

SECURITATEA PĂRȚILOR ÎN ACTELE JURIDICE CIVILE ELECTRONICE

SECURITY OF THE PARTIES IN ELECTRONIC CIVIL LEGAL DEEDS

RUSNAC Aliona,

dr. în drept, conf. univ., Departamentul Drept Privat, Director Filiera Anglofonă,
Facultatea de Drept USM, Absolventă Fulbright

CZU: 347.921:347.931:004

Summary

Electronic legal documents have become an indispensable means related to the daily activity of individuals in particular in the Pandemic Covid 19 period. In this article we set out to analyze the security aspects of the parties in the process of concluding and directly in the process of executing electronic legal acts. In this study we aim to deepen the knowledge in the field of contracts and other legal acts that are concluded in electronic form or by electronic means, and to highlight the risks to which the parties are exposed in these contracts or other acts. We will investigate the security of the parties of civil legal acts that have been concluded in the electronic environment in terms of the typology of civil legal acts: unilateral and bilateral legal acts.

Keywords: *civil legal acts, security of the parties, electronic form of the legal act, legal act signed via electronic means, third party security, consumer, user, Pandemic, Health crisis.*

Actele juridice electronice au devenit un mijloc indispensabil legat de activitatea zilnică al persoanelor fizice. În acest articol ni-am propus analiza aspectelor de securitate al părților în procesul încheierii și nemijlocit în procesul executării actelor juridice electronice. Actele juridice electronice au devenit o activitate zilnică indispensabilă al persoanelor fizice și persoanelor juridice, în special în perioada pandemiei Covid 19 (crizei de sănătate), care a catalizat numărul actelor juridice în formă electronică prin limitarea circulației persoanelor atât în hotarele țării dar mai ales la nivel transfrontalier și prin riscurile la care se expun aceștia.

Conform art. 9 alin. 2 Cod civil al RM, *drepturile și obligațiile civile apar: din contracte și din alte acte juridice*, principalele izvoare de apariție al drepturilor și obligațiilor civile sunt contractele și alte acte juridice. În acest studiu ne propunem să aprofundăm cunoștințele în domeniul contractelor și altor acte juridice ce se încheie în formă electronică sau prin mijloace electronice, și să evidențiem riscurile la care se expun părțile în aceste contracte sau alte acte. Astfel, în conformitate cu prevederile codului civil în vigoare sunt reglementate forma electronică a actului juridic (art. 318 Cod Civil al RM) și actul juridic încheiat prin utilizarea mijloacelor electronice (art. 318 Cod Civil al RM). Actul juridic are formă electronică dacă se

cuprinde într-un document electronic care întrunește condițiile legii conform alin. 1 art. 318 Cod civil al RM [1].

Definiția dată de Legea nr. 91 din 27.06.2014 privind semnătura electronică și documentul electronic, prevede **document electronic** – *informație în formă electronică, creată, structurată, prelucrată, păstrată și/sau transmisă prin intermediul computerului sau al altor dispozitive electronice, semnată cu semnătură electronică în conformitate cu prezenta lege* [2], în consecință legislatorul a reglementat actul juridic civil în formă electronică, în același timp a fost definit și documentul electronic ca fiind *informație în formă electronică*. Conform art. 1245 Codul civil al României forma contractelor electronice, *contractele care se încheie prin mijloace electronice sunt supuse condițiilor de formă prevăzute de legea specială* [3], prin analiza legislației din Republica Moldova și România observăm că legislația României expres prevede noțiunea de ”contract electronic”, ceea ce în codul civil din Republica Moldova lipsește fiind prezente noțiunile de act juridic în formă electronică, comerț electronic, dar lipsește definiția expresă al contractului electronic.

Totodată în alin. 2 al art. 318 Cod civil al RM prevede *Tipurile de semnături electronice care pot fi aplicate unui document electronic, gradul de protecție al fiecărui tip și valoarea lui juridică sînt determinate de lege*, astfel este prevăzut obligativitatea semnăturii electronice în vederea consemnării acordului părților, în același timp, alin. 3 al art. 318 Cod civil al RM stabilește că, actul juridic în format electronic este echivalent actului juridic în formă scrisă, astfel fiind aplicate și prevederile formei scrise ale actului juridic în cazul în care poartă semnătură electronică de orice tip prevăzută de lege a persoanei care încheie actul, dacă prin acordul părților nu se prevede cerința de utilizare a unui tip concret de semnătură electronică, precum și în alte cazuri prevăzute de lege [1]. Definiția semnăturii electronice o găsim în art. 2 din Legea 91/2014 *semnătură electronică – date în formă electronică, care sînt atașate la sau logic asociate cu alte date în formă electronică și care sînt utilizate ca metodă de autentificare*, în același sens, **semnatar** – *persoana care deține un dispozitiv de creare a semnăturii electronice și care acționează fie în nume propriu, fie în numele persoanei fizice, al persoanei juridice sau al entității pe care o reprezintă*.

