ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVII, SUPLIMENT 2, ŞTIINŢE JURIDICE, 2021

**DOI: 10.47743/jss-2021-67-4-5**

# Cunoaşterea clientelei pe piaţa criptoactivelor – între teorie şi practică

# Know Your Customer on the Crypto Assets Market – Between Theory and Practice

**Alina V. Popescu**[1]

**Rezumat:** Cunoaşterea clientelei[2] reprezintă o modalitate de a evita producerea unor fraude ori implicarea în activităţi infracţionale, cum ar fi cele de spălare a banilor sau de finanţare a terorismului. Măsurile privind KYC sunt importante atât pentru mediul de afaceri, cât şi pentru clienţi şi, deşi cele mai cunoscute publicului sunt măsurile KYC pe care le aplică mediul bancar, legislaţia a extins obligativitatea aplicării acestor măsuri şi asupra altor instituţii financiare, nefinanciare şi furnizori de servicii.
Un element de noutate privind KYC îl reprezintă obligarea furnizorilor de servicii de schimb între criptoactive şi moneda fiduciară să aplice măsurile de cunoaştere a clientelei, pe fondul specificului pe care aceste active îl prezintă şi ţinând cont de faptul că aceşti furnizori îşi desfăşoară activitatea pe o piaţă nereglementată.

**Cuvinte-cheie:** spălarea banilor; cunoaşterea clientelei; criptoactive; pieţe nereglementate

**Abstract:** Knowing Your Customers is a way to avoid fraud or involvement in criminal activities, such as money laundering or terrorist financing. KYC measures are important for both business and customers, and although the best known to the public KYC measures are those applied by the banking environment, the legislation has extended the obligation to apply these measures to other financial, non-financial institutions and service providers. A novelty regarding KYC is the obligation of exchange service providers between crypto assets and fiat currency to apply measures to know the customers, on the background of the specificity of these assets and taking into account the fact that these providers operate in an unregulated market.

**Keywords:** money laundering; know your customer; crypto assets; unregulated market

[1] Lector univ. dr., Universitatea „Constantin Brâncoveanu” Piteşti, Facultatea de Ştiinţe Juridice, Administrative şi ale Comunicării, e-mail: avpalina_16@yahoo.com.

[2] Pe parcursul studiului vom utiliza prescurtarea KYC de la denumirea în limba engleză *„Know Your Customer”.*

## *1. Consideraţii generale*

Deşi oferirea de servicii în domeniul criptoactivelor[3] este privită cu suspiciune de o parte a pieţei, nu se poate nega existenţa pieţei criptoactivelor şi, prin urmare, din punct de vedere juridic, problematica trebuie abordată bidimensional: pe de o parte, asigurarea unei pieţe cu risc cât mai mic pentru clienţi, pe de altă parte, prevenirea săvârşirii de infracţiuni pe o piaţă nereglementată, corelat cu conformarea furnizorilor de servicii din domeniu la prevederile legale.

Criptoactivele sunt utilizate ca depozit de valoare, precum şi ca metodă de plată pentru bunuri şi servicii legitime. Cu toate acestea, criptoactivele pot constitui mijloace de facilitare a criminalităţii, în principal pentru hackeri, elementele de crimă organizată şi teroriști.

După atacurile teroriste din anul 2001, Statele Unite ale Americii au adoptat o legislaţie referitoare la tranzacţiile financiare, prin care impuneau obligaţia de cunoaştere a clientelei ca modalitate de descurajare a finanţării terorismului.

Şi Uniunea Europeană a aliniat legislaţia din domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului, astfel încât activitatea KYC să fie cât mai bine reglementată, iar statele membre să aibă o abordare unitară, care să nu împiedice totuşi libera circulaţie a serviciilor financiare sau nefinanciare.

Raportul EU SOCTA 2021 evidenţiază faptul că: „Îmbunătăţirea legislaţiei UE în domeniul combaterii spălării banilor, având drept rezultat creşterea supravegherii financiare în sectorul bancar, a făcut să fie mai dificil, pentru reţelele criminale, să introducă venituri ilicite în economia legală prin canalele bancare tradiţionale. În consecinţă, este probabil ca încercările de spălare a banilor să fie deplasate către sectoare cu controale incipiente sau supraveghere limitată. Aceasta ar putea include utilizarea agenţiilor de remitere de bani, neautorizate, a platformelor bancare alternative[4], a comerţului internaţional şi a monedelor virtuale anonime. Utilizarea criptomonedelor este un domeniu de îngrijorare crescândă, din cauza absenţei unui regim comun de reglementare şi a nivelului de anonimat pe care îl oferă aceste produse”[5].

