotriva falsificării sau fraudei (semnături electronice avansate și calificate).

Lipsa unor sisteme securizate de identificare electronică este percepută de către utilizatori ca un obstacol major. Lipsa unui cadru juridic armonizat privind identificarea electronică înseamnă că este imposibil să se stabilească în mod obiectiv nivelul de securitate și fiabilitate a identificărilor electronice oficiale în cazul unor operațiuni transfrontaliere. Acest fapt creează obstacole transfrontaliere, ceea ce duce la o lipsă de încredere și la o piață fragmentată.

Un alt motiv de îngrijorare este furtul de identitate. Identificările electronice securizate pot reduce acest risc. Pe de altă parte, identificările electronice insuficient securizate permit infractorilor să obțină identificări electronice false sau compromise.

D: Lipsa de sensibilizare/de adoptare de către utilizatori

Complexitatea tehnologiilor utilizate pentru tranzacțiile electronice și rolul-cheie jucat de părțile terțe demne de încredere dau naștere unui mediu în care este dificil să se evalueze încrederea. În special utilizatorii finali, care în general nu au suficientă expertiză, trebuie să se poată baza pe norme care instituie drepturi și responsabilități clare pentru toate părțile interesate (prestatori de servicii de asigurare a încrederii, utilizatori finali și organisme de guvernanță).

3. SCENARIUL DE REFERINȚĂ

Scenariul de referință al acestei inițiative este absența oricărei noi intervenții de reglementare. Se anticipează că în cadrul acestui scenariu, problemele actuale vor evolua după cum urmează:

Problemele legate de fragmentare și interoperabilitate nu ar fi soluționate: este probabil că statele membre vor continua să pună în aplicare și să asigure respectarea Directivei 99/93/CE.

Nu ar fi asigurată certitudinea juridică: problemele generate de lipsa recunoașterii reciproce a semnăturilor electronice și de absența unui cadru juridic care să reglementeze recunoașterea și acceptarea reciprocă a identificării electronice și a serviciilor conexe de asigurare a încrederii ar împiedica recunoașterea juridică a unei serii de interacțiuni transfrontaliere.

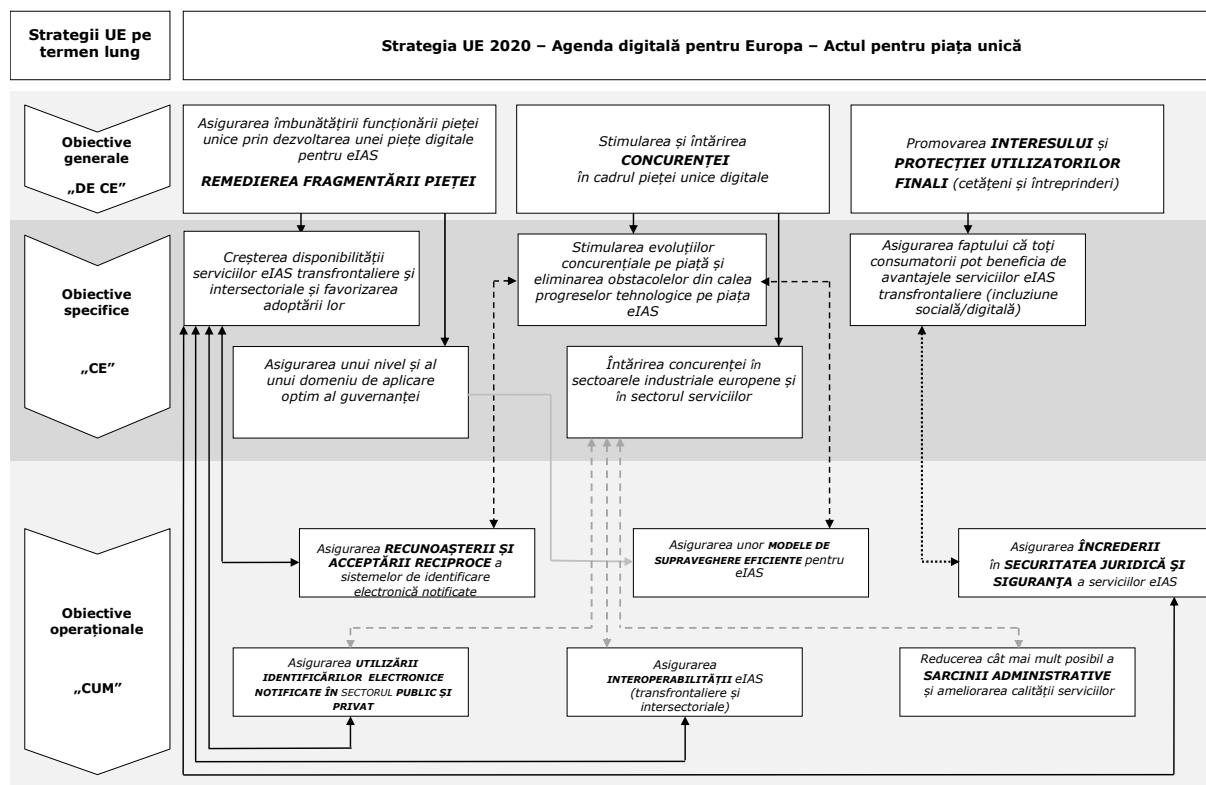
Nevoile utilizatorilor nu ar fi pe deplin satisfăcute: cadrul actual nu oferă posibilitatea de a profita din plin de oportunitățile oferite de progresele tehnologice.