Tărâmul electronic poate fi utilizat de către persoane fizice sau juridice practic în toate sferile de activitate care pot fi desfășurate în mediul online, fie este posibilă utilizarea mijloacelor tehnice și de program ce permit crearea, prelucrarea, expedierea, recepționarea, păstrarea, modificarea și/sau nimicirea informației în formă electronică. În acest sens, documentul electronic poate fi folosit având drept obiectiv transmiterea informației, păstrarea/arhivarea corespondenței, încheierea actelor juridice civile electronice, precum și în calitate de document care reflectă fapte economice.

Conform prevederilor art. 15 din Legea 91/2014 sunt prevăzute cerințele principale ale documentului electronic:

- să fie creat, prelucrat, expeditat, recepționat, păstrat, modificat și/sau nimit cu ajutorul mijloacelor tehnice și/sau de program;
- să conțină, pentru confirmarea autenticității acestuia, una sau mai multe semnături electronice ce corespund condițiilor și cerințelor stabilite de prezenta lege;
- să fie creat și utilizat prin metode și într-o formă ce ar permite identificarea semnatarului;
- să fie afișat într-o formă perceptibilă;
- să permită utilizarea sa repetată .

În vederea stabilirii validității (autenticității) documentului electronic, acesta trebuie să întrunească cumulativ următoarele condiții:

- a) este semnat de persoana abilitată, în modul stabilit, să semneze cu semnătură olografă documentul echivalent pe suport de hârtie;
- b) este semnat cu semnătura electronică autentică a semnatarului indicat în document [2].

Procesul de solicitare și obținere a semnăturii electronice este caracteristică fiecărui prestator de servicii de certificare individual și poate fi consultată pe paginile oficiale ale fiecărui prestator. Semnăturile electronice existente în Republica Moldova sunt: Msign eliberată de Agenția de Guvernare Electronică, sunt oferite dispozitive de verificare a semnăturii electronice online pe situl msign.gov.md, valabilă pe teritoriul Republicii Moldova [4], Compania M Orange SA eliberează semnătură electronică .denumită și semnătura mobilă [5]. Compania M Moldcell SA eliberează semnătură electronică/mobilă [6], P Centrul de Tehnologii Informaționale în Finanțe [7], P. Serviciul Tehnologia Informației și Securitate Cibernetică [8], IP Agentia Servicii Publice [9] etc.

Astfel, tipurile de semnături electronice, ale căror principii și mecanisme de utilizare sunt reglementate de Legea privind semnătura electronică și documentul electronic, sunt următoarele:

a) Semnătura electronică simplă - este semnătura electronică utilizată ca metodă de autentificare, fără a face trimitere exclusiv la semnatar. Documentul electronic se consideră semnat cu semnătură electronică simplă dacă este întrunită una dintre următoarele condiții:

- semnătura electronică simplă se conține nemijlocit în documentul electronic sau este logic asociată cu documentul electronic;
- datele de creare a semnăturii electronice simple se aplică în corespundere cu regulile stabilite de către operatorul sistemului informatic prin intermediul căruia se efectuează crearea și/sau expedierea documentului electronic și în documentul electronic se conține informația care identifică persoana în numele căreia a fost creat și expeditat documentul electronic.

