ANALELE ŞTIINŢIFICE
ALE
UNIVERSITĂŢII "ALEXANDRU IOAN CUZA"
DIN IAŞI

(SERIE NOUĂ)

ŞTIINŢE JURIDICE

TOM LXIII Nr. II - 2017

EDITURA UNIVERSITĂŢII "ALEXANDRU IOAN CUZA"
IAŞI

Volumul are bază lucrările Conferinței *Perspective juridice asupra Internetului*, care s-a desfăşurat în data de 28 octombrie 2017 la Universitatea „Alexandru Ioan Cuza" din Iaşi, în cadrul evenimentului „Dies Academici".

Organizarea Conferinței a fost coordonată de Profesor dr. Carmen Tamara Ungureanu, Conferențiar dr. Ioana Maria Costea și Lector dr. Nicolae Horia Țiț.

ISSN-L 1221-8464

ANALELE ŞTIINTIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ŞTIINȚE JURIDICE, 2017, NR. II

C U P R I N S

SCIENTIFIC ANNALS OF „AL. I. CUZA" UNIVERSITY OF IAȘI
TOMUL LXIII, JURIDICAL SCIENCES, 2017, NR. II

TABLE OF CONTENTS

ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

IMPLICAȚIILE INTERNETULUI ÎN VIAȚA JURIDICĂ

THE IMPLICATIONS OF THE INTERNET IN LEGAL LIFE

CARMEN TAMARA UNGUREANU[1]

Rezumat: Prin lucrarea *Implicațiile Internetului în viața juridică* se urmărește o prezentare generală a domeniilor juridice în care Internetul este prezent, insistându-se asupra contractelor încheiate online, protecției datelor cu caracter personal, soluționării litigiilor online și a acelora la care dă naștere cea mai utilizată rețea de socializare, Facebook.
Cuvinte-cheie: Internet, contracte online, protecția datelor cu caracter personal, Facebook

Abstract: Through *The Implications of the Internet in Legal Life*, a general overview of the legal domains in which the Internet is present is aimed, insisting on contracts concluded online, personal data protection, online dispute resolution and litigation of the most commonly used social network, Facebook.
Keywords: Internet, online contracts, personal data protection, Facebook

Introducere

Internetul este omniprezent. Toți suntem utilizatori de Internet, fie în viața noastră privată, fie și în activitatea noastră profesională. De regulă, juriștii nu se întreabă ce este Internetul și nici cum funcționează el, ci se mărginesc doar să-l folosească, în diferite scopuri personale și profesionale.

Puțini dintre noi sunt aceia care au cunoștințe de informatică. Internetul a fost conceput pentru a fi utilizat de oricine. Și poate tocmai de aceea, Internetul prin multiplele lui implicații în lumea juridică, în toate domeniile, conduce și la apariția de probleme juridice. Soluționarea acestor probleme nu este lipsită de dificultăți, deoarece informatica este cu mulți pași înaintea dreptului, a reglementărilor juridice. Evoluția tehnologiei are un ritm atât de rapid, încât provoacă limitele legislației.

[1] Profesor univ. dr., Universitatea „Alexandru Ioan Cuza" din Iași, Facultatea de Drept, e-mail: carment_ungureanu@yahoo.com

Soluții există și juriștii au acest talent, de a le găsi.

Unde folosim Internetul? Cel mai simplu răspuns este: în toate domeniile, care au legătură cu dreptul. Pe scurt, prin intermediul Internetului se încheie contracte, fie că părțile sunt consumatori sau profesioniști, se colectează și se prelucrează date cu caracter personal, este pus în discuție dreptul la proprietate intelectuală, concurența loială, salariații pot deveni telesalariați, muncind „de acasă" (teleworking), se fac declarații de impozit online prin *e-guvernare*, se fac plăți, se fac investiții, are loc cyberbullying, se joacă jocuri de noroc, se eliberează rețete, publicitatea se face eficient prin intermediul așa numiților „*influencers*"[2], prin aplicația Uber se asigură servicii de transport, se cumpără medicamente din farmacii online, se dau consultații medicale, se face publicitate, se fură bani, iar Facebook reunește o mare parte din toate acestea, și în plus, oferă nemurirea.

Pentru că nu pot fi detaliate toate aceste teme, voi încerca o prezentare succintă a „infiltrării" Internetului în drept, oprindu-mă la câteva domenii.

1. Internetul și contractele[3]

Perioada în care contractele se încheiau printr-o strângere de mână, în care părțile contractante se întâlneau personal și în care reputația și respectul erau în joc, în caz de neexecutare a obligațiilor contractuale, a trecut. În prezent, părțile, într-o societate în care totul se desfășoară cu viteză, nu se mai întâlnesc față în față, mai ales în cazul contractelor în care una dintre părți este consumator.

Evoluția tehnologiei informației a influențat și modalitățile de încheiere a contractelor. Prin mijloacele electronice, profesioniștii și consumatorii au acces nu numai la o piață limitată de granițele unui stat, ci la piața mondială. Utilizarea mijloacelor electronice la încheierea contractelor

[2] *Influencers* sunt persoanele, care prin intermediul rețelelor sociale (YouTube, Instagram, Twitter, Snap), promovează produse și servicii, frecvent fără a le „eticheta" ca reclame, modelând atitudinile audienței. Utilizarea în comerțul electronic a „influențatorilor" este un fenomen în dezvoltare accelerată la nivelul mondial al marketing-ului. Pentru detalii, a se vedea, C. Abidin, M. Ots, *Influencers Tell All?Unravelling Authenticity and Credibility in a Brand Scandal*, în M. Edstrǿm, A.T. Kenyon, E.-M. Svensson (eds.), *Blurring the lines, Market-Driven and Democracy-Driven, Freedom of Expression*, Nordicom 2016, p. 153 și urm., [Online] la:www.nordicom.gu.se, accesat 23.10.2017.

[3] Pentru o prezentare detaliată, a se vedea, C.T. Ungureanu, *Contractul electronic*, în revista „Dreptul" nr. 9/2015, pp. 158-185.

prezintă mari avantaje: profesioniștii pot face publicitate produselor și serviciilor lor pe plan național și mondial, pot comunica informații referitoare la prețuri și condiții de livrare, folosind resurse financiare minime în acest scop și având asigurată o celeritate maximă, iar cei interesați, consumatori sau profesioniști, având posibilitatea de a alege dintr-o multitudine de oferte, pot accepta condițiile, totul în mod electronic.

Pentru a utiliza Internetul ca mijloc electronic de încheiere a unui contract, părțile trebuie să aibă o conexiune la Internet. Pentru a avea o conexiune este necesară încheierea unui contract cu un furnizor de acces la Internet. Acest contract este de *prestări servicii* și este contra cost. Există și o excepție, când accesul la Internet este pseudogratuit și anume atunci când utilizatorul are acces la rețeaua Wi-Fi, în hoteluri, restaurante, aeroporturi, ș.a. acces inclus, de regulă, în serviciile prestate clientului în temeiul unui alt contract (de hotelărie, de alimentație publică, de transport).

Prin urmare, este vorba despre două contracte: contractul încheiat de fiecare dintre părțile contractante ale contractului electronic cu un furnizor de acces la Internet și contractul electronic propriu zis, care, în principal, poate fi de vânzare sau de prestări servicii. De exemplu, dacă un consumator român cumpără produse de la un magazin virtual, cum este H&M online, Benvenuti online, mai întâi trebuie să aibă conexiune la Internet, pe care o poate obține, de exemplu, de la Telekom, Vodafone și apoi poate perfecta contractul de vânzare, prin intermediul conexiunii la Internet.

Prin urmare, Internetul are două componente: infrastructura în care este transmis conținutul și a doua componentă este formată din conținutul însuși. Infrastructura este reglementată de dreptul telecomunicațiilor, iar conținutul este supus diferitelor reglementări, în funcție de domeniul din care face parte, cum ar fi dreptul civil, dreptul comercial, dreptul comerțului internațional, dreptul muncii, ș.a.

Contractele încheiate prin Internet pot fi clasificate după mai multe criterii.

După modul de încheiere, sunt contracte *click-wrap* sau *click-through*; contracte *browse-wrap*și contracte care poartă o semnătură electronică extinsă calificată. Cele mai utilizate sunt contractele *click-wrap*.

▪ *Contractele click-wrap sau click-through* sunt acele contracte de adeziune pentru încheierea cărora destinatarul unei oferte făcută online (pe Internet) trebuie doar să bifeze într-o casetă (să facă un simplu click pe o pictogramă), butonul „Da”, „I accept”, „Yes” sau „I agree”, ori altul similar

și contractul se perfectează. Atunci când la încheierea unui contract de adeziune tradițional aderentului i se cere să semneze contractul, acesta poate ezita, cunoscând sau măcar intuind implicațiile juridice ale semnăturii sale olografe. Dacă i se cere doar să bifeze într-o casetă nu va ezita s-o facă, deoarece, cel mai frecvent, nu conștientizează că încheie un contract[4]. De asemenea, de cele mai multe ori nu citește contractul. De exemplu, în 2012, magazinul online GameStation din Marea Britanie a făcut un experiment: a inclus în contract (care în cazul contractelor încheiate prin Internet se numește „Termeni și Condiții") o clauză prin care cei care făceau o comandă online acceptau să transfere pe vecie și sufletul lor; cei care nu doreau să-și transfere sufletul, puteau să bifeze un buton și să primească un cupon-cadou de 5 lire; numai 12% din clienți au bifat butonul respectiv[5]. Cu trecerea timpului, situația nu s-a ameliorat, dimpotrivă. În iulie 2017, compania Purple din Manchester, care oferă *Wi-Fi hotspots* pentru mai multe întreprinderi, printre care *Legoland*, *Outback Steakhouse* și *Pizza Express*, a inclus timp de două săptămâni o clauză în contract (Termeni și Condiții), prin care persoanele care accesau *Wi-Fi (*gratuit) și semnau contractul erau obligate să presteze 1000 ore de muncă în folosul comunității, constând, mai ales, în curățarea toaletelor la festivaluri, eliminarea gumei de mestecat de pe străzi și desfundarea manuală a canalizării. Purple a oferit, de asemenea, un premiu pentru oricine a citit efectiv termenii și condițiile și a semnalat „clauza de serviciu comunitar". Doar o persoană din 22.000 l-a primit[6].

Contractele click-wrap sunt contracte prin care se achiziționează bunuri sau servicii.

▪ *Contractele browse-wrap* sunt acelea care se încheie prin simpla folosire a unei pagini de Internet (website) sau printr-o anumită acțiune a

[4] E. Mik, *The Unimportance of being "electronic" or – popular misconceptions about "Internet contracting"*, în „International Journal of Law and Information Technology", vol. 19, nr. 4/2011, p. 327.

[5] J.T. Calloway, *Cloud computing, clickwrap agreements, and limitation on liability clauses: a perfect storm?*, în „Duke Law and Technology Review", vol. 11, nr. 1/2012, p. 163-164, [Online] la:

http://scholarship.law.duke.edu/cgi/ /viewcontent.cgi?article=1232&context=dltr, accesat 2.07. 2017.

[6] [Online] la: https://purple.ai/purple-community-service/, accesat 15.10. 2017.

utilizatorului pe pagina respectivă, care echivalează cu acceptarea condițiilor și clauzelor contractuale impuse de furnizorul website-ului[7].

Aceste contracte, de regulă, nu sunt contracte prin care se achiziționează bunuri sau servicii, ci contracte prin care utilizatorul consimte la instalarea unor „spioni" (spyware) pe computerul personal, cum sunt așa numitele *cookies*, care spionează preferințele utilizatorului sau contracte prin care utilizatorul acceptă să îi fie colectate datele personale (de exemplu, toate aplicațiile software oferite utilizatorilor de un furnizor de servicii informatice, cum este de exemplu, Google, aparent gratuit, presupun transferul datelor cu caracter personal către furnizorul de astfel de servicii), ori contracte care permit deeplinking-ul. Deeplinking înseamnă legătura (link-ul) de pe un site web către o pagină a unui alt site, alta în afară de pagina principală.

Recent, în SUA, contractele *browse-wrap* au fost considerate valabile și în alte situații. În septembrie 2017, o instanță americană, în cauza *Meyer v. Uber Technologies, Inc*., a considerat valabil încheiat un contract *browse-wrap* prin care utilizatorul doar a putut constata că există Termeni și Condiții disponibili via *hiperlink*, chiar dacă nu și-a dat acordul expres și nici nu i-a citit[8]. Instanța, astfel, a considerat aplicabilă clauza de arbitraj inserată în Termeni și Condiții.

Multe site-uri folosesc ambele forme de contractare, adică atât *click-wrap*, cât și *browse-wrap*, iar altele le combină într-un hibrid de contract *clickbrowse-wrap*, ceea ce produce confuzii pentru utilizatori, iar în caz de litigii, și pentru instanțele de judecată[9]. De exemplu, în cauza *Fteja v. Facebook* din 2012 instanța a apreciat că Termenii și Condițiile Facebook reprezintă un fel de contract *browse-wrap*, pentru că Termenii sunt vizibili via *hiperlink*, dar, de asemenea prezintă caracteristici de contract *click-wrap*,

[7] Pentru detalii, a se vedea, E. Macdonald, *When is a contract formed by the browse-wrap process?*, în „International Journal of Law and Information Technology", vol. 19, nr. 4/2011, p. 285 și urm..

[8] [Online] la: https://www.metzlewis.com/recent-decision-provides-guidance-making-browsewrap-agreements-enforceable/, accesat 18.10. 2017.

[9] N.S. Kim, *Wrap contracting and the online environment: Causes and cures*, în J.A. Rothchild (editor), *Research Handbook on Electronic Commerce Law*, Edward Elgar Publishing, Massachusetts, USA, 2016, pp. 25-26.

deoarece utilizatorul trebuie să apese pe butonul *Sign up* pentru a consimți cu privire la termenii la care trimite *hiperlink*-ul[10].

Un alt exemplu, pe site-ul companiei aeriene *Ryanair*,actualizat 2017[11], după selectarea zborului pentru care se urmărește achiziționarea unui bilet de avion online, apare avertizarea: „Printr-un click pe *Mai departe*, sunt de acord cu Condițiile de utilizare a paginii de internet"; aceasta înseamnă că se exprimă consimțământul pentru încheierea unui contract *clickbrowse-wrap*, chiar dacă aceste condiții din *hiperlink* nu sunt citite sau măcar parcurse.

▪ *Contractele care poartă o semnătură electronică extinsă calificată*.

Semnătura electronică extinsă este bazată pe un certificat calificat și generată prin intermediul unui dispozitiv securizat de creare a semnăturii (semnătură electronică extinsă calificată). Acest tip de semnătură electronică este asimilat semnăturii olografe. Pentru a obține un certificat calificat, persoana fizică sau juridică trebuie să se adreseze unui furnizor de servicii de certificare, să semneze un contract cu respectivul furnizor, pe baza căruia i se eliberează un certificat (creat pe baza datelor din formularul de solicitare a certificatului) și dispozitivul de creare a semnăturii electronice, valabil pentru un an de zile, contra unei sume de bani. După parcurgerea procedurii, persoana fizică sau juridică poate transmite documente în formă electronică, având atașată o semnătură electronică extinsă calificată. Destinatarul documentelor electronice folosește o așa numită cheie publică a expeditorului din certificatul acestuia, pentru a decripta semnătura expeditorului. Pentru o mai mare siguranță, destinatarul poate consulta și Registrul furnizorilor de servicii de certificare pentru semnătură electronică pentru a obține cheia publică a furnizorului de servicii de certificare, necesară verificării semnăturii furnizorului de pe certificatul expeditorului.

Procedura este relativ complexă. În prezent, furnizorii sunt acreditați de către Ministerul Comunicațiilor și Societății Informaționale și sunt înscriși pe o listă ce poate fi consultată online[12].

Semnătura electronică extinsă calificată nu se utilizează pe scară largă în România datorită complexității ei și a faptului că presupune anumite

[10] N.S. Kim, *op. cit.*, p. 26.

[11] [Online] la: https://www.ryanair.com/ro/ro/, accesat 18.10.2017.

[12] [Online] la: https://www.comunicatii.gov.ro/semnatura-electronica/, accesat 13.10.2017.

costuri. Încheierea de contracte între consumatori şi profesionişti, precum şi între profesionişti, dar care nu au o valoare foarte mare, nici nu justifică folosirea semnăturii electronice extinse calificate. Se justifică doar atunci când contractele au un obiect de o valoare mare, pentru a avea siguranța probării lor. De exemplu, este indicată în contractele de stat, încheiate între stat/instituție de stat şi un profesionist (investitor) (*Government to Business* - G2B).

Semnătura electronică extinsă calificată este impusă de lege în raporturile dintre profesionişti şi stat, în mai multe domenii, cum este acela al furnizării de servicii medicale[13], la depunerea declarațiilor vamale[14], în cadrul Sistemului Electronic de Achiziții Publice (SEAP), ș.a.

Aceste contracte nu sunt dintre cele mai obișnuite în achiziționarea de bunuri sau servicii online. Majoritatea contractelor în formă electronică se încheie prin simpla manifestare de voință a aderentului, utilizând semnătura electronică simplă. Semnătura electronică simplă reprezintă date în formă electronică, care sunt ataşate sau logic asociate cu alte date în formă electronică şi care servesc ca metodă de identificare (art. 4 pct. 3 din Legea 455/2001 privind semnătura electronică[15]); de exemplu, scrierea numelui la sfârşitul unei corespondențe pe e-mail, identificarea putându-se face în acest caz nu atât prin nume, cât prin adresa de e-mail a expeditorului.

După *obiect*, contractele electronice încheiate prin Internet pot fi:

- *Contracte de vânzare* având ca obiect bunuri corporale sau incorporale; în cazul bunurilor corporale, regulile comerțului electronic se aplică numai în faza de încheiere a contractului, deoarece executarea se face prin metode tradiționale[16]; de exemplu, dacă se cumpără o carte oferită spre vânzare online, livrarea se va face prin poștă sau prin curier, iar plata se

[13] H.G. nr. 205/2015 privind modificarea şi completarea H.G. nr. 400/2014 pentru aprobarea pachetelor de servicii şi a Contractului-cadru care reglementează condițiile acordării asistenței medicale în cadrul sistemului de asigurări sociale de sănătate pentru anii 2014-2015, publicată în M.Of. nr. 208, 30.03.2015.

[14] Companiile care depun declarații sumare de intrare prin aplicația ICS-RO (aplicația informatică a autorității vamale) pentru mărfurile ce urmează a fi introduse în Uniunea Europeană prin birourile vamale din România au obligația de a utiliza semnătura electronică extinsă începând cu data de 1 martie 2015, conform Ordinului Agenției Naționale de Administrare Fiscală nr. 2781/2014, publicat în M.Of. nr. 672, 12.09.2014.

[15] Republicată în M.Of. nr. 316, 30.04.2014.

[16] M. Tudorache, *Contractul încheiat prin mijloace electronice, în reglementarea din noul Cod civil*, Editura C. H. Beck, București, 2013, p. 69.

poate face fie prin mijloace electronice, de exemplu, cu card de credit, care este și regula, sau la livrare, în numerar; dacă se cumpără o carte în format electronic (e-book), care reprezintă un bun incorporal, regulile comerțului electronic se aplică, atât pentru faza încheierii contractului, cât și pentru aceea a executării lui; cartea în format electronic va fi livrată online (prin intermediul Internetului) și plata se va face prin mijloace electronice de plată; este, însă, posibil ca produsul cumpărat (e-book) să fie livrat pe un suport material (pe un CD sau DVD), caz în care va fi considerat un bun corporal.

- *Contracte având ca obiect prestări de servicii*; de exemplu, contractul prin care se încheie un contract de transport aerian, prin achiziționarea online a unui bilet de avion; contractul de prestări servicii este reglementat de normele generale din materia contractelor sau a acelora speciale din domeniul în care se utilizează (dacă există), cum ar fi reparații, transporturi, hotelărie, de servicii informatice, ș.a.

Contractele de finanțare, cum este de exemplu, contractul de *crowdlending* sau contractul de *reverse factoring* ar putea intra în categoria contractelor de prestări servicii.

Contractul de *crowdlending* / *crowdfunding/ peer to peer lending– P2P lending*(de multifinanțare)[17] este un contract de împrumut, care se încheie prin intermediul unei platforme online. Poate avea un scop personal sau profesional. Împrumuturile de tip P2P reprezintă o alternativă directă la un împrumut bancar, cu diferența că, în loc să împrumute dintr-o singură sursă, companiile și persoanele fizice pot împrumuta direct de la zeci, uneori sute de persoane. *Zopa* este prima platformă înființată în acest scop în 2005 în Marea Britanie. În Europa, în prezent, deși marea majoritate a împrumuturilor P2P este concentrată în Marea Britanie - care reprezintă peste 84% din întreaga piață europeană –în Germania, Franța și în țările nordice se înregistrează o creștere semnificativă[18].

În ultimii ani, aceste împrumuturi s-au transformat în scheme complicate de finanțare, utilizate, mai ales, pentru întreprinderile mici și mijlocii și pentru *start-up*-uri (întreprinderi noi).

---

[17] R. Kulms, *Multifinanțarea sau crowdlending-ul – o alternativă la banking*, în Revista română de drept privat, nr. 2/2017, p.53 și urm.

[18] [Online] la: http://fintechnews.ch/p2plending/europes-top-11-peer-to-peer-lending-platforms/4960/, accesat 13.10.2017.

Contractul de *reverse factoring. Factoring*-ul este operațiunea prin care o întreprindere, numită aderent, transmite unei societăți specializate/instituție bancară, numită *factor*, creanțele sale născute din vânzarea de bunuri sau prestarea de servicii, iar factorul asigură întreprinderii, finanțarea și urmărirea creanțelor acesteia. De regulă, contractul se încheie cu privire la un ansamblu de creanțe (și nu cu privire la o creanță unică).

Reverse factoring-ul este operațiunea care presupune participarea celor trei părți din *factoring* (aderentul, care este creditorul, adică furnizorul de bunuri sau servicii, factorul, care este o instituție financiară, de regulă o bancă, și debitorii, care sunt cumpărătorii sau beneficiarii serviciilor) și utilizarea unei *platforme electronice*, prin intermediul căreia are loc managementul facturilor și finanțarea aderentului prin plata în avans a facturilor, în considerarea bonității debitorilor[19]. Este factoring invers pentru că inițiatorul acestui program este debitorul și nu aderentul. Debitorul centralizează toate facturile creditorilor săi pe platforma finanțatorului (factorului) și îl mandatează pe acesta să facă plățile către toți creditorii înregistrați pe platformă. În acest mod, debitorul, oferind finanțare creditorilor săi prin intermediul factorului, poate obține condiții mai bune de plată de la furnizorii săi.

