

Bruxelles, 26.6.2017
COM(2017) 340 final

RAPORT AL COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU
privind evaluarea riscurilor privind spălarea banilor și finanțarea terorismului care
afectează piața internă și sunt legate de activități transfrontaliere

{SWD(2017) 241 final}

1. INTRODUCERE

Spălarea banilor și finanțarea terorismului sunt provocări semnificative, aflate în evoluție, care ar trebui abordate la nivelul Uniunii Europene (UE). Atentatele teroriste recente și scandalurile financiare recurente necesită acțiuni mai ferme în acest domeniu.

În contextul pieței interne, fluxurile financiare sunt integrate, având caracter transfrontalier, iar banii pot trece rapid, dacă nu instantaneu, de la un stat membru la altul, permițând infractorilor și teroriștilor să transfere fonduri între state fără a fi depistați de autorități.

Pentru abordarea acestor fenomene transfrontaliere, cadrul UE pentru combaterea spălării banilor și combaterea finanțării terorismului a definit normele comune în materie de control și obligații de raportare de către instituțiile financiare și alți actori economici și a stabilit un cadru solid pentru ca unitățile de informații financiare (FIU) ale UE să poată analiza tranzacțiile suspecte și să coopereze între ele. În ciuda progreselor substanțiale și constante în acest domeniu, sunt încă necesare eforturi reînnoite și măsuri suplimentare de acoperire a eventualelor lacune pentru combaterea eficientă a spălării banilor și a finanțării terorismului.

Prezentul raport privind evaluarea supranațională (SNRA) a riscurilor de spălare a banilor și de finanțare a terorismului care afectează piața internă și au legătură cu activitățile transfrontaliere, este primul raport întocmit la nivel supranațional în UE. Raportul analizează riscurile de spălare a banilor și de finanțare a terorismului cu care s-ar putea confrunta UE și propune o abordare cuprinzătoare pentru soluționarea acestora.

În temeiul articolului 6 din Directiva (UE) 2015/849 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului (cea de-a patra Directivă în domeniul combaterii spălării banilor, sau cea de-a patra DCSB)¹ i se solicită Comisiei să întocmească, până la 26 iunie 2017, un raport de identificare, analiză și evaluare a riscurilor de spălare a banilor și de finanțare a terorismului la nivelul Uniunii. Publicarea acestei evaluări supranaționale a riscurilor (SNRA) reprezintă totodată unul dintre obiectivele Agendei europene privind securitatea² și ale Planului de acțiune privind combaterea finanțării terorismului³.

Înțelegerea clară și analiza riscurilor de spălare a banilor și de finanțare a terorismului reprezintă o condiție indispensabilă și prealabilă elaborării oricărui răspuns strategic eficient și adecvat. Evaluarea riscurilor este importantă în mod special pentru piața internă, dat fiind faptul că fluxurile financiare sunt integrate și au caracter transfrontalier.

Evaluarea supranațională a riscurilor (SNRA) aplică o metodologie bine definită⁴ pentru furnizarea unei analize sistematice a riscurilor asociate spălării banilor și finanțării terorismului, legate de modurile de operare folosite de infractori. Scopul nu este acela de a emite judecăți asupra sectorului în ansamblul său, ci de a identifica situațiile în care serviciile și produsele pe care le furnizează sau livrează

¹ Termenul pentru transpunerea directivei respective în legislația națională este 26 iunie 2017.

² COM(2015) 185 final din 28.4.2015

³ COM(2016) 50 final din 2.2.2016

⁴ Pentru o descriere mai detaliată a metodologiei, a se vedea Documentul de lucru al serviciilor Comisiei (2017) 241.

ar putea fi deturnate în scopul spălării banilor sau finanțării terorismului. Această evaluare supranațională a riscurilor (SNRA) se bazează pe Directiva 2005/60/CE (cea de-a treia DCSB), legislația în vigoare la momentul analizei. Evaluarea descrie domeniile în care, la momentul respectiv, cadrul juridic al UE nu era la fel de armonizat sau complet precum a fost imediat ce au intrat în vigoare revizuirile ulterioare ale celei de-a treia DCSB.

Această evaluare supranațională a riscurilor (SNRA) se concentrează pe vulnerabilitățile identificate la nivelul UE, atât în privința cadrului juridic, cât și în privința aplicării efective a acestuia. Evaluarea nu aduce atingere măsurilor de atenuare pe care anumite state membre le aplică sau pot decide să le aplice ca reacție la propriile riscuri de spălare a banilor și de finanțare a terorismului. Prin urmare, ar putea să implementeze deja câteva dintre recomandările de mai jos sau ar fi putut adopta norme mai stricte decât normele minime definite la nivelul UE. Evaluarea măsurilor de atenuare a vulnerabilităților identificate în acest raport ar trebui considerată, prin urmare, referința care ar putea fi adaptată în funcție de măsurile naționale deja în vigoare.

În temeiul articolului 6 din cea de-a patra DCSB, în cazul statelor membre care decid să nu aplice niciuna dintre recomandările propuse în regimurile lor naționale privind combaterea spălării banilor și a finanțării terorismului, acestea ar trebui să notifice Comisia cu privire la decizia lor și să prezinte o justificare în acest sens („conformare sau justificare”).

Acest raport prezintă riscurile principale pentru piața internă într-o gamă largă de sectoare și vulnerabilitățile la nivel orizontal care pot afecta aceste sectoare. Pe această bază, prezentul raport descrie măsurile de atenuare care ar trebui aplicate la nivelul UE și la nivel național pentru abordarea acestor riscuri și formulează mai multe recomandări pentru diverșii actori implicați în eforturile de combatere a spălării banilor și a finanțării terorismului.

Deși Comisia recunoaște riscurile prezentate de anumite țări terțe cu un grad ridicat de risc, o astfel de analiză a riscurilor geografice nu a făcut parte din această primă evaluare supranațională a riscurilor (SNRA). Acest lucru se datorează faptului că analiza riscurilor prezentate de aceste jurisdicții este efectuată în prezent în contextul unui proces separat, mai precis actele delegate ale Comisiei care identifică jurisdicțiile țărilor terțe care au deficiențe strategice ce reprezintă amenințări semnificative la adresa sistemului financiar al UE privind spălarea banilor și finanțarea terorismului⁵.

2. REZULTATELE EVALUĂRII SUPRANAȚIONALE A RISCURILOR (SNRA)

Comisia a identificat 40 de produse sau servicii considerate a fi potențial vulnerabile la riscurile asociate spălării banilor și finanțării terorismului care influențează piața internă. Acestea acoperă 11 sectoare profesionale, inclusiv toate acele sectoare definite în cea de-a patra DCSB, împreună cu anumite sectoare care nu sunt incluse în domeniul de aplicare al directivei, dar care sunt considerate relevante pentru evaluarea supranațională

⁵ Regulamentul delegat (UE) 2016/1675 al Comisiei din 14 iulie 2016 de completare a Directivei (UE) 2015/849 a Parlamentului European și a Consiliului prin identificarea țărilor terțe cu un grad ridicat de risc care au deficiențe strategice. În plus, la nivelul UE, se continuă procesul de înscriere pe liste a țărilor terțe în scopul identificării și abordării țărilor terțe care nu respectă standardele de bună guvernanta fiscală [COM(2016) 24 final].

a riscurilor (SNRA)⁶. Acest lucru i-a permis Comisiei să identifice domeniile pieței interne care prezintă cel mai mare risc și reprezintă cele mai răspândite mijloace utilizate de infractori. Evaluarea supranațională a riscurilor (SNRA) se axează, în primul rând, pe riscurile asociate fiecărui sector relevant. În același timp, pentru a evalua măsurile recomandate pentru abordarea acestor riscuri, Comisia a supus analizei cele mai răspândite mijloace utilizate de infractori.

2.1. Riscurile principale pentru piața internă în sectoarele acoperite de evaluarea supranațională a riscurilor (SNRA)⁷

2.1.1. Sectorul financiar

Sectorul financiar este acoperit de cadrul UE privind combaterea spălării banilor și a finanțării terorismului din anul 1991 și pare să aibă o bună conștientizare a riscurilor sale. Deși teroriștii și infractorii încearcă în continuare să folosească sectorul financiar pentru activitățile lor, evaluarea arată că nivelul riscurilor asociate spălării banilor și finanțării terorismului pentru sectorul financiar este moderat datorită măsurilor de atenuare deja în vigoare.

Cu toate acestea, riscul spălării banilor rămâne semnificativ pentru anumite segmente din sectorul financiar, cum ar fi **serviciile bancare personalizate și investițiile instituționale** (în special prin intermediul brokerilor). Acest lucru se datorează unui grad mai ridicat în ansamblu de expunere la riscurile aferente produselor și clienților, la presiunile exercitate de concurență în sectorul respectiv și la înțelegerea limitată în rândul autorităților de supraveghere a riscurilor operaționale legate de spălarea banilor și finanțarea terorismului. **Serviciile de custodie** sunt considerate, de asemenea, a fi expuse în mod semnificativ riscurilor de spălare a banilor din cauza limitărilor din cadrul capacităților de monitorizare pentru entitățile obligate – și a existenței unităților de depozitare nereglementate (de exemplu zone libere).

Moneda electronică sau serviciile de transmitere a banilor sau valorilor (de exemplu, remiteri de bani)⁸ sunt considerate a fi expuse în mod semnificativ și chiar foarte semnificativ la riscurile asociate spălării banilor și finanțării terorismului - în primul sector din cauza particularităților anonimatului în temeiul celei de-a treia DCSB și în al doilea sector din cauza capacităților de monitorizare inconsecventă la nivelul entităților obligate. În ceea ce privește **casele de schimb valutar și remiterile de bani**, aplicarea normelor privind combaterea spălării banilor și a finanțării terorismului pentru tranzacțiile ocazionale doar pentru sume mai mari de 15 000 EUR pare să ridice probleme întrucât infractorii pot face transferuri mai mici în timp. În special, acest aspect este problematic în absența unei definiții comune a operațiunilor care sunt legate sau au o componentă reală de durată.

⁶ Aceste riscuri sunt legate de utilizarea de numerar, monede virtuale, finanțarea participativă, asigurarea generală și organizațiile nonprofit, precum și de furnizorii de servicii monetare hawala și de alte servicii similare de transferuri neoficiale de valoare.