Totodată, raportul atenţionează că aceste criptoactive sunt din ce în ce mai utilizate pentru a efectua plăţi către oficiali corupţi, precum şi în scopuri de spălare a banilor. Acestea sunt considerate atractive pentru reţelele de infracţionalitate datorită faptului că nu sunt reglementate şi asigură o doză de anonimitate.

---

[3] Noțiunea de „criptoactive” este sinonimă, în practică, cu „criptomonede”, „active virtuale” sau „monede virtuale”. La data de 25.09.2020, a fost finalizată propunerea de Regulament al Parlamentului European și al Consiliului privind piețele criptoactivelor și de modificare a Directivei (UE) 2019/1937, [Online] la https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2020)593&lang=ro,accesat 30.11.2021.

[4] Situate în afara sistemului bancar tradițional, reglementat.

[5] Europol (2021), European Union serious and organised crime threat assessment, *A Corrupting Influence: The Infiltration and Undermining of Europe's Economy and Society by Organised Crime (t.a.)*, Publications Office of the European Union, Luxembourg, [Online] la https://www.europol.europa.eu/ publication-events/main-reports/ european-union-serious-and-organised-crime-threat-assessment-socta-2021, accesat 30.11.2021.

Este important pentru instituţiile financiare, nefinanciare şi pentru furnizorii de servicii[6] să îşi cunoască clientela pentru a se putea conforma cerinţelor legale de raportare a tranzacţiilor suspecte. De aici decurge şi obligaţia de *„customer due dilligence – CDD"* a entităţilor raportoare de a solicita clienţilor mai multe informaţii, care pot include sursa fondurilor, scopul relaţiei de afaceri, ocupaţia, situaţii financiare, referinţe bancare etc., astfel încât să se atingă obiectivul KYC. Entităţile raportoare au obligaţia de a sesiza orice fel de tranzacţii suspecte şi trebuie să abordeze KYC prin prisma riscurilor pe care relaţia de afaceri le implică.

Cunoaşterea clientelei în domeniul bancar este deja o practică bine cunoscută, fapt pentru care persoanele implicate în infracţiuni de spălare a banilor şi finanţare a terorismului s-au reorientat spre alte sectoare economice, unde anonimatul este mai uşor de păstrat. O astfel de piaţă este considerată şi piaţa criptoactivelor, care se consideră că este independentă de influenţa băncilor centrale şi poate oferi variante mai facile pentru disimularea sursei fondurilor.

La fel ca în domeniul bancar, furnizorii de servicii de schimb între criptoactive şi monedă fiduciară trebuie nu doar să verifice identitatea clienţilor, ci să monitorizeze tranzacţiile derulate în platformele prin intermediul cărora furnizează serviciile, să elimine orice posibilitate de derulare a tranzacţiilor sub anonimat.

Totuşi, trebuie avut în vedere faptul că entităţile raportoare trebuie să investească sume de bani mai mari pentru a se conforma la legislaţia din materia CSB/CFT[7], ceea ce se poate traduce în costuri mai mari pentru clienţi (creşterea comisioanelor, a dobânzilor etc.). De asemenea, conformarea la legislaţia CSB/CFT poate deveni supărătoare pentru clienţi, care o consideră o birocraţie suplimentară.

Piaţa criptoactivelor, ca potenţial loc de săvârşire a unor infracţiuni, se află în atenţia autorităţilor, care trebuie să colaboreze cu furnizorii de servicii de pe această piaţă, pentru a putea atinge obiectivul de a oferi clienţilor o piaţă cât mai sigură. La nivelul Europol a fost organizată, în luna iunie 2019, o conferinţă[8] la care au participat peste 300 de experţi, atât din cadrul agenţiilor de aplicare a legii, cât şi din sectorul privat. Conferinţa a avut drept scop analizarea oportunităţilor de cooperare şi parteneriat între autorităţi şi mediul privat, pentru prevenirea şi combaterea criminalităţii legate de piaţa criptoactivelor[9]. Şi cu acest prilej, s-a reiterat importanţa implementării unor politici şi mecanisme KYC eficiente, precum şi a abordării bazate pe risc pentru tranzacţiile suspecte. De asemenea,

[6] Entități raportoare, conform prevederilor Legii nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative, publicată în Monitorul Oficial al României, Partea I, nr. 589 din 18 iulie 2019, cu modificările și completările ulterioare.

