

CZU 347.7

MECANISME JURIDICE DE PROTECȚIE A DATELOR ÎN RELAȚIILE COMERCIALE INTERNAȚIONALE ÎN ARHITECTURA PROTECȚIEI DREPTURILOR FUNDAMENTALE ȘI A SECURITĂȚII PUBLICE

Evghenia GUGULAN,

*doctor în drept, șefă a Catedrei „Drept privat”,
Academia „Ștefan cel Mare” a MAI
ORCID: 0000-0002-5960-1164*

Ana-Maria KARATEKIN,

*masterandă, Academia „Ștefan cel Mare” a MAI
ORCID: 0009-0004-3502-1837*

Rezumat

Intensificarea relațiilor comerciale internaționale și digitalizarea accelerată a activităților economice au adus în prim-plan problematica protecției datelor cu caracter personal, în special în contextul transferurilor transfrontaliere de date [11]. Articolul analizează mecanismele juridice de protecție a datelor aplicabile relațiilor comerciale internaționale, evidențiind rolul acestora în arhitectura protecției drepturilor fundamentale și a securității publice. Studiul examinează cadrul normativ european instituit prin Regulamentul (UE) 2016/679 (GDPR), cu accent pe aplicabilitatea sa extrateritorială și pe impactul direct asupra structurii contractelor comerciale internaționale [18, art. 3, art. 44–49].

O atenție deosebită este acordată clauzelor contractuale standard (SCC) ca instrument principal de legitimare a transferurilor de date către state terțe, precum și limitelor acestora, reliefate în jurisprudența Curții de Justiție a Uniunii Europene [3], în special în cauza C-311/18 Schrems II [4]. Articolul analizează, totodată, regimul derogărilor prevăzute de art. 49 GDPR și rolul evaluării impactului transferului (TIA) ca mecanism esențial de verificare substanțială a nivelului de protecție oferit în statul terț de destinație.

Din perspectivă comparativă, este examinată situația Republicii Moldova, aflată în proces de armonizare legislativă cu standardele europene, fiind evidențiate provocările practice cu care se confruntă operatorii implicați în relații comerciale internaționale [12, p.103-110]. Concluziile subliniază necesitatea unei abordări prudente și responsabile a transferurilor de date, în care libertatea comerțului internațional este echilibrată cu exigențele protecției efective a drepturilor fundamentale și cu imperativele securității juridice.

Cuvinte-cheie: protecția datelor cu caracter personal, relații comerciale internaționale, transferuri transfrontaliere de date, Regulamentul (UE) 2016/679 (GDPR), clauze contractuale standard (SCC), drepturi fundamentale, securitate juridică.

Abstract

The intensification of international commercial relations and the accelerated digitalisation of economic activities have brought to the forefront the issue of personal data protection, particularly in the context of cross-border data transfers. This article analyses the legal mechanisms governing data protection in international commercial relations, highlighting their role within the broader architecture of fundamental rights protection and public security. The study examines the European regulatory framework established by Regulation (EU) 2016/679 (GDPR), with a particular focus on its extraterritorial applicability and its direct impact on the structure of international commercial contracts.

Special attention is devoted to Standard Contractual Clauses (SCCs) as the primary legal instrument for legitimising personal data transfers to third countries, as well as to their inherent limitations, as clarified by the case law of the Court of Justice of the European Union, notably in Case C-311/18 Schrems II. The article further analyses the regime of derogations provided for under Article 49 GDPR and the role of the Transfer Impact Assessment (TIA) as an essential mechanism for the substantive verification of the level of data protection ensured in the destination third country.

From a comparative perspective, the situation of the Republic of Moldova is examined, as a jurisdiction undergoing legislative harmonisation with European standards, with particular emphasis on the practical challenges faced by operators involved in international commercial relations.

The conclusions underline the necessity of adopting a prudent and responsible approach to international data transfers, in which the freedom of international trade is balanced against the requirements of effective fundamental rights protection and the imperatives of legal certainty.

Keywords: personal data protection; international commercial relations; cross-border data transfers; Regulation (EU) 2016/679 (GDPR); Standard Contractual Clauses (SCCs); fundamental rights; legal certainty.