⁷ Documentul de lucru însoțitor al serviciilor Comisiei conține analiza detaliată a nivelului de amenințare și vulnerabilitate față de spălarea banilor și finanțarea terorismului cu care se confruntă fiecare sector când furnizează anumite produse sau servicii.

⁸ Articolul 4 alineatul (22) din Directiva (UE) 2015/2366 definește „remitterile de bani” drept un serviciu de plată în cadrul căruia se primesc fonduri de la un plătitor, fără crearea unui cont de plăți în numele plătitorului sau al beneficiarului plății, cu scopul unic de a transfera o sumă echivalentă unui beneficiar al plății sau unui alt prestator de servicii de plată care acționează pe seama beneficiarului plății și/sau în cadrul căruia aceste fonduri sunt primite pe seama beneficiarului plății și sunt puse la dispoziția acestuia.

Produsele nou apărute – cum ar fi **platformele de finanțare participativă și monedele virtuale** – par a fi expuse în mod semnificativ riscurilor asociate spălării banilor și finanțării terorismului. Anumite state membre au decis să abordeze aceste produse financiare în legislația națională, însă, în general, cadrul juridic al UE în temeiul celei de-a treia DCSB rămâne inadecvat. **FinTech**⁹ vizează introducerea de soluții tehnologice noi pentru produse financiare mai rapide, mai sigure și mai eficiente, dar ar putea deschide, de asemenea, oportunități noi pentru infractori. Pentru adaptarea la evoluțiile tehnologice continue, vor fi necesare analize suplimentare pentru a înțelege ce riscuri pot prezenta produsele din acest sector aflat în expansiune rapidă și pentru a canaliza posibilitățile noilor tehnologii în vederea intensificării eforturilor pentru combaterea spălării banilor/combaterii finanțării terorismului.

În final, evaluarea a arătat că utilizarea frauduloasă de **credite de consum și de împrumuturi cu valoare redusă** a reprezentat o practică recurentă în cazurile recente de terorism. La nivel național, există un nivel scăzut de conștientizare și o aplicare divergentă a cerințelor privind combaterea spălării banilor și combaterea finanțării terorismului pentru aceste produse.

2.1.2. Sectorul jocurilor de noroc

În temeiul celei de-a treia DCSB, sectorul jocurilor de noroc nu s-a aflat sub incidența cerințelor privind combaterea spălării banilor și combaterea finanțării terorismului, cu excepția cazinourilor. În temeiul celei de-a patra DCSB, toți furnizorii de servicii de jocuri de noroc devin entități obligate. Cu toate acestea, statele membre pot decide să acorde furnizorilor anumitor servicii de jocuri de noroc scutiri totale sau parțiale, pe baza riscului redus dovedit. Statele membre ar trebui să ia în considerare constatările relevante din această evaluare supranațională a riscurilor (SNRA).

În acest moment, anumite produse din sectorul jocurilor de noroc sunt considerate a fi expuse în mod semnificativ riscurilor legate de spălarea banilor. În cazul **serviciilor de pariuri și pocher clasice**, acest risc pare a fi cauzat în special de controalele ineficiente. Această situație se datorează fie faptului că, prin natura lor, aceste activități implică volume semnificative de tranzacții rapide și anonime, bazate adesea pe numerar sau pe un element „peer-to-peer”, împreună cu lipsa unei supravegheri adecvate. În cazul **jocurilor de noroc online**, există o mare expunere la riscuri din cauza volumelor uriașe de tranzacții/fluxuri financiare și din cauza tranzacțiilor la distanță. Jocurile de noroc online permit mijloace anonime de plată, dar, în același timp, oferă o măsură atenuantă importantă sub forma urmăririi tranzacției. **Loteriile și aparatele de jocuri** (din afara cazinourilor) prezintă un nivel moderat de riscuri asociate spălării banilor și finanțării terorismului. Loteriile au dezvoltat un anumit nivel de controale, în special în scopul prevenirii riscurilor asociate cu câștigurile mari. Deși **cazinourile** prezintă, în mod inerent, o mare expunere la riscuri, includerea acestora în cadrul pentru combaterea spălării banilor și combaterea finanțării terorismului din 2005 a avut efect de atenuare a riscurilor asociate spălării banilor și finanțării terorismului. **Jocul tradițional de bingo** este considerat ca prezentând un nivel scăzut de riscuri asociate spălării banilor și finanțării terorismului datorită mizelor și câștigurilor relativ reduse ale acestuia.

⁹ „FinTech” se referă la serviciile financiare bazate pe tehnologie și sprijinite de tehnologie. Tehnologia are potențialul de a facilita accesul la serviciile financiare și de a eficientiza sistemul financiar. „Reg Tech” se referă la adoptarea de noi tehnologii pentru a facilita respectarea cerințelor în materie de reglementare.

2.1.3. *Societățile comerciale și profesiile nefinanciare desemnate*

În general, expunerea sectorului nefinanciar la riscurile asociate spălării banilor și finanțării terorismului este considerată ca fiind semnificativă și foarte semnificativă. Identificarea **beneficiarului real** al clientului pare a fi principala deficiență în acest sector, în special în cazul **furnizorilor de servicii pentru fonduri fiduciare și societăți, consilierilor fiscali, auditorilor, experților contabili externi, notarilor și altor persoane care exercită profesii juridice liberale**. Analiza a arătat că, uneori, conceptul de beneficiar real, în sine, ori nu este înțeles în mod corespunzător, ori nu este verificat în mod corect atunci când se începe o relație comercială.

În cazul special al membrilor profesiilor liberale care desfășoară activități protejate de principiul privilegiului juridic profesional (consilieri fiscali, auditori, experți contabili externi, notari și alte persoane care exercită profesii juridice liberale), punerea în aplicare a normelor privind combaterea spălării banilor și a finanțării terorismului pare a fi dificilă. Privilegiul juridic profesional este un principiu important, recunoscut la nivelul UE. Acesta reflectă echilibrul fragil determinat de jurisprudența Curții de Justiție cu privire la dreptul la un proces echitabil¹⁰, reflectând în sine principiile Curții Europene a Drepturilor Omului și Carta Drepturilor Fundamentale a Uniunii Europene (cum ar fi articolul 47).

În cadrul UE privind combaterea spălării banilor¹¹, acești profesioniști sunt exonerati de obligațiile de raportare atunci când îi asistă pe clienți în cadrul unei proceduri judiciare (privilegiu juridic profesional), fapt care sporește riscul de abuz. De fapt, există cazuri în care acești profesioniști desfășoară uneori activități care sunt protejate în mod clar prin însăși esența privilegiului juridic profesional (de exemplu, stabilirea situației juridice a clientului acestora sau apărarea sau reprezentarea clientului în cadrul procedurilor judiciare) în paralel cu activități neprotejate de privilegiul juridic profesional, cum ar fi oferire de asistență juridică în contextul creării, operării și gestionării de companii. Reiese că există situații în care unii dintre acești profesioniști ar putea considera toate aceste activități ca fiind cuprinse în principiul privilegiului juridic profesional. Acest lucru ar putea avea ca rezultat nerespectarea obligațiilor de combatere a spălării banilor și combatere a finanțării terorismului pentru o parte din activități. Este important de subliniat că respectarea normelor privind combaterea spălării banilor și a finanțării terorismului nu interferează în niciun fel cu principiul privilegiului juridic profesional. În același timp, **interpretarea și aplicarea acestuia** de către profesioniștii care desfășoară activități protejate de principiul privilegiului juridic profesional, ar putea fi îmbunătățite. De asemenea, ar fi utilă o mai bună înțelegere de către consilierii fiscali, auditori, experți contabili externi, notari și alte persoane care exercită profesii juridice liberale, întrucât aceștia sunt considerați a fi și entități obligate în temeiul celei de-a patra DCSB.

În plus, pe baza cadrului juridic actual al UE, organismele de autoreglementare sunt desemnate să supravegheze consilierii fiscali, auditorii, experții contabili externi, notarii și alte persoane care exercită profesii juridice liberale și agenții imobiliare¹². Statele membre au libertatea de a decide dacă aceste organisme de autoreglementare sunt competente să primească rapoartele de tranzacții suspecte (RTS) direct de la entitățile obligate, cărora le revine astfel responsabilitatea de a le transmite către unitatea de

¹⁰ A se vedea cauza C-305/05.

¹¹ A se vedea articolul 23 alineatul (2) din Directiva 2005/60/CE.

¹² Directiva (UE) 2015/849 definește organismul de autoreglementare ca un organism care reprezintă membrii unei profesii sau care joacă un rol în reglementarea acestora, în realizarea anumitor funcții de supraveghere sau de monitorizare și în asigurarea punerii în aplicare a normelor referitoare la aceștia.

informații financiare (FIU) cu promptitudine și nefiltrate. Consultările au arătat că entitățile obligate și organismele de autoreglementare din acest sector nu raportează multe tranzacții suspecte către unitățile de informații financiare (FIU), în special în anumite state membre. Acest lucru ar putea indica faptul că fie tranzacțiile suspecte nu sunt detectate și raportate în mod corect, fie că organismul de autoreglementare nu asigură transmiterea sistematică a rapoartelor de tranzacții suspecte (RTS).

Sectorul imobiliar este, de asemenea, expus unor riscuri semnificative de SB, din cauza numărului mare de profesioniști implicați în tranzacțiile imobiliare (agenți imobiliari, instituții de credit, notari și avocați). O altă modalitate obișnuită de spălare a banilor este reprezentată de suprafacturarea în cadrul tranzacțiilor comerciale, „**spălarea banilor bazată pe activități comerciale**”) sau constituirea de împrumuturi fictive. Infractorii folosesc aceste metode ca mijloc de justificare a transferului produselor provenite din săvârșirea de infracțiuni prin intermediul canalelor bancare, utilizând deseori documente false pentru comerțul cu bunuri și servicii. În mod similar, împrumuturile fictive sunt deseori constituite între aceștia pentru crearea unei tranzacții financiare fictive, în vederea justificării transferurilor de fonduri de origine ilegală. Autoritățile de aplicare a legii consideră că acest risc este semnificativ.

