O ANALIZĂ A LEGISLAȚIEI DIN DOMENIUL SEMNĂTURILOR ELECTRONICE ȘI A ȘTAMPILELOR DE TIMP

Cristian Marinescu

cristian.marinescu@omicron.at

Universitatea Politehnica *Bucureşti*

Rezumat: Existența unor canale sigure de comunicație s-a dovedit a fi foarte importantă odată cu dezvoltarea rapidă a Internet-ului. Din aceste motive, atât semnăturile electronice cât și ștampilele digitale de timp au căpătat o importanță sporită pentru aplicațiile ce necesită un minim de securitate. Utilizarea acestor tehnici necesită un cadru legal care să asigure echivalența dintre semnăturile olografe și noile metode digitale. Prezentul articol realizează o analiză a problemelor cu care se confruntă legislația din acest domeniu la nivel internațional, european și național, propunând și modalități de îmbunătățire a situației existente.

Cuvinte cheie: legislație, semnături electronice, ștampile digitale de timp.

Abstract: The existence of secure communication channels in the daily use of the World Wide Web has proven to be very important. Therefore, electronic signatures and digital time-stamps have become of critical importance for any application concerned with security. The use of these techniques requires a legal framework, which is essential to securing the equivalence between classic signatures on paper and the new electronic methods. This article presents an analysis of the problems related to international, European and Romanian legislation on electronic signatures, and also discusses possibilities of making improvements to the existing laws.

Keywords: digital time-stamps, electronic signatures, legislation.

1. Introducere

Semnăturile olografe (scrise de mână), reprezintă o practică veche de sute de ani, ce a avut la bază necesitatea societății umane de a încheia înțelegeri sau acorduri pe care părțile semnatare să se oblige a le respecta și, totodată, pentru a conferi documentelor un caracter personal, individual sau de nereprodus. Aceste semnături sunt ataşate unor documente (contracte, operații bancare, scrisori) și sunt utilizate pentru a exprima originea datelor sau acordul semnatarului cu conținutul documentului, care fără această semnătură nu poate fi utilizat în mod curent.

Semnăturile olografe au caracter de unicat prin faptul că sunt create de către ființe umane, fiind totodată uşor de recunoscut, dar aproape imposibil de reprodus. Prin apariția tehnologiilor informaționale, semnătura clasică s-a demodat în mare parte, dar proprietățile și avantajele acesteia au fost recunoscute ca fiind esențiale și pentru protejarea informației utilizate în sistemele informatice.

Semnăturile electronice pot fi considerate echivalentul semnăturilor olografe în lumea informatică, reprezentând o modalitate practică de a semna date în format electronic [1]. Documentul, împreună cu semnătura electronică, poate fi stocat, transmis sau replicat în format electronic. Semnăturile digitale reprezintă o subcategorie a semnăturilor electronice, ele fiind realizate cu ajutorul algoritmilor asimetrici. De aceea, trebuie diferențiat în mod clar între semnăturile electronice și semnăturile digitale. În general, numim semnături electronice, semnăturile realizate cu ajutorul oricărui fel de tehnologie electronică, indiferent de natura acesteia. În schimb, semnăturile digitale presupun utilizarea unor algoritmi cu chei publice în procesul de generare a semnăturilor. Practic, se poate afirma că semnăturile digitale reprezintă o submulțime a mulțimii semnăturilor electronice. La o analiză foarte atentă a cerințelor pe care trebuie să le îndeplinească orice fel de semnături electronice pentru a înlocui în practică semnăturile olografe, se poate observa că singura tehnologie capabilă să pună la dispoziție o soluție este tehnologia semnăturilor digitale, ce se bazează pe infrastructurile cu chei publice.

În practică există o dependență foarte mare între semnăturile digitale și ștampilele digitale de timp. Ștampilele de timp sunt necesare în ciclul de viață al semnăturilor digitale, datorită faptului că pun la dispoziție o metodă de determinare a momentului de timp când semnătura a fost generată. Totodată, semnăturile digitale reprezintă o metodă importantă de realizare a schemelor de ștampile digitale de timp, fiind de cele mai multe ori utilizate pentru realizarea ștampilelor de timp.

Pentru utilizarea într-un cadru legal a semnăturilor electronice și a ștampilelor de timp este foarte importantă înțelegerea aspectelor legale cu care se confruntă acestea și a legislației din acest domeniu. Atât semnăturile digitale, cât și ștampilele digitale de timp pot aduce un real folos în crearea unor servicii electronice sigure, dar fără un cadru legal adecvat nu se poate vorbi despre utilizarea acestora la scară largă.