Introducere. Fenomenul globalizării economice a determinat o intensificare fără precedent a fluxurilor comerciale transfrontaliere, ceea ce a adus în prim-plan problematica protecției datelor cu caracter personal în contextul relațiilor comerciale internaționale. În condițiile în care o parte semnificativă a activităților comerciale se desfășoară în condiții și regim digital, iar partenerii contractuali pot aparține unor jurisdicții distincte, apare necesitatea asigurării unui cadru juridic coerent, care să gverneze transferurile internaționale de date.

Această problematică este deopotrivă relevantă pentru statele membre ale Uniunii Europene, cât și pentru jurisdicții terțe, inclusiv Republica Moldova, aflate într-un proces continuu de armonizare și aliniere a legislației interne la standardele europene în domeniu. Regulamentul UE 2016/679

privind protecția datelor cu caracter personal [18] (GDPR) constituie în prezent cel mai avansat sistem normativ dedicat protecției datelor, fiind considerat un model de referință în plan internațional.

Prin regimul riguros pe care îl instituie asupra transferurilor de date către state terțe, GDPR influențează direct arhitectura juridică a contractelor comerciale internaționale și stabilește un standard minimal de conformitate aplicabil tuturor operatorilor economici care intenționează să proceseze sau să transfere date personale în afara spațiului european. Astfel, impactul sau nu se limitează la teritoriul Uniunii Europene, ci se extinde asupra tuturor partenerilor comerciali ai entității europene, condiționând implicit structura juridică a fluxurilor comerciale globale.

În Republica Moldova, protecția datelor cu caracter personal este reglementată prin Legea nr. 133/2011 [17, art.1], act normativ care urmărește alinierea progresivă la standardele europene în materie. Deși cadrul național păstrează particularități proprii, acesta este puternic influențat de către principiile și mecanismele consacrate pe Regulamentul UE 2016/679 [18], în special în ceea ce privește transferurile de date de către state terțe.

În consecință, operatorii și persoanele împuternicite din Republica Moldova care participă în raporturi de natură comercial-internațională, se confruntă cu necesitate de a se raporta atât la legislația națională, cât și la exigențele europene aplicabile în material fluxurilor transfrontaliere de date. Având în vedere aceste premise, se impune o analiză coerentă a cadrului juridic care guvernează transferurile internaționale de date personale, precum și a mecanismelor utilizate în practica relațiilor comerciale.

Metode aplicate și materiale utilizate. Cercetarea este fundamentată pe un demers metodologic complex, care îmbină metodele clasice ale analizei juridice cu instrumente specifice cercetării comparative și interdisciplinare. În cadrul studiului au fost utilizate metodele de analiză doctrinară și normativă, prin examinarea cadrului juridic european și național în materia protecției datelor cu caracter personal, cu accent pe Regulamentul (UE) 2016/679 [18] (GDPR) și legislația relevantă a Republicii Moldova. Metoda interpretării sistematice și teleologice a fost aplicată pentru a evidenția finalitatea normelor juridice analizate și pentru a releva rolul acestora în arhitectura protecției drepturilor fundamentale și a securității juridice.

Totodată, cercetarea recurge la metoda comparativă, prin raportarea regimului juridic al transferurilor internaționale de date din Republica Moldova la standardele Uniunii Europene, în scopul identificării convergențelor, diferențelor și lacunelor existente. Analiza jurisprudențială a constituit un instrument esențial al studiului, fiind valorificate hotărârile relevante ale Curții de Justiție a Uniunii Europene, în special cauza C-311/18 Schrems II [4], pentru clarificarea limitelor și condițiilor de aplicare a mecanismelor de

transfer transfrontalier de date.

Materialele utilizate includ acte normative europene și naționale, jurisprudență relevantă, documente de orientare emise de instituțiile Uniunii Europene și ale Comitetului European pentru Protecția Datelor, precum și lucrări doctrinare de specialitate din domeniul dreptului protecției datelor, al dreptului comercial internațional și al drepturilor fundamentale. Acest ansamblu metodologic permite o analiză coerentă și riguroasă a mecanismelor juridice examinate, asigurând fundamentarea teoretică și aplicativă a concluziilor formulate.