[7] Combaterea spălării banilor – CSB, combaterea finanțării terorismului – CFT.

[8] Astfel de întâlniri au fost organizate și în anii 2014-2018.

[9] Europol, Comunicat de presă, *Cryptocurrency experts meet at Europol to strengthen ties between law enforcement and private sector*, [Online] la https://www. europol. europa.eu/newsroom/news/cryptocurrency-experts-meet-europol-to-strengthen-ties-between-law-enforcement-and-private-sector, accesat 30.11.2021.

Europol a atras şi specialişti din mediul academic care să contribuie cu expertiza lor la îmbunătăţirea securităţii platformelor de tranzacţionare.

Utilizarea legitimă a criptoactivelor nu se poate realiza decât prin politici ferme în domeniul KYC, colaborarea între autorităţi şi mediul privat, asigurarea trasabilităţii tranzacţiilor realizate şi păstrarea informaţiilor despre clienţi şi tranzacţii, pentru un termen rezonabil, de regulă, stabilit de legislaţia privind CSB/CFT.

## *2. Prevederi legale privind obligaţia de cunoaştere a clientelei*

La nivel european, Directiva (UE) 2015/849[10], în considerentul 3, invocă necesitatea unor măsuri sporite în ceea ce priveşte identificarea şi verificarea clientelei, în situaţiile cu risc mărit de spălare a banilor sau de finanţare a terorismului, precum şi de controale mai puţin riguroase, justificate de un risc mai redus, în temeiul recomandărilor din anul 2003 al Grupului de Acţiune Financiară Internaţională (FATF/GAFI)[11]. Măsurile de precauţie privind clientela includ: identificarea şi verificarea clientului şi a beneficiarului real, monitorizarea tranzacţiilor sau a relaţiei de afaceri etc.

Directiva defineşte la art. 2 care sunt entităţile obligate[12] să adopte măsurile necesare astfel încât să se prevină utilizarea sistemului financiar al Uniunii în

[10] Directiva (UE) 2015/849 a Parlamentului European şi a Consiliului din 20 mai 2015 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, de modificare a Regulamentului (UE) nr. 648/2012 al Parlamentului European și al Consiliului și de abrogare a Directivei 2005/60/CE a Parlamentului European și a Consiliului și a Directivei 2006/70/CE a Comisiei, publicată în Jurnalul Oficial al Uniunii Europene L 141 din 05.06.2015

[11] The Financial Action Task Force (FATF), *Who we are*, [Online] la https://www.fatf-gafi.org/about/, accesat 30.11.2021.

[12] *„Prezenta directivă se aplică următoarelor entități obligate:*

*1. instituții de credit;*

*2. instituții financiare;*

*3. următoarele persoane fizice sau juridice, în exercitarea activităților lor profesionale:*

*(a) auditori, experți contabili externi și consilieri fiscali;*

*(b) notari și alte persoane care exercită profesii juridice liberale, atunci când participă, în numele și pe seama clientului, la orice tranzacție financiară sau imobiliară, sau când acordă asistență pentru planificarea sau efectuarea tranzacțiilor pentru client referitoare la:*

*(i) cumpărarea și vânzarea de bunuri imobile sau entități comerciale;*

*(ii) gestionarea banilor, a valorilor mobiliare sau a altor active ale clientului;*

*(iii) deschiderea sau gestionarea de conturi bancare, conturi de economii sau conturi de valori mobiliare;*

*(iv) organizarea contribuțiilor necesare pentru crearea, funcționarea sau administrarea societăților;*

*(v) crearea, funcționarea sau administrarea de fiducii, societăți, fundații sau structuri similare;*

*(c) furnizori de servicii pentru fiducii sau societăți care nu fac obiectul literei (a) sau (b);*

*(d) agenți imobiliari;*

scopul spălării banilor şi finanţării terorismului. Capitolul II al Directivei (UE) 2015/849 este dedicat reglementărilor referitoare la „Precauţia privind clientela" şi stabileşte principalele măsuri ce trebuie adoptate de către entităţile obligate pentru cunoaşterea clientelei.