Tot contracte de prestări servicii sunt și contractele având ca obiect un conținut digital. Contractul având ca obiect un conținut digital (sau contractul pentru furnizare/livrare de conținut digital) este un contract a cărui denumire apare pentru prima oară în legislația din România, în O.U.G. nr. 34/2014 privind drepturile consumatorilor în cadrul contractelor încheiate cu profesioniștii[20]. Potrivit art. 2 punctul 11 din acest act normativ, conținut digital înseamnă „acele date care sunt produse și livrate în formă digitală".

Această definiție a conținutului digital este foarte largă, scopul fiind acela de a acoperi o mare varietate de situații care implică furnizarea de date în formă digitală[21]. Astfel, prin conținut digital se înțeleg acele date care sunt

[19] I. Regenbogen, *Reverse factoring- funding the un-fundable*, înRevistaromână de dreptprivat, nr. 2/2017, p. 115 șiurm.

[20] O.U.G nr. 34/2014, publicată în M.Of. nr. 427, 11.06.2014, reprezintă transpunerea în legislația națională a Directivei 2011/83/UE privind drepturile consumatorilor.

[21] A se vedea, Ghidul de aplicare a Directivei 2011/83/UE (*DG Justice Guidance Document*, concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and

produse și livrate în formă digitală, cum sunt programele de calculator, aplicațiile, jocurile, muzica, înregistrările video sau textele, indiferent dacă sunt accesate prin descărcare (*downloading*) sau prin flux continuu (*streaming*), de pe un suport material sau prin orice alte mijloace.

Spre deosebire de contractele de vânzare și acelea de prestări servicii, în care consumatorul plătește sau se angajează să plătească prețul (art. 2, punctele 5 și 6 din O.U.G. nr. 34/2014), în cazul contractelor de livrare de conținut digital, nu există prevederi referitoare la preț. Deși acestea au caracteristicile unui contract de prestări servicii, frecvent, furnizorul de conținut digital nu pretinde utilizatorului plata prețului în schimbul prestării lor. În Ghidul de aplicare a Directivei 2011/83/UE (care nu are caracter obligatoriu) se apreciază că trebuie considerate contracte de livrare de conținut digital, indiferent dacă utilizatorul a plătit sau nu pentru serviciile prestate. Această explicație își are originea în propunerea de Regulament privind Legislația europeană comună în materie de vânzare[22], în care, în considerentele de la nr. 18 se prevede că: „Conținutul digital este adesea furnizat nu în schimbul unui preț ci în combinație cu mărfuri sau servicii plătite separat, implicând considerente nepecuniare, cum ar fi oferirea de acces la datele cu caracter personal sau accesul gratuit, în cadrul unei strategii de marketing (pe baza așteptării ca, într-o fază ulterioară, consumatorul va cumpăra produse cu conținut digital suplimentare sau mai complexe)[...]". Din diferite motive, acest regulament nu a fost adoptat, în prezent urmărindu-se preluarea dispozițiilor acestuia în propunerea de directivăprivindanumite aspecte referitoare la contractele de vânzare online și la altetipuri de contracte de vânzare la distanță de bunuri[23].

O formă de contract pentru livrare de conținut digital este contractul *cloud computing*[24].

Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council), ghid disponibil [Online] la: http://ec.europa.eu/consumers/consumer_rights/rights-contracts/directive/index_en.htm, p. 64, accesat 2.10.2017.

[22] Propunere de Regulament al Parlamentului European și al Consiliului privind Legislația europeană comună în materie de vânzare din 11 octombrie 2011, COM(2011) 635 final.

[23] [Online] la:

http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A52015PC0635, accesat 2.10.2017.

[24] Pentru o prezentare detaliată, a se vedea, C.T. Ungureanu, *Contractul cloud computing în comerțul internațional*, în Revista moldovenească de Drept Internațional și Relații

Ce înseamnă *cloud computing*? Fiecare dintre noi foloseşte serviciile de *cloud computing*, uneori fără a conştientiza acest lucru. Astfel, dacă avem o adresă de e-mail, înseamnă că suntem utilizatori de *cloud*, dacă avem un cont deschis într-o rețea de socializare, cum este, de exemplu, Facebook, Twitter, LinkedIn, utilizăm servicii de *cloud computing*, dacă depozităm documente în Dropbox, fotografii în Instagram folosim *cloud computing* şi exemplele pot continua. Pentru a lua un exemplu „național", dacă am încheiat un contract cu revista „Dreptul" pentru un „abonament pe suport electronic", suntem utilizatori de *cloud*, pentru că o perioadă de timp determinată (de exemplu, 1 an), avem acces, contra cost, la o bază de date în care putem consulta revista.

În literatura de specialitate sunt formulate definiții diverse ale noțiunii de *cloud computing*, care pentru juriști sună ca limbajul juridic pentru informaticieni[25]. În una dintre aceste definiții se consideră că termenul *cloud computing* poate fi definit ca fiind o formă de *computing* în care capacități IT (*Information Technology*) evolutive şi elastice sunt furnizate unui mare număr de clienți, utilizând tehnologia Internet[26]. Capacitate IT evolutivă înseamnă că furnizorul de cloud poate adapta capacitatea de stocare şi de procesare a datelor conform cerințelor clientului. Capacitate IT elastică înseamnă că adaptarea capacității de stocare şi procesare a datelor se poate face rapid, pe măsura schimbărilor în cerințele clientului.

Noțiunea de *cloud computing* este folosită pentru a indica platforme virtuale sau infrastructuri, care permit, printre altele, stocarea (depozitarea) şi procesarea de date, executarea de aplicații şi furnizarea de servicii în diverse forme, prin intermediul Internetului. *Cloud computing* este accesibil şi disponibil oriunde în lume există o conexiune la Internet.

Internaționale, vol. 37, nr. 3/2015, [Online] la:http://rmdiri.md/wp-content/uploads/2015/01/RMDIRI-Nr.-3-20157.pdf, pp. 25-36, accesat 3.10.2017.

[25] C.T. Ungureanu, *Contractul cloud computing: autoritatea competentă pentru soluționarea litigiilor*, în Modernizarea legislației naționale în contextul uniformizării dreptului la nivel european şi implicațiile socio-politice asupra sistemului administrativ, Editura Hamangiu, București, 2015, pp. 297-305.

[26] D.C. Plummer, *Experts Define Cloud Computing: Can we get a Little Definition in our definitions?*, 2009,

[Online] la: http://blogs.gartner.com/daryl_plummer/2009/01/27/experts-define-cloud-computing-can-we-get-a-little-definition-in-our-definitions/, accesat 29.01.2015.

Utilizarea resurselor informatice din spațiul virtual, situate în *cloud*, oferă multe beneficii atât clientului consumator, cât și profesionistului, care ia decizia să stocheze datele sale în *cloud*, precum rapiditatea accesului la date, flexibilitatea, costuri mici pentru infrastructură, personal și software. „Norul" de resurse informatice permite profesionistului/consumatorului să dispună de putere informatică, fără a fi obligat să achiziționeze infrastructura informatică.

Din punctul de vedere al utilizatorului, *cloud computing* se reduce la un număr de servicii puse la dispoziția lui de furnizorul de *cloud*.

De *cloud computing* beneficiază și autoritățile publice, instituțiile guvernamentale etc., devenind funcțional așa numitul *G Cloud* (*Governmental Cloud*) în multe state europene, precum Marea Britanie, Germania, Austria, Finlanda, Danemarca, Franța, Spania. În acest mod, se reduc substanțial costurile pentru achiziționarea infrastructurii informatice (autoritățile publice nu trebuie să achiziționeze *hardware* și *software*) și pentru întreținerea bazelor de date informatice în domeniul public.

În România este operațional portalul *e-guvernare*, prin care Agenția pentru Agenda Digitală a României (AADR), instituție publică de specialitate a administrației publice centrale, are rolul de a gestiona și opera sistemul e-guvernare (S.E.N.) disponibil la adresa www.e-guvernare.ro, Sistemul Electronic de Achiziții Publice (S.E.A.P.) disponibil la adresa www.e-licitatie.ro, Sistemul informatic pentru atribuirea electronică a autorizațiilor de transport internațional rutier de marfă și pentru atribuirea electronică a traseelor naționale din programele de transport prin serviciile regulate județene și interjudețene (S.A.E.T.) disponibil la adresa www.autorizatiiauto.ro, Sistemul National Electronic de Plată online cu cardul a taxelor și impozitelor (S.N.E.P.) disponibil la adresa www.ghiseul.ro și a Punctului de Contact Unic electronic (P.C.U.e) disponibil la adresa http://www.edirect.e-guvernare.ro/.

După *calitatea părților*, contractele electronice încheiate prin Internet pot fi:

- contracte încheiate între profesioniști[27] (așa numitele contracte *Business-to-Business* – B2B); de exemplu, contractul prin care un medic cumpără online aparatură medicală pentru dotarea cabinetului său;

- contracte încheiate între un profesionist și un consumator[28] (așa numitele contracte *Business-to-Consumer* – B2C); de exemplu, contractul prin care consumatorul achiziționează bunuri de la un magazin online; contractul prin care un absolvent de drept se înscrie la cursuri de pregătire pentru admiterea în magistratură[29];

- contracte încheiate între un consumator și un profesionist (așa numitele contracte *Consumer-to-Business* – C2B); de exemplu, Elance – oDesk[30]este o platformă online, unul dintre liderii mondiali pe piața muncii „de acasă", care permite angajatorilor să posteze locuri de muncă, căutând lucrători independenți (*freelancers*[31]); fiecare lucrător independent (care are calitatea de consumator) poate posta CV-ul său și poate face oferte angajatorilor, în anumite condiții;

- contracte încheiate între consumatori (așa numitele contracte *Consumer-to-Consumer* – C2C); de exemplu, contractele încheiate folosind site-ul și aplicația eBay, prin care un consumator poate cumpăra de la un alt consumator un produs *second hand* (ca la un talcioc online)[32].

2. Internetul și datele cu caracter personal

Datele cu caracter personal sunt considerate a fi *orice informaţie* privind persoana fizică identificată sau identificabilă (persoana vizată).

---

[27] Se are în vedere noțiunea de profesionist în accepțiunea art. 3 C. civ., coroborat cu prevederile art. 8 din Legea nr. 71/2011 pentru punerea în aplicare a Legiinr. 287/2009, privind Codul civil (publicată în M. Of. nr. 409, 10.06.2011).

[28] Consumatorul este, potrivit Codului consumului (O.G. nr. 21/1992 privind protecția consumatorilor, republicată în M. Of. nr. 208, 28.03.2007, cu modificările și completările ulterioare), orice persoană fizică sau grup de persoane fizice constituite în asociaţii, care acționează în scopuri din afara activităţii sale comerciale, industriale sau de producție, artizanale ori liberale.

[29] [Online] la: http://www.eurobestteam.ro/admitere-magistratura, accesat 16.05.2015.

[30] [Online] la: http://www.elance-odesk.com/homepage, accesat 15.10.2017.

[31] Lucrător *freelance* este o persoană care lucrează independent, care desfășoară o profesie fără un angajament pe termen lung cu un angajator ([Online] la: http://ro.wikipedia.org/wiki/Freelancer, accesat 2.05.2017).

[32] Pentru detalii, [Online] la: https://www.ebay.com/, accesat 15.10.2017.

Dreptul la protecția datelor cu caracter personal este un drept fundamental al omului, indisolubil legat de dreptul la viață privată.

Utilizarea Internetului în rutina zilnică facilitează colectarea și transferul de date cu caracter personal, punând în discuție posibilitatea protecției datelor.

Astfel, sunt transmise și colectate date/informații ori de câte ori comunicăm prin e-mail, WhatsApp, Facebook, Twitter, folosim un *smartphone*, plătim cu cardul la supermarket, facem plăți prin Internet banking, chemăm un taxi prin aplicația Uber, ș.a.

Bruce Schneier în lucrarea *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*[33]arată că Google știe ce gândim, pentru că salvează toate căutările noastre de pe diferite site-uri; Facebook știe care este orientarea noastră sexuală, chiar dacă nu am menționat niciodată acest lucru; toate cumpărăturile online fiind înregistrate, dezvăluie dacă suntem șomeri, bolnavi, dacă avem copii sau suntem pe cale să dobândim.

În era Internetului, a *Big Data*, *Internet of Things* (IoT), a rețelelor de socializare (Facebook, LinkedIn ș.a.) protecția datelor este dificilă.

Big Data, adică acele cantități de date foarte mari, privite tridimensional, în volum, viteză și varietate, provin dintr-o diversitate de surse. Internetul captează o mulțime de date. Cardurile de credit și de debit, cecurile și alte activități financiare implică un flux constant de miliarde de tranzacții financiare. Din ce în ce mai multe rețele de senzori - camere de supraveghere video, computere încorporate în automobile, telefoane mobile - înregistrează locații, mișcări și activități. Colectarea datelor este omniprezentă; aproape tot ceea ce facem are ca rezultat colectarea și stocarea datelor de către una sau mai multe părți, fie operatori de date, împuterniciți de operatorul de date, terți, destinatari, pentru a folosi terminologia din legislația UE. Aceste date sunt digitale. Ele pot fi stocate, partajate, căutate, combinate și duplicate cu o viteză foarte mare și la un cost foarte mic[34].

---

[33] B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, p. 9,

[Online] la: https://www.schneier.com/books/data_and_goliath/, accesat 22.10.2017.

[34] Ch. Kuner, F.H. Cate, Ch. Millard, D. Jerker, B. Svantesson, *The challenge of 'big data' for data protection*, înInternational Data Privacy Lawvol. 2nr. 2/2012, p. 48, [Online] la:https://academic.oup.com/idpl/article/2/2/47/755343/The-challenge-of-big-data-for-data-protection, accesat 20.06.2017.

Internet of Things (IoT) înseamnă senzori electronici incluși în produse de consum, disponibile la scară largă și la prețuri din ce în ce mai accesibile. Acești senzori convertesc fenomene fizice, precum mișcarea, căldura, presiunea sau localizarea, în informații digitale. Există diferite tipuri de dispozitive IoT: dispozitive pentru monitorizarea stării de sănătate, pentru fitness, pentru automobile, pentru aparate casnice, dispozitive concepute special pentru monitorizarea angajaților, ș.a.[35]. IoT presupun transferuri de date cu caracter personal. De exemplu, în cazul unui aparat de cafea conectat la Internet se poate pune întrebarea cine este operatorul de date: întreprinderea care a fabricat aparatul, proprietarul care l-a cumpărat și îl folosește, serviciul care monitorizează funcționarea aparatului, furnizorul de servicii care îl monitorizează pentru a asigura o mai bună funcționare a acestuia?[36].

Majoritatea transferului de date și a prelucrării acestora are loc în rutina zilnică a contractelor. Multe dintre aceste contracte sunt contracte *cloud computing*. Persoana vizată, operatorul de date, împuternicitorul operatorului de date, autoritățile de supraveghere de cele mai multe ori nu știu unde se află datele. De exemplu, datele sunt transferate de la operatorul de date la împuternicitul operatorului de date, care, la rândul lui, poate avea subfurnizori, astfel încât datele să fie transferate către aceștia și să fie stocate în baze mari de date (*Data Farms* sau *Server Farms*), care pot fi situate în multe puncte geografice. Să spunem că un avocat colectează informații cu caracter personal de la clienții săi, pe care le stochează în Dropbox; clienții au rolul de persoane vizate, avocatul, de operator de date cu caracter personal, Dropbox, are calitatea de împuternicit al operatorului de date. Dropbox, care este un furnizor de *cloud*, poate avea subfurnizori, un lanț de furnizori, ceea ce face foarte dificil pentru operator să controleze și să știe unde sunt prelucrate datele; operatorul de date –avocatul - nu mai deține controlul localizării datelor, care se pot afla oriunde în lume, la un moment dat. Furnizorul de *cloud* sau subfurnizorii pot copia și „replica” datele

[35] Pentru detalii, S.R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, în Texas Law Review, vol. 93/2014, [Online] la:http://www.texaslrev.com/wp-content/uploads/2015/08/Peppet-93-1.pdf, accesat 20.10.2017.

[36] P.de Hert, V. Papakonstantinou, *The new General Data Protection Regulation: Still a sound system for the protection of individuals?*ÎnComputer Law & Security Review, Vol. 32, nr. 2, 2016, p. 184.

clientului de *cloud*, a avocatului, în mai multe baze de date, situate în state diferite. Există baze de date (*server farms*) situate chiar și pe mari vase maritime, care circulă în marea liberă și care tind să se sustragă controlului statal[37].

Utilizarea unui *cloud* presupune încheierea unui contract, care ar trebui să prevadă un anumit control. Furnizorul de *cloud* are, însă, mult mai multe resurse decât operatorul. Faptul că datele se află în permanentă mișcare creează nesiguranță în ceea ce privește respectarea regulilor protecției datelor. „*Personal data may end up in data havens*"[38].

Protecția datelor cu caracter personal impune utilizarea de norme de drept public și de drept privat, fiind un subiect care poate fi tratat interdisciplinar, prin prisma drepturilor omului, dreptului administrativ, dreptului penal, dreptului civil, comerțului internațional.

3. Internetul și soluționarea litigiilor

Deși soluționarea litigiilor se face în mod tradițional într-o sală de judecată, Internetul face posibilă rezolvarea disputelor prin mijloace alternative. Un exemplu este soluționarea online a litigiilor dintre consumatori și profesioniști, reglementată prin O.G.nr. 38/2015 privind soluționarea alternativă a litigiilor dintre consumatori şi comercianţi[39], care reprezintă transpunerea în legislația națională a Directivei nr. 2013/11/UE privind soluționarea alternativă a litigiilor în materie de consum (Directiva privind SAL în materie de consum)[40]. Soluționarea online a litigiilor (SOL)[41]înseamnă „soluţionarea independentă, imparţială, transparentă, eficace, rapidă şi echitabilă, pe cale extrajudiciară, a litigiilor care privesc obligaţiile contractuale rezultate din contractele de vânzare sau de prestări servicii *online* dintre un consumator care îşi are reşedinţa în Uniune (U.E.-s.n. CTU) şi un comerciant stabilit în Uniune" prin intermediul unei

[37] S.R. Swanson, *Google Sets Sail: Ocean-Based Server Farms and International Law*, în Connecticut Law Review, Vol. 43, February 2011, no. 3, pp. 709-751.

[38] P. Blume, *It is time for tomorrow: EU data protection reform and the Internet*, în Journal of Internet Law, Vol. 18, No. 8, 2015, p. 8.

[39] Publicată în M. Of. nr. 654, 28.08.2015.

[40] Publicată în J.O. nr. L 165/63, din 18.06.2013.

[41] Pentru o prezentare detaliată, C.T. Ungureanu, *Soluționarea alternativă a litigiilor (SAL) dintre profesioniști și consumatori conform O.G. nr. 38/2015*, în volumul conferinței „160 de ani de învățământ juridic ieșean", Editura Hamangiu, București, 2015, pp. 87-98.

platforme europene de soluționare online a litigiilor, numită platforma SOL (creată prin Regulamentul privind SOL în materie de consum[42]). Rezultă că soluționarea online a litigiilor nu poate avea loc prin intermediul unor furnizori de servicii privați, care administrează platforme pentru soluționarea litigiilor, cum este, de exemplu, Modria Resolution Center[43], ci numai prin platforma SOL creată în UE[44].

4. Facebook

Facebook, cea mai utilizată rețea de socializare, „alimentează" instanțele de judecată din toată lumea cu cauze al căror obiect poate fi încadrat în multe ramuri ale dreptului. Voi face o scurtă trecere în revistă a celor mai recente.

Protecția datelor cu caracter personal – drept fundamental al omului. La 6 octombrie 2015, Curtea de Justiție a Uniunii Europene (CJUE) a invalidat, în cauza *Schrems* (C-362/14), Decizia Comisiei Uniunii Europene privind mecanismul referitor la sfera de siguranță (*Safe Harbour*) cu Statele Unite ale Americii (SUA). Ca urmare a acestei decizii, cadrul *Safe Harbor* SUA-UE a fost considerat un mecanism nevalid pentru a se conforma cerințelor UE privind protecția datelor cu caracter personal, atunci când transferul de date cu caracter personal are loc din UE către SUA.La 12 iulie 2016, a fost adoptat un nou mecanism pentru transferul datelor, *Privacy Shield Framework*[45](Scutul de confidenţialitate).

La acest rezultat s-a ajuns în urma soluționării cauzei Schrems.Schrems, avocat și utilizator de Facebook din 2008, a depus, inițial, o plângere la autoritatea irlandeză de protecție a datelor, considerând că, după dezvăluirile făcute în 2013 de Edward Snowden cu privire la activitățile serviciilor de informații ale SUA, dreptul și practicile din Statele

[42] Regulamentul (UE) nr. 524/2013privind soluționarea online a litigiilor în materie de consum (Regulamentul privind SOL în materie de consum), publicat în J.O. nr. L 165/1, din 18.06.2013, care se aplică în statele membre UE, deci şi în România, din 9 ianuarie 2016.

[43] Modria Resolution Center este o platformă online (bazată pe cloud computing), care este utilizată de profesioniști pentru soluționarea litigiilor. ([Online] la: https://www.tylertech.com/solutions-products/modria, accesată 20.10.2017).

[44] Pentru detalii referitoare la organisme private de soluționare online a litigiilor, P. Cortes, A.R. Lodder, *Consumer Dispute Resolution Goes Online: Reflections on the Evolution of European Law for out-of-court redress*, p. 15 și urm., [Online] la: http://www.maastrichtjournal.eu/pdf_file/ITS/MJ_21_01_0014.pdf, accesat 1.10.2015.

[45] [Online] la: https://www.privacyshield.gov/Program-Overview, accesat 15.10.2017.

Unite nu asigură o protecție suficientă a datelor transferate către această țară împotriva supravegherii de către autoritățile publice. Acțiunile lui Schrems au ajuns în final la CJUE.

Deși a fost adoptat *Privacy Shield Framework*[46], la 3 octombrie 2017, Înalta Curte de Justiție Irlandeză a solicitat CJUE să se pronunțe cu privire la securitatea transferului de date cu caracter personal între UE și SUA prin Facebook[47]. Cauza se află în curs de soluționare.

Drepturile fundamentale ale omului – Dreptul la liberă exprimare. La 5 mai 2017, o instanță austriacă a obligat Facebook să suprime de pe platforma sa postările care instigă la ură[48].

Drepturi succesorale și dreptul la viață privată. La 31 mai 2017, o instanță germană a admis apelul formulat de Facebook împotriva unei hotărâri din 2015 prin care Facebook era obligată să comunice părinților unei adolescente decedate conținutul de pe pagina acesteia de Facebook. Adolescenta s-a sinucis, iar părinții au suspectat că ar fi fost vorba de *cyberbullying*. Instanța a motivat decizia sa prin invocarea dreptului la viață privată a utilizatorilor cu care adolescenta a comunicat[49].