*2.1.4. Activele în numerar și cele similare*¹³

Evaluarea supranațională a riscurilor a arătat că **numerarul** rămâne modalitatea cel mai frecvent utilizată în scopul spălării banilor și a finanțării terorismului, întrucât le permite infractorilor să își ascundă identitatea. Din acest motiv, apare în aproape fiecare investigație privind spălarea banilor și finanțarea terorismului. În temeiul celei de-a treia DCSB, tranzacțiile în numerar nu au fost monitorizate în mod corespunzător pe piața internă din cauza lipsei unei reglementări clare și a cerințelor de control. Anumite state membre au introdus rapoarte de tranzacții cu numerar (RTN) sau limitări ale plăților în numerar. Însă, în lipsa cerințelor comune pentru toate statele membre, infractorii pot profita cu ușurință de diferențele dintre legislații. În mod asemănător, cadrul UE pentru controale privind curierii de numerar la frontierele externe ale UE¹⁴ nu asigură niveluri adecvate de atenuare, în special pentru că acesta nu acoperă echivalente de numerar precum mărfuri cu grad mare de lichiditate care includ aur, diamante sau carduri anonime preplătite cu capacitate ridicată de stocare.

În plus, riscurile prezentate de **comercianții de bunuri cu valoare ridicată** care acceptă plățile în numerar în valoare de peste 15 000 EUR sunt considerate semnificative din cauza expunerii inerente la riscuri și a nivelului scăzut de controale. Faptul că acești comercianți se află sub incidența normelor privind combaterea spălării banilor și a finanțării terorismului doar în măsura în care acceptă plățile în numerar cu valoare ridicată pare să conducă la ineficiența aplicării acelor norme. Provocarea este chiar mai importantă cu privire la **întreprinderile cu flux crescut de lichidități**. Acestea nu intră sub incidența normelor privind combaterea spălării banilor și a finanțării terorismului, cu excepția cazului în care se încadrează în categoria de mai sus a comercianților de bunuri cu valoare ridicată. Însă pot fi utilizate, în mod foarte convenabil, pentru spălarea produselor bazate pe numerar obținute din activități infracționale.

¹³ Nu sunt vizate transferurile în numerar cu scopuri multiple în cadrul operațiunilor de ajutor umanitar finanțate de UE.

¹⁴ Regulamentul (CE) nr. 1889/2005 din 26 octombrie 2005 privind controlul numerarului la intrarea sau ieșirea din Comunitate.

Evaluarea subliniază, de asemenea, că activele care oferă facilități asemănătoare celor oferite de numerar (**aur, diamante**) sau bunuri cu valoare ridicată privind „stilul de viață”, comercializabile cu ușurință, (de exemplu **artefacte culturale, mașini, bijuterii, ceasuri**) prezintă risc ridicat din cauza controalelor de nivel slab. S-au exprimat preocupări specifice în legătură cu jaful și traficul de antichități și alte artefacte: artefactele jefuite pot servi ca sursă a finanțării terorismului – sau, în mod alternativ, reprezintă o opțiune de plasament atractivă pentru spălarea banilor.

2.1.5. Organizațiile non-profit

Organizațiile non-profit (ONP) pot fi expuse riscurilor de a fi utilizate abuziv în scopul finanțării terorismului. Analiza vulnerabilității sectorului organizațiilor non-profit la finanțarea terorismului a constituit mai degrabă o provocare, întrucât acest sector se caracterizează printr-o varietate de structuri și activități care prezintă grade diferite de expunere la risc și de conștientizare a riscurilor. Acest lucru se datorează în mare parte divergențelor din domeniul organizațiilor non-profit și diferențelor cu privire la cadrele juridice și practicile naționale. „Organizațiile non-profit sugestive”¹⁵ prezintă o anumită vulnerabilitate, deoarece în cadrul acestora se pot infiltra organizații criminale sau teroriste care pot ascunde beneficiarul real, făcând mai dificilă trasabilitatea colectării de fonduri, în timp ce unele tipuri de „organizații non-profit furnizoare de servicii”¹⁶ sunt vulnerabile într-un mod mai direct din cauza naturii intrinseci a activității acestora. Aceasta se datorează faptului că organizațiile respective pot presupune finanțarea în și din zonele de conflict sau țările terțe identificate de Comisie ca prezentând deficiențe strategice în regimurile acestora de combatere a spălării banilor și a finanțării terorismului¹⁷. Cu toate acestea, pe parcursul analizei s-a considerat că această varietate în cadrul organizațiilor non-profit nu împiedică identificarea caracteristicilor comune ale vulnerabilităților din sectorul organizațiilor non-profit.

În acel context, analiza a arătat că cerințele existente de combatere a spălării banilor și de combatere a finanțării terorismului nu sunt considerate în mod obligatoriu de autoritățile competente ca fiind adecvate pentru a răspunde nevoilor specifice ale sectorului organizațiilor non-profit, iar controalele aplicate diferă în funcție de statul membru vizat. Este admis faptul că acele controale aplicate sunt mai eficiente atunci când gestionează colectarea de fonduri în interiorul UE, ceea ce face ca nivelul vulnerabilităților să fie mai scăzut decât în cazul transferurilor de fonduri sau al cheltuielilor din afara UE, unde rămân deficiențe majore.

În termeni mai generali, evaluarea sectorului organizațiilor non-profit a arătat că acesta poate fi supus unei reduceri a riscurilor, de exemplu, unele instituții financiare pot fi reticente în a furniza servicii financiare acestui sector, cum ar fi deschiderea unui cont bancar. Este posibil ca unele tranzacții financiare să fie refuzate, în funcție de țara de destinație a fondurilor. În plus, este posibil ca organizațiile mai mici, care nu sunt în măsură să demonstreze că dețin acreditarea sau dovada înregistrării fiscale, să se afle în

¹⁵ „Organizațiile non-profit sugestive” sunt organizații non-profit implicate, în principal, în activități sugestive care includ programe axate pe sport și recreere, artă și cultură, reprezentarea intereselor și apărarea anumitor interese.

¹⁶ „Organizațiile non-profit furnizoare de servicii” sunt acele organizații non-profit implicate în activități diverse, cum ar fi programele axate pe furnizarea de servicii de asigurare de locuințe, de asistență socială, de educație sau medicale.

¹⁷ Regulamentul delegat (UE) 2016/1675 al Comisiei din 14 iulie 2016 de completare a Directivei (UE) 2015/849 a Parlamentului European și a Consiliului prin identificarea țărilor terțe cu un grad ridicat de risc care au deficiențe strategice.

imposibilitatea de a deschide conturi bancare. Conform reprezentanților organizațiilor non-profit, excluderea de la furnizarea de servicii financiare crește utilizarea numerarului, care este mult mai vulnerabil în fața abuzurilor de spălare de bani/finanțare a terorismului.

Problema reducerii riscurilor sau a excluderii financiare reprezintă o preocupare de care ar trebui să se țină seama atunci când se abordează politica privind combaterea spălării banilor și combaterea finanțării terorismului. Clienții nu trebuie să fie respinși de furnizorii de servicii financiare reglementate și obligați să utilizeze servicii bancare ilegale sau servicii de transferuri ilegale. Cu toate acestea, combaterea spălării banilor și combaterea finanțării terorismului reprezintă doar unul dintre factorii multipli de reducere a riscurilor. La nivelul UE, adoptarea „directivei privind conturile de plăți”¹⁸ va crește foarte mult accesul la serviciile financiare de bază care ar limita, probabil, încrederea în canalele neoficiale.

2.1.6. Furnizorii de servicii monetare hawala

În timp ce serviciile de transfer de valoare prezintă propriile riscuri, serviciile monetare hawala¹⁹ și alte astfel de servicii neoficiale de transfer de valoare prezintă o amenințare specifică, în special în contextul finanțării terorismului. În mod normal, toți operatorii care furnizează servicii de plată, astfel cum sunt definiți la articolul 4 alineatul (3) din a doua directivă privind serviciile de plată (DSP2)²⁰ ar trebui să fie înregistrați și reglementați în mod corespunzător. Acești furnizori ar trebui să solicite statutul de instituții de plată autorizate sau, în anumite condiții, instituții de plată înregistrate. Sistemul hawala și alte astfel de servicii neoficiale de transfer de valori se califică, de obicei, ca ilegale întrucât, de obicei, acestea nu sunt înregistrate și nu respectă cerințele din DSP2. Această problemă este agravată de dificultatea de detectare a existenței sistemului hawala sau a altor astfel de servicii: tranzacțiile sunt adesea grupate, compensate cu importuri/exporturi de bunuri, permițând o urmărire limitată a informațiilor. De asemenea, reducerea riscurilor este relevantă în acest sens, întrucât clienții respinși de către furnizorii de servicii financiare reglementate recurg uneori la servicii ilegale de acest tip.

2.1.7. Falsificarea banilor

Falsificarea banilor reprezintă un tip de activitate ilegală transnațională, cu un nivel ridicat al circulației transfrontaliere atât a infractorilor, cât și a monedelor contrafăcute, și implică adesea grupuri infracționale organizate. Plasarea banilor falși generează produse ale infracțiunilor, care trebuie să fie spălate pentru a fi integrate în fluxul financiar regulat. În plus, banii contrafăcuți ar putea fi distribuiți prin rețele teroriste pentru finanțarea instruirii, recrutării, atacurilor și propagandei care necesită fonduri importante. Produsele obținute din contrafacere ar putea fi investite pentru consolidarea infrastructurii de sprijinire a terorismului.

¹⁸ Directiva 2014/92/UE din 23 iulie 2014 privind comparabilitatea comisioanelor aferente conturilor de plăți, schimbarea conturilor de plăți și accesul la conturile de plăți cu servicii de bază.

¹⁹ Furnizorii de hawala și alte servicii similare (HOSSP) asigură transferul și primirea de fonduri sau valoare echivalentă și efectuează decontări prin operațiuni comerciale, numerar și decontare netă pe o perioadă îndelungată de timp. Ceea ce îi face să fie diferiți de alte societăți de transfer de bani este faptul că folosesc metode de decontare nebankare.

²⁰ Directiva (UE) 2015/2366 din 25 noiembrie 2015 privind serviciile de plată în cadrul pieței interne, de modificare a Directivelor 2002/65/CE, 2009/110/CE și 2013/36/UE și a Regulamentului (UE) Nr. 1093/2010 și de abrogare a Directivei 2007/64/CE.