Rezultate și discuții obținute. Cadrul internațional aplicabil protecției datelor cu caracter personal joacă un rol determinant în funcționarea corectă a relațiilor comerciale transfrontaliere, întrucât majoritatea operațiunilor economice moderne implică, direct sau indirect, prelucrarea și transferul de date personale între entități situate în jurisdicții diferite. În acest context, existența unor norme internaționale coerente și a unor mecanisme juridice recunoscute pe plan global devine indispensabilă pentru asigurarea unui nivel adecvat de protecție și pentru prevenirea riscurilor juridice asociate transferurilor.

Regulamentul UE 2016/679 [18] (GDPR) reprezintă în prezent standardul de referință în materia protecției datelor, având un impact semnificativ asupra relațiilor comerciale internaționale datorită aplicabilității sale extraterritoriale [14, p. 115-118]. Exigențele sale privind transferurile de date către state terțe, în special principiul nivelului de protecție substanțial echivalent condiționează modul în care operatorii economici pot structura contractele comerciale internaționale. În consecință, orice parte potențial contractuală care intenționează să dezvolte o anumită relație contractual-comercială, atât și de prestări de servicii, trebuie să demonstreze respectarea acestui standard, chiar dacă este situat într-o jurisdicție care nu face parte din UE.

Clauzele Contractuale Standard (SCC) reprezintă unul dintre cele mai frecvent utilizate instrumente juridice pentru legitimarea transferurilor internaționale de date cu caracter personal în absența unei decizii de adecvare. Instituite de Comisia Europeană în temeiul Art. 46 alin. (2) lit. c) și d) din Regulamentul UE 2016/679 [18], clauzele contractuale standard constituie un mecanism uniform care permite operatorilor și persoanelor împuternicite să transfere date către state terțe, cu condiția asumării unor obligații contractuale menite să asigure un nivel de protecție substanțial echivalent cu cel european.

Regimul juridic al clauzelor contractuale standard se caracterizează prin două elemente esențiale. Primul este caracterul predefinit, întrucât clauzele sunt aprobate în mod expres de Comisia Europeană și nu pot fi mo-

dificate în substanță de către părți, acestea având doar posibilitatea de a le completa cu informații specifice operațiunii de transfer. Această structură rigidă urmărește să prevină deteriorarea nivelului de protecție prin negociere contractuală, garantând un cadru minim obligatoriu. Al doilea element îl constituie efectul lor direct în raporturile dintre părțile contractante, deoarece clauzele produc obligații juridice ferme pentru importatorul de date, chiar dacă acesta operează într-o jurisdicție care nu consacră un regim legal comparabil cu cel al Uniunii Europene.

Utilizarea Clauzelor contractuale standard în relațiile comerciale internaționale presupune o analiză prealabilă atentă a circumstanțelor transferului și a legislației aplicabile în statul terț de destinație. Hotărârea Curții de Justiție a Uniunii Europene din 16 iulie 2020 în cauza C-311/18 [4] („Schrems II”) reprezintă una dintre cele mai influente decizii în materie de transferuri internaționale de date [7, p. 547–551]. Aceasta a redefinit exigențele aplicabile Clauzelor Contractuale Standard (SCC) și a impus operatorilor obligații care depășesc simpla inserare formală a acestor clauze în contractele comerciale.

Litigiul a pornit de la o plângere formulată de cetățeanul austriac Maximilian Schrems împotriva transferurilor de date realizate de Facebook Ireland către serverele companiei-mamă din Statele Unite [2]. Argumentul central a vizat faptul că legislația americană privind accesul autorităților publice la date – în special în baza FISA Section 702 și Executive Order 12333 – nu oferea garanții echivalente celor prevăzute de dreptul european, iar persoanele vizate nu dispuneau de un control jurisdicțional efectiv. Curtea de Justiție a confirmat, în esență, aceste preocupări și a constatat că mecanismele interne de protecție disponibile în Statele Unite nu asigurau o protecție substanțial echivalentă cu cea din Uniunea Europeană.

Deși Curtea a menținut valabilitatea generală a SCC-urilor, ea a subliniat că acestea nu pot garanta prin ele însele un nivel adecvat de protecție în toate jurisdicțiile [13, p. 240–245]. În consecință, operatorii care intenționează să se bazeze pe SCC au obligația de a evalua, înainte transferului, dacă legislația statului terț permite respectarea garanțiilor contractuale. Dacă această compatibilitate nu poate fi demonstrată, operatorul este obligat fie să implementeze măsuri suplimentare, fie să suspende complet transferul. Decizia a introdus, astfel, un standard de diligență sporită, care se materializează în practica actuală prin necesitatea efectuării unei evaluări a impactului transferului (TIA).