Drept administrativ. Facebook a fost amendată de *Commission nationale de l'informatique et des libertés* (CNIL) din Franța, la 16 mai 2017, cu 150.000 euro pentru utilizarea masivă a datelor cu caracter personal în scopuri publicitare[50].La 11 septembrie 2017, Agenția spaniolă de protecție a datelor cu caracter personal a amendat Facebook cu 1,2 milioane de euro pentru colectarea datelor personale ale utilizatorilor fără a obține consimțământul lor clar exprimat[51].

---

[46] [Online] la: https://www.facebook.com/about/privacyshield, accesat15.10.2017.

[47] [Online] la: http://www.lemonde.fr/pixels/article/2017/10/03/la-justice-europeenne-va-examiner-les-transferts-de-donnees-de-facebook-vers-les-etats-unis_5195643_4408996.html#XA2AbIacAxpSp9oW.99, accesat15.10.2017.

[48] [Online] la: http://www.lemonde.fr/pixels/article/2017/05/09/discours-haineux-facebook-epingle-par-la-justice-autrichienne_5124835_4408996.html#YP8oELSmhMdOvZJc.99, accesat15.10.2017.

[49] [Online] la:https://www.theguardian.com/technology/2017/may/31/parents-lose-appeal-access-dead-girl-facebook-account-berlin, accesat15.10.2017.

[50] [Online] la: https://www.la-croix.com/Sciences-et-ethique/Numerique/Donnees-personnelles-Facebook-condamne-Cnil-2017-05-17-1200847843, accesat15.10.2017.

[51] [Online] la: https://fr.reuters.com/article/technologyNews/idFRKCN1BM1W3-OFRIN, accesat15.10.2017.

Drept procesual. *Protecția consumatorilor*. Curtea de apel din Paris[52],în februarie 2016, s-a declarat pentru a doua oară competentă să judece un litigiu dintre Facebook și un utilizator francez, al cărui cont a fost închis. Curtea a confirmat ordonanța tribunalului din Paris din 5 martie 2015, care a stabilit drept abuzivă clauza exclusivă de competență în favoarea unei instanțe din California, obligatorie pentru toți utilizatorii de Facebook[53]. La originea acțiunii este un profesor care a postat pe pagina sa Facebook, în 2011, o pictură de Gustave Courbet,*"L'Origine du monde"*, și, ca rezultat, Facebook i-a închis contul. Avocatul profesorului a arătat că Facebook a făcut confuzie între o operă de artă și pornografie și a pus problema libertății de exprimare în rețelele sociale.

Și în SUA Facebook este parte în multe litigii. De exemplu, în 2011 a fost introdusă în California o *class action* împotriva Facebook (*Fraley, et al. v. Facebook, Inc., et al.*) invocându-se utilizarea numelor utilizatorilor în reclame numite „*Sponsored Stories*". Părțile au ajuns la o tranzacție (*settlement*) în noiembrie 2016.

În cauza *Chia Hong v. Facebook, Inc., Anil Wilson, et. al.* din 2015, Facebook a fost acuzată de discriminare sexuală și rasială de Chia Hong fostă angajată a acesteia. Și în acest caz părțile au ajuns la o înțelegere în urma unei medieri[54].

În concluzie, Internetul este în „slujba" dreptului, servind nevoile consumatorilor și profesioniștilor și „hrănind" instanțele de judecată și pe cei care se implică în soluționarea multiplelor litigii la care dă naștere. Oricât de optimiști am fi în legătură cu reglementarea legislativă a noilor raporturi apărute prin utilizarea Internetului, tehnologia informatică evoluează într-un ritm atât de rapid, încât greu poate fi prinsă din urmă. Este ca și cum am alerga să prindem avionul care deja a decolat. Cu toate acestea, juriștii au la îndemână instrumente care să asigure găsirea de soluții.

---

[52] [Online] la: http://www.latribune.fr/technos-medias/internet/facebook-la-justice-francaise-confirme-qu-elle-pourra-juger-la-censure-de-l-origine-du-monde-550534.html, accesat15.10.2017.

[53] Punctul 15 din condițiile de utilizare Facebook, [Online] la: https://ro-ro.facebook.com/legal/terms, accesat15.10.2017.

[54] [Online] la: https://www.law360.com/articles/712826/ex-facebook-employee-drops-suit-alleging-gender-race-bias, accesat15.10.2017.

ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

INTERPRETAREA PRINCIPIILOR *PRIVACY BY DESIGN* ÎN ERA CLOUD COMPUTING

INTERPRETING THE *PRIVACY BY DESIGN* PRINCIPLES IN THE CLOUD COMPUTING ERA

LENUȚA ALBOAIE[1]

Rezumat: Odată cu existența unor tehnologii accesibile pe scară largă, numărul de utilizatori de servicii Internet a crescut și, ca efect, și cantitatea de date generată și stocată (inclusiv cele cu caracter personal) a crescut. În acest context, probleme ca securitatea și confidențialitatea datelor sunt de un real interes, iar soluțiile perfecte par un deziderat greu de atins. În lucrarea de față, în prima parte, creăm imaginea de ansamblu a evoluției tehnologice care a condus la tehnologii arondate Cloud Computing. În acest ecosistem, realizăm în partea a doua a lucrării o interpretare tehnică a principiilor *Privacy by Design* și deschidem o cale către o soluție software de respectare a acestora.
Cuvinte cheie: Cloud Computing, Privacy by Design, GDPR

Abstract: With the availability of widely available technologies, the number of Internet service users has increased and as a result the amount of data generated and stored (including personal data) has increased. In this context, issues such as data security and confidentiality are of real interest, and perfect solutions seem a difficult task to achieve. In the present paper, in the first part, we create the overall picture of the technological evolution that has led to Cloud Computing technologies. In this ecosystem, in the second part of the paper, we realize technical interpretation of the principles of *Privacy by Design* and open a path to a software solution to their compliance.
Keywords: Cloud Computing, Privacy by Design, GDPR

1. Cloud Computing

Cloud Computing este, conform Gardner, unul din principalele trend-uri în lumea IT alături de IoT (*Internet of Things*), *Business Analytics*,

[1] Conferențiar dr., Universitatea „Alexandru Ioan Cuza" din Iași, Facultatea de Informatică.

Inteligență Artificială sau *Machine Learning*. Secțiunea de față crează o imagine de ansamblu asupra pașilor care au fost necesari pentru atingerea nivelului tehnologic oferit de Cloud Computing în zilele noastre.

1.1 Pași înspre Cloud Computing

Cloud Computing reprezintă un conglomerat de tehnologii, iar forma actuală nu ar fi fost posibilă fără momente de referință din evoluția sistemelor distribuite[2].

Perioada anilor 1945 o putem considera esențială în evoluția calculatoarelor (cu transformări la nivelul memoriei, stocării, procesorului) și a rețelelor de calculatoare (apariția suitei de protocoale TCP/IP, a Internetului). Încă din această perioadă existau previziuni asupra modului cum va fi folosită puterea de calcul: *"(...) computing may someday be organised as a public utility just as the telephone system is a public utility..."*[3].

Realitatea de astăzi demonstrează că puterea de calcul a devenit cea de cincea utilitate, furnizata într-un mod similar utilităților tradiționale (gaz, electricitate, apă sau telefonie).

Din punct de vedere tehnologic, un moment important a fost reprezentat de apariția în anii '90 a conceptului de Grid Computing, denumit în acest fel prin analogie cu rețelele electrice (power grids)[4].

Studiile și experimentele din acea perioadă au observat că aproximativ 90% din puterea unui procesor nu era utilizată. Acest lucru se întâmpla în contextul în care numeroase probleme de calcul, de optimizare sau de simulare necesitau super-computere cu capabilități computaționale crescute.

Grid era o infrastructură de calcul distribuit destinată inițial proiectelor științifice și mai apoi și celor industriale. A permis executarea de task-uri pe mai multe mașini, privite ca un calculator unic. Grid Computing asigură de asemenea partajarea flexibilă, sigură și coordonată a resurselor

---

[2] L. Alboaie, *Cloud Computing – Nucleul Vieții Digitale a utilizatorilor*, în Revista Columna, Nr. 6/2017, Supliment cultural-științific al revistei STUDII ȘI COMUNICĂRI/DIS a Diviziei de Istoria Științei a CRIFST al Academiei Române, Comitetul Român de Istorie și Filosofia Științei și Tehnicii, Academia Română, ISSN: 1841-9852, 2017.

[3] S. Garfinkel, *The Cloud Imperative*, Business Report, 2011.

[4] C. Kesselman, I. Foster, S. Tuecke, *The Anatomy of the Grid: Enabling Scalable Virtual Organization*, în International Journal of High Performance Computing Applications, 2001, 15(3), pp. 200-222.

între colecții dinamice de indivizi, instituții și resurse. Dacă în faza inițială în Grid erau partajabile doar resursele hardware, integrarea cu tehnologiile arondate Web-ului au permis și partajarea aplicațiilor. Și astfel, din punct de vedere al specialiștilor, utilizarea aplicațiilor și serviciilor Grid a devenit o soluție completă[5].

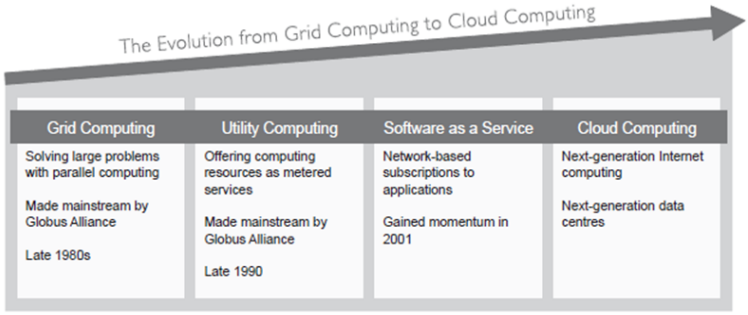
Din punctul de vedere al utilizatorilor finali, acest lucru nu a avut loc, motiv pentru care Grid Computing nu s-a bucurat de mediatizarea tehnologiilor asociate cu Cloud Computing.

În paralel cu dezvoltarea la nivel de Grid, prin furnizarea de putere computațională la cerere în stilul plătești ceea ce utilizezi (*pay-per-use*), a apărut paradigma SaaS (Software-as-a-Service).

SaaS desemnează software care este deținut, furnizat și gestionat de un furnizor. Comparând cu un sistem software tradițional, în acest caz utilizatorul plătește funcționalitatea pentru timpul de utilizare, dar utilizatorul nu deține softul și nu face investiții în infrastructura, în licențe etc[6].

Serviciile în acest caz sunt consumate pe principiul *pay-per-use* via unui Web browser sau API (*Application Programming Interface*). Ceea ce remarcam la acest nivel este faptul că orice utilizator este capabil să folosească servicii dacă folosește un simplu client browser.

Și am ajuns astfel, printr-o concurență a tehnologiei și a contextului mondial economic, la momentul în care Cloud Computing a prins formă[7].



The Evolution to Cloud Computing (adapted from IBM 2009)

Figura 1. Pași tehnologici spre Cloud Computing

[5] L. Alboaie, *op.cit.*
[6] *Ibidem.*
[7] M. Cafaro, G. Aloisio, *Grids, Clouds and Virtualization*, 2011.

Avem în figura 1 o perspectivă completa a pașilor care au condus la apariția Cloud Computing.

Apariția soluțiilor oferite de Cloud au fost salvatoare în special pentru companii mici și mijlocii, în contextul crizei economice din anii 2008. În acel moment, greu din punct de vedere economic, companiile mici/mijlocii au putut să se concentreze pe cheltuieli operaționale și mai puțin pe cele de capital, astfel s-a preferat achiziționarea de servicii/abonamente, decât plata unor sume mari într-o investiție[8].

1.2 Cloud Computing: servicii, avantaje și provocări

Denumirea de Cloud Computing a fost inspirată din diagramele care erau folosite pentru reprezentarea Internetului. Într-o definiție simplificată, putem vedea Cloud ca un sistem distribuit, care furnizează în Internet, într-un mod eficient, accesul la o mare varietate de servicii atât pentru specialiști, dar și pentru utilizatorii obișnuiți.

Acest lucru poate fi asigurat prin existenta mai multor categorii de servicii și amintim pe cele mai uzuale:

IaaS (Infrastructure as a Service)[9]

Aceste servicii permit închirierea de infrastructură (noduri de calcul, sisteme de stocare etc.) și construirea unui sistem IT. În acest caz, mediul poate fi controlat în totalitate de cel care l-a configurat/creat. Remarcăm însă faptul că sistemul este închiriat, deci resursele fizice efective sunt în grija (depozitare, răcire, securitate fizică) unui furnizor de servicii IaaS.

PaaS (Platform as a Service)[10]

Aceste servicii permit dezvoltarea unui sistem IT pe o platformă Cloud existentă, fără grija managementului resurselor la nivel scăzut. În acest caz, mediul nu mai poate fi controlat în totalitate, ci doar anumite aspecte pot fi personalizate.

SaaS (Software as a Service)

În acest caz se folosesc sisteme IT existente, oferite de un furnizor de servicii Cloud. Aceste servicii nu necesită cunoașterea de detalii tehnice.

---

[8] K. Stanoevska-Slabeva, T. Wozniak, S. Ristol, *Grid and Cloud Computing - A Business Perspective on Technology and Applications*, Editura Springer-Verlag Berlin Heidelberg, DOI 10.1007/978-3-642-05193-7, 2010.

[9] L. Alboaie, *op.cit.*

[10] L. Alboaie, *op.cit.*

Existența acestui nivel de servicii a asigurat de altfel o cunoaștere și utilizare a serviciilor Cloud până la nivelul utilizatorului obișnuit. Aceste servicii pot fi folosite în mod uniform (de pe orice platformă Windows, iOS, Android, Linux) și folosind dispozitive diverse.

Avem în figura 2 un top al celor mai buni furnizori de servicii Cloud în 2017[11]:

Figura 2. Top furnizori de servicii cloud în 2017

Dacă dorim să avem o imagine asupra numărului de utilizatori de servicii Cloud, putem în Internetlivestats[12] să vizualizăm în timp real statistici privind utilizarea diverselor sisteme și să avem în vedere că majoritatea aplicațiilor ca YouTube, Instagram, Facebook et.al. se bazează pe tehnologii arondate Cloud Computing.

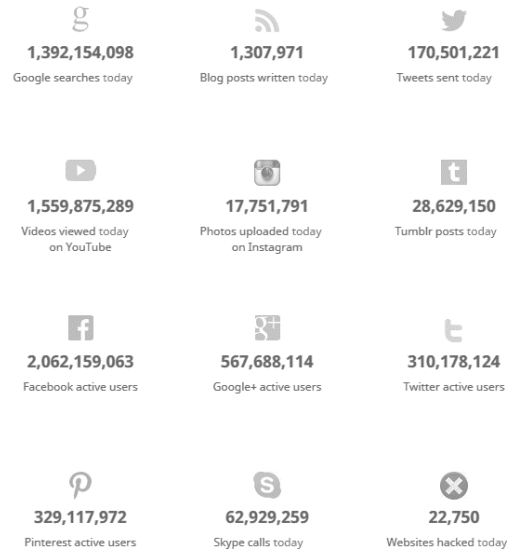


Figura 3. Utilizatori/clienți de servicii/aplicații Cloud

[11] Toptenreviews, [Online] la: www.toptenreviews.com/services/web-hosting/best-cloud-services/.

[12] Internetlivestats, 2017, [Online] la: http://www.internetlivestats.com/.

Dacă ne oprim asupra Facebook, mulți dintre utilizatori nu realizează că folosesc serviciile unor furnizori de Cloud și ignoră aspecte care țin de securitatea și confidențialitatea datelor lor. Trebuie să înțelegem că tehnologiile ne pot fi un bun aliat, dar și dușman dacă nu sunt folosite în mod corespunzător. Viața pe Internet, o concurează "cu succes" pe cea reală, și dacă în viata de zi cu zi ne pasă de siguranța noastră, acest lucru trebuie să se oglindească și în mediul online.

Într-adevăr, securitatea în Cloud ridică mari dificultăți, în contextul în care vorbim atât de asigurarea securității calculatoarelor, dar și a rețelelor de calculatoare. Este nevoie de un set larg de politici, tehnologii și controale care sa fie desfășurate pentru a proteja datele, aplicațiile și infrastructura din Cloud.

Un studiu realizat de CIGI (Centre for International Governance Innovation) asupra 24,225 utilizatori de Internet din 24 de tari, în perioada Decembrie 23, 2016 - Martie 21, 2017 în ţări ca Australia, Brazilia, Canada, China, Egipt, Franţa, Germania, Hong Kong (China), India, Indonesia, Italia, Japonia, Kenya, Mexic, Nigeria, Pakistan, Polonia, Republica Korea, Africa de Sud, Suedia, Tunisia, Turcia, Regatul Unit al Marii Britanii şi Irlandei de Nord şi Statele Unite ale Americii, arată că pas cu pas utilizatorii de servicii Cloud și servicii Internet în general, devin conștienți de problema securității[13]:

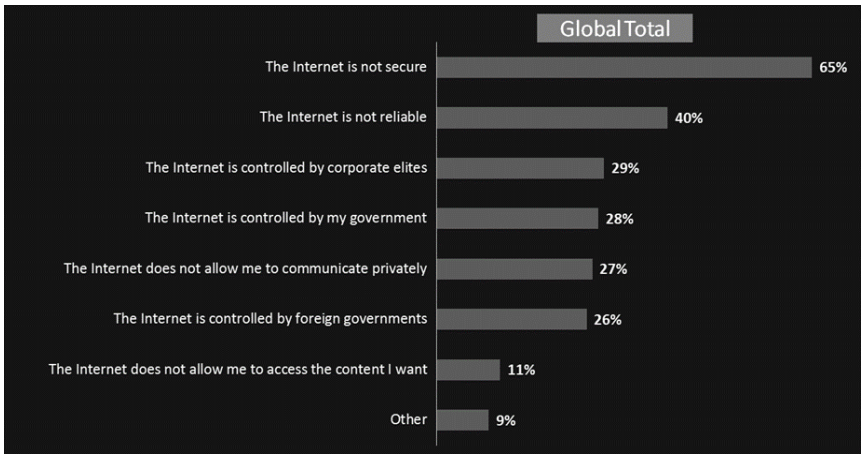


Figura 4. Temeri ale utilizatorilor legate de securitatea și confidențialitatea serviciilor

[13] CIGI – Centre for International Governance Innovation, https://www.cigionline.org/.

Înțelegând sau intuind aceste probleme existente, reacții diverse (utilizarea selectivă a unor aplicații, teama de a spune ce gândești, limitarea aplicațiilor utilizate, utilizarea Internetului mai puțin etc.) par a fi în opoziție cu scopul Internetului și Web-ului, cel de a avea un sistem deschis care să ofere un ecosistem în care cunoștințele și experiențele oamenilor să fie partajate, toate acestea contribuind la colaborarea care duce implicit la evoluția noastră globală.

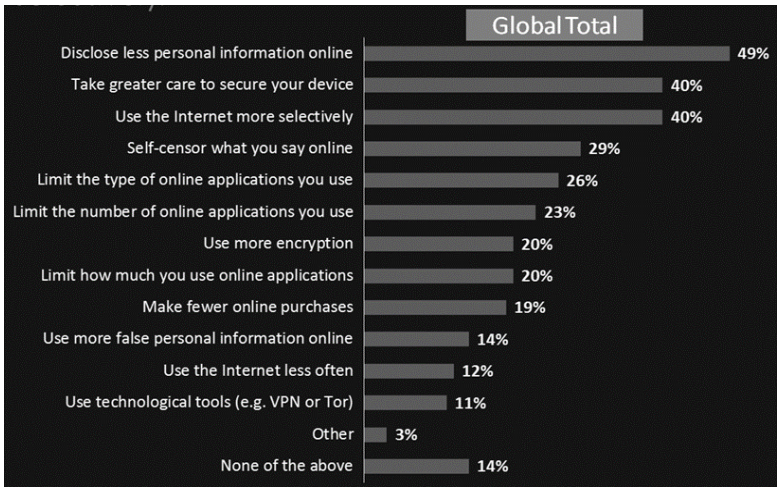


Figura 5. Potențiale reacții ale utilizatorilor la amenințările legate de securitate și confidențialitate

Evitarea apariției unui curent global, cu un comportament anti-Internet, ne conduce la încercarea de a găsi soluții pentru asigurarea securității și confidențialității datelor. Acest al doilea aspect este subiectul dezbătut în continuare în cadrul acestei lucrări.

2. Interpretarea principiilor Privacy by Design

Vom începe această secțiune prin a face distincția între conceptul de confidențialitate (eng. *privacy*) și securitate a unui sistem.

Privacy poate fi privit ca un nivel imediat peste nivelul de securitate. Într-un sistem putem avea securitate fără a avea *privacy*, dar nu putem avea *privacy* fără securitate. *Privacy* oferă o modalitate de acces granular la informație. Pentru clarificarea conceptului, să considerăm că o persoană fizică deține un cont bancar, accesibil din orice filială a băncii. Implicit, angajații băncii au acces la acest cont și se presupune că nimeni

altcineva. Până la acest nivel putem vorbi de asigurarea securității. Confidențialitatea intervine la nivelul în care accesul la datele asociate contului se face doar dacă există un *business case* sau o solicitare în acest sens și nu dacă un angajat al băncii "devine curios" în ceea ce privește informațiile particulare asociate contului.

Gândirea modernă asupra confidențialității gravitează în jurul principiilor *Privacy By Design* și a interpretării lor legale dată de GDPR (*EU General; Data Protection Regulation*).

Principiile *Privacy by Design* (PbD)[14] pot fi considerate ca stând la baza analizelor legate de probleme de confidenţialitate. Aceste principii sunt văzute ca fiind relativ vagi, fără a veni cu indicaţii concrete asupra modului lor de implementare, ceea ce conduce la multe interpretări, care fac aceste principii ca fiind greu de implementat din punct de vedere tehnic[15].

În această lucrare, ne vom referi prin termenul tehnic PbD ca să înțelegem o unificare a conceptelor consacrate de *Privacy by Design* şi *Privacy by Default*.

Privacy by Design (tradus uneori prin protecția datelor încă din faza de proiectare) presupune că anumite reguli trebuiesc încorporate în metodologiile de dezvoltare de software atunci când este vorba de prelucrarea datelor cu caracter personal. *Privacy by Default* (tradus uneori prin protecția datelor cu ajutorul setărilor implicite) înseamnă că, atunci când folosește un produs, consumatorul trebuie să îl găsească setat pe parametrii care oferă cea mai mare protecție.

În continuare vom realiza o interpretare a celor șapte principii PbD, așa cum se regăsesc ele în literatura științifică. Pentru o tratare mai elaborata, recomandăm *Privacy Policies Are Not Enough: We Need Software Transparency*[16], *Privacy Engineering: Proactively Embedding Privacy, by Design*[17], *Privacy by design: delivering the promises, Identity in the Information Society*[18].

---

[14] Privacy by Design, *The 7 Foundational Principles,* [Online] la: www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf , 2011.