2.2. Vulnerabilități orizontale

Comisia a identificat o serie de vulnerabilități comune tuturor sectoarelor.

2.2.1. *Caracterul anonim al tranzacțiilor financiare (produse financiare în numerar și alte produse financiare anonime)*

Organizațiile criminale sau grupurile teroriste încearcă să evite urmărirea oricăror informații și să rămână nedetectate când comit activități ilegale. Prin chiar natura lor, tranzacțiile în numerar permit anonimatul complet, ceea ce le transformă în metode de plăți/de transferuri foarte atractive pentru infractori. Sectoarele expuse unui nivel ridicat de tranzacții cu numerar sunt considerate în mod special ca fiind expuse riscului. Acest lucru este relevant în special pentru întreprinderile cu flux crescut de lichidități, comercianții care furnizează bunuri și servicii și acceptă plăți în numerar și operatorii economici care acceptă plăți în valori nominale mari, cum ar fi bancnotele de 500 EUR și de 200 EUR.

Produsele financiare care prezintă caracteristici de anonimat similare în anumite împrejurări (cum ar fi produsele de monedă electronică anonime, monedele virtuale sau platformele de finanțare participativă) sunt, de asemenea, vulnerabile la spălarea banilor și finanțarea terorismului. Nivelurile de risc ale acestora diferă față de tranzacțiile în numerar întrucât necesită o planificare mai sofisticată, acoperă volume mai mici de tranzacții și pot fi supuse unui anumit nivel de monitorizare. Totuși, caracteristicile anonimatului acestora impun o limitare intrinsecă a posibilităților de identificare și de monitorizare. Aceeași analiză se aplică și altor tipuri de active, precum aurul și diamantele, care pot fi comercializate cu ușurință sau pot fi depozitate în condiții de siguranță. Acestea sunt ușor de transferat și, în același timp, permit păstrarea anonimatului.

2.2.2. *Identificarea și accesul la informațiile referitoare la beneficiarul real*

Infractorii utilizează sistemul financiar și pentru plasarea produselor ilegale ale acestora pe piețele financiare, în sectorul imobiliar sau economia legală într-un mod mai structurat decât în cazul tranzacțiilor financiare în numerar sau anonime. În primul rând, toate sectoarele sunt vulnerabile față de riscul de infiltrare, integrare sau proprietate de către organizațiile de criminalitate organizată și grupurile teroriste. Pe de altă parte, tehnica obișnuită a infractorilor este aceea de a crea societăți de tip „cutie poștală”, fiducii sau structuri corporative complexe pentru a-și ascunde identitățile. În astfel de cazuri, deși fondurile implicate pot fi identificate în mod clar, beneficiarul real rămâne necunoscut. Conform informațiilor deținute de autoritățile de aplicare a legii, în cazurile importante de spălare a banilor și finanțare a terorismului s-au folosit în mod recurent structuri opace cu scopul ascunderii beneficiarilor reali. Această problemă foarte răspândită nu se limitează la anumite jurisdicții sau anumite tipuri de entități juridice sau construcții juridice. Infractorii utilizează cea mai convenabilă, ușoară și sigură modalitate în funcție de expertiza, localizarea acestora și de practicile de piață din jurisdicția lor.

Cea de-a treia DCSB cuprinde norme referitoare la definirea beneficiarului real în momentul începerii unei relații comerciale. Pragul de deținere de 25 % pentru beneficiarul real pentru definirea unui element de control este doar orientativ, iar identificarea „directorului principal” ca beneficiar real trebuie să se facă doar în ultimă instanță, atunci când nu poate fi identificat niciun alt beneficiar real după o evaluare aprofundată și documentată (de exemplu, titluri de participare divizate). Cu toate acestea,

este posibil ca normele să fie aplicate în mod mecanic în practică de anumite entități obligate. În aceste cazuri, este discutabil dacă acest lucru duce la identificarea beneficiarului real.

2.2.3. Supravegherea în cadrul pieței interne a UE

Sunt evidente anumite vulnerabilități față de eficacitatea supravegherii financiare în context transfrontalier. Conform avizului comun al autorităților europene de supraveghere (AES)²¹, evaluarea de către autoritățile competente a conformității sectorului pe care acestea îl supraveghează variază în mod semnificativ. Cel mai dificil aspect se referă la situațiile în care entitățile care aparțin aceluiași grup financiar sunt supuse supravegherii autorităților competente din mai multe state membre. Aceste situații fac destul de complexă punerea în aplicare a normelor privind combaterea spălării banilor și a finanțării terorismului din cauza diferențelor persistente în abordarea autorităților competente referitoare la supravegherea combaterii spălării banilor și a finanțării terorismului și din cauza incertitudinii privind responsabilitățile de supraveghere ale statelor membre de origine și ale celor gazdă, în special pentru instituțiile de plată și agenții lor străini. Acest lucru creează riscul ca încălcările sau cazurile de abuz în scopul infracțiunilor financiare să rămână neidentificate. În plus, se pare că uneori informațiile relevante nu sunt difuzate suficient sau în timp util între autoritățile de supraveghere competente pentru combaterea spălării banilor/combaterarea finanțării terorismului.

Există mai multe motive care explică această situație:

- diferențe de statut ale omologilor;
- un cadru inadecvat pentru schimbul de informații confidențiale privind combaterea spălării banilor/combaterarea finanțării terorismului;
- concentrarea excesivă asupra supravegherii pur prudențiale; și
- lipsa unui cadru juridic/a mecanismelor pentru schimbul de informații între autoritățile de supraveghere prudențială și autoritățile de supraveghere financiare privind combaterea spălării banilor/combaterarea finanțării terorismului²².

În sfârșit, într-un număr limitat de cazuri, autorităților de supraveghere le este greu să identifice omologii competenți întrucât, în anumite state membre, supravegherea privind combaterea spălării banilor/combaterarea finanțării terorismului este fragmentată. Avizul comun menționează, de asemenea, că anumite autorități de supraveghere nu identifică în mod adecvat riscurile legate de spălarea banilor și finanțarea terorismului, aferente sectoarelor pe care le supraveghează și/sau nu dețin proceduri suficiente sau relevante, bazate pe o analiză a riscurilor în scopul supravegherii acestora, mai ales în domeniul finanțării terorismului.

În ceea ce privește sectoarele nefinanciare, statele membre pot permite organismelor de autoreglementare să îndeplinească funcții de supraveghere pentru consilieri fiscali, auditori, experți contabili externi, notari și alte persoane care exercită profesii juridice liberale și agenți imobiliari. Indiferent de modelul de supraveghere urmat, aceasta

²¹<http://www.eba.europa.eu/documents/10180/1759750/ESAS+Joint+Opinion+on+the+risks+of+money+laundry+and+terrorist+financing+affecting+the+Union%E2%80%99s+financial+sector+%28JC-2017-07%29.pdf>

²² De exemplu, în prezent, BCE nu poate furniza autorităților de supraveghere naționale pentru combaterea spălării banilor/combaterarea finanțării terorismului informații prudențiale și confidențiale, care să fie relevante și pentru supravegherea privind combaterea spălării banilor/combaterarea finanțării terorismului.

prezintă lipsuri din punct de vedere al controalelor, orientării și nivelului de raportare în marea majoritate a statelor membre.

2.2.4. Cooperarea între unitățile de informații financiare (FIU)

Unitățile de informații financiare (FIU) sunt responsabile de primirea și analiza informațiilor referitoare la activitățile financiare suspecte relevante pentru spălarea banilor, finanțarea terorismului și infracțiunile premergătoare aferente și de difuzarea rezultatelor analizei lor către autoritățile competente. Această analiză este fundamentală pentru ca autoritățile de aplicare a legii să înceapă investigații noi sau să completeze pe cele existente. Deși colaborarea dintre unitățile de informații financiare (FIU) din cadrul UE a crescut în mod semnificativ în ultimul deceniu, rămân totuși anumite vulnerabilități în cooperarea între unitățile de informații financiare (FIU).

Un raport sinoptic privind platforma unităților de informații financiare (FIU)²³ a identificat pe larg obstacolele în calea accesului, schimbului și utilizării de informații și a cooperării operaționale dintre unitățile de informații financiare (FIU). Raportul sinoptic a fost încheiat în decembrie 2016²⁴. Acesta evidențiază, de asemenea, aspecte legale, practice și operaționale de bază. Pe baza acestuia și a propriei analize, Comisia a subliniat direcțiile posibile pentru îmbunătățirea cooperării dintre unitățile de informații financiare (FIU) din cadrul UE într-un document de lucru separat al serviciilor Comisiei²⁵.

2.2.5. Alte vulnerabilități comune tuturor sectoarelor

Evaluarea supranațională a riscurilor (SNRA) a arătat că toate sectoarele identificate sunt expuse unor vulnerabilități suplimentare:

- **infiltrarea infractorilor**: uneori, infractorii pot deveni proprietari ai unei entități obligate sau pot identifica entități obligate dispuse să îi sprijine în activitățile lor de spălare a banilor. Aceasta face ca testele de competență și onorabilitate să fie relevante pentru toate sectoarele analizate;
- **documente falsificate**: tehnologia modernă facilitează crearea de documente falsificate și toate sectoarele se străduiesc să instituie mecanisme solide pentru detectarea acestora;
- **schimb de informații insuficient între sectorul public și cel privat**: toate entitățile obligate au subliniat necesitatea mecanismelor corespunzătoare de feedback din partea unităților de informații financiare (FIU) și a schimbului de informații cu autoritățile competente. Raportarea tranzacțiilor suspecte de către entitățile obligate care își desfășoară activitatea în jurisdicțiile naționale reprezintă o altă dificultate vădită;
- **resurse insuficiente, conștientizarea riscurilor și know-how pentru implementarea normelor privind combaterea spălării banilor și a finanțării terorismului**: întrucât anumite entități obligate investesc în instrumente de conformitate sofisticate, multe dintre ele au un nivel mai redus al gradului de conștientizare, al instrumentelor și capacităților în acest domeniu; și
- **riscuri noi care decurg din FinTech**: se preconizează că utilizarea serviciilor online va crește și mai mult în economia digitală, stimulând cererea de identificare online, prezentând în același timp un risc crescut ce rezultă din tranzacțiile la distanță. Folosirea și fiabilitatea unei identificări electronice este fundamentală în acest sens.