2. Considerații generale privind legislația în domeniul semnăturilor electronice

Atunci când semnăturile digitale sunt utilizate în practică pentru a înlocui semnăturile olografe există necesitatea unor legi și regulamente noi, pentru a face posibilă o utilizare echivalentă din punct de vedere juridic. Din punct de vedere tehnic, semnăturile realizate trebuie să întrunească aceleași cerințe ca și semnăturile olografe:

- să fie ușor de recunoscut;
- să fie dificil de falsificat;
- să fie ușor de produs.

Procesul de legiferare al semnăturilor digitale a fost și este unul destul de lung și greoi, primii pași în această direcție fiind efectuați în cadrul Asociației Baroului American încă din 1995 [2]. Cu această ocazie, au fost documentate modalitățile tehnice permise de implementare a semnăturilor digitale, cât și condițiile ce trebuie îndeplinite de către acestea pentru a putea fi acceptate din punct de vedere juridic ca echivalent al semnăturilor olografe. În tot acest timp, au existat preocupări în direcția introducerii unui cadru legislativ adecvat, la nivelul mai multor state. În această direcție sunt de remarcat inițiativele internaționale, precum *Model of Law on Electronic Signatures* [3], document redactat de *United Nations Commision on International Trade Law* (UNCITRAL). Parlamentul și Consiliul Europei au aprobat în 1999 documentul *Community Framework for Electronic Signatures* [4], pentru a crea un cadru legislativ adecvat și uniform în Europa, având ca scop reducerea barierelor interstatale ce amenințau să apară chiar și la nivelul continentului european. În Statele Unite ale Americii, a urmat în anul 2000 promulgarea legii *US Electronic Signatures in Global and National Commerce Act* [5], ce are ca scop declarat introducerea semnăturilor digitale în viața economică, politică și publică a cetățenilor Statelor Unite ale Americii.

Trebuie subliniat faptul că doar eforturile susținute la nivel internațional, în cadrul unor organizații precum ONU, au șanse reale de succes. Este foarte important de înțeles faptul că rețeaua globală, Internet-ul, nu cunoaşte granițe în sensul clasic al cuvântului. Un server amplasat într-un stat fără legislație sau cu o legislație laxă în domeniul semnăturilor digitale sau electronice, iese practic de sub jurisdicția națională a autorităților din alte state. De exemplu, un certificat generat de o autoritate aflată într-o astfel de țară nu va îndeplini, cel mai probabil, minimul de cerințe necesare impus de legislația altor state. În cazul unui litigiu, va fi practic dificil, dacă nu chiar imposibil de impus o hotărâre judecătorească, acest fapt fiind dependent și de relațiile și acordurile diplomatice dintre cele două state. Dat fiind faptul că, atunci când navigăm pe Internet, nu se realizează și o autentificare a poziției geografice a server-ului de pe care se aduc datele sau a server-ului ce a generat certificatul, devine lesne de înțeles cât de ușor se pot ocoli chiar și cele mai drastice legi din domeniul semnăturilor electronice.

La elaborarea acestor legi trebuie ținut cont și de aspectele tehnologice. Legislatorul trebuie să decidă dacă va elabora o lege neutră din punct de vedere tehnologic sau va opta pentru dependența tehnologică. Ambele abordări au atât avantaje, cât și dezavantaje. Legea dependentă de o anumită tehnologie va putea ține cont de toate aspectele tehnologice, utilizând la maxim avantajele acesteia. Ea are însă dezavantajul de a nu permite alte tehnologii, limitând practic flexibilitatea, independența și libera circulație a serviciilor, astfel încât soluțiile ce respectă această legislație nu vor putea interacționa cu alte soluții și standarde. Un exemplu în acest sens îl reprezintă legislația Statelor Unite ale Americii. La rândul său, legile neutre permit orice abordare tehnologică, dar nu iau în considerare în nici un fel dezavantajele introduse de realitățile tehnologice. Uniunea Europeană a optat pentru specificarea legislației sale în varianta independentă de orice tehnologie.

În continuare, vom analiza reglementările legislative existente în acest domeniu atât la nivel internațional, la nivel european, cât și la nivel național. O dată cu intrarea României în Uniunea Europeană, se poate observa o apropiere și o compatibilizare a legislației naționale cu cea creată la nivelul Uniunii Europene. Acest proces de armonizare a legislației din acest domeniu a avut și are loc ca urmare a angajamentelor asumate de România ca membru cu drepturi depline în cadrul Uniunii Europene.

3. Legislația internațională

În domeniul legislației internaționale vom analiza pe scurt reglementările valabile în cadrul Organizației Națiunilor Unite. UNCITRAL a elaborat încă din 1996 *Model of Law on Electronic Signatures*, acest model stând la baza mai multor legi naționale (Statele Unite, Australia, Franța etc.). Aceasta a fost modificată și readoptată în forma sa actuală în anul 2001, aducându-se câteva îmbunătățiri

la modelul vechi al legii. Documentul este alcătuit sub forma unui text legislativ, acesta putând fi folosit drept punct de plecare în elaborarea legislațiilor naționale.