Prevederile Directivei (UE) 2015/849 au fost transpuse în legislaţia naţională prin adoptarea Legii nr. 129/2019[13], care preia categoriile de entităţi obligate stabilite de directivă, dar le denumeşte entităţi raportoare. De asemenea, legea defineşte noţiunea de client/clientelă, care înseamnă *„orice persoană fizică, juridică sau entitate fără personalitate juridică cu care entităţile raportoare desfăşoară relaţii de afaceri ori cu care desfăşoară alte operaţiuni cu caracter permanent sau ocazional. Se consideră client al unei entităţi raportoare orice persoană cu care, în desfăşurarea activităţilor sale, entitatea raportoare a negociat o tranzacţie, chiar dacă respectiva tranzacţie nu s-a finalizat, precum şi orice persoană care beneficiază sau a beneficiat, în trecut, de serviciile unei entităţi raportoare"*[14].

Totodată, legea stabileşte că persoanele expuse public sunt *„persoanele fizice care exercită sau au exercitat funcţii publice importante"*[15] şi determină categoriile de persoane fizice care se încadrează în noţiunea de „beneficiar real"[16].

---

*(e) alte persoane care comercializează bunuri, numai în măsura în care plățile sunt efectuate sau încasate în numerar și au o valoare de cel puțin 10 000 EUR, indiferent dacă tranzacția se efectuează printr-o singură operațiune sau prin mai multe operațiuni care par a avea o legătură între ele;*

*(f) furnizorii de servicii de jocuri de noroc".*

[13] Legea nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative, publicată în Monitorul Oficial al României, Partea I, nr. 589 din 18 iulie 2019.

[14] Art. 2 lit. r) din Legea nr. 129/2019.

[15] În conformitate cu prevederile art. 3 alin. (2) din Legea nr. 129/2019, *„prin funcții publice importante se înțeleg:*

*a) șefi de stat, șefi de guvern, miniștri și miniștri adjuncți sau secretari de stat;*

*b) membri ai Parlamentului sau ai unor organe legislative centrale similare;*

*c) membri ai organelor de conducere ale partidelor politice;*

*d) membri ai curților supreme, ai curților constituționale sau ai altor instanțe judecătorești de nivel înalt ale căror hotărâri nu pot fi atacate decât prin căi extraordinare de atac;*

*e) membri ai organelor de conducere din cadrul curților de conturi sau membrii organelor de conducere din cadrul consiliilor băncilor centrale;*

*f) ambasadori, însărcinați cu afaceri și ofițeri superiori în forțele armate;*

*g) membrii consiliilor de administrație și ai consiliilor de supraveghere și persoanele care dețin funcții de conducere ale regiilor autonome, ale societăților cu capital majoritar de stat și ale companiilor naționale;*

*h) directori, directori adjuncți și membri ai consiliului de administrație sau membrii organelor de conducere din cadrul unei organizații internaționale".*

[16] Art. 4 din Legea nr. 129/2019 prevede că prin *„beneficiar real se înțelege orice persoană fizică ce deține sau controlează în cele din urmă clientul și/sau persoana fizică în numele ori în interesul căruia/căreia se realizează, direct sau indirect, o tranzacție, o operațiune sau o activitate".*

În anul 2018, a fost adoptată Directiva (UE) 2018/843[17] care observă[18] că „[f]urnizorii implicaţi în servicii de schimb între monedele virtuale şi monedele fiduciare (adică monedele şi bancnotele desemnate ca având curs legal şi moneda electronică ale unei ţări, acceptate ca mijloc de schimb în ţara emitentă), precum şi furnizorii de portofele digitale nu au nicio obligaţie stabilită de Uniune" în materie de CSB/CFT, prin urmare nu sunt constrânse să adopte măsuri în domeniul KYC, iar „anonimatul monedelor virtuale permite posibila utilizare abuzivă a acestora în scopuri criminale"[19].

Drept urmare, Directiva (UE) 2018/843 a completat art. 2 al Directivei (UE) 2015/849, incluzând în categoria entităţilor obligate „furnizorii implicaţi în servicii de schimb între monede virtuale şi monede fiduciare" şi „furnizorii de portofele digitale". Pe cale de consecinţă, aceste entităţi urmează a fi obligate de către statele membre să adopte măsuri în domeniul CSB/CFT, inclusiv măsurile în materia KYC.

România a transpus prevederile Directivei (UE) 2018/843 prin adoptarea Ordonanţei de urgenţă a Guvernului nr. 111/2020[20], astfel încât au fost incluse în categoria entităţilor raportoare furnizorii de servicii de schimb între monede virtuale şi monede fiduciare şi furnizorii de portofele digitale. Au fost definite şi noţiunile de „monede virtuale"[21] şi „furnizor de portofel"[22].