Actele normative și/sau acordul părților, care stabilesc cazurile de recunoaștere a documentelor electronice semnate cu semnătură electronică simplă, echivalente documentelor pe suport de hârtie semnate cu semnătură olografă, trebuie să prevadă următoarele:

- modalitatea de identificare a persoanei în numele căreia este semnat documentul electronic în baza semnăturii electronice simple a acesteia;
- obligația persoanei care creează și/sau utilizează date de creare a semnăturii electronice simple de a asigura confidențialitatea acestora.

b) Semnătura electronică avansată necalificată - este semnătura electronică ce îndeplinește următoarele cerințe:

- face trimitere exclusiv la semnatar;
- permite identificarea semnatarului;
- este creată prin mijloace controlate exclusiv de semnatar;
- este legată de datele la care se raportează, astfel încât orice modificare ulterioară a acestor date poate fi detectată.

c) Semnătura electronică avansată calificată - este o semnătură electronică care îndeplinește toate cerințele semnăturii electronice avansate necalificate și, suplimentar:

- se bazează pe un certificat calificat al cheii publice emis de un prestator de servicii de certificare acreditat în domeniul aplicării semnăturii electronice avansate calificate;

- este creată prin intermediul dispozitivului securizat de creare a semnăturii electronice și se verifică securizat cu ajutorul dispozitivului de verificare a semnăturii electronice și/sau al produsului asociat semnăturii electronice, care dispune de confirmarea corespunderii cu cerințele prevăzute de prezenta lege [2].

În prezentul studiu vom cerceta securitatea părților actelor juridice civile care au fost încheiate în mediul electronic prin prisma tipologiei actelor juridice civile: actele juridice unilaterale și bilaterale.

După cum am menționat anterior, alin. 2 al art. 9 Cod civil al RM face referință că *drepturile și obligațiile apar din contracte...* Într-adevăr unul din izvoarele principale de apariție al obligațiilor dar în special al celor ce apar din acte juridice în format electronic sunt contractele. Atât la nivel doctrinar cât și la nivel legislativ noțiunea de contract o găsim drept a fi acordul de voință realizat prin care părțile (două sau mai multe persoane) stabilesc, modifică sau sting raporturi juridice, în cazul contractelor în formă electronică etapele negocierilor, etapa încheierii se realizează de regulă de asemenea electronic, între persoane absente fizic, dar prezente online, ceea ce și adaugă un grad de risc și o valoare de precauție din partea acestora în vederea evitării situațiilor de declarării nule a contractului sau unui alt act juridic (spre exemplu o procură). La etapele încheierii contractului, executării (efectelor contractului) și nemijlocit la încetarea acestuia părțile urmează să monitorizeze toate circumstanțele în vederea evitării insecurității precum colectarea sau introducerea în act juridic în formă electronică a unei informații false, sau fraudele ce pot avea loc prin schimbarea identității, fraude bancare (sub forma fraudelor legate de cardurile bancare, introducerea datelor bancare și lipsirea de mijloacele financiare aflate pe conturile bancare) ș.a.. Astfel, va fi multi aspectual prezentat domeniul securității părților.

Părțile în cazul comerțului electronic sunt: business to consumer – situații în care companiile vând produse și servicii consumatorilor; business to business - companiile vând produse altor companii (persoane juridice); consumer to consumer – consumatorii/participanții își vând produsele online reciproc; business to government – companiile pot vinde bunuri și servicii agențiilor de stat (guvernamentale); process to business – evaluarea clienților sau consumatorilor de către companiile de marketing, în același timp repartizând asemenea informații în mod monitorizat cu clienții, furnizorii, angajații și partenerii de afaceri [10, pag. 2].

Scopul prezentului studiu a fost de a prezenta subiecții la o scară mai largă. Astfel, la etapa precontractuală înainte ca cealaltă parte să facă oferta sau să accepte oferta, obligațiile profesioniștilor față de consumatori constau în primul rând în informare detaliată privind etapele încheierii contractului prin mijloace electronice privind următoarele:

- a) pașii tehnici care trebuie urmați pentru a încheia contractul;
- b) dacă profesionistul va genera un document care reprezintă contractul și dacă documentul va fi accesibil;
- c) mijloacele tehnice pentru identificarea și corectarea erorilor comise la introducerea datelor înainte ca cealaltă parte să facă oferta sau să accepte oferta;
- d) limbile în care poate fi încheiat contractul;
- e) toate clauzele contractuale art. 1020 Cod civil al RM.

În cazul în care profesionistul nu îndeplinește obligațiile de informare enunțate anterior la etapa precum încheierii contractului prin mijloace electronice și obligație de a garanta prin punerea la dispoziție a textului în formă electronică, consumatorul are dreptul la revocarea contractului, notificând profesionistul în termen de termenul de revocare este de 14 zile și începe să curgă de la data încheierii contractului. Pentru acțiunile sale profesionistul poartă răspundere în fața consumatorului pentru neexecutarea obligațiilor enunțate anterior.