Hotărârea „Schrems II” [4] a produs efecte imediate asupra tuturor operatorilor economici care transferau date în Statele Unite sau în alte jurisdicții cu regim extins de acces al autorităților publice. În context comercial, aceasta a generat obligația reevaluării arhitecturii tehnice și contractuale a

transferurilor, ajustarea clauzelor contractuale standard și aplicarea unor măsuri tehnice suplimentare, precum criptarea cu gestionarea exclusivă a cheilor pe teritoriul Uniunii Europene sau minimizarea strictă a datelor transferate.

Relevanța deciziei depășește însă cadrul specific al transferurilor către Statele Unite, deoarece Curtea a consacrat principiul general potrivit căruia operatorii sunt responsabili să evalueze în mod concret circumstanțele fiecărui transfer și să stabilească dacă garanțiile contractuale pot fi efectiv respectate în statul terț. Acest principiu transformă SCC dintr-un instrument formal într-un mecanism care impune o analiză substanțială a riscurilor, având ca scop protejarea drepturilor persoanelor vizate și menținerea unui nivel ridicat de protecție în toate fluxurile transfrontaliere.

În acest sens, „Schrems II” [4] constituie exemplul practic cel mai relevant pentru a înțelege limitele SCC-urilor și responsabilitatea operatorilor în utilizarea lor. Decizia a consacrat obligația de verificare prealabilă a compatibilității legislației statului terț, a făcut necesară instituirea evaluării impactului transferului și a demonstrat că mecanismele contractuale nu pot contracara în mod automat potențialele ingerințe ale autorităților publice asupra datelor transferate.

Această cerință a dobândit un rol central în urma hotărârii Curții Supreme de Justiție a Uniunii Europene în cauza „Schrems II” [4], care a subliniat că simpla existență a clauzelor contractuale standard nu garantează automat legalitatea transferului, operatorul având obligația să verifice, dacă și în practică garanțiile oferite de clauze sunt și pot fi efectiv respectate, ținând cont de eventualele prerogative ale autorităților publice din statul importator privind accesul la date. În situația în care riscurile depășesc posibilitatea de a asigura protecția necesară, operatorul trebuie să implementeze măsuri tehnice și organizatorice suplimentare, fie să suspende transferul.

În practică, clauzele contractuale standard sunt integrate în contracte comerciale internaționale fie ca anexă obligatorie, fie ca parte a principalelor dispoziții contractuale privind prelucrarea datelor. Această integrare condiționează validitatea transferului și reprezintă o garanție pentru partenerii din Uniunea Europeană că operatorii situați în state terțe vor respecta obligațiile privind confidențialitatea, securitatea și limitarea scopului prelucrării. Totodată, includerea clauzelor contractuale standard în contracte facilitează procedura de audit intern al respectării cerințelor GDPR și oferă o bază juridică certă în eventualitatea unor controale ale autorităților de supraveghere.

Efectele juridice ale SCC-urilor se manifestă atât în raporturile dintre operator și persoana împuternicită, cât și în relația cu persoana vizată. În mod particular, clauzele consacră un drept direct al persoanei vizate de a

invoca și solicita executarea anumitor obligații asumate de importator, conferindu-i acestea un nivel sporit de protecție în raport cu transferurile către jurisdicții cu standarde inferioare de protecție a datelor. Aceasta reprezintă o particularitate care diferențiază SCC-urile de alte instrumente juridice utilizate în transferurile internaționale și contribuie la consolidarea securității juridice în relațiile comerciale transfrontaliere.

Prin urmare, rolul Clauzelor contractuale standard în contextul juridic internațional este fundamental, întrucât acestea oferă un instrument uniform, previzibil și recunoscut pe scară largă pentru asigurarea conformității transferurilor de date. Deși nu substituie necesitatea unor evaluări suplimentare privind legislația staturilor terțe, SCC-urile reprezintă un pilon central al arhitecturii juridice care permite funcționarea eficientă și sigură a relațiilor comerciale internaționale.