Furnizorii de servicii de schimb între monede virtuale şi monede fiduciare au fost incluşi, din punct de vedere al funcţionării, în sfera de autorizare a Ministerului Finanţelor Publice şi în sfera de supraveghere a Oficiului National de Prevenire şi

[17] Directiva (UE) 2018/843 a Parlamentului European și a Consiliului de modificare a Directivei (UE) 2015/849 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, precum și de modificare a Directivelor 2009/138/CE și 2013/36/UE, publicată în Jurnalul Oficial al Uniunii Europene L 156 din 19.06.2018.

[18] Considerentul 8 al Directivei (UE) 2018/843.

[19] Considerentul 9 al Directivei (UE) 2018/843.

[20] Ordonanța de urgență a Guvernului nr. 111/2020 privind modificarea și completarea Legii nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative, pentru completarea art. 218 din Ordonanța de urgență a Guvernului nr. 99/2006 privind instituțiile de credit și adecvarea capitalului, pentru modificarea și completarea Legii nr. 207/2015 privind Codul de procedură fiscală, precum și pentru completarea art. 12 alin. (5) din Legea nr. 237/2015 privind autorizarea și supravegherea activității de asigurare și reasigurare, publicată în Monitorul Oficial al României, Partea I, nr. 620 din 15 iulie 2020, adoptată cu modificări prin Legea nr. 101/2021, publicată în Monitorul Oficial al României, Partea I, nr. 446 din 27 aprilie 2021.

[21] Conform prevederilor art. 2 lit. t[1]) *„monede virtuale înseamnă o reprezentare digitală a valorii care nu este emisă sau garantată de o bancă centrală sau de o autoritate publică, nu este în mod obligatoriu legată de o monedă instituită legal și nu deține statutul legal de monedă sau de bani, dar este acceptată de către persoane fizice sau juridice ca mijloc de schimb și poate fi transferată, stocată și tranzacționată electronic".*

[22] Conform prevederilor art. 2 lit. t[2]) *„furnizor de portofel digital înseamnă o entitate care oferă servicii de păstrare în siguranță a unor chei criptografice private în numele clienților săi, pentru deținerea, stocarea și transferul de monedă virtuală".*

Combatere a Spălării Banilor[23], cu privire la îndeplinirea obligaţiilor de conformare la legislaţia CSB/CFT, inclusiv aceea de KYC.

Legea nr. 129/2019 stabileşte, în capitolul IV, obligativitatea entităţilor raportoare de a adopta măsuri de cunoaştere a clientelei. Măsurile standard de cunoaştere a clientelei[24] trebuie să permită:

*„a) identificarea clientului şi verificarea identităţii acestuia pe baza documentelor, datelor sau informaţiilor obţinute din surse sigure şi independente, inclusiv, dacă sunt disponibile, a mijloacelor de identificare electronică şi a serviciilor de încredere relevante prevăzute de Regulamentul (UE) nr. 910/2014 al Parlamentului European şi al Consiliului din 23 iulie 2014 privind identificarea electronică şi serviciile de încredere pentru tranzacţiile electronice pe piaţa internă şi de abrogare a Directivei 1.999/93/CE sau a oricărui alt proces de identificare sigur, la distanţă sau electronic, reglementat, recunoscut, aprobat sau acceptat la nivel naţional de către Autoritatea pentru Digitalizarea României;*

*b) identificarea beneficiarului real şi adoptarea de măsuri rezonabile pentru a verifica identitatea acestuia, astfel încât entitatea raportoare să se asigure că a identificat beneficiarul real, inclusiv în ceea ce priveşte persoanele juridice, fiduciile, societăţile, asociaţiile, fundaţiile şi entităţile fără personalitate juridică similare, precum şi pentru a înţelege structura de proprietate şi de control a clientului;*

*c) evaluarea privind scopul şi natura relaţiei de afaceri şi, dacă este necesar, obţinerea de informaţii suplimentare despre acestea;*

*d) realizarea monitorizării continue a relaţiei de afaceri, inclusiv prin examinarea tranzacţiilor încheiate pe toată durata relaţiei respective, pentru ca entitatea raportoare să se asigure că tranzacţiile realizate sunt conforme cu informaţiile deţinute referitoare la client, la profilul activităţii şi la profilul riscului, inclusiv, după caz, la sursa fondurilor, precum şi că documentele, datele sau informaţiile deţinute sunt actualizate şi relevante".*

Entităţile raportoare pot să adopte şi măsuri simplificate în domeniul KYC, însă au *„responsabilitatea de a demonstra autorităţilor cu atribuţii de supraveghere şi control sau organismelor de autoreglementare că măsurile de cunoaştere a clientelei aplicate sunt corespunzătoare din punctul de vedere al riscurilor de spălare a banilor şi de finanţare a terorismului care au fost identificate"*[25].