Textul cuprinde 12 articole și un ghid de punere în aplicare a legii [3]. Primul articol se ocupă cu sfera de aplicare a legii, enunțând faptul că aceasta se poate folosi ori de câte ori sunt utilizate semnături electronice în cadrul unor activități economice. Articolul 2 se ocupă cu definirea diverșilor termeni, de exemplu certificat, semnatar, semnătură electronică etc., pentru a clarifica și a crea o bază comună de înțelegere a termenilor întâlniți în cadrul modelului de lege. Articolul 3 enunță principiul egalității tehnologiilor, ce permite utilizarea oricăror metode de creare a semnăturilor electronice, atâta timp cât acestea respectă principiile și proprietățile enunțate în articolul 6. În continuare, articolul 4 tratează diverse moduri de interpretare a reglementărilor propuse, subliniind totodată caracterul internațional al legii. În articolul 5 este descrisă autonomia ce este lăsată la latitudinea unui stat, care permite acestuia un anumit grad de flexibilitate în stabilirea unor reguli proprii în procesul de utilizare a semnăturilor. Articolul 6 reglementează condițiile în care o semnătură electronică realizată asupra unui set de date trebuie recunoscută, principala condiție fiind aceea ca semnătura să fie sigură. În cadrul articolului 7 se statuează faptul că, indiferent de tehnologiile utilizate, acestea trebuie să îndeplinească standardele tehnice internaționale, fără a îngrădi însă libertatea fiecărui stat de a alege o altă tehnologie. Articolul 8 reglementează normele de comportament ale utilizatorilor ce creează semnături electronice, pentru a nu permite spre exemplu, utilizarea informațiilor de creare a semnăturilor de către persoane neautorizate. Aceste reguli au ca scop delimitarea răspunderii în cazul compromiterii unor informații confidențiale, ce sunt utilizate pentru generarea semnăturilor electronice. Articolul 9 stabilește un set de reguli de conduită pentru furnizorii de certificate, cât și o serie de cerințe ce trebuie îndeplinite de către aceștia. Articolul 10 stabilește modalitățile prin care un furnizor de servicii de certificare poate determina gradul de încredere atât în sistemele, cât și în personalul ce îi stau la dispoziție. Articolul 11 definește în continuare comportamentul și conduita unei terțe părți (om sau mașină), implicată în procedurile de validare și verificare ale unei semnături electronice. Aceasta trebuie să se asigure că semnătura poate fi verificată și că certificatul era valabil la momentul semnării. Articolul 12 stabilește regulile de recunoaștere a certificatelor și semnăturilor ce provin din altă țară. Modalitatea de stabilire a unui grad de echivalență, din punct de vedere al securității, trebuie făcută în baza unor standarde internaționale.

4. Legislația Uniunii Europene

Pe plan european au existat încă din anii '90 încercări de creare a unui cadru legislativ uniform în domeniul semnăturilor electronice. La sfârșitul anului 1999, Parlamentul și Consiliul Europei au promulgat Directiva 93/1999 asupra semnăturilor electronice [4], recunoscând implicit faptul că acest set de recomandări reprezintă instrumentul principal pentru asigurarea unei baze legislative comune în acest domeniu. Directiva are ca principal scop crearea unui cadru legal uniform la nivelul tuturor statelor membre, acestea având obligația de a crea legi naționale conforme până la sfârșitul anului 2001. Directiva este alcătuită din 14 articole și 4 anexe, fiind enunțată neutru din punct de vedere tehnologic.

Majoritatea statelor din Uniunea Europeană au trecut la implementarea Directivei 93/1999 emisă de Parlamentul European pentru a crea cadrul legal necesar utilizării semnăturilor electronice în practică. La o analiză atentă a stadiului de implementare a Directivei 93/1999 în diverse țări, se pot observa atât problemele ce au apărut datorită procesului de legiferare, cât și problemele legate de aplicarea în practică a tehnologiilor în cauză. Pe baza acestor observații pot fi făcute o serie de recomandări în scopul modificării și îmbunătățirii legislației, ținând cont de aspectele tehnologice, economice și al dezvoltărilor juridice ulterioare, cât și de consecințele practice ale implementării Directivei.