Nu ar fi exploatate pe deplin inițiativele-cheie europene: politicile UE puse în aplicare prin intermediul directivelor privind serviciile, achizițiile publice sau TVA (facturi electronice) sau proiectele-pilot la scară largă din cadrul programului de sprijin strategic în domeniul TIC¹ menite să elimine dificultățile privind interoperabilitatea și recunoașterea transfrontalieră legate de anumite tipuri de interacțiuni electronice ar putea funcționa numai la nivel-pilot, ca urmare a lipsei unui cadru legislativ transsectorial.

4. OBIECTIVELE POLITICII

S-au identificat patru **obiective generale**: asigurarea dezvoltării unei piețe digitale unice; promovarea dezvoltării de servicii publice transfrontaliere cheie; stimularea și consolidarea concurenței în cadrul pieței unice; ameliorarea ușurinței utilizării (pentru cetățeni și întreprinderi). Aceste obiective sunt în conformitate cu politicile strategice ale UE precum *Strategia UE 2020, Agenda digitală pentru Europa, Actul privind piața unică și Foaia de parcurs către stabilitate și creștere*.

Obiectivele specifice exprimă rezultatele dorite ale punerii în aplicare a *obiectivelor operaționale* („cum”) în ceea ce privește piața eIAS („ce”). Pentru fiecare obiectiv specific, au fost identificate o serie de **obiective operaționale**.



¹ http://ec.europa.eu/information_society/activities/ict_psp/about.

5. OPȚIUNI DE POLITICĂ

Pentru a rezolva problemele și pentru a atinge obiectivele menționate mai sus, au fost evaluate trei serii de opțiuni: (1) domeniul de aplicare al cadrului de reglementare propus, (2) instrumentul juridic și (3) nivelul de supraveghere:

- În cadrul primei serii, „*domeniul de aplicare al cadrului de reglementare*”, sunt analizate patru opțiuni:

Opțiunea 0: Abrogarea Directivei 93/99/CE și absența oricăror măsuri de reglementare privind identificarea electronică sau serviciile conexe de asigurare a încrederii.

Această opțiune constă în încetarea tuturor activităților UE în domeniul semnăturilor electronice. Directiva 99/93/CE ar fi abrogată și nu ar fi propusă nicio măsură legislativă pentru recunoașterea reciprocă a identificării electronice.

- *Opțiunea 1:* Nicio modificare a politicii (scenariu de referință)

Directiva 99/93/CE ar fi menținută ca atare. Nu s-ar propune nicio legislație cu privire la identificarea electronică.

- *Opțiunea 2: Consolidarea certitudinii juridice, stimularea coordonării supravegherii naționale și garantarea recunoașterii și acceptării reciproce a identificărilor electronice*

Domeniul de aplicare al Directivei 93/99/CE ar fi extins, astfel încât să se adauge dispoziții referitoare la recunoașterea și acceptarea transfrontalieră „a sistemelor notificate de identificare electronică”². Dispozițiile directivei privind semnăturile electronice ar fi revizuite pentru a remedia actualele deficiențe și pentru a realiza astfel o mai bună armonizare a modelelor naționale de supraveghere.

- *Opțiunea 3: Includerea anumitor servicii conexe de asigurare a încrederii*

Această opțiune extinde opțiunea 2 prin includerea serviciilor conexe de asigurare a încrederii și informațiile de identificare în domeniul de aplicare al propunerii.

Elementele esențiale conexe care ar fi incluse în legislație sunt următoarele: marcarea temporală, sigiliile electronice, păstrarea pe termen lung a informațiilor, furnizarea de documente electronice certificate, admisibilitatea documentelor electronice și autentificarea site-urilor internet.