Regimul derogă consacrate de articolul 49 din Regulamentul (UE) 2016/679 [18] este unul dintre cele mai restrictive mecanisme care pot fundamenta transferurile internaționale de date cu caracter personal. Spre deosebire de instrumentele standardizate, precum clauzele contractuale standard, derogările nu constituie un temei de transfer obișnuit, ci un mecanism cu caracter rezidual, destinat unor situații strict delimitate și aplicabil doar atunci când nu există alte modalități adecvate de asigurare a unui nivel de protecție, echivalent celui european. Prin urmare, aplicarea lor într-un context de relații comerciale internaționale trebuie realizată cu prudență și în urma unei evaluări riguroase a circumstanțelor concrete ale transferului.

Articolul 49 instituie mai multe ipoteze distincte, fiecare condiționată de îndeplinirea unor criterii cumulative. Dintre acestea, cele mai relevante pentru sfera comercială sunt transferurile necesare pentru executarea unui contract sau pentru implementarea unor măsuri precontractuale adoptate la cererea persoanei vizate. Aceste derogări sunt aplicabile în situații în care transferul de date reprezintă o condiție indispensabilă pentru realizarea unei obligații contractuale, cum ar fi furnizarea unui serviciu, livrarea unui produs sau menținerea unei relații contractuale cu o entitate stabilită într-un stat terț. Totuși, necesitatea trebuie interpretată în sens restrâns, astfel încât operatorul să poată demonstra că transferul reprezintă unica modalitate rezonabilă de executare a obligațiilor asumate.

O altă derogare semnificativă este cea privind consimțământul explicit al persoanelor vizate, utilizabil în situațiile în care nu există o altă bază legală pentru transfer. Această derogare prezintă însă limitări semnificative, întrucât consimțământul trebuie să fie liber exprimat, iar persoana vizată trebuie să fie avertizată în mod explicit cu privire la riscurile potențiale ale transferului în absența unor garanții adecvate. În practica relațiilor comerciale internaționale, această derogare este rar utilizată ca temei principal ,

întrucât caracterul său fragil și revocabil poate afecta stabilitatea raporturilor contractuale.

Derogările pot fundamenta transferuri și în alte ipoteze expres reglementate, precum protejarea intereselor vitale ale persoanei vizate, transferuri necesare pentru formularea, exercitarea sau apărarea unor pretenții juridice, sau transferuri realizate din motive importante, de interes public. Deși aplicabile și în context comercial, aceste situații sunt rare în practică, având un rol preponderent punctual sau sectorial. Prin natura lor, ele nu pot constitui un temei recurent pentru fluxuri continue sau sistematice de date între parteneri comerciali.

Un element esențial articolului 49 îl constituie caracterul excepțional al derogărilor. Comitetul European pentru Protecția Datelor a subliniat în mod repetat faptul că acestea nu pot fi utilizate pentru activități care implică transferuri repetate, masive și structurate. Derogările nu sunt menite să substituie implementarea unor mecanisme de conformitate adecvate, precum SCC-urile sau alte instrumente prevăzute de art. 46 GDPR [18], ci să ofere o soluție punctuală în situații în care nici un alt temei nu este aplicabil. Operatorii care recurg frecvent la derogări în relațiile comerciale internaționale se expun unui risc semnificativ de neconformitate, întrucât autoritățile de supraveghere pot interpreta un astfel de comportament ca fiind contrar principiilor fundamentale ale protecției datelor.

Totodată, aplicarea derogărilor implică obligația Operatorilor de a documenta în mod riguros analiza prealabilă, justificarea necesității transferului și evaluarea proporționalității acestuia. În contextul Republicii Moldova, operatorii implicați în relații comerciale cu partenerii europeni trebuie să acorde o atenție sporită acestor cerințe, având în vedere absența unei decizii de adecvate și necesitatea demonstrării compatibilităților transferurilor cu normele europene.

Constatăm că derogările prevăzute la articolul 49 GDPR [18] constituie un mecanism juridic indispensabil în arhitectura transferurilor internaționale de date, însă aplicarea lor rămâne strict limitată la ipoteze excepționale și bine justificate. În relațiile comerciale internaționale, ele pot fi utilizate doar punctual, în situații concret determinabile, nicidecum nu ca fundament pentru fluxuri recurente de date. Regimul lor restrictiv subliniază importanța mecanismelor principale de conformitate și obligă Operatorii să adopte o abordare prudentă și responsabilă în material protecției datelor în tranzacțiile transfrontaliere.