²³ Platforma unităților de informații financiare (FIU) este un grup neoficial, înființat de Comisie în 2006, care reunește unitățile de informații financiare ale statelor membre ale UE.

²⁴ Platforma unităților de informații financiare din UE (referință E03251) <http://ec.europa.eu/transparency/regexpert/>

²⁵ SWD (2017)/275.

3. MĂSURI DE ATENUARE PENTRU ABORDAREA RISCURILOR IDENTIFICATE

După evaluarea nivelurilor de risc, prezentul raport descrie măsurile despre care Comisia consideră că ar trebui aplicate la nivelul UE și al statelor membre. Acestea rezultă din evaluarea eventualelor opțiuni de abordare a riscurilor identificate. În cadrul acestui exercițiu comparativ, Comisia a luat în considerare:

- nivelul de riscuri asociate spălării banilor și finanțării terorismului;
- necesitatea și proporționalitatea implicate în luarea de măsuri sau recomandarea luării de măsuri de către statele membre;
- necesitatea și proporționalitatea implicate în recomandarea de măsuri de reglementare sau fără caracter de reglementare; și
- impactul asupra dreptului la viață privată și asupra drepturilor fundamentale .

În plus, Comisia a analizat necesitatea de a evita orice potențial abuz sau interpretare eronată a recomandărilor sale care ar conduce la excluderea unor categorii întregi de clienți și încetarea relațiilor cu clienții, fără a lua în considerare pe deplin și în mod corespunzător nivelul de risc dintr-un anumit sector.

În cadrul evaluării, Comisia a identificat, de asemenea, produse care prezintă doar un nivel slab (sau moderat) de risc pentru care, în acest moment, nu se consideră a fi necesare alte măsuri suplimentare de atenuare. Prin urmare, măsurile prezentate în prezentul raport privesc doar riscurile despre care Comisia consideră că necesită atenuare suplimentară. Această abordare este menită să permită statelor membre să identifice mai bine acțiunile prioritare în conformitate cu abordarea bazată pe risc. Deși recomandările pentru statele membre cuprind multe domenii variate, cele mai multe se referă la punerea în aplicare a legislației UE²⁶. Recomandările au fost concepute să sprijine statele membre să se concentreze pe domenii de risc cheie în aplicarea obligațiilor lor. Această evaluare nu aduce atingere măsurilor de atenuare pe care unele state membre le aplică sau este posibil să decidă să le aplice ca reacție la propriile riscuri naționale, asociate spălării banilor și finanțării terorismului. Prin urmare, statele membre ar putea să pună în aplicare deja câteva dintre recomandările de mai jos sau să fi adoptat norme mai stricte decât normele minime definite la nivelul UE.

Evaluarea supranațională a riscurilor (SNRA) încearcă să ofere o imagine instantanee a riscurilor asociate spălării banilor și finanțării terorismului la data publicării sale. Acest exercițiu a început și s-a încheiat în perioada în care cadrul legislativ relevant în vigoare a fost reprezentat de Directiva 2005/60/CE (cea de-a treia DCSB). Deși cea de-a patra DCSB era adoptată deja la momentul respectiv, termenul de transpunere nu expirase încă. Din acest motiv, nu a fost posibil să se includă nicio evaluare a efectelor concrete pe care le-ar avea punerea în aplicare a acesteia. Însă, modificările cadrului UE de combatere a spălării banilor prin cea de-a patra DCSB și modificările propuse la acesta²⁷ au fost luate în considerare în definirea măsurilor de atenuare, având în vedere că aceste două instrumente vor consolida în mod substanțial cadrul juridic de prevenire și astfel, atenuează câteva vulnerabilități și riscuri menționate anterior.

²⁶ De exemplu, evaluări ale riscurilor naționale, registre ale beneficiarilor reali, supraveghere, alocarea resurselor, feedback pentru sectorul privat și sectoarele care prezintă riscuri asociate spălării banilor și finanțării terorismului, care sunt reglementate de cea de-a patra DCSB.

²⁷ COM (2016) 450 final.

3.1. Măsuri de atenuare conform celei de-a patra DCSB

Conform celei de-a patra DCSB, începând cu data de 26 iunie 2017, cadrul juridic al UE include cerințe noi:

- domeniul de aplicare al entităților obligate a fost extins pentru a cuprinde furnizorii de servicii de jocuri de noroc, comercianții care acceptă plăți în numerar în valoare de peste 10 000 EUR și tranzacții ocazionale ce constituie transfer de fonduri (inclusiv remiteri de bani) de peste 1 000 EUR;
- a fost consolidată abordarea bazată pe risc;
- sunt create registre privind informațiile despre beneficiarii reali pentru a facilita identificarea beneficiarilor reali ai entităților juridice și ai unor construcții juridice;
- se reduce anonimatul produselor de monedă electronică;
- noul nivel al sancțiunilor crește efectul de descurajare;
- se stabilește un nou regim în ceea ce privește cooperarea dintre unitățile de informații financiare (FIU) din cadrul UE.

Se așteaptă ca aceste măsuri noi să reducă în mod semnificativ nivelurile de risc din toate sectoarele. Comisia va evalua conformitatea cu cea de-a patra DCSB și va publica un raport de evaluare a implementării până în iunie 2019.

3.2. Măsuri de atenuare deja în vigoare sau în curs de desfășurare la nivelul UE

În plus, evaluarea supranațională a riscurilor (SNRA) a confirmat că este nevoie să se facă mai mult cu privire la unele aspecte care necesită măsuri legislative sau alte inițiative strategice lansate la nivelul UE.

3.2.1. Măsuri legislative

- **Propunerea Comisiei de modificare a celei de-a patra DCSB:** conform acestei propuneri, atât platformele de schimb pentru monedele virtuale, cât și furnizorii de portofele digitale, ar trebui să devină entități obligate pentru reducerea caracterului anonim al tranzacțiilor. Posibilitatea ca produsele de monedă electronică să fie scutite de cerințele privind combaterea spălării banilor/combateră finanțării terorismului va fi limitată și mai mult. Eficiența unităților de informații financiare (FIU) va fi consolidată și vor fi instituite registre centralizate ale conturilor bancare sau sisteme de recuperare care să permită solicitări mai bine direcționate. Normele mai stricte privind cooperarea între autoritățile competente, inclusiv autoritățile de supraveghere, vor asigura un schimb eficient de informații. Natura măsurilor sporite de precauție privind clientela, care se vor aplica țărilor terțe cu grad ridicat de risc, va fi specificată în continuare pentru stabilirea unei abordări mai armonizate în această privință. Domeniul de aplicare și accesul la informațiile din registrele beneficiarilor reali vor fi extinse. În plus, există o serie de dispoziții care aliniază cea de-a patra DCSB la obligațiile de precauție privind clientela în temeiul Directivei 2014/107/UE privind cooperarea administrativă pentru informații privind conturile financiare.

- **Revizuirea regulamentului privind controlul numerarului**²⁸: această propunere urmărește să permită autorităților să acționeze cu privire la sumele mai mici decât pragul de declarare actual de 10 000 EUR, în cazul în care există suspiciuni de activitate infracțională, pentru îmbunătățirea schimbului de informații dintre autorități și să solicite divulgarea numerarului expediat prin transporturi neînsoțite, cum ar fi coletele poștale sau transporturile de marfă. Definiția „numerarului” ar fi extinsă pentru a include, de asemenea, mărfurile prețioase care acționează ca rezerve de valoare foarte lichide precum aurul, împreună cu cardurile de plată preplătite.
- Comisia intenționează să adopte în vara anului 2017 o propunere care urmărește combaterea finanțării terorismului prin **traficul ilicit de bunuri culturale** – indiferent de țara de proveniență – pentru eliminarea deficiențelor actuale din sectorul artei²⁹. În mod asemănător, **traficul ilegal cu specii sălbatice** este recunoscut din ce în ce mai mult ca o nouă sursă de finanțare a activităților teroriste și conexe³⁰. Comisia va continua să pună în aplicare planul de acțiune al UE pentru combaterea fluxurilor financiare ilicite legate de traficul cu specii sălbatice³¹.
- **Directiva privind combaterea terorismului**³² include definiția la nivelul UE a infracțiunii de finanțare a terorismului și stabilește norme minime referitoare la sancțiunile acestei infracțiuni. Propunerile de **directivă privind combaterea prin măsuri de drept penal a spălării banilor**³³ și de **regulament privind recunoașterea reciprocă a ordinelor de înghețare și de confiscare**³⁴ vor completa, de asemenea, abordarea preventivă a UE prin asigurarea unei aplicări corespunzătoare a legii și a răspunsului judiciar atunci când se detectează cazuri de spălare a banilor și de finanțare a terorismului.

3.2.2. Inițiative de politică

- Comisia analizează în prezent lansarea unei inițiative pentru **o mai mare transparență a plăților în numerar**. Aceasta va efectua o evaluare a impactului, având în vedere rezultatele unui studiu și ale unei consultări publice deschise. Comisia va analiza posibile opțiuni, inclusiv posibilitatea introducerii unei restricții privind plățile în numerar. Acest demers ar putea contribui la stoparea finanțării terorismului, întrucât necesitatea utilizării mijloacelor de plată care nu sunt anonime ar acționa ca o măsură de descurajare împotriva activității sau ar facilita detectarea și investigarea sa. Acesta ar putea încuraja, de asemenea, lupta împotriva spălării banilor, a fraudei fiscale și a crimei organizate. În plus, decizia Băncii Centrale Europene de a întrerupe producerea și emisiunea de bancnote de 500 EUR va reduce și mai mult riscul prezentat de plățile în numerar.
- Pe baza **raportului sinoptic** de mai sus al platformei unităților de informații financiare (FIU) la nivelul UE cu privire la **competențele FIU și la obstacolele în calea cooperării**, care a fost elaborat în decembrie 2016 și pe baza analizei suplimentare, Comisia a subliniat direcțiile posibile pentru îmbunătățirea cooperării

²⁸ COM(2016) 825 final.

²⁹ http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_taxud_004_cultural_goods_synthesis_en.pdf

³⁰ SWD(2016) 38 final.

³¹ COM(2016) 87 final.

³² COM(2015) 625 final.

³³ COM(2016) 826 final.