Se pune întrebarea care este de fapt necesitatea reală a semnăturilor electronice? În majoritatea statelor, numărul autorităților de certificare este limitat (una sau două autorități), neexistând practic o piață foarte mare de desfacere a serviciilor oferite de acestea. Majoritatea aplicațiilor ce necesită cu adevărat semnături electronice aparțin domeniului bancar (e-banking), dar cum acestea se desfășoară într-un cadru privat client – bancă, Directiva nu are nici o influență asupra acestora. Există în practică o necesitate destul de mică de a realiza la momentul actual semnături electronice în domeniul public și aceasta se întâmplă, în special, în domeniul e-government. Acest domeniu este cofinanțat și subvenționat în mare măsură de către guvernele diverselor state. Totodată, se poate remarca o anumită reticență a societății civile de a utiliza aceste tehnologii, în special la grupele de persoane peste o anumită vârstă. Se poate însă aprecia faptul că, o dată cu evoluția diverselor tehnologii și a modificării percepției publicului, vor apare modificări ale numărului de persoane ce utilizează semnăturile electronice.

Conform prevederilor Directivei, semnăturile calificate sunt semnături avansate, bazate pe un certificat calificat și generate cu ajutorul unui dispozitiv securizat de generare a semnăturilor. Aceste semnături sunt echivalente, din punct de vedere juridic, cu semnăturile olografe (Figura 1).

În urma unei analize atente, se poate afirma că toate țările Uniunii Europene au transpus în legislația națională Directiva menționată, fiind însă observate deosebiri la nivelul tuturor țărilor. Totodată, o serie de țări ce nu fac parte din Uniunea Europeană sau țări ce aspiră la statutul de membru al Uniunii Europene au preluat Directiva și și-au întemeiat legislația națională pe aceasta [6]. Din punct de vedere tehnic, se poate afirma că Directiva a influențat și procesul de standardizare internațional, comitetele de standardizare ținând cont de recomandările acesteia atât din punct de vedere tehnologic, cât și din punct de vedere al terminologiei.

Majoritatea problemelor ce pot fi observate în legislația națională a diverselor state pot fi atribuite unor interpretări greșite ale Directivei, care conduc însă la neconcordanțe între diferitele legi atunci când se are în vedere depășirea granițelor existente și aplicarea lor în practică. Există însă și câteva cazuri în care se pare că legile naționale au urmărit cu bună știință nerespectarea sau interpretarea diferită a Directivei, în prim plan situându-se probabil interese și raționamente naționale, și nu cele europene. Vom analiza, în continuare, câteva aspecte concrete.

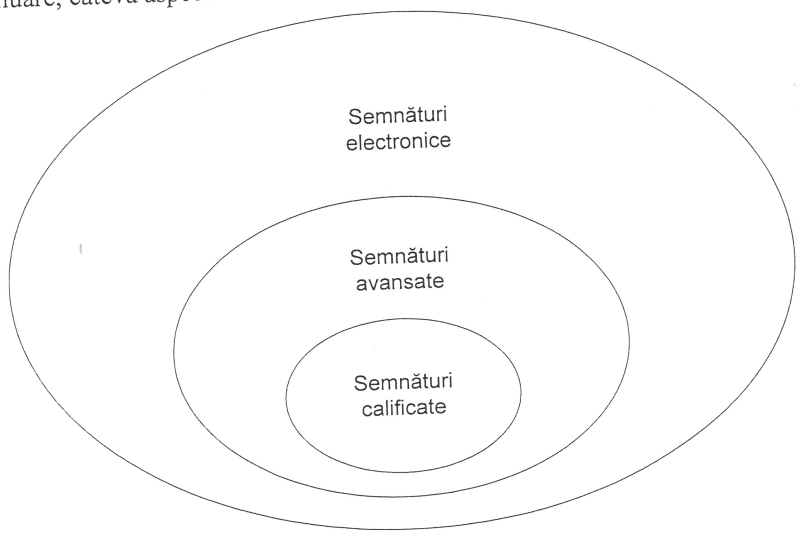

Figura 1. Relația dintre mulțimea semnăturilor electronice, cea a semnăturilor avansate și mulțimea semnăturilor calificate

În privința accesului la piața liberă se poate observa că toate țările europene au deschis piața serviciilor de *Certificate Service Provider* (CSP) și entităților autorizate pe teritoriul altor țări din Uniune, respectând astfel articolul 3.1. Astfel, o autoritate autorizată într-o țară a Uniunii poate oferi servicii de CSP și în altă țară, fără a mai fi necesară parcurgerea procedurii de certificare și în acest stat [6]. Pe de altă parte, unele din statele membre ale Uniunii au apelat la scheme de supervizare a CSP-urilor, scheme foarte asemănătoare cu procedura de autorizare, astfel încât există posibilitatea de a încălca spiritul Directivei și de a ocoli implementarea în practică a articolului 3.1. În momentul de față, nu se pot calcula efectele schemelor de supervizare asupra activităților autorităților CSP, tot ceea ce se poate remarca însă, este că schemele de supervizare diferă foarte mult de la un stat la altul. Deși efectele acestor diferențe este limitat prin faptul că majoritatea CSP-urilor acționează la nivel național, va veni un moment în care aceste diferențe își vor face simțită prezența.