Cu toate că legislatorul a stabilit rigori stricte al profesionistului, sunt două excepții de la regula generală în cazul în care clauzele care nu au fost negociate individual pot fi incluse prin următoarele metode și anume:

- a) clauzele sînt prezentate celeilalte părți în formă textuală înainte ca acestea să i se permită să încheie contractul, iar ea își dă consimțămîntul expres pentru aplicabilitatea clauzelor și, în final, încheie contractul;
- b) cealaltă parte este informată despre existența clauzelor și i se acordă posibilitatea clar identificabilă să acceseze clauzele înainte de a i se permite încheierea contractului și, în final, să încheie contractul.

Pe lângă obligațiile enunțate anterior profesionistul este obligat să pună la dispoziția consumatorului mijloacele tehnice adecvate, efective și accesibile pentru identificarea și corectare erorilor comise la introducerea datelor înainte ca cealaltă parte să facă o ofertă sau să accepte o ofertă (art. 1021 Cod civil al RM) [1]. În continuare vom prezenta opiniile autorilor vizavi de subiectul colectării informațiilor de la consumatori precum volumul informațiilor solicitate de profesioniști, calita-

tea acestora, datele cu caracter personal, fiind precaut cu obligațiile prevăzute de legislația privind protecția și stocarea datelor cu caracter personal [11].

Ținem să atenționăm că, profesionistul răspunde pentru față de respectiva persoană pentru prejudiciul cauzat prin această neîndeplinire.

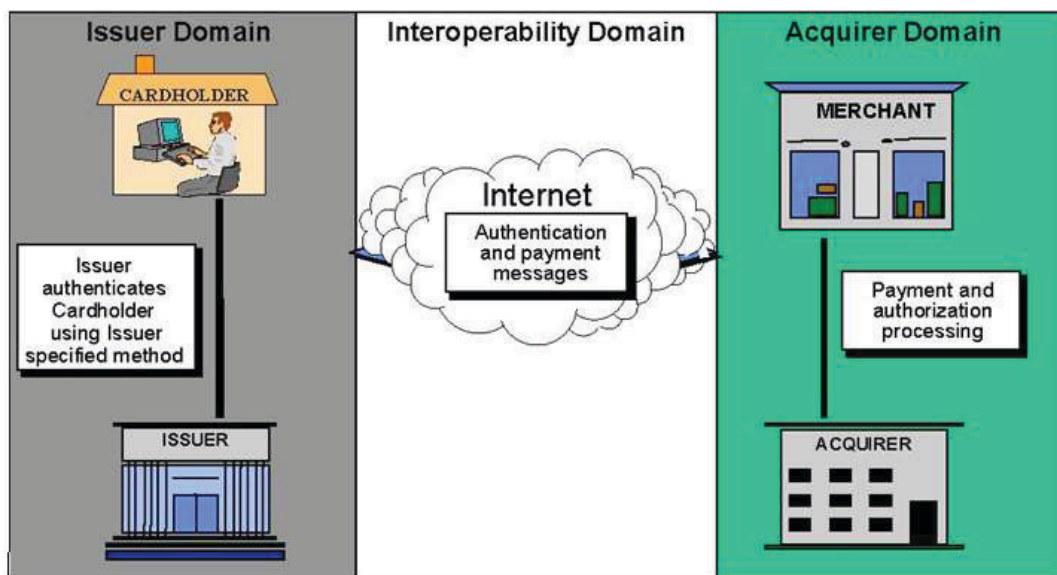
Profesionistul de asemenea are obligația de a confirma prin intermediul mijloacelor electronice, că a recepționat oferta sau acceptarea parvenită de la cealaltă parte la încheierea contractului prin intermediul mijloacelor electronice. În cazul nerecepționării confirmarea sau recepționării întârziate și nejustificate, cealaltă parte are dreptul la revocarea ofertei sau după caz la revocarea contractului, totodată profesionistul poartă răspundere pentru neexecutarea obligației de confirmare a recepției neîntârziată (art. 1022 Cod civil al RM) [1], astfel am expus un risc suplimentar la care este expus atât profesionistul în cazul neexecutării obligațiilor sale importante cât și consumatorul în cazul necunoașterii drepturilor sale. Legislatorul totuși a prevăzut o limitare al obligațiilor enunțate în cazul încheierii contractului prin intermediul poștei electronice sau altor mijloace de comunicare individuală [1].