[15] R. McKean, *EU Data Protection Reform – privacy-by-design,* [Online] la: http://www.olswang.com, 2014.

[16] A. Cavoukian, D. Jutla, *Privacy Policies Are Not Enough: We Need Software Transparency*, 2014.

[17] A. Cavoukian, S. Shapiro, R. J. Cronk, *Privacy Engineering: Proactively Embedding Privacy, by Design*, 2014.

[18] P. Hustinx, *Privacy by design: delivering the promises, Identity in the Information Society*, Volume 3, Issue 2, 2010, pp 253–255.

a) Proactive not reactive; Preventative not remedial

Primul principiu PbD stipulează faptul că protecția datelor private trebuie făcută în mod preventiv și nu reactiv. În mod evident, remedierea furtului datelor sau detecția faptului ca datele au fost copiate nu pot să mai împiedice răul care poate fi făcut prin folosirea ilegală a acestor date.

Acest principiu se refera atât la mijloace tehnice de prevenție, dar și la mijloace de natura organizațională (politici, standarde, cultura organizațională care să acorde importanţă problemelor de securitate și *privacy*).

b) Privacy as the default setting

Sistemele moderne tind să aibă un mare nivel de configurabilitate de către utilizatori și administratori. Principiul doi spune că toate configurațiile implicite pentru un utilizator nou ar trebui să activeze doar comportamentele sistemului care protejează datele personale și nu pe cele care permit scurgeri ale datelor personale. Să considerăm că avem o rețea socială şi setările asociate. Chiar dacă în sistem există o setare care face disponibil sau indisponibil către alții numărul de telefon sau email-ul, conform acestui principiu, setarea implicită ar trebui să fie cea în care datele private nu sunt disponibile. Din motive ce țin de exploatarea comercială, multe servicii internet actuale nu respectă acest principiu. O cauză a acestui comportament potențial dăunător social îl reprezintă beneficiile ce se pot obține din învățarea comportamentelor și colectarea datelor private de la utilizatori.

Acest principiu, aplicat în practică, se poate traduce prin implementarea unor mecanisme care asigură verificarea următoarelor aspecte: specificarea scopului de colectare a datelor, limitarea colectării de date doar la scopul specificat, minimizarea datelor (*Data Minimization*) colectate sau partajate, limitarea în timp a stocării datelor, limitarea folosirii datelor private doar pentru scopurile specificate.

c) Privacy embedded into design

Acest principiu PbD stipulează faptul că protecția datelor private trebuie să fie analizată și adăugata în design de la început, în mod preventiv și nu reactiv. În mod ideal, mecanisme ce asigură protecția datelor private ca și a mecanismelor de securitate ar trebui să fie verificabile formal încă din faza de proiectare a sistemelor. Totuși, din motive de complexitate și lipsa metodelor, această practică nu este larg întâlnită în acest moment. Efortul nostru de cercetare în domeniul coreografiilor verificabile este o contribuție

în acest sens[19,20,21].

d) Full functionality – positive-sum, not zero-sum

Acest principiu PbD își propune să nu prioritizeze interesele private în faţa intereselor de grup și sociale. Ca cetățeni ne dorim beneficiile comunicării între diferite organizații și actori sociali. Progresul și abundenţa materială se bazează pe exploatarea încrederii și a informațiilor cu caracter personal. Pentru a promova exploatarea comercială și pentru a facilita schimbul de bunuri și servicii în mod sănătos social, avem nevoie de sisteme robuste care să permită accesul la date conform legilor. Acest principiu este unul din cele mai puțin înțelese în comunitatea academică și uneori și în industrie datorită încercării de a rezolva probleme sociale cu mijloace tehnice. Acest principiu necesită o înțelegere mai amplă și o acceptare din arhitectura sistemelor a forțelor inevitabil contradictorii ce definesc conceptul de *privacy*. În esență, acest principiu respinge ideea ca protecția datelor reduce posibilitățile de exploatare comercială a datelor.

e) Visibility and transparency – keep it open

Ca urmare a principiului anterior, devine evident că nu se pot crea cutii magice care respectă la modul absolut drepturile și legile în vigoare. Datorită implicării umane, sistemele software vor fi mereu vulnerabile în faţa utilizatorilor lor. Totuși, existența unor mecanisme de audit sau logare detaliată a operațiilor și a accesului la datele sensibile pot diminua în mod semnificativ riscurile asociate. Acest principiu propune ca prin design să fie maximizată vizibilitatea și transparența asupra funcționarii și asupra modului cum este exploatat sistemul de către utilizatori. Orice implementare incorectă a acestui principiu poate transforma transparența într-o sursa de probleme legate de securitate și de protecție a datelor. Pe scurt, acest principiu se poate traduce prin verificarea următoarelor aspecte:

Atribuirea responsabilității - orice acces la date private ar trebui să fie logat și un audit ulterior ar trebui să poată verifica legalitatea accesului;

---

[19] L. Alboaie, S. Alboaie, A. Panu, *Swarm Communication – A Messaging Pattern Proposal for Dynamic Scalability in Cloud*, 15th IEEE International Conference on High Performance Computing and Communications (HPCC 2013), IEEE, pp. 1930-1937.

[20] S. Alboaie, L. Alboaie, A. Panu, *Levels of Privacy for e-Health systems in the cloud era*, 24th International Conference on Information Systems Development Harbin, China, August 25-27, 2015.

[21] S. Alboaie, L. Alboaie, M.-F. Vaida, *Web service transformations in a federated Enterprise Service Bus based on executable choreographies*, Proceedings of the Conference on Mathematical Foundations of Informatics MFOI 2016, Chișinău, Republic of Moldova, 2016.

Transparența - politicile și practicile legate de managementul datelor private trebuiesc făcute cunoscute celor cu un interes legitim în acest sens;

Conformitate - organizațiile care manipulează date private trebuie să respecte reguli, standarde și proceduri bine definite cu privire la modul în care folosesc aceste date.

f) End-to-end security – full lifecycle protection

Acest principiu scoate în mod explicit la lumina faptul că toate aspectele ce țin de exploatarea unui sistem pot contribui la respectarea sau încălcarea regulilor și politicilor referitoare la datele private. Protecția datelor trebuie să fie o preocupare continuă începând cu analiza, implementarea, mentenanța și modul cum sunt proiectate și respectate procedurile de exploatare a sistemelor software.

Acest principiu, intuitiv indică faptul că aspectele de securitate și modul de aplicare a standardelor și bunelor practici de securitate, constituie o necesitate în vederea obținerii unor sisteme ce respecta protecția datelor.

g) Respect for user privacy – keep it user-centric

În ciuda conflictului dintre interesele private și interesele de grup, acest principiu stipulează că atunci când exista dubiu ar trebui să fie prioritare interesele private ale utilizatorului. Acest principiu se poate traduce prin verificarea următoarelor aspecte:

Obținerea consimțământului: deținerea și folosirea datelor personale trebuie să se facă doar după obținerea acceptului;

Acuratețea: datele private trebuie sa fie corecte, complete, actualizate pentru a nu provoca daune persoanelor;

Accesul: persoanele trebuie sa aibă acces la propriile date și să poată să ceară ștergerea lor.

Dincolo de aspectele organizaționale adresate de PbD, o sumarizarea și operaționalizare a acestor principii ce s-ar adresa implementatorilor (arhitecți software și programatori) și nu specialiștilor în drept ar putea fi sumarizată prin următoarele puncte: *obținerea consimțământului, păstrarea calității datelor, obținerea doar a datelor de care este nevoie, dreptul de a fi uitat, transparență și acces, monitorizare, auditare și reacție imediate la breșe.*

Dat fiind caracterul interpretabil al acestor principii, dacă aspectele ce țin de *privacy* sunt lăsate doar în seama specialiștilor tehnici și a decidenților de business orientați spre eficiență și profit, interpretarea

principiilor poate fi mult mai relaxată decât ar fi optimul social.

În acest context, efortul echipei de cercetare din cadrul laboratorului ADS - Applied Distributed Systems (Facultatea de Informatica, Universitatea Alexandru Ioan Cuza din Iași), prin intermediul proiectului PrivateSKY[22] în domeniul coreografiilor verificabile este o contribuție în acest sens.

Fără a intra în detalii tehnice, menționăm că în cadrul *Towards a smart society through personal assistants employing executable choreographies*[23], pe baza cercetărilor efectuate[24,25,26] s-a prezentat o soluție prin care principiile PbD pot beneficia de suportul tehnic pentru implementarea de sisteme în acord cu cerințele legislației în vigoare.

3. Concluzii

Curentul actual este fără îndoială așa numitul *data-centric computing*, în care datele sunt nucleul societății informaționale[27] și ne referim aici la toate datele existente, atât cele cu caracter public, cât și cele cu caracter personal. Asa cum am văzut, tehnologiile Cloud sunt adânc încrustate în viața noastră și utilizatorii „plătesc" utilizarea Facebook, Google, ITunes, Instagram etc., deoarece toate acțiunile, legăturile și căutările lor sunt înregistrate și folosite în scopuri diverse. În acest context, este dificilă stabilirea unui echilibru între utilizarea acestor date care să ducă la un beneficiu global sau utilizarea acestora cu scopul de obținere a unor profituri punctuale. PbD si GDPR vin ca suport pentru crearea de sisteme informatice într-un viitor apropiat, capabile speram noi, să asigure un *safe data-centric computing*.

[22] PrivateSky, [Online] la https://profs.info.uaic.ro/~ads/PrivateSky.

[23] L. Alboaie, *Towards a smart society through personal assistants employing executable choreographies*, At 26th International Conference on Information Systems Development, Cyprus, 6-8 September 2017.

[24] L., Alboaie, S. Alboaie, A. Panu, *Swarm Communication (…).*

[25] S. Alboaie, L. Alboaie, A. Panu, *Levels of Privacy for e-Health systems (…).*

[26] S. Alboaie, L. Alboaie, M.-F. Vaida, *op.cit.*

[27] L. Alboaie, *Evoluția prelucrării și transmiterii datelor în societatea umană (in Romanian)*, în Revista Noema, Comitetul Român de Istorie și Filosofia Științei și Tehnicii, Volumul XI, Academia Română, ISSN: 1841-9852, 2012, pp.253-270.

ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

SCURTE CONSIDERAȚII PRIVIND SANCȚIONAREA FRAUDELOR COMISE PRIN SISTEME INFORMATICE ŞI MIJLOACE DE PLATĂ ELECTRONICE

BRIEF CONSIDERATIONS ON THE SANCTIONING OF FRAUDS COMMITTED THROUGH COMPUTER SYSTEMS AND ELECTRONIC PAYMENT INSTRUMENTS

RUXANDRA RĂDUCANU[1]

Rezumat: Acest articol îşi propune să evidenţieze particularitatea faptelor incriminate de C.pen. (2009) în capitolul „Fraude comise prin sisteme informatice şi mijloace de plată electronice", dar şi să sublinieze elementele comune care au determinat această grupare. În plus, asemănarea şi delimitarea lor de alte incriminări necesită o detaliere a elementelor constitutive, astfel încât să fie evitată confuzia între acestea sau, dimpotrivă, reținerea cumulativă a acestora cu infracțiuni asemănătoare.
Cuvinte-cheie: fraudă, sistem informatic, mijloc de plată electronic, înşelăciune, pagubă, date informatice, operațiuni financiare

Abstract: This paper aims to emphasise particularity of the facts incriminated by penal law in chapter „Fraud commited using computer systems and electronic payment methods", but also to punctuate the common elements that have determine this grouping. More, their resemblance and delimitation of other offensesrequire to detail their essential elements in order to avoid confusion between them, or, on the contrary, to cumulate with similar offenses.
Key-words: fraud, computer system, electronic payment methods, misrepresentation, damage, digital data, financial operations.

1. Introducere

Utilizarea mijloacelor frauduloase este din ce în ce mai frecventă în cazul infracțiunilor contra patrimoniului. Generarea de prejudicii în urma

[1] Profesor univ. dr., Facultatea de Drept, Universitatea din Craiova, e-mail: raducanuruxandra@gmail.com.

utilizării unor mijloace frauduloase îmbracă forme diverse, de la cele mai simple la cele mai complexe. Ținând cont de această realitate, legiuitorul a încercat să incrimineze toate fațetele acestui fenomen infracțional. Evoluția tehnică a creat posibilitatea fraudării sistemelor informatice şi a mijloacelor de plată electronice în scopul obținerii injuste a unor beneficii. Producerea unor prejudicii prin aceste fapte şi specificitatea acestui fenomen infracțional a justificat incriminarea lor în cadrul unei categorii distincte de infracțiuni contra patrimoniului.

Cele trei infracțiuni reglementate înpartea specială, titlul II, capitolul IV, au fost inițial prevăzute în legi speciale, în preluarea lor în C.pen. (2009) a fost justificată, pe de o parte, de particularitatea şi frecvența acestor fraude comise prin sisteme informatice şi mijloace de plată electronice, iar, pe de altă parte, de obiectivul pe care şi l-au propus autorii acestui Cod penal de sistematizare a legislației penale.

Astfel cum reiese chiar din denumirea capitolului unde sunt reglementate, aceste infracțiuni au la bază frauda în urma căreia se generează un prejudiciu material unei persoane fizice sau juridice.

Infracțiunea cea mai des întâlnită care are la bază frauda este aceea de înşelăciune[2], frauda fiind adesea echivalată cu înşelarea încrederii victimei, cu inducerea în eroare a acesteia, aşa încât, chiar victima este de acord cu actul păgubitor. Frauda se metamorfozează şi primeşte o reglementare distinctă în funcție de domeniul în care se produce (fiscal, medical, informatic, finanțări din fonduri europene etc.). Aceeaşi situație o găsim şi în alte sisteme de drept, cu criticile aferente[3], întrucât incriminarea comportamentelor frauduloase nu apare mereu justificată, fiind dat ca exemplu cazul în care reglementarea infracțiunii derivate se suprapune peste infracțiunea „mamă".

În capitolul IV „Fraude comise prin sisteme informatice şi mijloace de plată electronice", legiuitorul a incriminat trei infracțiuni: frauda

[2] Reglementată de dispozițiile art. 244 C.pen. (2009) potrivit cărora *„ (1) Inducerea în eroare a unei persoane prin prezentarea ca adevărată a unei fapte mincinoase sau ca mincinoasă a unei fapte adevărate, în scopul de a obţine, pentru sine sau pentru altul, un folos patrimonial injust şi dacă s-a pricinuit o pagubă se pedepseşte cu închisoarea de la 6 luni la 3 ani. (2) Înşelăciunea săvârşită prin folosirea de nume sau calităţi mincinoase ori de alte mijloace frauduloase se pedepseşte cu închisoarea de la unu la 5 ani."*.

[3] M.-L. Rassat, *Droit pénal spécial. Infractions des et contre les particuliers*, 5[e]édition, Paris, Dalloz, 2006, p. 155.

informatică, efectuarea de operațiuni financiare în mod fraudulos, acceptarea operațiunilor financiare efectuate în mod fraudulos. Elementul comun al celor trei reglementări este reprezentat de obținerea unui beneficiu material prin astfel de fapte săvârşite utilizând mijloace sofisticate (sisteme informatice şi mijloace de plată electronice), ceea ce a determinat prevederea lor distinctă în cadrul infracțiunilor patrimoniale.

Aşa cum reiese chiar din denumirea dată de legiuitor acestui capitol, infracțiunile reglementate aici au ca punct de plecare frauda. Şi în denumirea fiecărei infracțiuni se regăseşte condiția fraudei sau a folosirii de mijloace frauduloase de către făptuitor în comiterea infracțiunii. După cum s-a apreciat[4] sublinierea nu este inutilă, ci, dimpotrivă, accentuează gravitatea faptei generată de comportamentul fraudulosşi, în plus, evidențiază condiția ca făptuitorul să cunoască împrejurarea că acțiunea sa contravine voinței titularului. Aşadar, obiectul juridic comun acestor infracțiuni care a determinat gruparea lor într-un capitol distinct este reprezentat de relațiile sociale de ordin patrimonial care implică utilizarea sistemelor informatice şi mijloacelor de plată electronice în mod corect, fără fraudarea acestora.

2. Reglementarea fraudelor comise prin sisteme informatice şi mijloace de plată electronice în C. Pen. (2009)

În C.pen. (2009) în Titlul II „Infracțiuni contra patrimoniului", capitolul IV au fost prevăzute trei incriminări ce presupun fraude comise prin sisteme informatice şi mijloace de plată electronice.

Prima dintre ele, infracțiunea de fraudă informatică a fost inițial reglementată prin L. nr. 161/2003, şi constă în *„introducerea, modificarea sau ştergerea de date informatice, restricționarea accesului la aceste date ori împiedicarea în orice mod a funcționării unui sistem informatic, în scopul de a obține un beneficiu material pentru sine sau pentru altul, dacă s-a cauzat o pagubă unei persoane"*[5], iar pedeapsa este închisoarea de la 2 la 7 ani.

Reglementarea infracțiunii porneşte de la situația premisă a existenței unor date informatice sau a unui sistem informatic fără de care nu poate fi săvârşită infracțiunea în oricare din modalitățile ei normative.

[4] E. Dreyer, *Droit pénal spécial*, Ellipses Éditions marketing S.A., Paris, 2008, p. 367.

[5] Potrivit dispozițiilor art. 249 C.pen. (2009).

Analiza reglementării este completată de explicarea acestor noțiuni în partea generală a C.pen. (2009). Astfel, prin sistem informatic se înțelege *„orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic”*[6], iar prin date informatice se are în vedere *„orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic”*[7].

Infracțiunea a fost privită cel mai adesea ca o variantă a infracțiunii de înşelăciune, mai ales având în vederea producerea pagubei de care legiuitorul leagă existența infracțiunii, dar şi scopul făptuitorului de a obține un beneficiu material pentru sine sau pentru altul, elemente care se regăsesc şi în structura infracțiunii de înşelăciune. Pe de altă parte, oricare dintre variantele în care se poate realiza elementul material al fraudei informatice – introducerea, modificare, ştergerea de date informatice, restricționarea accesului la aceste date sau împiedicarea în orice mod a funcționării unui sistem informatic – pot crea persoanei păgubite o stare de eroare care o împiedică să acționeze pentru a-şi proteja patrimoniul. Într-o altă opinie[8], pornind tot de la producerea pagubei ca element constitutiv al infracțiunii, frauda informatică este considerată o specie de furt, particularitatea ei fiind că este comisă printr-un sistem informatic. Apreciem însă că suntem în prezența unei variante de înşelăciune, iar elementul esențial care o apropie de această infracțiune este starea de eroare produsă victimei prin acțiunile incriminate, eroare care îi permite făptuitorului să acționeze nestingherit, fără opoziția victimei.

Aceasta a fost şi motivația care a determinat, în practică, respingerea cererii inculpatului de schimbare a încadrării juridice din infracțiunea de înşelăciune în infracțiunea de fraudă informatică. Astfel, a fost reținută infracțiunea de fraudă informatică prin postarea de anunțuri de vânzare a unor bunuri pe platforme specializate, urmată de solicitarea de către inculpat a achitării unui avans la perfectarea tranzacției după care victimele nu mai beneficiau de bunurile tranzacționate. Instanța[9] a reținut că inducerea în

[6] Potrivit dispozițiilor art. 181 alin. 1 C.pen. (2009).

[7] Potrivit dispozițiilor art. 181 alin. 2 C.pen. (2009).

[8] V. Cioclei, *Drept penal. Parte specialăI. Infracțiuni contra persoanei şi contra patrimoniului*, Ed. C.H.Beck, Bucureşti, 2016, p. 375.

[9] Curtea de Apel Craiova, secția penală şi pentru cauze cu minori, dec. nr. 301/2017, [Online] la www.rolii.ro.

eroare, invocată de inculpat ca element constitutiv al infracțiunii de înşelăciune la încheierea contractului, a fost prezentă încă din momentul introducerii datelor informatice constând în postarea anunțurilor de vânzare on line.

În practica judiciară s-a apreciat că, din aceste considerente, infracțiunea de înşelăciune nu va fi reținută în concurs cu infracțiunea de fraudă informatică, deoarece aceasta din urmă reprezintă „o variantă a infracțiunii de înşelăciune săvârşită în mediul virtual”[10], aplicându-se exclusiv norma specială reprezentată de infracțiunea de fraudă informatică.

De asemenea, incriminarea distinctă a infracțiunii de fraudă informatică era necesară având în vederea particularitatea săvârşirii înşelătoriei, mediul virtual în care operează făptuitorul. În doctrina juridică franceză, discutându-se despre incriminarea distinctă a unor fapte de înşelăciune s-a arătat[11], motivat, că aceasta este justificată fie în cazul în care infracțiunea de înşelăciune nu se poate aplica, fie în cazul în care aceasta nu acoperă decât parțial faptele cuprinse în varianta incriminată.

În ceea ce priveşte elementul material al infracțiunii, acesta poate fi realizat prin mai multe modalități alternative prevăzute în textul de lege: introducerea, modificarea, ştergerea de date informatice, restricționarea accesului la aceste date sau împiedicarea în orice mod a funcționării unui sistem informatic. Parțial, elementul material al infracțiunii se regăseşte şi într-o altă incriminare din C.pen. (2009) ceea ce pune problema reținerii cumulative a celor două infracțiuni, Astfel, în Titlul VII „Infracțiuni contra siguranței publice”, capitolul VI „Infracțiuni contra siguranței şi integrității sistemelor şi datelor informatice” este prevăzută infracțiunea de alterare a integrității datelor informatice ce constă în *„fapta de a modifica, şterge sau deteriora date informatice ori de a restricționa accesul la aceste date, fără drept”*[12], iar pedeapsa prevăzută de lege este închisoarea de la unu la 5 ani.

Infracțiunea de alterare a integrității datelor informatice nu are în comun cu infracțiunea de fraudă informatică decât anumite modalități de săvârşire a elementului material, şi anume, modificarea sau ştergerea datelor informatice ori restricționarea accesului la aceste date. Plecând de la această asemănare s-ar putea ajunge la concluzia unei suprapuneri de reglementare.

[10] Î.C.C.J., secția penală, dec. nr. 2106/2013, [Online] la www.scj.ro.

[11] M.-L. Rassat, *op. cit.*, p. 155.

[12] Potrivit dispozițiilor art. 362 C.pen. (2009).

În realitate, opinia corectă[13] este aceea că nu se poate reține o absorbție a infracțiunii prevăzute de art. 362 C.pen. (2009) în infracțiunea de fraudă informatică, fiind vorba de infracțiuni autonome.

Cele două infracțiuni sunt distinct reglementate, în capitole diferite ceea ce înseamnă că şi valorile sociale care sunt protejate prin aceste incriminări sunt diferite.