Regula acreditării voluntare din Directivă a fost interpretată greșit de majoritatea guvernelor naționale. Acestea au stipulat în legislațiile naționale posibilitatea ca, în baza schemelor de acreditare voluntară, autoritățile CSP să poată fi verificate dacă întrunesc condițiile cerute de Directivă. De aici rezultă faptul foarte grav că, în multe țări europene, acreditarea voluntară nu mai este de fapt deloc voluntară. Multe din programele naționale nu acceptă decât autorități CSP acreditate, obligând astfel autoritățile să parcurgă procesul de acreditare la nivel național.

Cu privire la capitolul excepțiilor din sectorul public (articolul 3.7), care permite statelor membre să impună condiții suplimentare atunci când semnăturile electronice sunt utilizate în domeniul public, se poate observa și aici o interpretare eronată a Directivei [6]. Este normal ca în fiecare stat să se permită impunerea unor condiții suplimentare (de exemplu, de securitate), dar în majoritatea cazurilor comunicarea dintre cetățeni și instituțiile statului respectiv necesită utilizarea unui certificat calificat. Dat fiind însă faptul că certificatele calificate sunt generate de autorități CSP acreditate, aceste restricții contravin spiritului Directivei și a legilor concurenței de piață.

În ceea ce priveşte desemnarea unei organizaţii responsabile cu evaluarea standardelor de securitate în cadrul echipamentelor de creare a semnăturilor, majoritatea statelor se opun desemnării acesteia, în special datorită greutăţii cu care se efectuează testele de evaluare [7]. Acestea sunt foarte costisitoare, iar producătorii de echipamente se opun, în majoritatea cazurilor, unei certificări, datorită faptului că orice modificare a software-ului sau hardware-ului echipamentului invalidează rezultatele testelor anterioare şi obligă la o nouă evaluare. Datorită acestui fapt, o evaluare este valabilă doar pentru scurt timp, timp în care dispozitivul de semnare trebuie produs exact în versiunea testată, orice îmbunătăţire sau modificare nefiind acceptată, aceasta invalidând evaluarea. Datorită faptului că Directiva impune cerinţe stricte din partea producătorilor de dispozitive hardware de generare a semnăturilor electronice, se poate observa că aceste dispozitive rămân în continuare destul de rare [6]. Trebuie simplificate şi flexibilizate procedurile de verificare a conformităţii şi a securităţii, astfel încât costurile asociate acestor operaţii să fie acceptabile pentru producători. De asemenea, trebuie elaborat un set de reguli pentru organismele naţionale, astfel încât criteriile minime definite să fie respectate, şi totodată să nu fie impuse cerinţe suplimentare.

Majoritatea statelor europene au introdus în legislaţie reguli stricte de recunoaştere a certificatelor calificate, generate pe teritoriul unei alte ţări. Există puţine excepţii (Marea Britanie şi Irlanda) unde nu se face o distincţie clară între certificatele locale şi cele străine. Articolul 8.2 privitor la protecţia datelor a fost implementat diferit în legislaţiile naţionale. În unele state, autoritatea CSP este obligată să respecte reguli stricte de protecţie a datelor, în timp ce în alte state nu există această obligaţie sau există, dar regulile nu sunt atât de stricte [7]. Totodată, doar două state interzic explicit folosirea de pseudonime în cadrul certificatelor.

Se recomandă verificarea compatibilităţii dintre iniţiativele e-government de la nivel naţional şi recomandările Directivei, având în vedere în special legile concurenţei şi ale pieţei libere. În acelaşi timp este necesară o evaluare detaliată a consecinţelor ce vor apare o dată cu utilizarea tot mai frecventă a semnăturilor electronice [6] şi, nu în ultimul rând, este necesar un sprijin cât mai activ al eforturilor efectuate în direcţia îmbunătăţirii interoperabilităţii între diversele programe e-government atât la nivel naţional, cât şi la nivel european.

Procesul de standardizare trebuie încurajat, algoritmi şi protocoale standardizate şi acceptate la nivel internaţional fiind cea mai bună soluţie de a impune standarde comune de securitate. La acest capitol trebuie avute în vedere valabilitatea semnăturilor electronice pe o perioadă cât mai lungă, un rol foarte important avându-l şi ştampilele digitale de timp. Capitolele referitoare la autorităţile CSP şi protecţia datelor trebuie clarificate, pentru a elimina o serie de neclarităţi şi interpretări greşite, strecurate în legile naţionale. Aceste deziderate nu sunt uşor de atins fără eforturi concertate în toate direcţiile mai sus menţionate, mai ales datorită faptului că interesele europene vin deseori în contradicţie cu interesele naţionale ale diverselor state.