³⁴ COM(2016) 819 final.

dintre unitățile de informații financiare (FIU) la nivelul UE într-un document de lucru separat al serviciilor Comisiei care menționează:

- probleme care pot fi soluționate prin mai multe orientări și cooperare sporită la nivel operațional, de exemplu, prin activitățile legate de platforma unităților de informații financiare (FIU) la nivelul UE (de exemplu cu privire la standardizarea raportării RTS);
- probleme care urmează să fie soluționate imediat ce au fost transpuse cea de-a patra DCSB și modificările propuse ale acesteia; și
- alte probleme care decurg din perspective juridice divergente în statele membre, care ar trebui să fie abordate prin măsuri cu caracter de reglementare³⁵.

Funcționarea unităților de informații financiare (FIU) ar putea fi îmbunătățită în mod substanțial, pe baza normelor specifice la nivelul UE pentru abordarea aspectelor precum cooperarea între FIU și autoritățile de aplicare a legii la nivel național și la nivelul UE. În această privință, Comisia va examina în continuare eventualele opțiuni în conformitate cu principiile privind o mai bună reglementare.

- Comisia a creat un **grup operativ intern FinTech** cu scopul evaluării evoluției tehnologiilor, a serviciilor bazate pe tehnologie și a modelelor de afaceri, pentru a stabili dacă normele și politicile existente sunt adecvate scopului și pentru a identifica opțiunile și propunerile de valorificare a oportunităților sau de abordare a riscurilor posibile. Activitățile în acest domeniu vor cuprinde, în special, finanțarea participativă, monedele digitale (inclusiv tranzacțiile între criptomonede și utilizarea monedelor virtuale pentru achiziția de bunuri de mare valoare), tehnologia registrelor distribuitorilor și autentificarea/identificarea. De asemenea, va fi analizată utilizarea identificării electronice și a integrării digitale. Comisia va realiza un studiu care să identifice și să analizeze practicile bancare de integrare din UE și vor fi evaluate toate măsurile următoare.

3.2.3. Măsuri de sprijin suplimentare pentru atenuarea riscului la nivelul UE

- **Îmbunătățirea colectării datelor statistice:** deținerea unor date cantitative relevante, fiabile și comparabile la nivelul UE va contribui la o mai bună înțelegere a riscurilor. Prin urmare, Comisia va urmări să îmbunătățească colectarea datelor statistice cu privire la combaterea spălării banilor și combaterea finanțării terorismului prin colectarea, consolidarea și analiza statisticilor oferite de statele membre prin obligațiile pe care le au în temeiul articolului 44 din cea de-a patra DCSB și prin colaborarea cu Eurostat pentru a crește comparabilitatea datelor.
- **Orientări suplimentare furnizate entităților obligate cu privire la conceptul de „tranzacții ocazionale și operațiuni care par să fie asociate”:** în prezent, în temeiul celei de-a treia DCSB, entităților obligate li se impune să aplice măsuri sporite de precauție privind clientela la stabilirea unei relații de afaceri sau la efectuarea unei tranzacții ocazionale în valoare de 15 000 EUR sau mai mult. Această noțiune de „tranzacții ocazionale” asigură o implementare eficace a normelor dificile, mai ales în serviciile de remitere de bani și de schimb valutar – însă și în sectorul jocurilor de noroc. Orientările suplimentare din partea Comisiei (în colaborare cu autoritățile naționale competente) ar contribui la atenuarea acestui risc.
- **Formarea profesioniștilor care desfășoară activități protejate de privilegiul juridic profesional:** aceștia ar trebui să aplice normele privind

³⁵ SWD (2017) 275

combaterea spălării banilor și a finanțării terorismului în mod mai eficace, respectând în același timp pe deplin dreptul la un proces echitabil și legitimitatea „privilegiului juridic profesional”. Activitățile de formare ar trebui să ofere orientări operaționale și informații practice pentru a-i ajuta pe acești profesioniști să recunoască operațiunile care ar putea fi legate de spălarea banilor sau finanțarea terorismului și pentru a le arăta cum să procedeze în astfel de cazuri. De asemenea, Comisia va evalua diversele opțiuni disponibile pentru îmbunătățirea gradului de conformitate în acest sector conform jurisprudenței Curții Europene de Justiție³⁶.

- **Analiza suplimentară a riscurilor prezentate de serviciile hawala și serviciile neoficiale de transfer de valori:** amploarea problemei și posibilele soluții de aplicare a legii ar trebui să fie analizate mai în detaliu. Implicarea autorităților de aplicare a legii, în special a Europol și a Eurojust, împreună cu autoritățile de supraveghere, este necesară pentru a permite măsuri disuasive împotriva actorilor necooperanți și a-i asista pe operatorii care doresc să efectueze servicii legitime într-un mediu care respectă legea.
- **Acțiuni suplimentare pentru intensificarea supravegherii la nivelul UE:** entitățile obligate trebuie să aplice normele actuale în mod eficient. Prin urmare, Comisia pune un accent mai mare pe activitatea realizată de către autoritățile de supraveghere a combaterii spălării banilor și a finanțării terorismului. Există anumite probleme care trebuie abordate: numărul mare de entități obligate din UE și diversitatea acestora; volumul de tranzacții și de clienți; perspectivele fragmentate ale autorităților de supraveghere a combaterii spălării banilor și a finanțării terorismului; și limitările privind conștientizarea riscurilor autorităților de supraveghere. Se vor face recomandări suplimentare către autoritățile europene de supraveghere (AES) și autoritățile naționale competente însărcinate cu supravegherea pentru a se asigura că autoritățile de supraveghere a combaterii spălării banilor și a finanțării terorismului înțeleg mai bine rolul pe care îl au în identificarea riscurilor și în deciziile referitoare la resursele care se vor aloca pentru supraveghere și acțiunile de supraveghere pe care ar trebui să le desfășoare asupra entităților obligate aflate în responsabilitatea lor.

4. RECOMANDĂRI

4.1. Recomandări pentru autoritățile europene de supraveghere (AES)

În sectorul financiar, autoritățile europene de supraveghere (AES) au rol central în creșterea capacității UE de a răspunde provocărilor din acest sector. Comisia recomandă ca autoritățile europene de supraveghere (AES):

- să mărească gradul de conștientizare cu privire la riscurile asociate spălării banilor și finanțării terorismului și să identifice măsurile corespunzătoare pentru consolidarea capacității autorităților de supraveghere cu privire la supravegherea combaterii spălării banilor și a finanțării terorismului³⁷. În acest context, acestea

³⁶ Cauza C-305/05.

³⁷ Orientările supravegherii bazate pe riscuri au fost publicate în noiembrie 2016 (https://esas-joint-committee.europa.eu/Publications/Guidelines/Final_RBSGL_for_publication_20161115.pdf).

ar trebui să realizeze evaluări inter pares cu privire la supravegherea practică, bazată pe riscuri și să identifice măsuri adecvate pentru a asigura supravegherea mai eficace a combaterii spălării banilor și a combaterii finanțării terorismului;

- să ia alte inițiative pentru îmbunătățirea colaborării dintre autoritățile de supraveghere. În această privință, autoritățile europene de supraveghere (AES) au decis recent să lanseze un flux de lucru special pentru ca acel cadru de cooperare dintre autoritățile de supraveghere financiare să funcționeze mai bine;
- să elaboreze alte soluții pentru operatorii de supraveghere care acționează conform procedurii „de pașaport”. Grupul operativ comun al Autorității Bancare Europene (ABE) privind serviciile de plată/combateră a spălării banilor a început deja să lucreze la acest aspect. Acesta urmărește să clarifice când agenții și distribuitorii sunt „sedii” reale și analizează diverse scenarii care vor contribui la abordarea riscurilor;
- să ofere orientări actualizate cu privire la guvernanța internă astfel încât să se clarifice în continuare așteptările referitoare la funcțiile responsabililor pentru conformitate din cadrul instituțiilor financiare;
- să ofere alte orientări referitoare la identificarea beneficiarilor reali pentru furnizorii fondurilor de investiții, mai ales în situațiile care prezintă un risc mai ridicat de spălare a banilor sau de finanțare a terorismului; și
- să analizeze riscurile operaționale privind combaterea spălării banilor și combaterea finanțării terorismului legate de modelul de afaceri între întreprinderi din sectoarele serviciilor financiar-bancare pe segmentul de corporate, ale serviciilor bancare personalizate și ale investițiilor instituționale pe de o parte și din cadrul serviciilor de transmitere a banilor sau valorilor și de monedă electronică, pe de altă parte. Această analiză ar trebui efectuată în contextul avizului comun viitor privind riscurile care afectează sectorul financiar în temeiul articolului 6 alineatul (5) din cea de-a patra DCSB.

4.2. Recomandări pentru autoritățile de supraveghere nefinanciare

Sectorul nefinanciar nu deține niciun organism sau agenție UE de tipul autorității europene de supraveghere (AES) care să funcționeze la nivelul UE. Conform cadrului UE de combatere a spălării banilor, statele membre pot permite organismelor de autoreglementare să îndeplinească funcții de supraveghere pentru consilieri fiscali, auditori, experți contabili externi, notari și alte persoane care exercită profesii juridice liberale și agenți imobiliari. În marea majoritate a statelor membre, supravegherea în aceste sectoare prezintă lipsuri din punct de vedere al controalelor, orientării și nivelului de raportare de către profesioniștii din domeniul juridic, în special către unitățile de informații financiare (FIU). Prin urmare, organismele de autoreglementare ar trebui să depună eforturi pentru creșterea numărului de inspecții și raportări tematice. De asemenea, ar trebui să organizeze activități de formare pentru o mai bună înțelegere a riscurilor și a obligațiilor de conformare cu privire la combaterea spălării banilor și combaterea finanțării terorismului.