Evaluarea impactului transferului (TIA) s-a impus ca instrument de analiză juridică necesar ori de câte ori datele cu caracter personal urmează să fie transferate către un stat terț, în temeiul unor garanții contractuale sau al altor mecanisme prevăzute de articolul 46 GDPR [8, p. 5 – 9]. Deși nu este

consacrată expres în textul Regulamentului, obligația efectuării unei astfel de evaluări decurge din jurisprudența Curții de Justiție a Uniunii Europene și din orientările Comitetului European pentru protecția datelor, care impun Operatorilor o verificare prealabilă a condițiilor în care datele vor fi tratate în statul de destinație.

Scopul unei evaluări este de a stabili dacă, în statul terț, cadrul legislativ și practicile autorităților permit menținerea garanțiilor asumate prin instrumentul juridic utilizat pentru transfer. Analiza nu se limitează o examinare formală a dispozițiilor legale, ci presupune o evaluare a compatibilității acestora cu standardele de protecție a datelor cu caracter personal ale Uniunii Europene, în special în ceea ce privește accesul autorităților publice la date, existența unor mecanisme de control jurisdicțional efectiv și posibilitatea persoanei vizate de a-și exercita drepturile real și eficient.

În mod obișnuit, o evaluare a impactului transferului cuprinde identificarea naturii datelor prelucrate, descrierea fluxului transfrontalier, stabilirea temeiului utilizat pentru transfer și o analiză a obligațiilor care revin importatorului în statul terț. O atenție particulară este acordată situațiilor în care legislația locală ar putea impune operatorului obligația de divulgare a datelor sau ar putea limita capacitatea acestuia de a respecta angajamentele contractuale asumate. În aceste cazuri, simpla încheiere a unui instrument standardizat nu este suficientă, iar operatorul trebuie să decidă dacă sunt necesare măsuri suplimentare de natură tehnică sau organizatorică.

Măsurile suplimentare care pot rezulta dintr-o evaluare a impactului variază în funcție de natura transferului. Ele pot include tehnici de minimizare a datelor, criptare în condiții care să excludă accesul entităților din statul terț, limitări stricte privind accesul intern sau revizuirea arhitecturii operaționale a furnizorului extern. În anumite situații, evaluarea poate conduce la concluzia că transferul nu poate fi realizat în condiții compatibile cu standardul european, caz în care operațiunea trebuie suspendată sau reconfigurată.

Pentru Operatorii din Republica Moldova, necesitatea efectuării unei astfel de analize decurge în primul rând din obligația partenerilor europeni, care trebuie să justifice legalitatea fiecărui flux de date. Chiar dacă legislația națională nu reglementează în mod autonom procesul de evaluare a impactului transferului, operatorii moldoveni implicați în tranzacții comerciale internaționale trebuie să fie în măsură să furnizeze informații privind modul în care sunt protejate datele, infrastructura tehnică utilizată, accesul instituțional la date și nivelul de control exercitat asupra furnizorilor lor.

TIA nu este un exercițiu birocratic, așa cum ar putea fi catalogat de unii, ci un demers analitic menit să stabilească dacă un transfer poate avea loc în condiții predictibile și conforme cu standardele internaționale. Importanța sa constă în caracterul său anticipativ: operatorii pot identifica înainte

de efectuarea transferului de date, incompatibilități dintre garanțiile contractuale și legislația statului terț, evitând astfel riscurile juridice, comerciale și operaționale care pot apărea ulterior.

În relațiile comerciale internaționale, transferul de date cu caracter personal apare, de regulă, ca un element accesoriu al executării unui contract principal, însă implicațiile sale juridice sunt suficient de complexe pentru a necesita o reglementare expresă în instrumentele contractuale ale părților. Integrarea mecanismelor de transfer prevăzute de GDPR în structura contractuală nu are doar rolul de a asigura conformitatea formală, ci determină modul în care partenerii comerciali își distribuie obligațiile, riscurile și responsabilitățile în legătură cu prelucrarea datelor în afara spațiului european.