Standardele recunoscute şi utilizate în cadrul Uniunii Europene sunt elaborate de organisme de standardizare europene precum *European Committee for Standardization - Information Society Standardization System* (CEN/ISSS) şi *European Telecommunications Standards Institute* (ETSI) împreună cu firme şi experţi din domeniu. Principala responsabilitate a ETSI o constituie infrastructurile şi serviciile de securitate din mediile electronice de comunicaţie, în timp ce CEN/ISSS se ocupă de elaborarea standardelor ce privesc furnizorii de servicii de certificare şi dispozitivele de creare şi verificare a semnăturilor.

Tabelul 1 redă situaţia autorităţilor CSP acreditate şi supervizate în câteva ţări europene la sfârşitul anului 2005 şi începutul anului 2006. Se pot uşor observa discrepanţele apărute la nivelul acestor ţări, chiar dacă legile naţionale cu privire la semnăturile electronice fuseseră emise şi intraseră în vigoare în toate statele analizate de cel puţin 3 ani. Această stare reflectă şi faptul că, în lipsa unei pieţe de desfacere şi a unei cereri de piaţă, au apărut şi au putut să se dezvolte autorităţi CSP doar în ţările care au sprijinit şi subvenţionat dezvoltarea semnăturilor electronice în cadrul unor programe de e-government.

Tabelul 1. Situaţia în domeniul autorităţilor acreditate în diverse ţări europene la nivelul anului 2005/2006

Ţara	Număr CSP acreditaţi (A)	Număr cert. emise de A	Număr CSP supervizaţi (S)	Număr cert. emise de S
Anglia	6	>15.000	4	necunoscut
Austria	5	>100.000	8	necunoscut

Elveția	2	>10.000	3	necunoscut
Germania	29	>230.000	31	necunoscut
Italia	19	>2.000.000	19	necunoscut

Directiva 93/1999 asupra semnăturilor electronice nu este un model de lege perfectă, așa cum ar fi fost de dorit. Ea reprezintă un compromis greu atins prin negocierile celor 15 state, membre ale Uniunii Europene la acea vreme. În condițiile în care între timp numărul statelor membre aproape s-a dublat, ajungând la 27, se poate afirma că atingerea unui compromis nou va fi mult mai dificilă de această dată. Din aceste motive, se recomandă păstrarea Directivei în forma ei actuală, fiind suficient de adecvată pentru a crea legile naționale, putându-se opta pentru o reinterpretare și clarificare a unor articole neclare sau îndoielnice din punct de vedere legal. Este recomandabilă păstrarea Directivei în forma sa actuală cu toate neajunsurile sale, procesul de renegociere a unei noi Directive fiind mult prea complicat.

Directiva a fost concepută pentru a ajuta la crearea unui cadrul general valabil la nivelul Uniunii Europene, pentru a facilita schimbul de produse și servicii fără granițe și fără restricții pe întregul teritoriu al Comunității Europene. Din păcate, acest deziderat nu a fost atins în totalitate, nu atât din cauza unor lipsuri sau erori ale Directivei, ci datorită modului în care aceasta a fost implementată la nivel național de către statele în cauză. Trebuie analizate posibilitățile de a influența statele membre pentru a modifica legile naționale spre o interpretare favorabilă întregii Comunități Europene (de exemplu, prin recomandări ale Comisiei Europene, prin atacarea legilor naționale la Curtea Europeană de Justiție etc.).

5. Legislația națională a României în domeniul semnăturilor electronice și a ștampilelor de timp

România s-a conformat încă din anul 2001 recomandărilor Comisiei Europene, implementând Directiva Europeană 93/1999/EC în cadrul Legii 455 asupra semnăturilor electronice [8]. Această lege constituie un pas major în crearea cadrului legislativ național necesar pentru utilizarea cu succes a semnăturilor electronice. Totodată a fost pusă baza recunoașterii semnăturilor electronice atât la nivel național, cât și la nivel european ca echivalent al semnăturilor olografe. Pe lângă regimul juridic al semnăturilor electronice, legea stabilește și condițiile în care acestea sunt echivalente cu semnăturile olografe, cât și condițiile ce trebuie îndeplinite de cei care doresc să furnizeze servicii de certificare în acest domeniu.