În lumina celor menționate anterior, a riscurile la care sunt expuse unele părți contractante, vom prezenta unele categorii de mijloace de mitigare a riscurile care au fost identificate. Instituțiile bancare sunt unul din supraveghetorii care monitorizează și într-o oarecare măsură păzesc mijloacele financiare ale depozitarilor săi, în acest sens, luând în considerare riscul sporit de preluare ilegală al datelor personale și utilizării acestor date în detrimentul părților, astfel securitatea cardurilor bancare care sunt cele mai utilizate mijloace de plată, băncile și prestatorii serviciilor de plată elaborează și dezvoltă noi metode de securizare pentru a preveni fraudele. Dintre cele mai răspândite sunt codurile CVC/CVV (cod format din 3-4 cifre, situat pe verso-ul cardului) sau protocolul 3D secure, metodele menționate fiind frecvent utilizate pentru tranzacțiile pe Internet. În continuare vom prezenta schematic și explica rolul 3D secure:

- issuer – emitentul, responsabil de gestionarea serviciului de înregistrare a deținătorului / proprietarului de card, care include verificarea fiecărui deținător de card la înregistrare, și autentificarea deținătorului de card la plata online;
- acquirer – achizitor, asigură că vânzătorul participant la contractul în format online exprimă acordul de voință cu Acquirer și furnizează procesarea tranzacției pentru autentificare;
- interoperability – interoperabilitatea ce facilitează schimbul între două domenii pe baza unui protocol obișnuit și împarte serviciile [10, pag. 12]

În perioada pandemiei băncile au inițiat și dublu sau triplu sistem de verificare, introducerea datelor bancare pe platformele online, verificare prin SMS sau prin email autentificare tranzacției bancare, uneori fiind aplicate ambele filtre.

În continuare prezentăm schematic ceea ce a fost explicat anterior privind sistemul de securitate.



Imagine preluată din Securitatea sistemelor de comerț electronic [10, pag. 13].

În doctrină se pune în discuție aspectul securității sistemelor de comerț electronic, Catalin Zorzini a identificat zonele de risc care pot să apară în comerțul online, fiind prezentate aspectele generale ale securității care este o prioritate în cazul vânzării bunurilor online indiferent de tipul tranzacțiilor chiar și în cazul celor mai simple. De cele mai multe ori departamentele de marketing ale companiilor în domeniul comerțului electronic (CE) solicită informații care nu sunt relevante vânzării, scopul acestor informații fiind: statistice, demografice sau alte informații inutile, spre regret pre-vânzarea probabil nu este spațiul îndreptățit de a solicita astfel de informații. Autorul a venit cu o serie de sugestii privind securitatea care trebuie să fie pe primul plan atât pentru companiile ce activează în sfera comerțului electronic cât și pentru consumatori. În acest sens, au fost prezentate că sunt anumite sfaturi (condiții) în care urmează să fie luate în considerare la colectarea datelor consumatorilor:

a) să nu fie stocate mai multe informații decât scopul actului juridic electronic [12, pag. 1];