În practică, clauzele privind transferurile de date sunt inserate fie în contractul comercial principal, fie într-un acord separat privind prelucrarea datelor (Data Processing Agreement – DPA), care devine parte integrantă a raportului contractual. Indiferent de formatul utilizat, aceste clauze trebuie să reflecte cu precizie instrumentul juridic ales pentru transfer, fie că este vorba despre clauzele contractuale standard, o derogare în sensul art. 49 GDPR [18] sau un set de măsuri tehnice și organizatorice identificate în urma unei evaluări a impactului transferului. Lipsa unei corelări între contract și mecanismul legal aplicabil creează incertitudine juridică și poate conduce la imposibilitatea justificării transferului în cazul unui control al autorităților de supraveghere.

În procesul de redactare a acestor dispoziții contractuale, un aspect esențial îl constituie delimitarea obligațiilor care revin fiecărei părți, în special în ceea ce privește securitatea datelor, notificarea incidentelor, accesul la date și colaborarea în cadrul evaluării impactului transferului. În acordurile cu parteneri situați în state terțe, importatorul de date trebuie să își asume expres obligații care decurg din mecanismul utilizat pentru transfer, inclusiv angajamente privind abținerea de la divulgarea datelor către autoritățile locale în absența unei cerințe legale imperative sau informarea exportatorului cu privire la orice solicitare de acces venită din partea acestora.

Un element important îl constituie și adaptarea clauzelor contractuale la rezultatele evaluării impactului transferului. În situațiile în care TIA evidențiază riscuri care nu pot fi eliminate exclusiv prin instrumentul juridic utilizat, contractul trebuie să includă măsuri complementare, cum ar fi cerințe tehnice specifice (criptare, controlul accesului, segregarea mediilor), limitări operaționale sau reguli privind localizarea anumitor categorii de date. Aceste dispoziții trebuie formulate într-un mod suficient de precis pentru a putea fi aplicate în mod efectiv, dar totodată flexibil pentru a permite adaptarea la eventuale modificări ale cadrului legislativ al statului terț.

În cazul operatorilor și persoanelor împuternicite din Republica Mol-

dova, integrarea acestor mecanisme în contractele cu parteneri europeni capătă o importanță particulară, deoarece obligațiile de conformitate derivă nu doar din legislația națională, ci și din cerințele impuse de partea europeană, care este obligată să asigure legalitatea transferului în propria jurisdicție. În lipsa unor dispoziții contractuale clare, partenerii europeni pot considera că transferul nu întrunește condițiile prevăzute de GDPR [18], ceea ce poate conduce la întârzieri în executarea contractului sau la refuzul colaborării.

În măsura în care relațiile comerciale internaționale implică fluxuri recurente de date, este recomandată instituirea unor mecanisme de revizuire periodică a obligațiilor contractuale, astfel încât părțile să poată adapta clauzele de transfer la modificările legislative din statele terțe sau la evoluțiile jurisprudențiale din Uniunea Europeană. O astfel de abordare conferă stabilitate juridică raportului contractual și permite gestionarea în timp real a riscurilor specifice transferurilor transfrontaliere.

Integrarea mecanismelor de transfer în contractele comerciale internaționale nu este, așadar, o simplă formalitate, ci o componentă esențială a conformității juridice. Prin modul în care sunt formulate și aplicate, aceste clauze determină nu doar legalitatea transferului, ci și poziția juridică a fiecărei părți în cadrul relației contractuale, nivelul de protecție acordat persoanelor vizate și viabilitatea pe termen lung a colaborării comerciale.

Concluzii. Cadrul juridic al transferurilor internaționale de date cu caracter personal reprezintă unul dintre cele mai complexe segmente ale dreptului protecției datelor, fiind situat la intersecția dintre exigențele comerțului global și imperativele protecției drepturilor fundamentale. Regulamentul (UE) 2016/679 [18] a consacrat principiul nivelului de protecție „substanțial echivalent”, transformând mecanisme precum clauzele contractuale standard, derogările art. 49 și evaluarea impactului transferului în instrumente esențiale pentru justificarea legalității fluxurilor de date. Jurisprudența CJUE, în special „Schrems II” [4], a consolidat obligația operatorilor de a analiza concret legislația statului terț și de a implementa măsuri suplimentare atunci când este necesar, mutând accentul de la conformitatea formală la o verificare substanțială a riscurilor.