În plus, in cazul infracțiunii de alterare a integrității datelor informatice, elementul material, chiar dacă presupune o parte din modalitățile de săvârşire ale infracțiunii de fraudă informatică cuprinde şi o cerință negativă care condiționează existența infracțiunii, aceea ca faptele să fie săvârşite fără drept. Condiția săvârşirii fără drept este necesară şi condiționează existența infracțiunii pentru că numai în aceste condiții se aduce atingere valorii sociale ocrotite de legea penală. Siguranța şi integritatea sistemelor şi datelor informatice sunt periclitate în cazul în care acțiunile incriminate sunt neautorizate, sunt comise fără drept. Lipsa acestei condiționări din elementul material al infracțiunii de fraudă informatică demonstrează că, în cazul acestei incriminări, legiuitorul nu a avut în vedere, nici măcar în subsidiar, protecția siguranței şi integrității sistemelor şi datelor informatice. Ceea ce este evident în cazul infracțiunii de fraudă informatică este paguba produsă prin acțiunile incriminate care denotă clar că intenția legiuitorului a fost aceea de a proteja patrimoniul.

Un alt argument pe care-l aduce acelaşi autor[14] în sprijinul soluției concursului de infracțiuni este acela că trebuie făcută o distincție între cel care săvârşeşte faptele având dreptul să o facă şi cel care comite aceleaşi fapte fără a fi îndreptățit.

În practica judiciară[15], infracțiunea de fraudă informatică a fost reținută în cazul în care au loc vânzări fictive de bunuri on-line, realizate prin intermediul platformelor specializate în tranzacționarea de bunuri on-line, care cauzează un prejudiciu persoanelor vătămate induse în eroare prin introducerea de date informatice cu privire la existența bunurilor şi determinate, în acest mod, să plătească prețul unor bunuri inexistente. De regulă, ea se reține în concurs cu infracțiunea de constituirea unui grup infracțional organizat, membrii unei grupări săvârşind multiple acte

[13] V. Cioclei, *op. cit.*, p. 377.

[14] *Idem.*

[15] Î.C.C.J., secția penală, dec. nr. 2106/2013, [Online] la www.scj.ro.

materiale specifice infracțiunii de fraudă informatică accesând, fără drept, în mod repetat, diferite sisteme informatice, obținând date informatice ale unor persoane fizice, modificând sau ştergând alte date informatice, dar şi restricționând accesul utilizatorilor autorizați la sistemele informatice prin postarea de bunuri fictive pe site-uri de vânzări on line creând conturi de acces cu date fictive şi folosind site-uri de phishing, operațiuni în urma cărora au obținut sume însemnate de bani[16].

Consumarea infracțiunii este dependentă de producerea rezultatului cerut de lege şi înscris în norma de incriminare – producerea unei pagube. Tentativa se pedepseşte.

A doua infracțiune prevăzută de C.pen.(2009) în cadrul capitolului privind fraudele comise prin sisteme informatice şi mijloace de plată electronice priveşte efectuarea de operațiuni financiare în mod fraudulos şi constă în „(1*) Efectuarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, prin utilizarea, fără consimțământul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia, se pedepseşte cu închisoarea de la 2 la 7 ani.(2) Cu aceeaşi pedeapsă se sancționează efectuarea uneia dintre operațiunile prevăzute în alin. (1), prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.(3) Transmiterea neautorizată către altă persoană a oricăror date de identificare, în vederea efectuării uneia dintre operațiunile prevăzute în alin. (1), se pedepseşte cu închisoarea de la unu la 5 ani.”*[17]

Infracțiunea este reglementată într-o variantă tip, o variantă asimilată şi o variantă atenuată şi are în vedere mai multe modalități de săvârşire. În cazul formei tip, elementul material poate fi realizat prin efectuarea de operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri. Oricare din aceste operațiuni trebuie să aibă loc prin utilizarea, fără consimțământul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia. Şi în varianta asimilată se au in vedere aceleaşi fapte săvârşite prin utilizarea neautorizată a oricăror date de

[16] Curtea de Apel Alba-Iulia, secția penală şi pentru cauze cu minori, dec. nr.688/A /2014, [Online] lawww.rolii.ro.

[17] Potrivit dispoziţiilor art. 250 C.pen. (2009).

identificare sau prin utilizarea de date de identificare fictive, iar varianta atenuată are în vedere doar actele de transmitere neautorizată a oricăror date de identificare în vederea efectuării uneia dintre operațiunile ce constituie elementul material al infracțiunii în varianta tip.

A treia incriminare din gruparea fraudelor comise prin sisteme informatice şi mijloace de plată electronice priveşte acceptarea operațiunilor financiare efectuate în mod fraudulos şi constă în *„(1) Acceptarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, cunoscând că este efectuată prin folosirea unui instrument de plată electronică falsificat sau utilizat fără consimțământul titularului său, se pedepseşte cu închisoarea de la unu la 5 ani.(2) Cu aceeaşi pedeapsă se sancționează acceptarea uneia dintre operațiunile prevăzute în alin. (1), cunoscând că este efectuată prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive. ”*[18]

Infracțiunea este reglementată în varianta tip şi într-o variantă asimilată. În varianta tip, elementul material constă în acceptarea uneia dintre operațiunile prevăzute în textul de lege cunoscând că este efectuată prin folosirea unui instrument de plată falsificat sau utilizat fără consimțământul titularului său. În varianta asimilată, elementul material se realizează prin acceptarea aceloraşi operațiuni, dar, de data aceasta este impusă condiția ca făptuitorul să cunoască efectuarea operațiunii prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.

3. Concluzii

Alegerea legiuitorului de a grupa cele trei incriminări într-un capitol separat în cadrul infracțiunilor patrimoniale are în vedere elementul comun ale acestora care priveşte atingerile aduse patrimoniului unei persoane. Valoarea socială protejată de legiuitor prin aceste incriminări trebuie avută în vedere pentru delimitarea acestora de fapte cu conținut asemănător. Condițiile impuse de legiuitor pentru existența infracțiunii vin să evidențieze elementul de fraudă care se regăseşte în fiecare dintre cele trei incriminări, iar particularitatea fraudei este mediul virtual în care aceasta se manifestă.

[18] Potrivit dispoziţiilor art. 251 C.pen. (2009).

ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

FACTURA ÎNTRE ORIGINAL, DUPLICAT ȘI DEMATERIALIZARE

THE INVOICE BETWEEN ORIGINAL, DUPLICATE AND DEMATERIALIZATION

IOANA MARIA COSTEA[1]

Rezumat: Prezentul studiu își propune să facă o analiză a unui mijloc specific de lucru al procedurilor de stabilire a creanțelor fiscale: factura. Acest instrument, document justificativ este extrem de prezent în mecanismele contractuale între profesioniști și generează efecte juridice predilect în plan fiscal. Asupra naturii juridice a acestui document, a forței sale probante și a efectelor sale, vom puncta o serie de nuanțe atât din perspectivă fiscală, cât și din practica litigiilor între profesioniști. În egală măsură, studiul va analiza sistemele contemporane de emitere și comunicare a facturilor, în medii electronice și efectele acestora.
Cuvinte-cheie: factură, on-line, electronic, copie, original

Abstract: The present study aims to analyze a specific instrument of the procedures for determining the tax debts: the invoice. This instrument, supporting document, is extremely present in contractual arrangements between professionals and generates legal effects primarily on a fiscal level. On the legal nature of this document, its probative force and its effects, we will point to a range of nuances both from a tax perspective and from the practice of litigation between professionals. Equally, the study will look at contemporary systems for issuing and communicating invoices in electronic environments and the effects of these invoices.
Keywords: invoice, online, electronic, copy, original

1. Sediul materiei privind factura. Definiția facturii

Sediul materiei este dat de art. 319 C.Fisc. – Legea nr. 207/2015. Art. 319 C.Fisc[2]. definește factura - (1) În înțelesul prezentului titlu sunt

---

[1] Conferențiar univ. dr., Facultatea de Drept, Universitatea "Alexandru Ioan Cuza" din Iași, ioana.costea@uaic.ro

[2] Conform OMFP nr. 2634/2015, publicat în M.Of. nr. 910 din 9 decembrie 2015, pct. 26. *Toate operațiunile privind factura (întocmire, utilizare, arhivare, corectare, reconstituire) se*

considerate facturi *documentele sau mesajele pe suport hârtie ori în format electronic, dacă acestea îndeplinesc condițiile stabilite în prezentul articol.* (4) În înțelesul prezentului titlu, prin factură electronică se înțelege *o factură care conține informațiile solicitate în prezentul articol și care a fost emisă și primită în format electronic.*

Din definițiile normative înțelegem că factura este un document sau mesaj, care se particularizează și confirmă ca natură juridică prin conținutul acestuia.

Conținutul facturii este reglementat prin dispozițiile art. 319 alin. (20) C. fisc. printr-o enumerare, pe care practica judiciară o indică ca fiind *de minimis* și cu condiționalizare absolută pentru efectele acestui document sau mesaj.

Distingem trei nivele de conținut. Un prim nivel conține elemente de individualizare a înscrisului. Factura este un document/mesaj extrem de individualizat și trasabil, prin aceea că include cu necesitate: a) numărul de ordine, în baza uneia sau a mai multor serii, care identifică factura în mod unic; b) data emiterii facturii. Această trasabilitate are o funcție semnificativă în materia controlului fiscal, în sensul că o operațiune impozabilă este identificabilă atât la furnizor, cât și la client prin unicitatea facturii.

Al doilea nivel de conținut privește elemente ”contractuale”[3]; având în vedere că suntem pe teritoriu de taxă pe valoare adăugată (TVA) pentru care faptul generator este ”vânzarea[4]„ unui bun (cu formele specifice livrarea de bunuri, achizițiile intracomunitare și importul, care răspund la problema aplicării teritoriale) ori prestarea de servicii. În context economic, aceste fapte juridice apar cel mai adesea, dacă nu unanim pe suport contractual, iar elementele contractuale sunt relevante inclusiv în plan fiscal. În sensul art. 319 alin. (20) C. fisc., factura cuprinde:

- informații privind data executării contractului*: c) data la care au fost livrate bunurile/prestate serviciile sau data încasării unui*

efectuează conform prevederilor Codului fiscal și ale Normelor metodologice de aplicare a acestuia.

[3] C.T. Ungureanu, *Dreptul comerțului internațional. Contracte de comerț internațional*, Editura Hamangiu, București, 2014, pp. 42-48.

[4] Definită generic și prudent de C. fisc. ca fiind *transferul dreptului de a dispune de bunuri ca și un proprietar* - art. 270 alin. 1 C. fisc.

avans, în măsura în care această dată este anterioară datei emiterii facturii;

- informații privind părțile contractului: *d) denumirea/numele, adresa și codul de înregistrare în scopuri de TVA sau, după caz, codul de identificare fiscală ale persoanei impozabile care a livrat bunurile sau a prestat serviciile*[5]*; f) denumirea/numele și adresa beneficiarului bunurilor sau serviciilor, precum și codul de înregistrare în scopuri de TVA sau codul de identificare fiscală al beneficiarului, dacă acesta este o persoană impozabilă ori o persoană juridică neimpozabilă*[6]*;*

- obiectul contractului, în sensul de obiect executat: *h) denumirea și cantitatea bunurilor livrate, denumirea serviciilor prestate, precum și particularitățile prevăzute la art. 266 alin. (3) în definirea bunurilor, în cazul livrării intracomunitare de mijloace de transport noi;*

- obiectul contractului, în sensul de contraprestație: *i) baza de impozitare a bunurilor și serviciilor ori, după caz, avansurile facturate, pentru fiecare cotă, scutire sau operațiune netaxabilă, prețul unitar, exclusiv taxa, precum și rabaturile, remizele, risturnele și alte reduceri de preț, în cazul în care acestea nu sunt incluse în prețul unitar;*

- cota de TVA: *j) indicarea cotei de taxă aplicate și a sumei taxei colectate, exprimate în lei, în funcție de cotele taxei;*

Al treilea nivel de conținut are funcții exclusiv fiscale, pentru că particularizează ipoteze specifice de lucru și individualizează conținutul facturii în scenarii de lucru. Aceste mențiuni sunt cumva cazuri speciale și alternative și se întâlnesc în scenarii paralele:

---

[5] Alternativ cuprinde pentru prestatorul care nu e stabilit în România: e) denumirea/numele furnizorului/prestatorului care nu este stabilit în România și care și-a desemnat un reprezentant fiscal, precum și denumirea/numele, adresa și codul de înregistrare în scopuri de TVA, conform art. 316, ale reprezentantului fiscal;

[6] Alternativ cuprinde pentru beneficiarul care nu e stabilit în România: g) denumirea/numele beneficiarului care nu este stabilit în România și care și-a desemnat un reprezentant fiscal, precum și denumirea/numele, adresa și codul de înregistrare prevăzut la art. 316 ale reprezentantului fiscal;

- autofacturarea (probabil singura ipoteză necontractuală): *k) în cazul în care factura este emisă de beneficiar în numele și în contul furnizorului, mențiunea "autofactură;"*
- aplicarea unei scutiri: *l) în cazul în care este aplicabilă o scutire de taxă, trimiterea la dispozițiile aplicabile din prezentul titlu ori din Directiva 112 sau orice altă mențiune din care să rezulte că livrarea de bunuri ori prestarea de servicii face obiectul unei scutiri;*
- aplicarea taxei de către ”client” și nu de către furnizor, la taxarea inversă: *m) în cazul în care clientul este persoana obligată la plata TVA, mențiunea "taxare inversă";*
- aplicarea unui regim de taxare special: *n) în cazul în care se aplică regimul special pentru agențiile de turism, mențiunea "regimul marjei - agenții de turism"; o) dacă se aplică unul dintre regimurile speciale pentru bunuri second-hand, opere de artă, obiecte de colecție și antichități, una dintre mențiunile "regimul marjei - bunuri second-hand", "regimul marjei - opere de artă" sau "regimul marjei - obiecte de colecție și antichități", după caz;*
- aplicarea mecanismului derogatoriu de ”TVA la încasare”, care afectează exigibilitatea TVA*: p) în cazul în care exigibilitatea TVA intervine la data încasării contravalorii integrale sau parțiale a livrării de bunuri ori a prestării de servicii, mențiunea "TVA la încasare";*
- mențiuni privind documente în legătură cu factura pentru operațiunile fragmentate: *r) o referire la alte facturi sau documente emise anterior, atunci când se emit mai multe facturi ori documente pentru aceeași operațiune.*

Astfel, definirea facturii (care a încetat să mai fie guvernată de condiții de formă stricte și de un format predefinit[7]) se face raportat la conținutul acesteia. De altfel, cu privire la formă, textul de la art. 319 alin.

[7] Reglementarea veche făcută prin HG nr. 831/1997 - pentru aprobarea modelelor formularelor comune privind activitatea financiara și contabilă și a normelor metodologice privind întocmirea și utilizarea acestora, publicat în M. Of nr. 368 din 19 decembrie 1997 – instituia un formular standard pentru cele doua variante ale facturii: factura fiscală (14-4-10/A) și factura (14-4-10/aA). Conform pct. 7 al art. VI din Legea nr. 343 din 17 iulie 2006, publicată în M. Of. nr. 662 din 1 august 2006, începând cu data de 1 ianuarie 2007, se abrogă prevederile referitoare la factura fiscală (cod 14-4-10/A) și factura (cod 14-4-10/aA) din Hotărârea Guvernului nr. 831/1997.

(1) C. fisc., vorbește despre document sau mesaj *pe suport hârtie ori în format electronic*; textul de la alin. (4) C. fisc. definește factura electronică ca fiind factura *care a fost emisă și primită în format electronic.*

Distingem între factura în format fizic și factura în format electronic, care are două momente dematerializate și anume atât emiterea cât și transmiterea-primirea între furnizor și beneficiar.

2. Dematerializarea. *Qui prodest*?

În mod tradițional, activitatea economică este încetinită de rigorile procedurilor și proceselor cu relevanță fiscală. Astfel, emiterea facturii este un efort suplimentar pentru profesionist, atât logistic, cât și financiar. Regimul relativ liberal al facturii din ultima perioadă normativă se justifică tocmai prin accentul pus de modelul normativ european (Directiva 112/2006/CE[8]) pe simplificarea acestor exigențe față de agentul economic.

În acest context, forma normativă *mesaj în format electronic* apare ca o alternativă mai facilă. Apetitul pentru dematerializarea se justifică prin automatizarea procesului de facturare, care permite gestiunea unui volum mare de clienți, cum este cazul marilor furnizori de utilități; prin diminuarea costurilor cu gestiunea informațiilor din facturi, întrucât gestiunea unei facturi nu se limitează doar la emitere, ci implică și colectarea acestor date, identificarea momentului plății, scadenței, accesoriilor etc. și centralizarea acestora; în urma procesului de centralizare, se impune desigur completarea registrelor contabile și a jurnalelor contabile cu aceste date.

Facturile în format electronic, în sisteme integrate de emitere, gestiune și comunicare permit de asemenea ameliorarea trasabilității unei operațiuni – indexarea facturilor pe ani, pe clienți, pe furnizori etc., gestiunea plăților și a termenelor de plată, ameliorarea procedurilor interne de validare a facturilor și nu în ultimul rând eliminarea arhivei imprimate (și a costurilor implicite).

În egală măsură, dematerializarea facturilor fiscale este suport pentru preluarea informațiilor în declarațiile fiscale de impunere ori informative. În acest context, dematerializarea urmează un traseu mai complex și se transferă către o dematerializare a controlului fiscal, aspect

[8] JO L 347, 11.12.2006, p. 1-118 (ES, CS, DA, DE, ET, EL, EN, FR, IT, LV, LT, HU, MT, NL, PL, PT, SK, SL, FI, SV) ediție specială în limba română: capitol 09 volum 003 p. 7 – 125, Alte ediții speciale (BG, HR)

asupra căruia probabil, că s-ar impune o analiză mai detaliată ce excede cadrul acestui studiu.

3. Funcția fiscală a facturii

Scopul reglementării este incontestabil legat de locul reglementării și anume textul din Codul fiscal privind TVA. Astfel, funcția primară a facturii este de a evidenția taxa pe valoarea adăugată, în două dimensiuni.

Pe de o parte, factura indică cuantumul efectiv al taxei colectate (pentru furnizor) ori taxei deductibile (client), inclusiv lipsa acesteia și temeiul legal al lipsei. Astfel, factura reprezintă un element matematic de contabilizare a taxei.

Pe de altă parte, factura cuprinde și elementele probatorii relevante pentru condiția de fond a deductibilității (părțile, obiect, trasabilitate prin număr și dată etc.).

Participarea facturii la verificarea condițiilor de deductibilitate ale taxei provenind dintr-o anumită tranzacție, este majoră, dacă nu chiar exclusivă. În acest raționament se încadrează inclusiv soluțiile de practică judiciară, dintre care cea mai sonoră și relativ rigidă dispune:

> ICCJ, s. reunite, RIL, dec. nr. V/2007: *Taxa pe valoarea adăugată nu poate fi dedusă şi nici nu se poate diminua baza impozabilă la stabilirea impozitului pe profit în situaţia în care documentele justificative prezentate nu conţin sau nu furnizează toate informaţiile prevăzute de dispoziţiile legale în vigoare la data efectuării operaţiunii pentru care se solicită deducerea TVA.*

Această soluție a Înaltei Curți, din fericire reconfigurată de practica mai recentă sanctifica textele privind conținutul documentelor justificative, mai ales factura și le consacra ca mijloc de probă absolut, irefragabil. Acest regim probatoriu unitar era desigur condiționat de completarea corectă a tuturor elementelor documentului justificativ, implicit factură (fiscală).

Față de acest reper de jurisprudență națională (care s-ar impune cumva revocat ca și izvor de drept, chiar dacă formal nu avem consacrată o procedură în acest sens), am invoca repere de jurisprudență CJUE în interpretarea textului sursă și anume art. 226 din Directiva 2006/112/CE. Amintim următoarele repere jurisprudențiale: statele membre pot stabili anumite particularități, doar dacă nu tind *să facă practic imposibilă sau excesiv de dificilă exercitarea dreptului de deducere*, prin numărul lor sau

prin tehnicitate[9]; nu este permis statelor membre să condiționeze exercitarea dreptului de deducere a TVA□ului de respectarea condițiilor privind conținutul facturilor, care nu sunt prevăzute în mod expres de dispozițiile Directivei 2006/112/CE[10] .

La nivel național, în jurisprudența instanțelor de contencios administrativ observăm o apreciere mai prudentă și mai relaxată a condiționalității dintre anumite elemente ale facturii și exercitarea dreptului de deducere, mai ales în materia TVA.

> ICCJ, s. cont. adm. fisc., dec. nr. 1880/2015[11]: *Cu privire la respingerea dreptului de deducere a TVA în sumă de 33.625 lei aferentă bunurilor achiziţionate de la SC B.C. SRL, instanţa de fond a reţinut că în perioada 5.01.2010-2.06.2010 reclamanta SC D.S.U.R. SRL a achiziţionat materiale consumabile (tablă, ţeavă, cornier) de la SC B.C. SRL în valoare totală de 210.600,71 lei, din care TVA în sumă de 33.625,33 lei, iar facturile îndeplinesc calitatea de document justificativ, având completate toate rubricile conform (...) Codului fiscal, iar susţinerea pârâtei că s-au înscris date eronate cu privire la numerele de înmatriculare a mijloacelor de transport cu care au fost efectuate aprovizionările de materiale consumabile, nu constituie o condiţie pentru deducerea TVA.*

Conchidem astfel că funcția primară a facturii este reglarea mecanismelor fiscale pentru identificarea taxei deductibile/taxei colectate ori a ipotezei de exceptare. Prin ricoșeu, în ipoteza persoanei impozabile, care determină și impozitul direct (impozit pe profit ori impozit pe venit) în funcție de evidențele contabile factura are funcția de document justificativ și pentru cheltuiala deductibilă, cu un transfer parțial de regim juridic.

4. Funcția ”comercială/civilă” a facturii

Dacă factura este o instituție de drept fiscal se ridică firesc întrebarea de ce am mai analiza acest element și în planul relațiilor sociale

---

[9] CJUE, C-123/87, Léa Jeunehomme et Société anonyme d’étude et de gestion immobilière „EGI” împotriva État belge, ECLI:EU:C:1988:408, pct. 17

[10] CJUE, C-368/09, Pannon Gép Centrum Kft împotriva APEH Központi Hivatal Hatósági Főosztály, ECLI:EU:C:2010:441, pct. 41.

[11] http://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=127358, consultată în data de 1.10.2017.

de drept comercial/civil (pentru conformitate terminologică, voi utiliza noțiunea de civil). Răspunsul la această întrebare derivă din aspectele prezentate la punctul 1 al prezentului studiu și anume elementele contractuale expuse destul de detaliat în factură (părțile contractului, obiectul contractului, confirmarea executării).

Astfel, s-a ridicat în doctrină întrebarea ce valoarea juridică are factura ca înscris sau ca mesaj electronic în registrul Codului civil.