4.3. Recomandări pentru statele membre³⁸

Pe baza nivelului riscurilor identificate în diversele sectoare cuprinse în evaluarea supranațională a riscurilor (SNRA), Comisia recomandă ca statele membre să ia măsurile de atenuare de mai jos. Acestea ar trebui considerate ca o referință care ar putea fi adaptată în funcție de măsurile naționale deja în vigoare:

➤ Domeniul de aplicare al evaluărilor riscurilor la nivel național

Statele membre ar trebui să acorde atenția cuvenită riscurilor prezentate de diverse produse în cadrul evaluărilor riscurilor la nivel național și să definească măsurile corespunzătoare de atenuare, în special cu privire la:

- întreprinderile cu flux crescut de lichidități și plățile în numerar: Statele membre ar trebui să definească măsurile corespunzătoare de atenuare, cum ar fi introducerea limitelor pentru plățile în numerar, a sistemelor de raportare a tranzacțiilor în numerar sau oricare alte măsuri adecvate pentru abordarea riscului;
- artefactele culturale și antichități: Statele membre ar trebui să analizeze riscul care decurge din acest sector, să promoveze campanii de creștere a gradului de conștientizare printre comercianții de obiecte de artă și să îi încurajeze să aplice măsuri de combatere a spălării banilor și de combatere a finanțării terorismului;
- sectorul organizațiilor non-profit: Statele membre ar trebui să asigure includerea corespunzătoare a organizațiilor non-profit în evaluările riscurilor la nivel național; și
- produsele de monedă electronică: Statele membre ar trebui să ia în considerare riscurile prezentate de produsele de monedă electronică anonimă și ar trebui să se asigure că pragurile de exceptare sunt cât mai mici posibil, pentru a evita utilizarea lor necorespunzătoare.

➤ Beneficiarul real

Statele membre ar trebui să se asigure că informațiile referitoare la beneficiarii reali ai entităților juridice și construcțiilor juridice sunt adecvate, corecte și actuale.

(1) Statele membre ar trebui să dezvolte instrumente potrivite pentru a se asigura că identificarea beneficiarului real este realizată în mod corespunzător atunci când se aplică măsurile de precauție privind clientela. În cazul entităților juridice, dacă entitățile obligate au identificat doar directorul principal ca fiind beneficiarul real, acest lucru ar trebui să fie subliniat de entitatea obligată (de exemplu prin înregistrarea specială a acestor informații). Este de dorit să se păstreze evidențe în cazul în care există îndoieli că persoana identificată este beneficiarul real. Ar trebui să se acorde o atenție specială structurilor complexe în cazul în care fondatorul, fiduciarul, protectorul, beneficiarii sau oricare altă persoană fizică ce exercită controlul în ultimă instanță asupra fiduciei, implică una sau mai multe entități juridice.

(2) De asemenea, normele prevăzute în cea de-a patra DCSB privind transparența informațiilor privind beneficiarii reali ar trebui să fie implementate rapid, pe baza introducerii registrelor beneficiarilor reali pentru toate tipurile de entități juridice și construcții juridice. Informațiile din registre ar trebui să fie verificate periodic, de exemplu, de către o autoritate desemnată, astfel încât să se evite discrepanțele cu

³⁸ Pentru mai multe detalii referitoare la recomandările specifice adresate statelor membre prin produse/servicii, a se vedea Anexa 1 la documentul de lucru al serviciilor Comisiei (2017)241

informațiile colectate de către entitățile obligate ca parte a procedurilor lor de precauție sporită privind clientela.

(3) Statele membre ar trebui să se asigure că sectoarele care sunt cel mai expuse la riscuri generate de mecanisme opace privind beneficiarii reali sunt monitorizate și supravegheate în mod eficient. Acesta este mai ales cazul intermediarilor cum sunt consilierii fiscali, auditorii, experții contabili externi, notarii și alte persoane care exercită profesii juridice liberale și al furnizorilor de servicii de consiliere pentru întreprinderi privind fuziunile/achizițiile³⁹. În ultimul caz, deși aceste servicii sunt cuprinse în cadrul UE privind combaterea spălării banilor și a finanțării terorismului, evaluarea supranațională a riscurilor (SNRA) subliniază aplicarea inefficientă a normelor cu privire la această categorie specială de întreprinderi.

➤ **Resurse corespunzătoare pentru autoritățile de supraveghere și unitățile de informații financiare (FIU)**

În temeiul celei de-a patra DCSB, statele membre trebuie să aloce resurse „adecvate” autorităților lor competente⁴⁰. Cu toate acestea, pe baza datelor colectate în această etapă, nu este posibil să se identifice nicio corespondență sistemică între resursele alocate și dimensiunea sectorului, numărul entităților obligate și nivelul de raportare. Statele membre ar trebui să demonstreze că se alocă resurse suficiente autorităților de supraveghere și unităților de informații financiare (FIU), astfel încât acestea să își poată îndeplini sarcinile.

➤ **Intensificarea inspecțiilor la fața locului efectuate de autoritățile de supraveghere**

În sectorul financiar, autoritățile de supraveghere trebuie să pună în aplicare un model de supraveghere bazat pe riscuri conform orientărilor comune ale autorităților europene de supraveghere (AES) referitoare la supravegherea bazată pe riscuri, publicate în noiembrie 2016⁴¹. Aceste orientări prevăd că autoritățile de supraveghere ar trebui să verifice – atât periodic, cât și ad-hoc – dacă modelul de supraveghere bazată pe riscuri al acestora cu privire la combaterea spălării banilor și combaterea finanțării terorismului produce rezultatul așteptat și, în special, dacă nivelul resurselor de supraveghere rămâne proporțional cu riscurile identificate în legătură cu spălarea banilor și finanțarea terorismului. În acest sens, este important ca autoritățile de supraveghere să desfășoare inspecții suficiente la fața locului și care să fie proporționale cu riscurile identificate în legătură cu spălarea banilor și finanțarea terorismului.

Statele membre ar trebui să se asigure că domeniul de aplicare al acestor inspecții la fața locului se axează pe riscurile operaționale specifice privind combaterea spălării banilor și combaterea finanțării terorismului, în funcție de vulnerabilitățile specifice și inerente unui produs sau serviciu. Aceasta vizează în special investițiile instituționale (în special, prin intermediul brokerilor); serviciile bancare personalizate în cazul în care autoritățile

³⁹ O întreprindere diferită de instituția de credit, care efectuează activitățile descrise la punctul (9) din Anexa I la Directiva 2013/36/UE.

⁴⁰ Articolul 32 alineatul (3) (privind unitățile de informații financiare - FIU) și articolul 48 alineatul (2) (privind autoritățile de supraveghere) din cea de-a patra DCSB.

⁴¹ A se vedea https://esas-joint-committee.europa.eu/Publications/Guidelines/Joint%20Guidelines%20on%20risk-based%20supervision_RO%20%28ESAs%202016%2072%29.pdf

de supraveghere ar trebui să evalueze punerea în aplicare a normelor privind identificarea beneficiarului real; și casele de schimb valutar și serviciile de transmitere a banilor sau valorilor („MVTs”) în cazul în care inspecțiile de supraveghere ar trebui să includă o revizuire a formării primite de agenți.

În sectorul nefinanciar, statele membre ar trebui să se asigure că autoritățile competente ale acestora desfășoară suficiente controale neanunțate la fața locului cu privire la comercianții de bunuri de valoare mare, în special pentru sectorul aurului și diamantelor, în scopul identificării eventualelor lacune în ceea ce privește respectarea cerințelor de precauție sporită privind clientela. În mod asemănător, numărul inspecțiilor la fața locului din sectorul profesioniștilor care realizează activități protejate de principiile privilegiului juridic profesional ar trebui să fie proporțional cu riscurile.

➤ **Autoritățile de supraveghere trebuie să efectueze inspecții tematice**

Autoritățile de supraveghere ar trebui să dezvolte o mai bună înțelegere a riscurilor asociate combaterii spălării banilor și combaterii finanțării terorismului la care este expus un anumit segment al afacerii. Această recomandare ar trebui să se aplice investițiilor instituționale (în special prin intermediul brokerilor) și serviciilor bancare personalizate; furnizorilor de servicii pentru fiducii și societăți (TCSP); consilierilor fiscali, auditorilor, experților contabili externi, notarilor și altor persoane care exercită profesii juridice liberale; furnizorilor de servicii de consiliere adresată întreprinderilor cu privire la structura capitalului, strategia industrială și întrebările și consilierea aferente, precum și serviciilor referitoare la fuziuni și achiziția de întreprinderi. Pentru aceste sectoare, autoritățile de supraveghere ar trebui să evalueze în mod specific implementarea normelor privind identificarea beneficiarului real. Acestea ar trebui să se aplice și pentru serviciile de transfer de valori și de bani (MVTs). În astfel de cazuri, statele membre ar trebui să se asigure că autoritățile de supraveghere realizează inspecții tematice în termen de 2 ani de la publicarea raportului evaluării supranaționale a riscurilor, cu excepția situațiilor în care astfel de inspecții au fost realizate recent.

➤ **Considerații privind extinderea listei entităților obligate**

În prezent, unele servicii/produse nu sunt incluse în cadrul UE privind combaterea spălării banilor și a finanțării terorismului. În temeiul articolului 4 din cea de-a patra DCSB, statele membre ar trebui să extindă domeniul de aplicare al regimului privind combaterea spălării banilor și a finanțării terorismului pentru profesioniștii expuși riscului în mod special. La aplicarea acestei dispoziții, statele membre ar trebui să aibă în vedere să supună cel puțin platformele de finanțare participativă, de schimb de monede virtuale și furnizorii de portofele digitale⁴², casele de licitații, comercianții de obiecte de artă și de antichități și comercianții speciali de bunuri cu valoare ridicată regimului lor privind combaterea spălării banilor și a finanțării terorismului, în cazul în care aceștia sunt identificați ca prezentând riscuri în baza evaluării supranaționale a riscurilor (SNRA).

➤ **Un nivel adecvat de precauție privind clientela pentru tranzacțiile ocazionale**

Pe baza cadrului juridic actual al UE, unele servicii/produse pot fi scutite de precauția privind clientela pentru tranzacțiile ocazionale care se află sub un anumit prag (15 000

⁴² În funcție de rezultatul negocierilor referitoare la revizuirea celei de-a patra DCSB, platformele de schimb de monede virtuale și furnizorii de portofele digitale ar putea să fie supuși cerințelor privind combaterea spălării banilor și combaterea finanțării terorismului la nivelul UE.