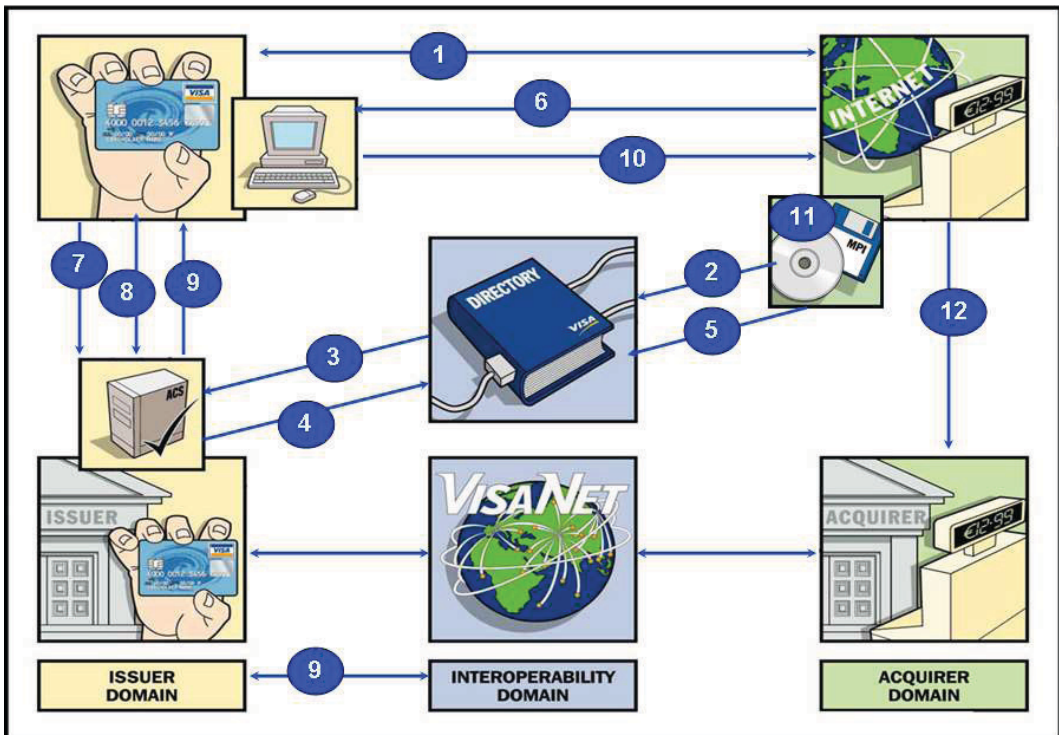
b) în cazul colectării informațiilor sensibile, este necesar de SSL (Secure Socket Layer – fiind cunoscut ca o modalitate de a securiza datele ce sunt colectate prin intermediul platformelor companiilor în domeniul CE pentru a oferi clienților un minim de securitate și protecție, logica SSL costă în faptul că utilizatorul orice acțiuni ar iniția pe site, rămâne în propria sa judecată și nicio persoană străină nu poate interfera în acțiunile acestuia) [13 pag. 1].

c) Luarea deciziilor corecte în cazul tranzacțiilor mari versus tranzacțiile mici, sistemelor de plăți și alți factori importanți. În cazul achiziționării produselor în mediul online este mult mai convenabil de a procesa tranzacțiilor cu volum mai

mare, decât tranzacțiile cu volum redus, și în particular de pe piața internă ce va diminua costurile de livrare și va fi economisit timpul. Spre exemplu, platformele online de achitare a serviciilor cum ar fi Paypal va încasa 4,5% din valoarea tranzacției, suma se va reduce cu volumul mai mare a tranzacției. Selectarea mijloacelor de achitare (sistemele de plăți) a produselor comandate online precum PayPal, Skrill și World Pay, urmează să fie efectuată foarte precaut. Paypal este mega securizat și blochează tranzacțiile la cea mai mici indicii de spălare a banilor, respectiv poate crea unele incomodități mai ales în cazul călătoriilor în alte țări sau utilizarea unor gadgeturi noi [12, pag.1].

d) Verificarea minuțioasă a produselor comandate de utilizatori (consumatori) variază în dependență de produsele solicitate. De exemplu, produsele digitale care se comandă instantaneu (cărțile electronice, programele soft) care se livrează consumatorului (utilizatorului) imediat și mărfurile fizice care necesită a fi livrate și respectiv necesită un control riguros al produsului ales, mărimii, calității, culorii în cazul produselor necomestibile și în cazul celor comestibile comensurabil calităților acestora inclusiv termenul de valabilitate fiind important să fie respectat.

În final autorul sugerează să se renunțe la obiceiurile companiilor mari și anume: "Nu vă spionați clienții; Nu colectați informații de care nu aveți strict nevoie; Protejați informațiile pe care le colectați; Delegați responsabilitatea conformității, dacă este posibil, utilizând procesarea tranzacțiilor cu terți; Examinați comenzile înainte de a expedia produse" [12, pag. 1].



Imagine preluată din Securitatea sistemelor de comerț electronic [10, pag. 15-16].

" Pas 1 – cumpărătorul creează coșul de cumpărături și declanșează procesul de plată;

Pas 2 – Merchant Server Plug-in (MPI) trimite (Primary Account Number) PAN și informații despre device utilizator la Directory Server (DS).

Pas 3 - DS interoghează Access Control Server (ACS). Pentru autentificarea este disponibil PAN și tipul de device. Dacă ACS nu este disponibil DS trimite mesaj la MPI și sare la pas 5.

Pas 4 - ACS răspunde către DS

Pas 5 - DS înaintează răspunsul de la ACS sau cel propriu la MPI.

Dacă nu s-a autentificat procesarea tranzacției se încheie.

Pas 6 - MPI trimite Payer Authentication Request la ACS prin echipamentul cumpărătorului (PC, device mobil..).