> ICCJ, s. a II-a civ., Decizia nr. 1017/2009[12]: *În aplicarea prevederilor art. 46 Cod comercial și ale art.6 din Legea nr. 82/1991, factura fiscală nu este decât un document justificativ, care stă la baza înregistrărilor în contabilitate furnizorului sau prestatorului și a cumpărătorului, respectiv beneficiarului, ea fiind un mijloc de probă cu privire la operaţiunea facturată, neavând calitatea de act juridic, care să trebuiască să îndeplinească cerinţele art. 948 Cod civil, nici chiar atunci când – ca în cauza de faţă – probează existenţa unui contract comercial consensual, pentru care părţile nu au confecţionat un instrumentum.*

Rezultă astfel fără prea mare surpriză, că factura este un înscris și nu un act juridic (desigur nu un contract). Această precizare se corelează cu interogația din petitul unor acțiuni în civil și anume dacă se poate solicita anularea unei facturi și evident că răspunsul este nu. Am vedea totuși o nuanță în cazul contractelor cu executare succesivă, întrucât determinarea valorii prestațiilor părților se face exclusiv prin factură[13]. Or, aceste prestații pot fi obiectul unor cereri în instanță, care să nu vizeze anularea contractului, ci doar elemente ale raportului contractual punctuale privind o

[12] http://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=83130, consultată în data de 1.10.2017.

[13] Jud. Slatina, s.civ. nr. 5107/2009: *În al doilea rând reţine instanţa că nici facturile fiscale neînsuşite de către cel căruia i se adresează nu pot fi considerate acte juridice unilaterale deoarece ele nu sunt rezultatul unei voinţe juridice cu intenţia de produce efecte juridice, reprezentând, în acest caz doar un înscris constatator prin care emitentul pretinde de la destinatarul facturii plata unei sume de bani determinată în baza unei convenţii verbale sau scrise. Aceasta din urmă reprezintă contractul încheiat între părţi şi doar acesta poate fi supus desfiinţării prin intermediul acţiunii în anulare*, consultată în data de 1.10.2017, https://legeaz.net/spete-civil-3/anulare-factura-fiscala-zi9

executare parţială[14]. Împărtăşim opinia exprimată în doctrină[15], că există interes în a invoca critici privitoare la aspectele ”constatate” pe calea unei

[14] C.A. Bucureşti: *Facturile de stornare a căror nulitate absolută se solicită, nu reprezintă acte juridice, ci doar un mod de calcul a unor sume de bani, pe care S.C. P G S I SRL le datoră în baza Contractului de prestări servicii de pază nr. 93/10501/02.06.2009. De altfel, potrivit dispoziţiilor art. 1092 şi următoarele Cod civil, doar plata este un act juridic, nu şi facturile emise în acest sens. Factura nu poate fi considerata un act juridic care să trebuiască să îndeplinească cerinţele art. 948 C. civ. (art. 1179 din noul Cod civil), nici în situaţia în care probează existenta unui contract comercial consensual, pentru care părţile nu au întocmit un instrumentum. Aşadar, nu se poate cere printr-o acţiune în justiţie constatarea nulităţii absolute a facturii pentru neîndeplinirea condiţiilor de validitate ale actului juridic, iar eventualele nereguli sau lipsuri din cuprinsul facturii pot fi invocate doar ca apărări vizând forţa probantă a acesteia cu privire la pretenţiile emitentului consemnate în document*, consultată în data de 1.10.2017, http://infodosar.ro/speta.php?id=3127

[15] A. Dumitrescu, Cum contestăm facturile emise de furnizorii de energie electrică?, pe juridice.ro, https://www.juridice.ro/385100/cum-contestam-facturile-emise-de-furnizorii-de-energie-electrica.html, consultată în data de 1.10.2017: *Pornind de la ipoteza că problema expusă nu îşi găseşte soluţia într-o acţiune în anulare a facturilor respective, starea de fapt reprezentată de existenţa unor documente fiscale care consfinţesc un debit nereal al consumatorului faţă de furnizor reclamă, per se, intervenţia instanţei de judecată, cu finalitatea obţinerii unor documente întocmite corect, conţinând obligaţii de plată într-un cuantum just stabilit.*

În acest context, contrar accepţiunii unor instanţe de judecată în sensul că nelegalitatea facturilor întocmite de furnizorul de electricitate şi incorectitudinea acestora nu pot fi invocate pe cale de acţiune principală, ci exclusiv în mod incidental în cadrul apărărilor formulate de consumator împotriva demersurilor în justiţie ale furnizorului, opinăm că, pe lângă acţiunea în anulare, legislaţia în materie oferă justiţiabililor şi alte instrumente legale în vederea iniţierii de cereri de chemare în judecată împotriva operatorilor sus-menţionaţi. Astfel, reţinem că legislaţia specifică (Legea nr. 123/2012 a energiei, Ordinele nr. 64/2014 şi, respectiv, nr. 18/2005 emise de către A.N.R.E.) impune furnizorilor de electricitate respectarea anumitor cerinţe imperative cu privire la întocmirea documentelor de plată şi la modalitatea de calcul şi stabilire a consumului de energie care a stat la originea emiterii celor dintâi şi că, de cele mai multe ori, valorile exagerat de mari ale unor facturi emise de aceşti operatori reprezintă consecinţa vădită a încălcării normelor sus-menţionate. Or, în ipoteza enunţată mai sus, apreciem că orice consumator nemulţumit de cuantumul exagerat al facturii emise de către furnizorul de electricitate şi care constată că aceasta nu îndeplineşte cerinţele legale minime de formă sau conţinut, fiind întocmită şi pe baza unui consum stabilit empiric de către operatorul economic, se poate adresa instanţei de judecată cu o acţiune împotriva acestuia din urmă, având ca obiect obligaţia de a face, demers susţinut în dreptul comun de dispoziţiile art. 1516 C. civ. Punctual, pe cale de acţiune, se poate solicita pronunţarea unei sentinţe prin care instanţa de judecată să oblige furnizorul la întocmirea unor facturi în conformitate cu prevederile Ordinului nr. 64/2014 al A.N.R.E., cu consecinţa ştornării facturilor incorecte şi nelegale, şi la calcularea unui consum în

acțiuni directe, nu numai prin apărări față de pretenția exprimată de creditor prin factură. Este cert că acest raport de contradictorialitate nu este ”firesc” în registrul ”civil” al pasivității debitorului, însă în anumite contracte, mai ales cele cu marii furnizori de utilități, debitorul poate avea interesul de a supune controlului judiciar o creanță constată printr-o factură, cu celeritate și fără a aștepta reacția contencioasă a creditorului său. Împărtășim cumva și soluția acțiunii în obligație de a face și anume obligarea creditorului la stornarea și eventual reemiterea facturii pentru segmentul de raport contractual în discuție. Exprimăm o rezervă cu privire la constructul juridic de a promova *o acțiune în obligație de a face*, care apare ca fiind nefiresc și contraproductiv, și apreciem sancțiunea inadmisibilității *unei acțiuni în anulare* ca fiind excesivă.

5. Factura - un înscris …

Dacă am calificat atât fiscal, cât și civil factura, am mai particulariza analiza cu privire la natura facturii, în sensul de a o califica ca și înscris, mai ales în ipoteză de la art. 319 alin. (4) C. fisc. privind factura electronică.

Pornind de la premisă, ca factura este un înscris, ne raportăm analiza la dispozițiile art. 274 și urm. C.proc.civ.

Observăm în primul rând că dispozițiile de la art. 274 și 275 nu se aplică, de vreme ce factura apare în condițiile art. 277 C. proc. civ., ca un înscris întocmit de profesioniști. Apreciem că în condițiile art. 3 C.civ. - (2) *Sunt consideraţi profesionişti toţi cei care exploatează o întreprindere*, (3) *Constituie exploatarea unei întreprinderi exercitarea sistematică, de către una sau mai multe persoane, a unei activităţi organizate ce constă în producerea, administrarea ori înstrăinarea de bunuri sau în prestarea de servicii, indiferent dacă are sau nu un scop lucrativ*, coroborat cu dispozițiile art. 269 C. fisc. - *Persoane impozabile și activitatea economică - (1) Este considerată persoană impozabilă orice persoană care desfășoară, de o manieră independentă și indiferent de loc, activități economice de*

conformitate cu modalităţile reglementate de acelaşi act normativ, pentru consumul uzual sau, în situaţia defectării grupului de măsurare, uzând de procedura regăsită în Ordinul nr. 18/2005 al A.N.R.E..

natura celor prevăzute la alin. (2), oricare ar fi scopul sau rezultatul acestei activități, o persoană impozabilă este întotdeauna un profesionist.

Pentru acest considerent, apreciem că factura este un înscris întocmit de un profesionist.

Dacă particularizăm raportat la factura electronică, corelăm analiza cu dispozițiile art. 282 C. proc. civ., privind înscrisurile pe suport informatic: *(1) Când datele unui act juridic sunt redate pe un suport informatic, documentul care reproduce aceste date constituie instrumentul probator al actului, dacă este inteligibil şi prezintă garanţii suficient de serioase pentru a face deplină credinţă în privinţa conţinutului acestuia şi a identităţii persoanei de la care acesta emană.* (2) *Pentru a aprecia calitatea documentului, instanţa trebuie să ţină seama de circumstanţele în care datele au fost înscrise şi documentul care le-a reprodus.* Observăm că C. proc. civ. dispune cu privire la *datele unui act juridic* și ne întrebăm dacă factura cuprinde datele unui act juridic, de vreme ce aceasta nu este un act juridic. Pentru celelalte condiții, apreciem că factura trebuie să verifice condiția de a fi inteligibilă și garanțiile impuse de C. proc. civ. și C. fisc.

Factura electronică (care ar trebuie să îndeplinească aceleași funcții ca și factura fizică de înscris probatoriu preconstituit) se emite pentru a proba parte a raportului contractual în format electronic și se comunică de una din părți (furnizorul) celeilalte părți (beneficiar) în format electronic, prin e-mail ori platforme securizate. Factura electronică nu este dublată și de o factură fizică (întrucât nu ar mai îndeplini condițiile de la art. 319 alin. (4) C. fisc.) de a fi emisă și comunicată electronic (condiții cumulative). Factura electronică nu este semnată. Din punctul nostru de vedere, factura electronică este un înscris electronic exclusiv.

Această calificare prezintă relevanță dacă ne raportăm la efectele probatorii ale facturii atât într-o procedură fiscală, cât și în una civilă. Pornim de la ipoteza probării unei cheltuieli deductibile ori chiar a unei pretenții contractuale în instanță și invocăm în primul rând tradiția juridică conform căreia deductibilitatea se acordă pe baza originalului.

ICCJ, s. cont. adm. fisc., dec. nr. 1693/2015[16]: *Reclamanta, susţinând pierderea facturii odată cu mutarea, a prezentat atât*

[16] http://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=127344 , consultată în data de 1.10.2017.

organelor de control, cât şi la dosarul cauzei o copie xerox şi nu un duplicat al acestei facturi, acest înscris fiind depus şi la dosarul cauzei, astfel că atât cele reţinute de instanţa de fond, cât şi concluziile expertului sunt lipsite de suport probator. De asemenea, se constată că înscrisul depus de intimata-reclamantă este ilizibil şi nu furnizează informaţiile prevăzute în mod riguros, (…) respectiv: data emiterii facturii, data la care au fost livrate bunurile, mijlocul de transport prin intermediul căruia au fost aduse bunurile.

Și ne întrebăm ce este un original al unui înscris emis și comunicat în spațiul virtual.

Pentru a răspunde, am afirma că în ipoteza facturii electronice nu există un original în format pe hârtie. Originalul este înscrisul exportat electronic din softul furnizorului (comunicat prin e-mail) ori pe platforma de comunicare cu beneficiarul (încărcat de către furnizori).

Și atunci, în momentul constituirii unui dosar fiscal (în arhiva contabilă) ori unui dosar civil (inclusiv în instanță), furnizorul și beneficiarul vor proceda la imprimarea unei ”copii” de pe acest original. Nu putem afirma cu certitudine că acest înscris ieșit din imprimantă este un original întrucât nu verifică condiția unicității și nici nu poartă însemne distincte specifice (cum ar fi semnătura părților). Nu putem afirma nici că suntem în prezența unui duplicat, de vreme ce textul de la art. 285 C. proc. civ, face vorbire despre *înscrisurile notariale sau alte înscrisuri autentice*.

Dacă menținem ipoteza că suntem în prezența unei copii, atunci raportarea la dispozițiile art. 286 C. proc. civ. nu aduce lămuririle necesare[17]. În primul rând, subliniem necorelarea dispozițiilor de la alin. (1)

[17] Art. 286 C. proc. civ. - Regimul copiilor - *(1) Copia, chiar legalizată, de pe orice înscris autentic sau sub semnătură privată nu poate face dovadă decât despre ceea ce este cuprins în înscrisul original. (2) Părţile pot să ceară confruntarea copiei cu originalul, prezentarea acestuia din urmă putând fi întotdeauna ordonată de instanţă, în condiţiile prevăzute la art. 292 alin. (2). (3) Dacă este imposibil să fie prezentat originalul sau duplicatul înscrisului autentic ori originalul înscrisului sub semnătură privată, copia legalizată de pe acestea constituie un început de dovadă scrisă. (4) Copiile de pe copii nu au nicio putere doveditoare. (5) Extrasele sau copiile parţiale fac dovada ca şi copiile integrale sau copiile asimilate acestora, însă numai pentru partea din înscrisul original pe care o reproduc; în cazul în care sunt contestate, iar originalul este imposibil să fie prezentat, instanţa are dreptul să aprecieze, în limitele prevăzute la alin. (3) şi (4), în ce măsură partea din original, reprodusă în extras, poate fi socotită ca având putere doveditoare, independent de părţile din original care nu au fost reproduse.*

și alin. (2) cu ipoteza în discuția și anume aceea a originalului emis exclusiv în mediu de stocare, care nu poate fi prezentat instanței.

Am mai sublinia că existența facturii originale doar în mediul electronic, face ca orice imprimare să fie o copie (care s-ar impune a primi mențiunea *conform cu originalul* atunci când se depune în instanță); și la nivel de probatoriu, ar mai ridica și problema copiei de pe copie.

În al doilea rând, rămânând pe tărâmul ipotezei de înscris exclusiv electronic se ridică problema procedurii de reconstituire. Procedura este reglementată de pct. 32 din OMPF nr. 2634/2015: 32. *În cazul în care documentul dispărut a fost emis de altă entitate, reconstituirea se va face de entitatea emitentă, prin realizarea unei copii de pe documentul existent la entitatea emitentă. În acest caz, entitatea emitentă va trimite entităţii solicitante, în termen de cel mult 10 zile lucrătoare de la primirea cererii, documentul reconstituit.33. Documentele reconstituite vor purta în mod obligatoriu şi vizibil menţiunea "DUPLICAT", cu specificarea numărului şi a datei dispoziţiei pe baza căreia s-a făcut reconstituirea.* Observăm că procedura are în vedere documentele în format fizic; apreciem că în ipoteza înscrisurilor electronice problema este mult mai simplă; originalul este unic și comun atât emitentului cât și beneficiarului. Oricare dintre aceștia poate recomunica înscrisul în format electronic, fără a fi necesară mențiunea duplicat. Desigur în această ipoteză sunt mai consistente amenințările de securitate cybernetică asupra mediului de stocare a acestor înscrisuri.

Concluzii

Reglementările analizate sunt în sine un progres; adaptarea normativului la dinamica vieții economice apare ca un deziderat firesc de acomodare a unor interese relativ divergente și totuși comune.

Interogațiile aferente regimului juridic ale facturii sunt parte din această evoluție și permit conturarea unor direcții de acțiune. Observăm astfel că modelul normativ este anticipat de nevoile practicii economice și judiciare și dezvoltat în direcții utile.

La nivel de legislație secundară, ca întotdeauna se impune corelarea normelor și consolidarea unui regim juridic unitar.

ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

UNELE CONSIDERAȚII PRIVIND INFRACȚIUNEA DE PERTURBARE A FUNCȚIONĂRII SISTEMELOR INFORMATICE

SOME CONSIDERATIONS REGARDING THE OFFENCE OF DISRUPTING THE FUNCTIONING OF COMPUTER SYSTEMS

ADRIAN CRISTIAN MOISE[1]

Rezumat: Pornind de la prevederile art. 5 din Convenția Consiliului Europei privind criminalitatea informatică și de la prevederile art. 4 din Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice, ambele referindu-se la afectarea integrității sistemului informatic, în prezentul articol se realizează o analiză a infracțiunii de perturbare a funcționării sistemelor informatice, prevăzută de art. 363 din Codul penal, urmărindu-se dacă legiuitorul român a transpus prevederile celor două instrumente juridice de la nivel internațional și european. Reglementarea legală urmărește să protejeze datele informatice stocate în cadrul sistemelor informatice, accentul fiind pus pe efectul pe care îl au pentru sistemele informatice afectate acțiunile asupra datelor informatice. Totodată, în articol se analizează atât cel mai cunoscut atac împotriva unui sistem informatic care afectează integritatea sistemului informatic, acesta fiind atacul DOS – Denial of Service –, cât și alte atacuri împotriva unui sistem informatic care afectează integritatea sistemului informatic, cum sunt atacurile bazate pe programele malițioase care au ca scop infectarea sistemului informatic.
Cuvinte cheie: perturbare, sistem informatic, date informatice, atac, programe malițioase.

Abstract: Starting from the provisions of Article 5 of the Council of Europe Convention on Cybercrime and the provisions of Article 4 of the Directive 2013/40/EU on attacks against information systems, both relating to illegal system interference, this Article performs an analysis of the offence of disrupting the functioning of the computer systems sanctioned by Article 363 of the Romanian Criminal Code, in order to ensure that the Romanian legislator transposed the provisions of the two legal instruments from international and European level. The

[1] Lector univ. dr, Universitatea Spiru Haret din București, Facultatea de Științe Juridice, Economice și Administrative, Craiova, România; avocat, Baroul Dolj; E-mail: adriancristian.moise@gmail.com.

legal regulation aims to protect the computer data stored in computer systems, focusing on the effect they have on computer systems affected by the actions on computer data. At the same time, the article analyzes both the most common attack against a computer system that affects the integrity of the computer system, such as the DOS (Denial of Service) attack, as well as other attacks against a computer system that affects the integrity of the computer system, such as the attacks based on malicious programmes aimed at infecting the computer system.
Keywords: disrupting, computer system, computer data, attack, malicious programmes.

1. Introducere

Infracțiunea de perturbare a funcționării sistemelor infoarmatice este prevăzută în art. 363 din Capitolul VI *Infracțiuni contra siguranței și integrității sistemelor și datelor informatice* din Codul penal. Textul de lege prevede că: *„Fapta de a perturba grav, fără drept, funcționarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la date informatice, se pedepsește cu închisoarea de la 2 la 7 ani”*.

Reglementarea legală urmărește să protejeze datele informatice stocate în cadrul sistemelor informatice împotriva atacurilor de piraterie informatică sau altor activități malițioase care au ca scop aducerea în stare de nefuncționare a sistemelor informatice. Spre deosebire de infracțiunea reglementată în art. 362 din Codul penal ce se referă la alterarea a integrității datelor informatice, în cazul infracțiunii de perturbare a funcționării sistemelor informatice, accentul este pus pe efectul pe care îl au pentru sistemele informatice afectate, acțiunile asupra datelor informatice (introducerea, transmiterea, modificarea, ștergerea, deteriorarea sau restricționarea accesului la datele informatice)[2].

2. Incriminarea faptei de afectare a integrității sistemului informatic în cadrul Convenției Consiliului Europei privind criminalitatea informatică

Pentru a proteja accesul operatorilor și utilizatorilor la tehnologia informațiilor și comunicațiilor, Convenția Consiliului Europei privind

[2] Romanian Information Technology Initiative și Guvernul României, *Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică*, București, 2004, p. 61, [Online] la: http://www.riti-internews.ro/ro/ghid.htm, accesat la 22.10.2017.

criminalitatea informatică[3] a prevăzut în art. 5 incriminarea afectării funcționării normale a unui sistem informatic. Art. 5 din Convenție se referă la infracțiunea de afectare a integrității sistemului informatic care implică afectarea gravă, intenționată și fără drept a funcționării unui sistem informatic prin introducerea, transmiterea, periclitarea, ștergerea, deteriorarea, modificarea sau suprimarea datelor informatice[4].

Pentru ca dispozițiile art. 5 să fie aplicate este necesar ca funcționarea sistemului informatic să fie afectată[5]. Termenul de afectare are semnificația oricărui act care interferează cu funcționarea corespunzătoare a sistemului informatic[6]. În plus, textul art. 5 din Convenția Consiliului Europei privind criminalitatea informatică prevede faptul că afectarea sistemului informatic să fie gravă. Este responsabilitatea statelor membre de a stabili criteriile care trebuie îndeplinite pentru ca afectarea sistemului informatic să fie considerată gravă[7].

Am remarcat faptul că acțiunile de introducere și transmitere a datelor informatice nu sunt definite de Convenția Consiliului Europei privind criminalitatea informatică, nici de Raportul Explicativ al Convenției Consiliului Europei privind criminalitatea informatică. Putem considera faptul că acțiunea de introducere a datelor informatice într-un sistem informatic poate fi definită ca orice act în legătură cu interfețele de intrare fizică pentru a transfera informațiile la un sistem informatic, în timp ce

---

[3] Convenția Consiliului Europei privind criminalitatea informatică a fost adoptată la Budapesta la data de 23.11.2001, disponibilă [Online] la: http://www.conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, accesat la 22.10.2017.

[4] În Raportul Explicativ al Convenției Consiliului Europei privind criminalitatea informatică pct. 61 sunt definiți următorii termeni: termenii de „periclitare” și „deteriorare” se referă la alterarea integrității datelor și programelor informatice; termenul de „ștergere” a datelor informatice semnifică acțiunea de îndepărtare a datelor informatice din dispozitivele de stocare; termenul de „suprimare” a datelor informatice reprezintă acțiunea care afectează disponibilitatea datelor informatice; termenul de „modificare” a datelor informatice se referă la acțiunea de alterare a datelor informatice existente în special prin instalarea unor programe distrugătoare.

[5] A. Savin, *EU Internet Law*. Edward Elgar Publishing Limited, Cheltenham, Glos, 2013, p. 238.

[6] Raportul Explicativ al Convenției Consiliului Europei privind criminalitatea informatică pct. 66, disponibil [Online] la: http://conventions.coe.int/treaty/en/reports/html/185.htm, accesat la 22.10.2017.

[7] Raportul Explicativ al Convenției Consiliului Europei privind criminalitatea informatică pct. 67, disponibil [Online] la: http://conventions.coe.int/treaty/en/reports/html/185.htm, accesat la 22.10.2017. M. Gercke, International Telecommunication Union. *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, Geneva, 2012, p. 33, [Online] la: www.itu.int/ITU D/cyb/cybersecurity/legislation.html, accesat la 22.10.2017.

acțiunea de transmitere a datelor informatice se referă la acte care necesită intrarea de la distanță a datelor în sistemul informatic[8].