Pe de altă parte, entităţile raportoare vor aplica măsuri suplimentare în materia KYC *„în toate situaţiile care, prin natura lor, pot prezenta un risc sporit de spălare a banilor sau de finanţare a terorismului, inclusiv în următoarele situaţii:*

*a) în cazul relaţiilor de afaceri şi tranzacţiilor care implică persoane din ţări care nu aplică sau aplică insuficient standardele internaţionale în domeniul prevenirii şi combaterii spălării banilor şi a finanţării terorismului sau care sunt cunoscute la nivel internaţional ca fiind ţări necooperante;*

*b) în cazul relaţiilor de corespondent cu instituţii de credit şi instituţii financiare din alte state membre sau state terţe;*

[23] Denumit în continuare O.N.P.C.S.B.

[24] Art. 11 alin. (1) din Legea nr. 129/2019.

[25] Art. 11 alin. (8) din Legea nr. 129/2019.

*c) în cazul tranzacţiilor sau relaţiilor de afaceri cu persoanele expuse public sau cu clienţi ai căror beneficiari reali sunt persoane expuse public, inclusiv pentru o perioadă de cel puţin 12 luni începând cu data de la care respectiva persoană nu mai ocupă o funcţie publică importantă;*

*d) în cazul persoanelor fizice sau juridice stabilite în ţări terţe identificate de Comisia Europeană drept ţări terţe cu grad înalt de risc;*

*e) în cazurile prevăzute în reglementările sau instrucţiunile sectoriale emise de autorităţile competente în aplicarea prevederilor art. 1 alin. (4)"*[26].

O.N.P.C.S.B. a emis Ordinul nr. 37/2021[27], incluzând furnizorii de servicii de schimb între monede virtuale şi monede fiduciare autorizaţi/înregistraţi de Ministerul Finanţelor în categoria entităţilor reglementate pentru care Oficiul este autoritatea de supraveghere şi control.

Astfel, furnizorii de servicii de schimb între monede virtuale şi monede fiduciare au obligaţia de adoptare a măsurilor KYC şi de raportare către Oficiu a tranzacţiilor suspecte, precum şi de a desemna una sau mai multe persoane cu responsabilităţi în aplicarea legislaţiei din domeniul prevenirii şi combaterii spălării banilor.

## *3. Aspecte practice legate de îndeplinirea obligaţiei de cunoaştere a clientelei*

Conform informaţiilor Europol[28], în anul 2018, o reţea de crimă organizată a folosit criptoactive şi cărţi de credit pentru a spăla mai mult de 8 milioane de euro din traficul de droguri. Infractorii au achiziţionat criptoactive pentru a disimula sursa ilicită a veniturilor, apoi au schimbat monedele virtuale din nou în monedă fiat.

Tot în anul 2018, două reţele de crimă organizată au fost destructurate, constatându-se că au utilizat piaţa criptoactivelor pentru spălarea a 2,5 milioane de euro[29]. Membrii reţelei au achiziţionat criptomonede, pe care le-au transferat în diferite portofele digitale, pentru a disimula sursa infracţională a fondurilor.

[26] Art. 17 alin. (1) din Legea nr. 129/2019.

[27] Ordinul nr. 37 din 2 martie 2021 privind aprobarea Normelor de aplicare a prevederilor Legii nr. 129/2019 pentru prevenirea şi combaterea spălării banilor şi finanţării terorismului, precum şi pentru modificarea şi completarea unor acte normative, pentru entităţile raportoare supravegheate şi controlate de Oficiul Naţional de Prevenire şi Combatere a Spălării Banilor, publicat în Monitorul Oficial nr. 240 din 9 martie 2021.

[28] Europol, Comunicat de presă, *Illegal network used cryptocurrencies and credit cards to launder more than EUR 8 million from drug trafficking*, [Online] la https://www.europol.europa.eu/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking, accesat 30.11.2021.