² „Sistemul de identificare electronică notificat” este un sistem de identificare electronică notificat Comisiei de un stat membru pentru a fi recunoscut și acceptat la nivel transfrontalier. Conceptul de sistem de identificare electronică notificat nu se limitează la sistemele de identificare electronică emise în sectorul public: Statele membre ar putea, de asemenea, să notifice sisteme de identificare electronică emise de sectorul privat, pe care le-ar recunoaște pentru a fi utilizate în cadrul propriilor lor servicii din sectorul public. Această abordare este necesară deoarece nu toate autoritățile statelor membre emit identificări electronice. Abordarea intersectorială a legislației ar permite sectorului privat să integreze utilizarea identificărilor electronice notificate în cadrul serviciilor electronice atunci când este necesară identificarea electronică securizată.

- În cadrul celei de-a doua serii de opțiuni, referitoare la „instrumentul juridic”, sunt luate în considerare patru opțiuni:

Fie un singur instrument legislativ cuprinzător (Opțiunea A) sau două instrumente separate (Opțiunea B)

Legislația ar putea consta într-o singură măsură cuprinzătoare care să reglementeze identificarea, autentificarea și semnătura electronică sau două instrumente, și anume o decizie a Comisiei privind identificarea electronică și o revizuire a directivei privind semnăturile electronice.

O directivă (Opțiunea C) sau un regulament (Opțiunea D):

Legislația ar putea consta într-o directivă sau un regulament.

- La cel de-al treilea nivel, referitor la „supraveghere”, se iau în considerare două opțiuni:

Opțiunea i): Menținerea sistemelor de supraveghere naționale

Sistemele actuale de supraveghere naționale ar fi menținute, însă ar exista un grad mai ridicat de armonizare prin cerințe esențiale comune.

Opțiunea ii): Instituirea unui sistem de supraveghere la nivelul UE

Un sistem de supraveghere la nivelul UE ar fi stabilit pentru a reduce sau a elimina diferențele dintre regimurile de supraveghere naționale. Această opțiune ar putea lua una din următoarele două forme:

Subopțiunea a): înlocuirea sistemelor de supraveghere naționale existente cu un sistem și un organism unic de supraveghere la nivelul UE.

Subopțiunea b): instituirea unui sistem și a unui organism de supraveghere la nivelul UE, menținând în același timp sistemele de supraveghere naționale (statele membre pot alege să folosească propriile lor sisteme sau sistemul european).

6. COMPARAREA OPȚIUNILOR DE POLITICĂ ȘI A IMPACTELOR

Opțiunile de politică au fost evaluate și au fost comparate cu scenariul de bază (Opțiunea 1), ținându-se cont de eficacitatea, eficiența și coerența lor.

6.1. Domeniul de aplicare al cadrului legislativ

Opțiunea 0 nu ar contribui la atingerea obiectivelor identificate în raportul de evaluare a impactului. Nu ar spori disponibilitatea serviciilor eIAS transfrontaliere și intersectoriale și nici adoptarea lor, nu ar asigura un nivel optim de guvernanță, nu ar stimula evoluțiile pieței, nu ar contribui la consolidarea competitivității industriei europene și a sectoarelor serviciilor și nu ar garanta faptul că toți utilizatorii finali ar putea beneficia de avantajul serviciilor eIAS. Dimpotrivă, ar împiedica evoluțiile tehnologice de pe piața eIAS, ar perturba procesul actual

de promovare a unor servicii electronice transfrontaliere și ar menține caracterul fragmentar al pieței UE și situația contrastantă privind încrederea utilizatorilor.

Opțiunea 1 nu ar permite atingerea obiectivelor. Ar menține ambiguitățile existente și disparitățile privind nivelul de încredere în sistemul de supraveghere. Ar exista în continuare incertitudini privind reglementarea, iar piața UE ar continua să fie fragmentată, ceea ce ar duce la denaturarea condițiilor de concurență de pe piața internă și ar crește probabilitatea adoptării unor abordări diferite la nivel național.

Opțiunea 2 ar consolida certitudinea juridică, ar stimula supravegherea și ar asigura recunoașterea și acceptarea reciprocă a identificărilor electronice, ar contribui în mod semnificativ la atingerea fiecăruia dintre obiectivele identificate în raportul privind evaluarea impactului și ar da naștere unor rezultate pozitive la nivel economic, social și de mediu.

Serviciile eIAS ar părea mai atrăgătoare, ceea ce ar duce la creșterea randamentului investițiilor realizate în cadrul serviciilor și infrastructurii eIAS. De asemenea, eIAS ar deveni disponibile pentru toate sectoarele și toate tipurile de societăți, iar obstacolele transfrontaliere ar fi eliminate. Opțiunea ar deschide noi piețe și posibilitatea unor noi investiții, stimulând astfel inovația.