Pas 7 - ACS recepționează Payer Authentication Request

Pas 8 - ACS autentifică cumpărătorul utilizând procesele aplicabile la PAN (password, chip, PIN, etc.) și formează Payer Authentication Response message cu valorile corespunzătoare și îl semnează.

Pas 9 - ACS returnează Payer Authentication Response la MPI prin device cumpărător și trimite datele selectate la Authentication History Server (AHS).

Pas 10 – MPI recepționează Payer Authentication Response.

Pas 11 - MPI validează semnatura Payer Authentication Response (fie singur, fie prin pasarea mesajului la un server de validare)

Pas 12 – Comerciantul începe autorizarea cu propriul achizitor [10, pag. 16]."

La finalizarea etapelor menționate achizitorul se autorizează cu un sistem de ex. Visa net și transmite rezultatele comercianților [10, pag. 17]

Concluzii:

În concluzie venim cu anumite recomandări în vederea securizării actelor juridice încheiate în formă electronică, mai nou în legislațiile statelor vecine definite drept contract electronic, după cum urmează:

- este o stringentă necesitate de educare juridică al participanților la actele juridice în formă electronică, educația populației privind securitatea în actele juridice în formă electronică.

- Segregarea informației colectate de către companiile ce activează în domeniul comerțului electronic și simplificarea și reducerea numărului de informații colectate de la utilizatori.

- Problema limitării aplicării semnăturii electronice doar pe teritoriul Republicii Moldova, respectiv în afara hotarelor acestuia este riscul de a nu fi recunoscut, destul de litigioasă procedura de recunoaștere al contractelor încheiate între părțile rezidente, sunt necesare introducerea unor standarde la nivelul incipient bilateral și ulterior la nivel regional respectiv internațional de recunoaștere a semnăturilor electronice.

- Introducerea reglementărilor legislative privind securitatea și riscurile la care sunt expuse părțile la etapa de negociere, încheiere, executare și încetare al actele juridice în format electronic.

Referințe bibliografice:

1. Legea nr.1107 din 22.06.2002. Codul civil al Republicii Moldova. În: *Monitorul Oficial al Republicii Moldova*, nr. 66-75, art.132, din 01.03.2019.
2. Legea cu privire la semnătura electronică și documentul electronic, nr. 91 din 27.06.2014. În: *Monitorul Oficial al Republicii Moldova*, nr. 174-177 art. 397.
3. Codul civil al României [citat 01.12.2021]. Disponibil: <https://www.codul-civil.ro/art-1245-Forma-contractelor-electronice/>
4. Servicii Publice Electronice [citat 10.12.2021]. Disponibil: <https://msign.gov.md/#/>
5. Ce este semnătura mobilă [citat 10.12.2021]. Disponibil: <https://www.orange.md/ro/business/semnatura-mobila>.
6. Servicii utile semnătura mobilă [citat 10.12.2021]. Disponibil: <https://www.moldcell.md/rom/servicii/utile/semn%C4%83tura-mobil%C4%83-1>
7. P „Centrul de Tehnologii Informaționale în Finanțe” [citat 10.12.2021]. Disponibil: <http://pki.ctif.md/>
8. P. „Serviciul Tehnologia Informației și Securitate Cibernetică” [citat 10.12.2021]. Disponibil: <https://semnatura.md/>
9. I.P. Agenția Servicii Publice [citat 10.12.2021]. Disponibil: <http://www.asp.gov.md/ro/node/1430>
10. Securitatea sistemelor de comerț electronic [citat 01.12.2021]. Disponibil: https://moodle.usm.md/pluginfile.php/234547/mod_resource/content/2/Securitatea%20comertului%20electronic.pdf
11. Legea privind protecția datelor cu caracter personal, nr. 133 din 08.07.2011. În: *Monitorul Oficial al Republicii Moldova*, nr. 170-175 art. 492 din 14.10.2011.
12. Zorzini C. Elementele esențiale ale securității comerțului electronic [citat 01.12.2021]. Disponibil: <https://ecommerce-platforms.com/ro/ecommerce-selling-advice/essentials-ecommerce-security>
13. Ivanocs A. Cum să alegeți tipul corect de SSL și furnizor SSL [citat 07.12.2021]. Disponibil: <https://ecommerce-platforms.com/ro/ecommerce-resources/choose-right-type-ssl-ssl-rovider>