[29] Europol, Comunicat de presă, *Two criminal groups dismantled for laundering EUR 2.5 million through smurfing and cryptocurrencies*, [Online] la https://www.europol.europa.eu/newsroom/news/two-criminal-groups-dismantled-for-laundering-eur-25-million-through-smurfing-and-cryptocurrencies, accesat 30.11.2021.

În anul 2019, a fost identificat un furnizor de servicii de pe piaţa criptoactivelor[30] care s-a implicat în activităţi de spălare a banilor. Furnizorul era considerat unul dintre cei mai mari la nivel mondial (cifra de afaceri estimată pentru anul 2018 fiind de aprox. 200 milioane dolari) şi a garantat anonimatul clienţilor săi. De fapt, furnizorul oferea clienţilor un serviciu de amestecare (mixare) a criptoactivelor, astfel încât să nu mai poată fi urmărită sursa originală a criptomonedelor potenţial identificabile sau „contaminate". Ancheta a reliefat faptul că multe dintre criptomonedele mixte de pe site-ul furnizorului de servicii aveau o origine sau o destinaţie infracţională, serviciile furnizorului fiind utilizate pentru a ascunde şi spăla fluxuri infracţionale de bani.

În luna februarie 2021, a fost destructurată o grupare de criminalitate organizată[31] care utiliza, pentru disimularea originii ilicite a veniturilor, *dark web*[32] şi platforme de tranzacţionare a criptoactivelor.

Aplicarea măsurilor KYC de către entităţile obligate trebuie să se facă ţinând cont de un echilibru, astfel încât procedurile să nu devină greoaie pentru clienţi sau costisitoare pentru entitate ori să afecteze libera concurenţă din domeniile reglementate. Procesul de cunoaştere a clientelei include pe de o parte programul de identificare a clienţilor (*Customer Identification Program* – CIP) şi, pe de cealaltă parte, manifestarea unei diligenţe corespunzătoare în relaţia cu clienţii (*Customer Due Diligence* – CDD).

În practică, apar diferite situaţii cu care se confruntă furnizorii de servicii de schimb între monede fiduciare şi criptoactive, cum ar fi refuzul clienţilor de a furniza datele cu caracter personal, sursa ori cuantumul veniturilor. Din acest motiv, la înregistrarea pe o platformă de tranzacţionare a criptoactivelor, identificarea clienţilor trebuie să se facă ţinând cont de asigurarea protecţiei datelor furnizate, să utilizeze tehnologii noi, avansate, capabile să facă o recunoaştere corectă şi să asigure conexiunea cu alte baze date date. Tehnologia trebuie să fie flexibilă, uşor de folosit, prietenoasă cu utilizatorul (de exemplu, serviciile să fie oferite cu interfaţa în mai multe limbi). Totodată, utilizarea unor servicii de identificare automată este în măsură să asigure conformarea la legislaţia CSB/CFT.

Furnizorii de servicii de verificare automată a identităţii oferă beneficiarilor (instituţii financiare, furnizori de servicii de schimb între monede fiduciare şi

[30] Europol, Comunicat de presă, *Multi-million euro cryptocurrency laundering service Bestmixer.io taken down*, [Online] la https://www.europol.europa.eu/ newsroom/news/ multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down, accesat 30.11.2021.

[31] Europol, Comunicat de presă, *International drug trafficking network disrupted,* [Online] la https://www.europol.europa.eu/newsroom/news/international-drug-trafficking-network-disrupted, accesat 30.11.2021.

[32] *„Termenul dark web se referă la conținut online criptat care nu este indexat de motoarele de căutare convenționale. Accesarea web-ului întunecat se poate face numai folosind anumite browsere, cum ar fi TOR Browser. Utilizarea dark web în comparație cu site-urile web tradiționale asigură o mai mare confidențialitate și anonimat"* [tr.n], [Online] la https://www.investopedia.com/terms/d/dark-web.asp, accesat 30.11.2021.

criptoactive etc.) posibilitatea de cunoaşte clientela prin verificarea identităţii lor în bazele de date privind persoanele expuse politic (aşa-numitele *„PEP lists”*), în listele globale privind sancţiunile internaţionale (*global sanctions lists*), în bazele de date guvernamentale ori ale organizaţiilor internaţionale privind persoanele urmărite (*watchlist*), precum şi prin identificarea ştirilor negative apărute despre persoanele respective (*adverse media & negative news*).