Pentru state precum Republica Moldova, aflate în proces de armonizare cu standardele europene, aceste exigențe dobândesc o relevanță deosebită, întrucât transferurile către parteneri din UE implică respectarea atât a legislației naționale, cât și a parametrilor impuși de GDPR. În acest context, mecanismele de transfer devin parte integrantă a arhitecturii contractelor comerciale internaționale și contribuie la creșterea încrederii între parteneri.

În ansamblu, regimul actual se caracterizează printr-o abordare prudentă și responsabilă, în care libertatea comerțului internațional este echilibrată cu protecția efectivă a persoanei vizate. Evoluția cadrului normativ

demonstrează că viabilitatea transferurilor transfrontaliere nu depinde doar de instrumentele juridice utilizate, ci de capacitatea operatorilor de a înțelege și gestiona riscurile asociate, în scopul menținerii unui nivel ridicat de securitate juridică și de protecție a datelor.

BIBLIOGRAFIE:

1. Charter of Fundamental Rights of the European Union. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>
2. CJEU, Case C-362/14, Schrems I, Judgment of 6 October 2015. <https://curia.europa.eu/juris/liste.jsf?num=C-362/14>
3. CJEU, Case C-582/14, Breyer v Germany, Judgment of 19 October 2016. <https://curia.europa.eu/juris/liste.jsf?num=C-582/14>
4. CJEU, Case C-311/18, Schrems II, Judgment of 16 July 2020. <https://curia.europa.eu/juris/liste.jsf?num=C-311/18>
5. Council of Europe – Convention 108. <https://www.coe.int/en/web/data-protection/convention108-and-protocol>
6. Cross-Border Data Flows, the GDPR, and Data Governance, W. Gregory Voss, University of Toulouse, 2020. https://www.researchgate.net/publication/342243358_Cross-Border_Data_Flows_the_GDPR_and_Data_Governance_29_Wash_Int'l_LJ_485_2020 (vizitat 11.10.2025).
7. Costello R. Á., Schrems II: Everything Is Illuminated?, European Papers, 2020. https://www.europeanpapers.eu/system/files/pdf_version/EP_EF_2020_I_037_Roisin_Aine_Costello_00396.pdf (vizitat 13.10.2025).
8. EDPB – Recommendations 01/2020 on measures that supplement transfer tools. https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures_en
9. EDPB – Guidelines 2/2018 on derogations of Article 49 GDPR. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49_en
10. European Commission – Implementing Decision (EU) 2021/914 on Standard Contractual Clauses (SCC). https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
11. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013. <https://www.oecd.org/digital/privacy/oecd-privacy-guidelines.htm>
12. Gugulan, E., Analiza cadrului normativ privind datele cu caracter personal. Anale științifice ale Academiei „Ștefan cel Mare” a MAI, nr. XVI-II(2)/2018. https://ibn.idsi.md/sites/default/files/imag_file/103-110_5.pdf
13. Juliussen B.A., The Third Country Problem under the GDPR”, International Data Privacy Law, vol. 13, nr. 3, 2023. <https://www.researchgate.net/publication/366111111>

- net/publication/373978714_The_third_country_problem_under_the_GDPR_enhancing_protection_of_data_transfers_with_technology
14. Kuner C., *Transborder Data Flows and Data Privacy Law*, Oxford University Press, 2013. https://www.researchgate.net/publication/259994485_Transborder_Data_Flows_and_Data_Privacy_Law (vizitat 10.10.2025).
 15. Kuner, C.; Bygrave, L.; Docksey, C. (eds.), *The GDPR: A Commentary*, Oxford University Press, 2020. <https://global.oup.com/academic/product/the-eu-general-data-protection-regulation-gdpr-9780198826492>
 16. Hijmans, H., *The European Union as Guardian of Internet Privacy*, Springer, 2016. <https://link.springer.com/book/10.1007/978-3-319-34090-6>
 17. Legea nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal. https://www.legis.md/cautare/getResults?doc_id=148996&lang=ro
 18. Regulation (EU) 2016/679 (GDPR) of the European Parliament and of the Council of 27 April 2016. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
 19. Treaty on the Functioning of the European Union (TFEU) – consolidated version. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016E/TXT>