În literatura de specialitate s-a abordat problema dacă spam-ul sau mesajul nesolicitat ar putea fi incriminat de prevederile art. 5 din Convenție, întrucât spam-ul poate suprasolicita funcționarea sistemului informatic. La ora actuală, Convenția Consiliului Europei privind criminalitatea informatică nu incriminează în mod explicit spam-ul. Legiuitorii Convenției au considerat că acest comportament nu poate conduce la grave afectări a sistemului informatic, iar acest comportament trebuie să fie incriminat numai în situația în care comunicația este afectată în mod intenționat și grav[9].

3. Incriminarea faptei de afectare ilegală a integrității sistemului informatic în cadrul Directivei 2013/40/UE privind atacurile împotriva sistemelor informatice

Infracțiunea de afectare ilegală a integrității sistemului informatic este prevăzută în art. 4 din Directiva 2013/40/UE[10] privind atacurile împotriva sistemelor informatice și constă în perturbarea gravă sau întreruperea funcționării unui sistem informatic prin introducerea, transmiterea, periclitarea, ștergerea, deteriorarea, modificarea, suprimarea datelor informatice sau prin a le face inaccesibile. Infracțiunea de afectare ilegală a integrității sistemului informatic se săvârșește cu intenție și fără drept și trebuie să nu reprezinte un caz minor.

4. Analiza infracțiunii de perturbare a funcționării sistemelor informatice prevăzută de art. 363 din Codul penal

4.1. Condiții preexistente

4.1.1. Obiectul infracțiunii

Obiectul juridic special îl constituie relațiile sociale care protejează integritatea datelor informatice conținute pe suporturile specifice sistemelor informatice.

---

[8] A.C. Moise, *Dimensiunea criminologică a criminalității din cyberspațiu*, Editura C.H. Beck, București, 2015, p. 102.

[9] Raportul Explicativ al Convenției Consiliului Europei privind criminalitatea informatică pct. 69, disponibil [Online] la: http://conventions.coe.int/treaty/en/reports/html/185.htm, accesat la 22.10.2017.

[10] Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Decizei-Cadru 2005/222/JAI a Consiliului, JO UE, 14.08.2013, L218/8.

Obiectul material este reprezentat de sistemul informatic a cărui activitate este grav perturbată de infractor. Astfel, constituie obiect material următoarele[11]: componentele sistemului informatic, adică unele dintre părțile care formează un sistem informatic (exemple de sisteme informatice: computer, telefon mobil, dispozitiv ATM – Automatted Teller Machine –, agendă computerizată, aparat de fotografiat digital, imprimantă, tabletă electronică) sau o rețea; computerele în sine, care reprezintă dispozitive care constau în una sau mai multe componente asociate, incluzând unități de procesare și periferice și care sunt controlate de programe stocate intern; rețeaua care reprezintă un grup interconectat de computere, echipamente de comutare și ramuri de interconectare; rețeaua Internet, care reprezintă o rețea de rețele.

Perturbarea gravă poate avea ca obiect fie întregul sistem informatic, fie părți ale acestuia sau servicii sau programe deservite sau rulate de acesta.

4.1.2. Subiecții infracțiunii

Subiectul activ al infracțiunii de perturbare a funcționării sistemelor informatice poate fi orice persoană care îndeplinește condițiile generale prevăzute de lege pentru a răspunde penal.

Participația penală este posibilă în toate formele sale: coautorat, instigare și complicitate.

Subiectul pasiv al infracțiunii de perturbare a funcționării sistemelor informatice este persoana fizică sau juridică care deține sau utilizează legitim sistemul informatic a cărui funcționare este perturbată.

4.2. Conținutul constitutiv

4.2.1. Latura obiectivă

Elementul material al infracțiunii de perturbare a funcționării sistemelor informatice se realizează prin acțiunea de a perturba grav funcționarea unui sistem informatic. În legătură cu această activitate, legiuitorul român prevede următoarele condiții esențiale pentru existența infracțiunii în această formă[12]: perturbarea să fie gravă; perturbarea să fie realizată fără drept; ingerința cu consecințe grave asupra funcționării sistemului informatic să aibă loc prin introducerea, transmiterea,

[11] S. Corlățeanu, C. Căşuneanu, *Delicte contra datelor şi sistemelor informatice*, în Dreptul nr.11/2004, p. 208.

[12] I. Vasiu, L. Vasiu, *Informatică juridică şi drept informatic*, Editura Albastră, Cluj-Napoca, 2007, p. 139.

modificarea, ștergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la datele informatice.

Autorii Convenției Consiliului Europei privind criminalitatea informatică au lăsat la latitudinea fiecărui stat-parte să își însușească și să interpreteze noțiunea de perturbare gravă[13]. Totuși, legiuitorul român nu oferă niciun criteriu pentru a putea aprecia dacă perturbarea a fost sau nu gravă. Astfel, în aceste circumstanțe, considerăm că sarcina aprecierii faptului dacă perturbarea este gravă sau nu va fi lăsată pe umerii instanțelor de judecată.

Perturbarea gravă trebuie să fie realizată fără drept, astfel încât ea nu va exista în situația în care ingerința într-un sistem informatic este permisă sau autorizată (cum ar fi, de exemplu, testarea securității sistemului informatic).

Textul legal precizează următoarele tipuri de ingerințe care pot da naștere la perturbări grave: introducerea de date informatice, care are în vedere atât introducerea de date exacte într-o manieră corectă, cât și introducerea de date incorecte; transmiterea de date informatice, care presupune efectuarea unor comunicări de date informatice, conducând la supraîncărcarea sistemelor informatice; modificarea datelor informatice, care se referă la alterarea datelor informatice, astfel încât acestea pot să fie utilizate, dar procesarea acestora va produce rezultate incorecte; ștergerea datelor informatice, care se referă la eliminarea datelor informatice de pe suportul fizic pe care sunt stocate; deteriorarea datelor informatice, care se referă la alterarea datelor, în așa fel încât acestea nu mai pot fi utilizabile; restricționarea accesului la datele informatice se referă la restricționarea totală sau parțială sau la întârzierea semnificativă a accesului la datele informatice, atunci când utilizatorul are nevoie de acestea.

Urmarea imediată constă în producerea unui rezultat, o consecință a ingerinței fără drept, rezultând o perturbare gravă a funcționării unui sistem informatic.

Între activitatea cybercriminalului și urmarea imediată produsă trebuie să existe o legătură de cauzalitate, aceasta rezultând din materialitatea faptei. Expertiza informatică poate să determine existența legăturii de cauzalitate, aceasta putând răspunde și la întrebarea care vizează

[13] I. Vasiu, L. Vasiu, *op.cit.*, p. 159; S. Schjolberg, S. Ghernaouti-Helie, *A Global Treaty on Cybersecurity and Cybercrime*. ed. a II-a, AIT, Oslo, 2011, pp. 41-42.

gravitatea perturbării și dacă acest rezultat reprezintă urmarea acțiunii făptuitorului.

4.2.2. Latura subiectivă

Pentru existența infracțiunii de perturbare a funcționării sistemelor informatice este necesar ca fapta să fie săvârșită cu vinovăție. În această situație, forma de vinovăție necesară este intenția, atât directă, cât și indirectă.

4.3. Formele infracțiunii

Actele pregătitoare sunt posibile, dar nu sunt incriminate și, ca atare, nu se pedepsesc.

Tentativa este posibilă și se pedepsește conform art. 366 C. pen.

Consumarea infracțiunii de perturbare a funcționării sistemelor informatice se realizează în momentul producerii urmării imediate, adică a perturbării grave a funcționării sistemului informatic. În situația în care această urmare nu se realizează, se poate vorbi doar de acte pregătitoare efectuate de infractor sau de săvârșirea altor infracțiuni (de exemplu, alterarea integrității datelor informatice sau accesul ilegal la un sistem informatic).

Epuizarea infracțiunii are loc în momentul săvârșirii ultimului act incriminat de lege comis de făptuitor.

Infracțiunea de perturbare a funcționării sistemelor informatice poate fi săvârșită în formă continuă sau continuată.

4.4. Modalități

Infracțiunea de perturbare a funcționării sistemelor informatice prezintă șase modalități normative în varianta tip: introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor informatice ori restricționarea accesului la datele informatice. Acestor modalități normative pot să le corespundă mai multe modalități de fapt.

4.5. Sancțiuni

Pedeapsa prevăzută pentru infracțiunea de perturbare a funcționării sistemelor informatice este închisoarea de la 2 la 7 ani.

Acțiunea penală se pune în mișcare din oficiu.

5. Atacuri frecvent întâlnite în criminalitatea informatică care afectează integritatea sistemului informatic

5.1. Atacurile Denial of Service

Cel mai cunoscut atac împotriva unui sistem informatic care afectează integritatea sistemului informatic este atacul Denial of Service – DOS – (Refuzul serviciului).

În această formă de atac, atacatorul încearcă să interzică utilizatorilor autorizați accesul la informații specifice, la sistemele informatice și la rețeaua însăși. Scopul unui astfel de atac poate fi prevenirea accesului la sistemul informatic țintă sau atacul poate fi utilizat împreună cu alte acțiuni în scopul de a obține accesul neautorizat la un sistem informatic sau la o rețea.

Atacul DOS reprezintă, de fapt, o încercare a infractorului de a face resursele informatice nedisponibile pentru utilizatorii legitimi. De exemplu, atacul SYN flooding poate fi utilizat pentru a împiedica temporar funcționarea sistemului informatic. Atacul SYN flooding reprezintă un exemplu de atac DOS care profită de modul în care rețelele de comunicații care utilizează protocolul de comunicații TCP/IP au fost proiectate să funcționeze, acest exemplu putând fi utilizat pentru a ilustra principiile de bază ale unui atac DOS. Datorită faptului că protocolul de comunicații TCP/IP reprezintă o conexiune orientată, o sesiune sau o legătură directă de comunicații trebuie să fie creată înainte de trimiterea datelor informatice. Sistemul informatic client inițiază comunicarea cu server-ul (computerul ale cărui resurse clientul dorește să le acceseze). Așadar, se vor parcurge următorii pași:[14]

1. Computerul client trimite o cerere de sincronizare (SYN).
2. Server-ul trimite un mesaj de confirmare (ACK) și un semnal de sincronizare SYN, care aprobă cererea computerului client care a fost făcută în Pasul 1. Computerul client și server-ul trebuie să se sincronizeze reciproc cu numere de secvențe.
3. Computerul client trimite un mesaj de confirmare (ACK) înapoi la server, confirmând cererea de sincronizare a server-ului.

Atacul SYN flooding utilizează acest proces prezentat mai înainte, pentru a inunda sistemul țintă, victimă a atacului, cu multiple pachete SYN care au o adresă IP care nu există. Acest fapt determină server-ul să răspundă prin mesaje SYN/ACK.

[14] D.L. Shinder, E. Tittel, *Scene of the cybercrime. Computer Forensics Handbook*, Syngress Publishing Inc., Rockland, Massachusetts, 2002, pp. 318-319.

Deoarece adresele IP sursă pentru pachetele SYN, trimise de atacator nu sunt bune, semnalele de confirmare (ACK) pe care server-ul le așteaptă nu vor veni niciodată. Prin urmare, serviciul este refuzat către clienții legitimi care așteaptă să stabilească comunicații cu server-ul.

Atacurile DOS sunt dirijate pentru un singur sistem informatic de atac. Un atac DOS care folosește multiple sisteme de atac, este cunoscut sub numele de Refuzul serviciului distribuit (Distributed Denial of Service – DDOS).

Scopul atacului DDOS este același: refuzul de a utiliza un serviciu sau sistem. Într-un atac DDOS, metoda folosită pentru refuzul serviciului este distrugerea țintei cu ajutorul comunicațiilor de la mai multe sisteme informatice diferite. O rețea cu agenți de atac (uneori numiți zombie) este creată de atacator, iar la primirea comenzii de atac de la atacatori, agenții de atac încep să trimită comunicații specifice împotriva țintei. Agenții de atac sunt sisteme informatice care au fost compromise și la care sofware-ul de atac DDOS a fost instalat. Crearea unei rețele de atac poate fi un proces în mai mulți pași, în care atacatorul mai întâi compromite câteva sisteme informatice, care sunt apoi utilizate ca intermediare sau conducătoare și care vor compromite alte sisteme informatice.

5.2. Atacurile bazate pe programele malițioase care au ca scop infectarea sistemului informatic

Există trei tipuri de programe malițioase care au ca obiectiv infectarea unui sistem informatic: virușii, viermii și caii troieni[15].

Un virus este un program care infectează fișiere executabile sau fișiere obiect[16]. Orice program care se multiplică fără acordul utilizatorului este un virus[17]. Mai întâi, virusul se va multiplica, răspândindu-se către alte sisteme informatice[18], după care acesta își va activa funcția sa malițioasă.

Un vierme reprezintă un program destinat pentru a obține avantajul față de o vulnerabilitate într-o aplicație sau într-un sistem de operare în

---

[15] L. Klander, *Anti Hacker –Ghidul securităţii reţelelor de calculatoare*, Editura All Educational, Bucureşti, 1999, p. 385.

[16] M. Dobrinoiu, *Infracţiunea de alterare a integrităţii datelor informatice*, în Revista Română de Dreptul Proprietăţii Intelectuale nr.3/2006, p. 62.

[17] C. Féral-Schuhl, *Cyberdroit. Le droit à l' épreuve de l' Internet*, ed. a VI-a, Dalloz, Paris, 2010, pp. 918-923.

[18] J. Traxler, J. Forristal, *Hach Proofing Your Web Applications*, Syngress Publishing Inc., Rockland, Massachusetts, 2001, p. 16; C. Easttom, J. Taylor, *Computer Crime, Investigation, and the Law*, Course Technology, Cengage Learning, Boston, Massachusetts, 2010, p. 57.

scopul de a penetra un sistem informatic. Odată ce viermele a exploatat vulnerabilitatea unui sistem informatic, acesta imediat cercetează alte sisteme informatice care au aceeași vulnerabilitate.

Spre deosebire de virus, viermele reprezintă un program de sine stătător care există independent de alte programe, iar pentru a rula nu are nevoie de alte programe[19]. Acțiunile pe care viermii le realizează includ ștergerea fișierelor unui sistem informatic, sau controlul de la distanță al sistemului informatic de către atacator.

Viermele se multiplică pe un sistem informatic și încearcă să infecteze și alte sisteme informatice, care ar putea fi atașate la aceeași rețea.

Calul Troian reprezintă un program, care în mod aparent efectuează o acțiune utilă, dar în fapt el efectuează acțiuni de distrugere care nu sunt cunoscute de utilizator[20].

Calul Troian este un program care apare pentru a executa funcții valide, dar conține ascunse în cadrul său instrucțiuni ce pot provoca daune sistemelor informatice pe care se instalează. Acest program reprezintă o metodă de inserare a unor instrucțiuni într-un program, astfel încât programul va executa o funcție neautorizată, în timp ce aparent execută una obișnuită.

Calul Troian efectuează următoarele acțiuni:[21] ștergerea sau modificarea fișierelor; transmiterea fișierelor prin rețea la cyber-atacator; instalarea în sistemul informatic a altor programe malițioase și viruși.

Concluzii

Dispozițiile din cuprinsul art. 363 C. pen. sunt inspirate din prevederile art. 5 din Convenția Consiliului Europei privind criminalitatea informatică și din prevederile art. 4 din Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice. Astfel, spre deosebire de textele Convenției Consiliului Europei privind criminalitatea informatică și Directivei 2013/40/UE privind atacurile împotriva sistemelor informatice, observăm faptul că legea română nu reține ca modalități alternative *periclitarea* sau *suprimarea* datelor informatice și introduce o modalitate nouă, cea de *restricționare* a accesului la aceste date informatice. Considerăm că acțiunea

[19] T. Amza, C.P. Amza, *Criminalitatea informatică*, Editura Lumina Lex, Bucureşti, 2003, p. 115.

[20] D.L. Shinder, E. Tittel, *Scene of the cybercrime. Computer Forensics Handbook*, Syngress Publishing Inc., Rockland, Massachusetts, 2002, p. 336.

[21] Ibidem.

de *suprimare* a datelor informatice, care reprezintă echivalentul unei distrugeri a datelor informatice, ar fi trebuit să fi fost reținută ca modalitate alternativă de săvârșire a infracțiunii, alături de *periclitare*.

Prin urmare, legiuitorul român a transpus în cadrul art. 363 C. pen. atât prevederile art. 4 (afectarea ilegală a integrității sistemului) din Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice, cât și prevederile art. 5 (afectarea integrității sistemului) din Convenția Consiliului Europei privind criminalitatea informatică.

Cu toate că cele mai importante instrumente juridice de combatere a criminalității informatice la nivel european nu incriminează în prezent unele comportamente care perturbă grav funcționarea sistemelor informatice, cum este de exemplu, spam-ul (mesajul nesolicitat), suntem de părere că legiuitorii celor două acte normative trebuie să le actualizeze, prin incriminarea și acestor comportamente ilegale care afectează grav sistemele informatice. Datorită efectelor pe care mesajele nesolicitate le pot produce într-un sistem informatic sau rețea, considerăm că spam-ul ar putea fi incriminat de prevederile art. 5 din Convenția Consiliului Europei privind criminalitatea informatică și de prevederile art. 4 din Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice, ambele prevederi referindu-se la afectarea integrității sistemelor informatice.

ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

APLICAREA PRINCIPIULUI LIBERTĂŢII DE EXPRIMARE PE INTERNET – ÎNTRE CARACTERUL ABSOLUT ŞI JUSTIFICAREA NECESITĂŢII LIMITĂRII ACESTUIA

APPLYING THE PRINCIPLE OF FREEDOM OF EXPRESSION ON THE INTERNET – BETWEEN ABSOLUTE NATURE AND THE JUSTIFICATION OF THE NEED TO SET LIMITS ON ITS EXERCISE

CARMEN MOLDOVAN[1]

Rezumat: Folosirea internetului pe scară largă a determinat crearea unui spaţiu virtual (*cyberspace*) caracterizat în primul rând prin diversitatea mesajelor, discursurilor, interacțiunii extrem de rapide dintre utilizatori aflaţi în zone diferite ale lumii, schimbând definitiv modul tradiţional de interacţiune şi de încheiere a raporturilor juridice în anumite domenii. Dezvoltarea rapidă a comunicării prin intermediul internetului şi interferenţa cu multiple domenii, atât ale dreptului privat, cât și public, nu a fost însoțită și de o reglementare unitară a folosirii internetului și a consecinţelor juridice în cazul depăşirii prerogativelor recunoscute juridic.
Prezenta lucrare are ca scop analiza libertăţii de exprimare pe internet, a caracterului absolut sau limitat al acesteia, din perspectiva dreptului internaţional, în principal. Demersul analitic are ca punct de plecare consacrarea libertăţii de exprimare în instrumentele juridice internaţionale (atât cele cu aplicare universală, cât şi cele aplicabile la nivel regional) și urmăreşte să clarifice dacă și în ce măsură în domeniul de aplicare al acestora poate fi inclusă și exprimarea pe internet.
Cuvinte-cheie: libertatea internetului, dreptul de a primi și căuta informații, intercondiționare, restricții admisibile.

Abstract: The use of the Internet on a large scale has led to the creation of a virtual space (cyberspace) characterized primarily by the diversity of messages, speeches, extremely rapid interaction between users in different areas of the world, which permanently changed the traditional way of interacting and concluding legal

[1] Lector univ. dr., Universitatea „Alexandru Ioan Cuza" din Iași, Facultatea de Drept, E-mail: *carmen.moldovan*@uaic.ro.

relationships in certain areas. The rapid development of Internet communication and the interference with multiple areas of both private and public law has not been accompanied by a unitary regulation on the use of Internet and legal consequences in the event of exceeding legal prerogatives.

This paper aims to analyze the freedom of expression on the Internet, its absolute or limited character, mainly from the perspective of international law. The analytical approach has as its starting point the consecration of the freedom of expression in international legal instruments (both universal and regional ones) and seeks to clarify if and to what extent their scope can also include expression on Internet.

Keywords: internet freedom, the right to recieve and seek information, interrelation, admisible restrictions.

1. Aspecte introductive – corelaţia dintre libertatea de exprimare şi informare şi internet ca spațiu de circulație liberă a ideilor

Libertatea de exprimare, de informare şi de opinie constituie valori esenţiale ale societăţii democratice, ale statului de drept, precum şi drepturi fundamentale ale omului, consacrate în numeroase instrumente juridice internaţionale, cu caracter universal sau regional ce stabilesc în acelaşi timp obligaţii ce revin statelor părţi pentru asigurarea exercitării acestora[2].

Dincolo de caracteristicile unui element esenţial al democraţiei, libertatea de exprimare reprezintă o condiţie pentru dezvoltarea şi exercitarea unor alte drepturi şi libertăţi fundamentale cu care se află în strânsă legătură, cum sunt libertatea de asociere, libertatea de gândire, conştiinţă, a credinţelor şi convingerilor religioase, dreptul de a participa la activităţi de natură politică, care contribuie în acelaşi timp atât la păstrarea caracteristicilor democratice, cât şi la dezvoltarea personalităţii şi autonomiei indivizilor. Totodată, libertatea de exprimare implică și protejarea mijloacelor de transmitere a ideilor și opiniilor, fără a fi luate în considerare frontierele statelor[3]. Această garanție este menționată începând cu articolul 19 din Declarația universală a drepturilor omului[4], în următoarea formulare: *„Orice*

[2] J.-F. Flauss, *La Cour européenne des droits de l`homme et la liberté d`expression*, în *La liberté d`expression aux Etats-Unis et en Europe*, E. Zoller (dir.), Dalloz, Paris, 2008, p. 126; C. Moldovan, *Libertatea de exprimare. Principii. Restricții. Jurisprudență*, Editura C.H. Beck, București, 2012, p. 2 și urm.

[3] C. Moldovan, *op. cit.*, 2012, pp. 29-30.

[4] *Declarația universală a drepturilor omului* a fost adoptată la 10 decembrie 1948 prin Rezoluţia nr. 217 A (III) a Adunării Generale a Naţiunilor Unite. România a semnat

om are dreptul la libertatea opiniilor și exprimării; acest drept include libertatea de a avea opinii fără imixtiune din afară, precum și libertatea de a căuta, de a primi și de a răspândi informații și idei prin orice mijloace și independent de frontierele de stat." Instrumentele juridice adoptate ulterior au preluat, aproape identic, această concepție asupra domeniului de aplicare al libertății de exprimare. Paragraful 2 al articolului 19 din Pactul internațional cu privire la drepturile civile și politice[5] statuează că *„Orice persoană are dreptul la libertatea de exprimare; acest drept cuprinde libertatea de a căuta, de a primi și de a răspândi informații și idei de orice fel, indiferent de frontiere, sub forma orală, scrisă, tipărită ori artistică sau prin orice alt mijloc, la alegerea sa."* La nivel regional, articolul 10 parag. 1 din Convenția europeană a drepturilor omului[6] prevede în mod expres: *„Orice persoană are dreptul la libertatea de exprimare. Acest drept cuprinde libertatea de opinie şi libertatea de a primi sau de a comunica informaţii ori idei fără amestecul autorităţilor publice şi fără a ţine seama de frontiere."*

Din cuprinsul dispozițiilor analizate se poate observa că, spre deosebire de Declarația universală și Pactul internațional, care pun accentul pe exercitarea libertății de exprimare prin orice mijloace și în orice formă, Convenția europeană a drepturilor omului nu prevede în mod expres o astfel de garanție, dar conține mențiunea că libertatea de exprimarea trebuie exercitată fără amestecul autorităților și fără frontiere.