Tot în cadrul proceselor KYC şi CDD, furnizorii de servicii de schimb între monede fiduciare şi criptoactive pot crea liste de supraveghere a clientelei (*internal watchlists*) care să includă clienţi deja înrolaţi în aplicaţie, dar care prezintă suspiciuni sau clienţi cu care s-a încheiat relaţia de afaceri din motive de suspiciune de fraudă ori CSB/CFT. Verificarea potenţialilor clienţi în aceste liste interne previne reînrolarea unui client cu grad de risc ridicat.

Aşa cum arătam în secţiunea introductivă, abordarea pe bază de riscuri a procesului KYC poate conduce la necesitatea solicitării de informaţii suplimentare de la client, atunci când riscul este pe cale să crească (spre exemplu, volumul sau frecvenţa tranzacţiilor creşte) şi entitatea raportoare trebuie să manifeste prudenţă privind derularea relaţiei comerciale, pentru reducerea riscurilor putând lua chiar decizia de a întrerupe derularea relaţiei de afaceri.

În ceea ce priveşte persoanele expuse public, în practică, trebuie avut în vedere că simpla apartenenţă a unei persoane la categoria respectivă nu trebuie să împiedice derularea unei relaţii comerciale, întrucât nu se poate pleca de la premisa că aceste persoane au săvârşit o ilegalitate. Cunoaşterea trebuie făcută la fel ca în cazul celorlalţi clienţi şi, doar dacă există suspiciuni privind tranzacţiile sau sursa fondurilor, să se aplice măsuri suplimentare de cunoaştere a acestora.

În ceea ce priveşte tranzacţiile suspecte, în practică, la analizarea operaţiunilor de schimb între criptoactive şi moneda fiduciară, trebuie să se aibă în vedere: complexitatea tranzacţiilor, valori neobişnuit de mari tranzacţionate, comportamentul uzual al clientului, scopul tranzacţiei, pentru a preîntâmpina realizarea unei tranzacţii cu risc ridicat.

## *4. Concluzii*

Furnizarea de servicii de schimb între criptoactive şi monedă fiduciară este o activitate exclusiv digitală. Într-o eră a digitalizării, în care fraudele informatice cunosc de asemenea o creştere semnificativă, investiţiile realizate pentru a face o bună cunoaştere a clientelei, deşi pot părea costisitoare, sunt importante atât pentru siguranţa afacerii, cât şi pentru menţinerea unei reputaţii neştirbite.

Dacă se va dovedi că piaţa criptoactivelor se extinde, furnizorii de servicii de pe această piaţă trebuie să adopte măsuri care să uşureze înrolarea pe platformă (de exemplu, utilizarea unor formulare cu autocompletare sau cu răspunsuri predefinite din care clientul poate alege, utilizarea serviciilor de identificare automată ş.a.), concomitent cu conformarea la cerinţele legale în materie.

În situaţia în care furnizorii de servicii de schimb între criptoactive şi monedă fiduciară nu respectă obligaţiile legale în domeniul KYC, aceasta poate atrage, după caz, răspunderea civilă, disciplinară, contravenţională, administrativă sau penală.

O.N.P.C.S.B. este abilitat să constate contravenţiile şi să aplice sancţiunile, cu menţiunea că, prin derogare de la prevederile O.G. nr. 2/2001[33], aplicarea sancţiunii amenzii contravenţionale se prescrie în termen de 5 ani de la data săvârşirii faptei.

De asemenea, pentru o prevenţie eficientă a fenomenului infracţional de spălare a banilor, este importantă cooperarea autorităţilor, a agenţiilor de aplicare a legii şi furnizorii de servicii de pe piaţa criptoactivelor.

**Referinţe**

Europol (2021), European Union serious and organised crime threat assessment, A Corrupting Influence: *The Infiltration and Undermining of Europe's Economy and Society by Organised Crime (t.a.)*, Publications Office of the European Union, Luxembourg

Europol, Comunicat de presă, *Cryptocurrency experts meet at Europol to strengthen ties between law enforcement and private sector*

Europol, Comunicat de presă, *Illegal network used cryptocurrencies and credit cards to launder more than EUR 8 million from drug trafficking*

Europol, Comunicat de presă, *Two criminal groups dismantled for laundering EUR 2.5 million through smurfing and cryptocurrencies*

Europol, Comunicat de presă, *Multi-million euro cryptocurrency laundering service Bestmixer.io taken down*

Europol, Comunicat de presă, *International drug trafficking network disrupted*

[33] Ordonanţa Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare, publicată în Monitorul Oficial al României, Partea I, nr. 410 din 25 iulie 2001.