La o analiză atentă se poate observa că legea introduce două concepte, și anume cel de semnătură electronică și cel de semnătură electronică extinsă. Primul tip de semnătură include orice metodă de identificare a semnatarului unui document electronic, în timp ce semnătura extinsă îndeplinește în plus o serie de criterii, care asigură atât o identificare sigură a semnatarului, cât și integritatea documentului semnat. Legea prevede faptul că numai semnătura electronică extinsă, generată cu ajutorului unui dispozitiv securizat și bazată pe un certificat calificat valabil la momentul creării semnăturii, este echivalentă din punct de vedere juridic cu o semnătură olografă. În aceste condiții, trei parametrii de timp sunt foarte importanți, furnizorii serviciilor de certificare având obligația de a menține o bază de date cu evidența certificatelor:

- data și ora exactă a generării certificatului;
- data și ora exactă a expirării certificatului;
- data și ora exactă la care un certificat a fost revocat sau suspendat.

La acești parametrii de timp se adaugă și data și ora exactă la care a fost efectuată semnătura. Toți acești parametrii de timp trebuie realizați cu ajutorul unor autorități de ștampile de timp, conform standardelor recunoscute: ETSI TS 101 861 Ștampilare temporală; ETSI TS 101 733 v1. 2. 2; RFC3161 Internet X.509 Protocol de ștampilare temporală.

Activitatea furnizorilor de servicii de certificare este supravegheată, conform legii, de către Autoritatea de Reglementare și Supraveghere care are următoarele atribuții:

- stabilește reglementările cu caracter general și structura registrului furnizorilor de servicii de certificare;
- stabilește modul de acces la registrul furnizorilor, fiind responsabilă și pentru gestiunea acestuia;
- stabilește conținutul certificatelor calificate și condițiile și procedura de agreare a agenților de omologare a dispozitivelor securizate de generare a semnăturilor electronice;

- stabileşte condiţiile minimale pentru furnizorii de servicii şi furnizorii de servicii cu drept de emitere a certificatelor acreditate;
- stabileşte alte reglementări cu privire la funcţionarea, gestionarea şi implementarea semnăturilor electronice conform legii în vigoare.

Tabelul 2 prezintă situaţia din luna august 2007 în domeniul furnizorilor de servicii de certificare, aşa cum rezultă din informaţiile furnizate de Autoritatea de Reglementare şi Supraveghere. După cum se poate observa, existau la acel moment doar 4 autorităţi CSP, care ofereau certificate simple, şi tot 4 autorităţi CSP, care ofereau certificate calificate, situaţia fiind relativ similară cu state precum Austria sau Anglia.

Tabelul 2. Situaţia furnizorilor de servicii de certificare din România în luna august 2007

Furnizor servicii de certificare	Situaţie furnizor	Tipuri de certificate emise			
		Simple	Calificate, cu distrib. la client	Calificate, fără distrib. la client	Acreditat
E-Sign Software Security SA	încetat activitatea	da	da	da	da
Internet DomReg SRL	operaţional	da	-	-	-
TRANS SPED SRL	operaţional	-	da	-	-
DigiSign SA	operaţional	da	da	da	da
Digital ID Company SRL	operaţional	da	da	da	da
CertSign SRL	operaţional	da	da	da	da

Ca o completare a legii semnăturilor electronice, au fost realizate şi:

- Legea 451/2004 privind marca temporală [9];
- Legea 589/2002 privind regimul juridic al activităţii electronice notariale [10];
- Hotărârea 1259/2001 privind aprobarea normelor tehnice şi metodologice pentru aplicarea Legii 455/2001 privind semnătura electronică [11];
- Legea 365/2002 asupra comerţului electronic;
- Legea arhivării documentelor electronice.

Vom analiza în continuare pe scurt legea 451/2004, care stabileşte cadrul de funcţionare al autorităţilor ce se ocupă cu generarea mărcilor de timp (ştampilelor de timp) şi regulile ce trebuie respectate pentru ca acestea să fie recunoscute din punct de vedere juridic. Legea conţine 15 articole, articolul 2 ocupându-se cu definirea diverşilor termeni, de exemplu certificat, amprentă, ştampilă temporală etc., pentru a clarifica şi a crea o bază comună de înţelegere.

Se poate observa că legiuitorul a optat pentru menţinerea unei forme generale a definiţiilor, independente de tehnologie, astfel încât să nu se ajungă la o discriminare a unor tehnologii faţă de altele. Cu toate acestea, în cadrul articolului 2, litera c, se vorbeşte despre certificatul asociat ştampilei de timp, astfel încât se ajunge involuntar la o îngustare a posibilităţilor tehnologice. Este de remarcat faptul că, la ora actuală, atât în ceea ce priveşte semnăturile electronice, cât şi ştampilele de timp, singurele metode de a îndeplini condiţiile impuse de legile menţionate sunt semnăturile digitale şi ştampilele digitale de timp. Cu toate acestea, este foarte importantă păstrarea neutralităţii textului juridic, mai ales în condiţiile în care această neutralitate a fost declarată o prioritate încă de la început.