Fragmentarea actuală a pieței s-ar reduce deoarece s-ar îmbunătăți interoperabilitatea transfrontalieră, ca urmare a utilizării standardelor tehnice.

Recunoașterea și acceptarea reciprocă a identificării electronice ar duce la eliminarea, în continuare, a obstacolelor existente în calea pieței unice. În fine, este probabil că cerințele esențiale comune ar favoriza o supraveghere omogenă, ceea ce ar duce la sporirea nivelului de încredere, ar ușura detectarea fraudelor și ar contribui la prevenirea furturilor de identitate.

Opțiunea 3 ar spori atractivitatea serviciilor eIAS și ar amplifica astfel impactul lor pozitiv deoarece ar extinde cadrul juridic pentru a include anumite servicii conexe esențiale de asigurare a încrederii.

*Se consideră că **opțiunea 3** ar avea un impact mai mare decât opțiunile 0, 1 sau 2 asupra operațiunilor electronice sigure și ușor de utilizat.*

6.2. Instrumentul juridic

Asigurarea unui cadru cuprinzător prin intermediul unui **singur instrument** ar garanta coerența măsurilor legislative care reglementează diferitele aspecte ale eIAS. Existența a **două instrumente separate** ar putea duce la divergențe în dispozițiile juridice adoptate pentru semnăturile electronice și identificarea electronică și, în special, în modul de abordare a inițiativelor.

Adoptarea unei **directive** nu ar contribui la rezolvarea problemelor actuale de interoperabilitate privind semnătura electronică care decurg din transpunerile divergente ale Directivei 93/99/CE. Un **regulament** este aplicabil imediat, fără interpretare, și permite astfel o mai bună armonizare și, prin urmare, este mai adecvat pentru atingerea obiectivelor legislației propuse.

Adoptarea unui singur regulament pare a fi modul cel mai eficient de realizare a obiectivelor.

6.3. Nivelul de supraveghere

În cadrul **opțiunii „i”**, noua legislație ar menține sistemele actuale de supraveghere la nivel național și ar impune cerințe esențiale comune privind prestatorii de servicii. O abordare armonizată la nivelul UE pentru semnătura electronică și pentru serviciile conexe de asigurare a încrederii ar îmbunătăți eficacitatea supravegherii, ar spori certitudinea juridică și ar crește securitatea tranzacțiilor electronice și încrederea de care se bucură acestea.

Opțiunea „ii” ar permite realizarea unei supravegheri omogene, eficiente și de calitate peste tot în UE. **Subopțiunea „b”** are avantajul de a oferi un grad mai mare de flexibilitate decât organismul unic de supraveghere UE prevăzut la **subopțiunea „a”**: ar putea fi avantajos, pentru statele membre în care nu există sau există puțini prestatori de servicii de asigurare a încrederii, să transfere sarcinile de supraveghere unui organism de supraveghere la nivelul UE. Alte state membre ar putea, dacă doresc, să își mențină sistemul lor propriu de supraveghere. Totuși, un model de supraveghere centralizată la nivelul UE ridică probleme de subsidiaritate.

Ținând cont de principiului subsidiarității, se consideră că opțiunea cea mai adecvată este (Opțiunea i).

7. LOGICA ACȚIUNII UE, VALOAREA ADĂUGATĂ A UE ȘI SUBSIDIARITATEA

Ca și în cazul Directivei 99/93/CE, temeiul juridic pentru propunerea legislativă este articolul 114 din TFUE privind piața internă, deoarece măsura urmărește să înlăture obstacolele existente în calea bunei funcționări a pieței interne, prin încurajarea recunoașterii și acceptării reciproce a identificării, autentificării și semnăturilor electronice și a serviciilor conexe de asigurare a încrederii la nivel transfrontalier, atunci când tranzacțiile electronice necesită acest lucru.

Datorită naturii inerente neteritoriale a serviciilor eIAS, acțiunea la nivel UE este adecvată și proporțională pentru punerea în aplicare a pieței digitale unice. Nu se poate presupune că măsurile de reglementare luate la nivelul statelor membre ar putea duce la obținerea aceluiași rezultat. Intervenția la nivelul UE este, prin urmare, necesară, adecvată și justificată.

8. MONITORIZARE ȘI EVALUARE

Comisia va monitoriza punerea în aplicare a legislației prin intermediul unui dialog permanent cu părțile interesate și colectarea de statistici. La patru ani de la data intrării sale în vigoare, Comisia va prezenta un raport Parlamentului European și Consiliului cu privire la impactul noii legislații.