EUR). Totuși, există situații în care aceste scutiri bazate pe pragul stabilit pot fi considerate ca fiind nejustificate și în care pragul de 15 000 EUR ridică probleme. În acel context, statele membre ar trebui să impună un prag mai scăzut al precauției privind clientela care să se aplice tranzacțiilor ocazionale pentru a se asigura că acesta este proporțional cu riscul asociat spălării banilor și finanțării terorismului, identificat la nivel național. Statele membre ar trebui să raporteze Comisiei pragul național al acestora pentru tranzacțiile ocazionale. Un prag similar celui pentru tranzacții ocazionale pentru transferurile de fonduri poate fi considerat proporțional cu riscul (de exemplu 1 000 EUR). În plus, statele membre ar trebui să ofere orientări pentru definirea tranzacțiilor ocazionale, punând la dispoziție criterii precum faptul că normele referitoare la precauția privind clientela care se aplică relațiilor de afaceri nu sunt eludate pentru casele de schimb valutar și, în așteptarea noilor cerințe ale celei de-a patra DCSB, pentru remiterile de bani.

➤ **Nivel adecvat de precauție privind clientela în cazul serviciilor de custodie și al serviciilor similare**

Pentru monitorizarea serviciilor de custodie în mod corespunzător, ar trebui să fie puse în aplicare măsuri de protecție adecvate. Această recomandare ar trebui să se aplice următoarelor sectoare:

- servicii de custodie furnizate de către instituții financiare: Statele membre ar trebui să se asigure că aceste servicii sunt oferite doar titularilor de cont bancar din cadrul aceleiași entități obligate și ar trebui să abordeze în mod corespunzător riscurile prezentate de accesul terților la seifuri. Ar trebui emise orientări pentru instituțiile de credit și financiare pentru a clarifica modul în care acestea ar trebui să monitorizeze conținutul seifului în mod eficient în cadrul cerințelor acestora legate de precauția privind clientela/de monitorizare; și

- servicii de depozitare similare oferite de către furnizori de servicii nefinanciare: Statele membre ar trebui să definească măsurile proporționale cu riscurile pe care le implică furnizarea acestor servicii, inclusiv în porturi libere, în funcție de circumstanțele la nivel național.

➤ **Cooperare periodică între autoritățile competente și entitățile obligate**

Această cooperare consolidată ar trebui să vizeze simplificarea detectării tranzacțiilor suspecte și să crească numărul și calitatea raportărilor RTS. Autoritățile de supraveghere ar trebui să ofere indicații clare despre riscurile asociate combaterii spălării banilor și combaterii finanțării terorismului, cerințele legate de precauția privind clientela, raportările RTS și modul de identificare a celor mai relevanți indicatori pentru detectarea riscurilor asociate combaterii spălării banilor și combaterii finanțării terorismului. Statele membre ar trebui să se asigure că unitățile de informații financiare (FIU) transmit feedback adecvat entităților obligate. Această recomandare ar trebui să se aplice în special următoarelor sectoare:

- sectorul jocurilor de noroc: Autoritățile de supraveghere ar trebui să ofere orientări mai clare pentru aparatele de jocuri în ceea ce privește riscul emergent legat de loteria video. În ceea ce privește jocurile de noroc online, autoritățile competente responsabile ar trebui să pună în aplicare, de asemenea, programe pentru creșterea gradului de conștientizare în rândul operatorilor de jocuri de noroc online cu privire la apariția factorilor de risc care ar putea avea impact asupra vulnerabilității sectorului. Acestea includ utilizarea de monedă electronică anonimă sau de monedă virtuală și apariția operatorilor neautorizați de jocuri de noroc online; feedback suplimentar de la unitățile de informații financiare (FIU) privind calitatea raportărilor RTS, modalitățile de îmbunătățire a raportărilor și despre

utilizarea informațiilor furnizate și luarea în considerare a caracteristicilor sectorului de jocuri de noroc la elaborarea standardizării modelului (modelelor) de raportare RTS/SAR de la nivelul UE.

- consilieri fiscali, auditori, experți contabili externi, notari și alte persoane care exercită profesii juridice liberale: Statele membre ar trebui să ofere orientări referitoare la factorii de risc care decurg din tranzacțiile ce implică consilieri fiscali, auditori, experți contabili externi, notari și alte persoane care exercită profesii juridice liberale. De asemenea, acestea ar trebui să ofere orientări cu privire la aplicarea privilegiului juridic profesional și la modalitatea de a distinge serviciile juridice supuse adevăratei esențe a privilegiului juridic profesional de alte servicii care nu sunt supuse privilegiului juridic profesional atunci când sunt furnizate unui singur client; și

- serviciile de transmitere a banilor sau valorilor (MVTs): autoritățile competente ar trebui să ofere sectorului serviciilor de transmitere a banilor sau valorilor (MVTs) un grad mai mare de conștientizare a riscului și indicatori de risc privind finanțarea terorismului.

➤ **Formare specială și permanentă pentru entitățile obligate**

Sesiunile de formare asigurate de autoritățile competente ar trebui să acopere riscul de infiltrare sau de proprietate a grupurilor infracționale organizate. Această recomandare ar trebui să se aplice următoarelor sectoare:

- sectorul jocurilor de noroc: în ceea ce privește activitatea de pariuri, în afară de responsabilii cu personalul și coordonatorii funcției de conformitate, statele membre ar trebui să conceapă sesiuni obligatorii de formare pentru comercianții cu amănuntul din sectorul de pariuri, axate pe evaluarea corespunzătoare a produselor/modelului lor de afaceri, bazată pe riscuri

- Furnizorii de servicii pentru fiducii și societăți (TCSP), consilierii fiscali, auditorii, experții contabili externi, notarii și alte persoane care exercită profesii juridice liberale, furnizorii de servicii de consiliere adresate întreprinderilor cu privire la structura capitalului, strategia industrială și întrebările și consilierea aferente, precum și serviciile referitoare la fuziuni și achiziția de întreprinderi: sesiunile de formare și orientările privind factorii de risc ar trebui să se axeze pe relațiile de afaceri la distanță, intermediari profesioniști offshore, clienți sau jurisdicții; și structuri complexe/paravan

- sectorul imobiliar: programele speciale de formare ar trebui să includă semnale de avertisment în situațiile în care mai mulți profesioniști sunt implicați în tranzacția imobiliară (agentul imobiliar, persoana care exercită o profesie juridică, instituția financiară); și

- SERVICIILE DE TRANSMITERE A BANILOR SAU VALORILOR (MVTs): entitățile obligate ar trebui să pună la dispoziție agenților programe obligatorii de formare cu scopul conștientizării de către aceștia a obligațiilor privind combaterea spălării banilor și a finanțării terorismului și pentru a le arăta cum să detecteze tranzacțiile suspecte.

➤ **Raportare anuală de către autoritățile competente/organismele de autoreglementare cu privire la activitățile de combatere a spălării banilor și a finanțării terorismului ale entităților obligate aflate sub responsabilitatea acestora.**

Această obligație de raportare va sprijini autoritățile naționale să desfășoare evaluările riscurilor la nivel național și va permite acțiuni mai proactive pentru a remedia deficiențele sau neconformitățile cu cerințele privind combaterea spălării banilor și combaterea finanțării terorismului în următoarele sectoare:

- sectorul imobiliar: raportul ar trebui să includă numărul de rapoarte primite de către organismul de autoreglementare și numărul de rapoarte transmise la unitățile de informații financiare (FIU) atunci când profesioniștii respectivi raportează prin intermediul unui organism de autoreglementare; și
- consilieri fiscali, auditori, experți contabili externi, notari și alte persoane care exercită profesii juridice liberale: raportul ar trebui să includă numărul de inspecții la fața locului efectuate de organismele de autoreglementare pentru monitorizarea respectării normelor de combatere a spălării banilor și a finanțării terorismului, numărul de rapoarte primite de către organismul de autoreglementare și numărul de rapoarte transmise la unitățile de informații financiare (FIU) atunci când profesioniștii respectivi raportează prin intermediul unui organism de autoreglementare.

5. CONCLUZII

Evaluarea supranațională a riscurilor (SNRA) arată că piața internă a UE este încă vulnerabilă față de riscurile asociate spălării banilor și finanțării terorismului. Teroriștii folosesc o gamă largă de metode pentru a strânge și a transfera fonduri, iar infractorii folosesc scheme mai complexe și profită de noile oportunități pentru spălarea banilor oferite de apariția de noi servicii și produse. Prevenirea utilizării ilegale a sistemului financiar este crucială pentru limitarea capacității de operare a teroriștilor și a infractorilor și privarea criminalității organizate de avantajele economice care constituie scopul final al activităților lor ilegale.

Evaluarea aprofundată realizată în ultimii doi ani a subliniat necesitatea perfecționării anumitor elemente ale cadrului legislativ și a consolidării capacităților actorilor publici și privați pentru punerea în aplicare a obligațiilor de conformitate ale acestora.

Unele măsuri sunt deja aplicate, iar Comisia va pune în aplicare măsuri noi evidențiate în prezentul raport pentru atenuarea riscurilor în mod corespunzător. Comisia invită statele membre să pună în aplicare rapid recomandările emise în prezentul raport. În temeiul articolului 6 din cea de-a patra DCSB, statele membre care decid să nu aplice niciuna dintre recomandări în regimurile naționale ale acestora cu privire la combaterea spălării banilor și a finanțării terorismului, ar trebui să notifice Comisia cu privire la decizia lor și să prezinte o justificare în acest sens („conformare sau justificare”). În absența acestor notificări, se așteaptă ca statele membre să pună în aplicare aceste recomandări.

Pentru a fi eficiente, politicile privind combaterea spălării banilor și a finanțării terorismului ar trebui să se adapteze la dezvoltarea serviciilor financiare, evoluțiile amenințărilor și apariția noilor riscuri. Din acest motiv, Comisia va monitoriza măsurile luate de statele membre pe baza constatărilor din evaluarea supranațională a riscurilor (SNRA) și va raporta aceste constatări cel târziu până în iunie 2019. Această examinare va evalua, de asemenea, modul în care măsurile puse în aplicare la nivelul UE și la nivel național au impact asupra nivelului riscurilor. Confrunțați cu o provocare în evoluție care profită de orice lacună nouă, toți actorii trebuie să rămână vigilenți și să își intensifice eforturile și cooperarea: acțiunea concertată este necesară mai mult ca oricând pentru combaterea spălării banilor și a finanțării terorismului și astfel, pentru consolidarea stabilității pieței interne și pentru îmbunătățirea securității cetățenilor UE și a societății, în ansamblul său.