Articolul 3 defineşte elementele pe care o ştampilă trebuie în mod necesar să le conţină:

- amprenta ataşată documentului electronic;
- data şi momentul de timp la care a fost creată ştampila, exprimate în timp universal;
- informaţiile care identifică în mod unic furnizorul ştampilei temporale;
- numărul de ordine (identificatorul) din registrul furnizorului de servicii de ştampilare temporală.

Totodată, se definesc informaţiile verificate la furnizorul ştampilei, acestea fiind:

- elementele de identificare ale certificatului cu a cărui cheie publică asociată se verifică ştampila;
- identificarea algoritmului utilizat pentru generarea amprentei.

Ştampila de timp poate conține și elemente de identificare ale solicitantului. În continuare, articolele 4 până la 8 stabilesc un set de reguli și condiții ce trebuie îndeplinite de către autoritatea de ştampilare, astfel încât ştampilele generate de aceasta să fie sigure, iar recunoașterea în fața legii să fie garantată. Articolele ce urmează definesc răspunderea în fața legii a furnizorului de servicii, amenzile ce pot fi aplicate în diverse cazuri, cât și faptul că Autoritatea de Reglementare și Supraveghere este organismul abilitat de supraveghere a domeniului în cauză.

6. Concluzii asupra situației legislative actuale

Tehnologia informației a evoluat în ultimele decenii cu o viteză uluitoare, depășind posibilitățile societății umane de a reacționa și accepta schimbările majore petrecute în ultimul timp. Semnăturile electronice pun la dispoziție un înlocuitor digital pentru semnăturile olografe. În acest context, ştampilele de timp reprezintă un mecanism foarte important, fără de care utilizarea semnăturilor electronice nu poate avea succes.

Lipsa unor originale electronice este o trăsătură ce deosebește în mod fundamental metodele vechi de a păstra documentele pe hârtie, de metodele electronice. În aceste condiții legile existente până de curând nu pot face față situației, fiind necesară introducerea unor legi noi, care să țină cont de noua situație creată. Sunt necesare tehnologii standardizate la scară internațională pentru a asigura o interoperabilitate ridicată, o recunoaștere națională și internațională, dar mai ales un nivel de securitate ridicat, fără de care semnăturile electronice nu își vor atinge scopul.

La o analiză atentă a situației legislative existente la momentul actual la nivel european se poate observa faptul că au fost făcuți o serie de pași importanți în direcția creării unui cadru legal pentru semnăturile electronice. Situația actuală este însă departe de a fi ideală. Se observă în practică încercări timide de utilizare a semnăturilor electronice la nivel național, dar acestea nu depășesc limitele impuse de granițele naturale ale statelor. Atâta timp cât vor exista diferențe legislative la nivelul continentului european, va fi greu de realizat o utilizare transfrontalieră, dificultățile din planul juridic răsfrângându-se în final asupra gradului de utilizare a semnăturilor electronice și a ştampilelor de timp.

Bibliografie

1. **BROWN, P.W.**: Digital Signatures: Are They Legal for Electronic Commerce? IEEE Communications Magazine, Vol. 32, No. 9, 1994, pp. 76-80.
2. * * *: American Bar Association, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Electronic Commerce, 1995, http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html
3. * * *: UNCITRAL, Model Law on Electronic Signatures with Guide to Enactment, 2001, http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html
4. * * *: The European Parlament and the European Council, Directive 1999/93/EC on a Community framework for electronic signatures, 1999, http://www.ictsb.org/EESSI/Documents/e-sign-directive.pdf
5. * * *: US Congress, US Electronic Signatures in Global and National Commerce Act, 2001, http://www.ftc.gov/os/2001/06/esign7.htm
6. **DUMORTIER, J., S. KELM, H. NILSSON, G. SKOUMA, P. VAN EECKE**: The Legal and Market Aspects of Electronic Signatures, Interdisciplinary centre for Law & Information Technology, Katholieke Universiteit Leuven, 2003.
7. **HOCHMANN, S.**: Elektronische Signatur. Technische Darstellung, rechtliche Entwicklung, und praktischer Einsatz anhand von Beispielen, Books on Demand, 2001.
8. * * *: Parlamentul României, Legea nr. 455/2001 privind semnătura electronică, Monitorul Oficial, nr. 429, 2001.
9. * * *: Parlamentul României, Legea nr. 451/2004 privind marca temporală, Monitorul Oficial, nr. 1021, 2004.
10. * * *: Parlamentul României, Legea nr. 589/2004 privind regimul juridic al activității electronice notariale, Monitorul Oficial, nr. 1227, 2004.
11. * * *: Guvernul României, Hotărârea 1259/2001 privind aprobarea normelor tehnice și metodologice pentru aplicarea Legii 455/2001 privind semnătura electronică, Monitorul Oficial, nr. 847, 2001.