Dezvoltarea și evoluția tehnologiei și a mijloacelor de informare, de la cele tradiționale, pe suport tipărit, la comunicarea online, a determinat necesitatea de a adapta cadrul normativ existent și garanțiile stabilite și aplicate deja, potrivit unor interpretări de jurisprudență bine conturate, la noile realități și a avut implicații multiple în modelarea acestora în funcție de modificările apărute, fără a putea fi inclusă în noțiunea *terra nullius* și lăsată

Declaraţia la 14 decembrie 1955 când prin Rezoluţia nr. 955 (X) a Adunării Generale a ONU, a fost admisă ca stat membru al ONU.

[5] *Pactul internaţional cu privire la drepturile civile şi politice* a fost adoptat şi deschis spre semnare de către Adunarea Generală a Naţiunilor Unite la 16 decembrie 1966. A intrat în vigoare la 23 martie 1976, conform art. 49, pentru toate dispoziţiile cu excepţia celor de la art. 41; la 28 martie pentru dispoziţiile de la art. 41.

[6] C*onvenţia privind respectarea drepturilor şi libertăţilor fundamentale* a fost adoptată în cadrul Consiliului Europei, la Roma, la 4 noiembrie 1950 şi a intrat în vigoare la 3 septembrie 1953. România a ratificat Convenţia la 20 iunie 1994 prin Legea nr. 30/1994, publicată în „Monitorul Oficial al României", partea I, nr. 135 din 31 mai 1994.

în afara oricăror reglementări[7]. Fiind o modalitate nouă de comunicare, în privința reglementării internetului s-au remarcat două mari curente divergente: cel al reglementării de către autoritățile naționale și cel al libertății absolute a internetului și a excluderii sale de la orice formă de reglementare din partea autorităților statelor[8], aplicabilă devenind prima.

Comunicarea pe internet și prin intermediul internetului implică protejarea tuturor drepturilor și libertăților garantate în mediul offline, luând în considerare particularitățile libertății de exprimare și informare și situația conflictuală ce poate apărea între acestea și drepturi individuale ca respectarea propriei imagini, protejarea datelor cu caracter personal, dreptul la protejarea vieții private și a inviolabilității corespondenței, cu alte cuvinte, eventuala stare de conflict dintre acestea se analizează potrivit acelorași criterii și elemente ca în cazul mijloacelor tradiționale de comunicare, astfel încât regula este principiul libertății internetului, care se află în centrul regimului juridic al diferitelor aspecte pe care le implică internetul[9], însă această libertate nu poate fi concepută ca având caracter absolut.

Încă din anul 1996, Comisia Europeană a subliniat rolul și caracteristicile pe care le prezintă internetul ca mediu de comunicare și în ciuda poziționării în timp a acestei calificări, apreciem că este relevantă și în prezent:

„O caracteristică unică a internetului este că funcționează simultan ca mediu pentru publicare și pentru comunicare. Spre deosebire de mass-media tradițională, internetul favorizează o varietate de moduri de comunicare: «unul la unul», «unul la mulți», «mulți la mulți». Un utilizator de internet poate «vorbi» sau «asculta» interschimbabil. În orice moment, receptorul mesajului poate și devine furnizor de conținut, din proprie inițiativă sau prin «republicarea» conținutului unui terț. Internetul este, prin urmare, radical diferit de difuzarea tradițională (a programelor de radio și

[7] A. S. Serrano, *Internet Regulation and the Role of International Law,* în Max Planck Yearbook of United Nations Law, 2006, pp. 193-194.

[8] Pentru o prezentare detaliată a fiecărei orientări și a argumentelor aduse în sprijinul fiecăreia dintre ele, a se vedea A. S. Serrano, *Internet Regulation and the Role of International Law,* în Max Planck Yearbook of United Nations Law, Volume 10, 2006, pp. 191- 272; R. Uerpmann□Wittzack, *Principles of International Internet Law,* în German Law Journal, Vol. 11, No. 11, 2010, pp. 1248-1250; D. Cimpoeru, *Dreptul internetului*, Editura C.H. Beck, București, 2012, pp. 11-12.

[9] R. Uerpmann□Wittzack, *op. cit.,* p. 1247.

televiziune, s. n.). De asemenea, acesta diferă radical de serviciile tradiționale de telecomunicație. Trecerea constantă de la «modul public» la «modul de comunicare privat» - două moduri reglementate în mod tradițional de regimuri juridice foarte diferite - constituie una dintre principalele provocări ale reglementării internetului."[10]

Legătura dintre libertatea de exprimare și internet a constituit preocuparea constantă a mai multor instituții internaționale, în cuprinsul prezentei lucrări urmând să aducem în discuție cele mai relevante aspecte ale acestora, fie că sunt incluse în categoria *soft law* sau reprezintă interpretări date de Curtea Europeană a Drepturilor Omului, ca instanță reprezentativă în privința protejării libertății de exprimare în spațiul juridic european.

2. Conturarea unui drept de acces la internet prin instrumente *soft law*

Instrumentele juridice internaţionale nu prevăd în mod expres libertatea internetului pentru toate persoanele și a exprimării pe internet. Cea mai evidentă dintre explicaţii este extrem de simplă: majoritatea acestora sunt mult anterioare proliferării comunicării pe internet, iar ulterior nu au fost adoptate convenţii speciale în această materie, deoarece nu a fost necesar, datorită punerii în aplicare în domeniul internetului, a principiilor generale şi standardele bine stabilite şi definite în privinţa libertăţii de exprimare.

La nivel internațional nu a fost adoptat un tratat internațional comprehensiv care să reglementeze aspectele juridice ale utilizării internetului și este dificil de afirmat dacă încheierea unui astfel de instrument este posibilă sau în mod real utilă în prezent, având în vedere apariția mai multor instrumente *soft law* la nivel universal și regional, ce tratează diferite niveluri ale interacțiunii internetului în raporturile juridice dintre particulari, cu un pronunțat caracter de interdisciplinaritate.

În anul 2011, Raportorul Special pentru promovarea și protejarea dreptului la libertatea de opinie și de exprimare[11], din cadrul Consiliului

[10] Commission of the European Communities, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the C ommittee of the Regions, *Illegal and harmful content on the Internet*, 16. I 0. 1996, COM(96) 487 p. 8, [Online] la: http://aei.pitt.edu/5895/1/5895.pdf.

[11] *Report of the Special Rapporteur to the General Assembly on the right to freedom of opinion and expression exercised through the Internet*, A/66/290, 10.08. 2011, [Online] la: https://documents-dds-

pentru Drepturile Omului al Organizației Națiunilor Unite, Frank La Rue a subliniat faptul că accesul la internet nu este încă recunoscut ca un drept al omului, dar că statelor le revine obligația pozitivă de a crea un mediu favorabil care să permită exercitarea dreptului la libertatea de exprimare și de opinie de către toate persoanele, ceea ce implică stabilirea unor politici efective și concrete care să asigure accesul universal la internet[12]. Această poziție accentuează importanța internetului în prezent și necesitatea de adaptare la noile cerințe. Analizând implicațiile textului articolului 19 din Declarația universală a drepturilor omului și din Pactul internațional cu privire la drepturile civile și politice, prin includerea mențiunii că orice persoană are dreptul să se exprime prin orice fel de mijloace media, Raportorul Special a subliniat că la momentul redactării dispozițiilor analizate s-a avut în vedere includerea și adaptarea viitoarelor evoluții ale mijloacelor tehnice prin care persoanele își vor putea exercita dreptul la libertatea de exprimare, prin urmare cadrul general al drepturilor omului a rămas relevant și în egală măsură aplicabil și formelor de comunicare din prezent, inclusiv în ceea ce privește internetul.[13]

Din cuprinsul concluziilor Raportorului Special, rezultă că legătura de conexitate dintre libertatea de exprimare și elementele sale componente și internet este neechivocă și nu necesită practic nicio demonstrație. Ca o recunoaștere și subliniere a acestei intercondiționări, Comitetul pentru Drepturile Omului din cadrul Organizației Națiunilor Unite (Human Rights Committee), în cadrul *Comentariului general nr. 34 la articolul 19 din*

---

ny.un.org/doc/UNDOC/GEN/N11/449/78/PDF/N1144978.pdf?OpenElement, accesată la 03 decembrie 2017.

[12] *Report of the Special Rapporteur to the General Assembly on the right to freedom of opinion and expression exercised through the Internet*, A/66/290, 10.08. 2011, [Online] la: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/449/78/PDF/N1144978.pdf?OpenElement, accesată la 03 decembrie 2017.

[13] *Report of the Special Rapporteur to the General Assembly on the right to freedom of opinion and expression exercised through the Internet*, A/66/290, 10.08. 2011, parag. 21, [Online] la: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/449/78/PDF/N1144978.pdf?OpenElement, accesată la 03 decembrie 2017. Pentru o expunere detaliată a dezbaterilor care au avut loc la negocierea Pactului internațional cu privire la drepturile civile și politice și a conținutului articolului 19, a se vedea, M. Land, *Toward an International Law of the Internet*, în Harvard International Law Journal, Vol. 54, Number 2, 2013, pp. 404-407.

Pactul internațional cu privire la drepturile civile și politice[14], din 2011, care a înlocuit *Comentariul general nr. 10* la același articol, a atras atenția statelor părți la Pactul internațional cu privire la drepturile civile și politice asupra evoluției tehnologiilor informației și comunicațiilor, cum sunt internetul și sistemele electronice mobile de diseminare a informațiilor, care au modificat comunicarea din întreaga lume și au creat o rețea globală a schimbului de idei și opinii ce nu se bazează pe intermediarii tradiționali ai mass-media[15], constatări ce nu sunt caracterizate prin elemente de noutate.

În schimb, Comitetul pentru Drepturile Omului prevede că statele ar trebui să ia toate măsurile pentru a proteja independența acestor noi mijloace și a asigura accesul indivizilor la acestea, ceea ce reprezintă o abordare nouă din partea unor instituții internaționale, urmare a conștientizării influenței internetului în foarte multe aspecte ale interacțiunii umane și a modalităților de încheiere a raporturilor juridice din anumite domenii, inclusiv în ceea ce privește exercitarea libertății de exprimare, informare și de opinie.

Această menționare expresă în cuprinsul *Comentariului general nr. 34*, deși poate părea firească, nu trebuie neglijată ca semnificație, deoarece prin această interpretare, în domeniul de aplicare al articolului 19 din Pactul internațional cu privire la drepturile civile este inclusă nu doar libertatea de exprimare, ci și mijloacele tehnice prin care aceasta este exercitată, ceea ce subliniază legătura foarte strânsă dintre internet și exprimare și determină un nivel de protecție sporită exprimării pe internet, față de protejarea doar a libertății de exprimare. [16]

Aceeași perspectivă a fost afirmată și în cadrul UNESCO[17], care a recunoscut potențialul de dezvoltare și evoluție al internetului, precum și faptul că reprezintă o resursă fără precedent de informații, ce deschide noi oportunități pentru comunicare și, în acest context, apare firească aplicarea principiilor libertății de exprimare și a drepturilor omului pentru comunicarea pe internet și pentru toate tipurile de platforme media, deoarece

[14] Human Rights Committee, *General comment No. 34. Article 19: Freedoms of opinion and expression* (CCPR/C/GC/34), 102nd session, Geneva, 11-29 July 2011, [Online] la: http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

[15] Paragrafele 11, 12 din *Comentariul general nr. 34*.

[16] M. Land, *op. cit.*, p. 394

[17] Organizația Națiunilor Unite pentru Educație, Știință și Cultură.

acestea vor contribui la dezvoltarea democrației și a dialogului[18], astfel că Organizația promovează ideea universalității internetului, cu respectarea regulilor drepturilor omului. Această idee este completată de afirmația Consiliului pentru Drepturile Omului din cadrul ONU, că aceleași drepturi protejate offline trebuie să fie protejate și online, în mod special, libertatea de exprimare, care se aplică indiferent de frontiere și prin orice tip de mijloace de comunicare, la alegere, astfel cum se prevede în articolul 19 din Declarația universală a drepturilor omului și Pactul privind drepturile civile și politice[19].

Urmând aceeași concepție, la nivelul Consiliului Europei, *Recomandarea Comitetului de Miniştri către statele membre cu privire la libertatea internetului*[20] din 2016, menționează că dispoziţiile Convenției europene a drepturilor omului se aplică atât pentru discursurile offline, cât și pentru cele online și că statelor membre ale Consiliului Europei le revin obligații negative și pozitive pentru respectarea, protejarea și promovarea drepturilor și libertăților fundamentale pe internet[21].

În sensul acestei Recomandări, noțiunea de libertate a internetului semnifică exercitarea pe internet a drepturilor omului și a libertăților fundamentale și protejarea lor în conformitate cu Convenția europeană și cu Pactul internațional privind drepturile civile și politice, astfel că statele membre ale Consiliului Europei trebuie să implementeze standardele Convenției și ale Consiliului în privința internetului[22], ce trebuie să stea la baza înțelegerii internetului și implicațiilor acestuia, de o manieră extensivă.

---

[18] United Nations Educational, Scientific and Cultural Organization, *Freedom of Expression and the Internet*, -2016, p. 17-20, [Online] la: https://en.unesco.org/themes/freedom-expression-internet, accesată la 04 decembrie 2017.

[19] Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/20/L.13, 29 June 2012, [Online] la: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement, accesată la 04 decembrie 2017.

[20] *Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom, Adopted by the Committee of Ministers on 13 April 2016 at the 1253rd meeting of the Ministers' Deputies*, [Online] la: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa, accesată la 04 decembrie 2017.

[21] *Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom*, parag. 1.

[22] *Recommendation CM/Rec(2016)5[1] of the Committee of Ministers to member States on Internet freedom*, parag. 1. Comitetul de Miniștri a adoptat mai multe recomandări și

La nivelul Uniunii Europene, Consiliul Uniunii Europene a subliniat caracterul de intercondiționare dintre libertatea de exprimare și informare și celelalte drepturi fundamentale și necesitatea protejării acestora și în mediul online, printr-un ghid adoptat în anul 2014 *EU Human Rights Guidelines on Freedom of Expression Online and Offline*[23], instrument juridic *soft law* al cărui relevanță este conștientizarea implicațiilor juridice ale internetului în privința exercitării libertății de exprimare și de informare și aplicarea standardelor internaționale deja stabilite în această privință.

3. Limitarea accesului la internet ca parte a dreptului de a primi informații și idei din perspectiva Curții Europene a Drepturilor Omului

declarații în domeniul libertății comunicării pe internet. Astfel, Declarația cu privire la drepturile omului și statul de drept în societatea informațională, CM (2005) 56 din 13 mai 2005, recunoaște în preambul că „accesul limitat sau lipsa de acces la [tehnologiile informației și comunicației (TIC)] pot priva persoanele de capacitatea de a-și exercita pe deplin drepturile lor fundamentale". În cuprinsul Declarației se stipulează că libertatea de exprimare, de informare și de comunicare trebuie respectată într-un mediu digital la fel ca într-un mediu non-digital și că nu trebuie supusă altor restricții decât cele prevăzute la articolul 10 din Convenția europeană a drepturilor omului pentru simplul motiv că se exercită în format digital. Aceeași cerință a fost anterior precizată în cuprinsul Declarației „Libertatea comunicării pe Internet", adoptată de Comitetul de Miniștri la 28 mai 2003, la a 840-a reuniune a Delegaților Miniștrilor, în care este menționat principiul conform căruia statele membre nu ar trebui să supună conținutul difuzat pe Internet unor restricții care le depășesc pe cele aplicabile altor mijloace de difuzare de conținut.

Recomandarea CM/Rec(2007)16 cu privire la măsurile de promovare a valorii serviciului public al internetului, adoptată în 2007 de către Comitetul Miniștrilor, a analizat probleme legate de accesibilitatea internetului și categoriile de restricții permise. Recomandarea CM/Rec(2007)11 privind promovarea libertății de exprimare și de informare în noul mediu de informare și de comunicare a subliniat ideea libertății de comunicare pe internet.

Recomandarea CM/Rec(2008) 6 din 2008 a Comitetului de Miniștri cuprinde liniile directoare cu privire la utilizarea și controlul filtrelor de internet pentru a exercita și a se bucura pe deplin de libertatea de exprimare și informare. Recomandarea CM/Rec(2012)3 privind protecția drepturilor omului în contextul motoarelor de căutare, adoptată la 4 aprilie 2012 subliniază că „motoarele de căutare permit publicului din întreaga lume să caute, să primească și să comunice informații, idei și alte conținuturi, și în special să aibă acces la cunoștințe, să participe la dezbateri și la procesele democratice".

[23] Council of the European Union, *EU Human Rights Guidelines on Freedom of Expression Online and Offline*, Foreign Affairs Council meeting, 12 May 2014, [Online] la: https://eeas.europa.eu/sites/eeas/files/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf, accesată la 02 decembrie 2017.

Dezvoltarea internetului şi implicit a comunicării pe şi prin intermediul internetului a impus adaptarea principiilor generale aplicabile libertăţii de comunicare şi la această modalitate particulară de comunicare care forţează în anumite situaţii limitele cunoscute sau acceptate ale diseminării informaţiilor prin mijloacele tradiționale, consacrate. Totodată, în acest context a apărut întrebarea dacă libertatea internetului presupune o libertate de exprimare absolută în mediul virtual (desemnat de asemenea şi ca ciber spaţiu[24] - *cyberspace*) ori dacă pot fi aplicate restricții în cazul depășirii limitelor admisibile ale exercitării acesteia ori dacă sunt necesare criterii speciale în analiza respectării sau încălcării acestor criterii.

Una dintre cele mai mari dificultăți legate de întinderea libertății pe internet este determinată de specificul accesibilității internetului, având în vedere că mesajele, textele, opiniile pot fi accesate și vizualizate simultan în întreaga lumea sau cel puțin în acele state care nu practică cenzura și restricționarea accesului la internet, trecând peste frontiere foarte ușor și întrunind caracteristici ale ubicuității, prin dispariția practică a frontierelor și a limitelor teritoriale ale comunicării și inaplicabilitatea condițiilor generale tradițional recunoscute ale comunicării.

Dreptul de a căuta și a primi informații, ca parte a libertății de comunicare, a fost analizat în mai multe situații de către Curtea Europeană a Drepturilor Omului, sub forma dreptului de acces la internet, în cele mai multe cazuri, instanța ajungând la concluzia încălcării articolului 10 din Convenție. Instanţa europeană a subliniat în toate cauzele care implică drepturi sau libertăți fundamentale și exercitarea lor pe internet, atât beneficiile internetului, cât şi pericolele pe care acesta le prezintă.

Un prim exemplu în acest sens este cauza *Ahmet Yildirim c. Turcia*, din 2012[25], în care Curtea a constatat încălcarea articolului 10 din Convenție, sub aspectul dreptului de a primi și de a transmite informații și idei. La originea cauzei se află o decizie a instanței naționale de a bloca accesul la platforma Google Sites unde era găzduită o pagină de internet al cărui proprietar se afla în fața unei proceduri penale, pentru insultarea memoriei lui Atatürk. Ca urmare a deciziei, accesul la toate celelalte site-uri

[24] V.-V. Patriciu, I. Vasiu, Ș.-G. Patriciu, *Dreptul și internetul*, Editura All Beck, București, 1999, pp. 1-2; D. Cimpoeru, *op. cit*., p. 21.

[25] Curtea Europeană a Drepturilor Omului, Hotărârea din 18 decembrie 2012, în cauza *Ahmet Yıldırım c. Turcia*. Textul integral al tuturor hotărârilor menționate în prezenta lucrare este disponibil la adresa: hudoc.echr.coe.int.

găzduite pe această platformă, a fost blocat. În cererea sa, reclamantul s-a plâns că nu a putut accesa propriul site de internet din cauza acestei măsuri dispuse în cadrul procedurilor penale, fără a avea nicio legătură cu el sau site-ul său, prin intermediul căruia acesta declară că-şi publică lucrările academice și punctele sale de vedere cu privire la diferite domenii și că măsura a încălcat dreptul său la libertatea de a primi şi de a transmite informații și idei. Curtea a constatat că a avut loc încălcarea articolului 10 din Convenție, în principal deoarece a constatat că efectele măsurii în cauză au fost arbitrare, iar revizuirea judiciară a blocării accesului a fost insuficientă pentru a preveni abuzurile.

Ingerința generată de aplicarea legii naționale nu întrunește cerințele de previzibilitate impuse de Convenție și nu a permis reclamantului să se bucure, în suficientă măsură, de protecția cerută de principiul preeminenţei dreptului într-o societate democratică. Mai mult decât atât, un astfel de text pare să intre în conflict chiar cu formularea paragrafului 1 al articolului 10 din Convenție, conform căruia drepturile aici recunoscute sunt valabile „indiferent de frontiere”[26].

În privința întinderii dreptului de acces la informații prin intermediul internetului și aplicabilitatea acestora și în cazul deținuților, relevanță prezintă interpretarea dată de către Curtea Europeană a Drepturilor Omului în 2016, în cauza *Kalda c. Estonia*[27].

Potrivit constatărilor la care a ajuns Curtea în această hotărâre, părțile contractante nu au obligația de a permite accesul deținuților la internet însă, dacă un stat este dispus să acorde acces deținuților, astfel cum este cazul statului pârât, trebuie să motiveze refuzul de a acorda acces la anumite adrese de internet.

Reclamantul a invocat îndeosebi că interdicția în baza legii estoniene de accesare a adreselor de internet a încălcat dreptul său de a primi informații prin intermediul internetului și l-a împiedicat să realizeze cercetări juridice pentru procedurile judiciare în care era parte. Curtea a reținut că dreptul la informare, ca parte componentă a libertății de exprimare garantate de articolul 10 al Convenției europene a drepturilor omului nu include

[26] Curtea Europeană a Drepturilor Omului, Hotărârea din 18 decembrie 2012, în cauza *Ahmet Yıldırım c. Turcia,* § 64.

[27] Curtea Europeană a Drepturilor Omului, Hotărârea din 16 ianuarie 2016, *în cauza Kalda c. Estonia (Cererea nr. 17429/10).* Textul integral al hotărârii este disponibil la adresa: hudoc.echr.coe.int.

garantarea dreptului de acces la internet a deținuților, fiind lăsată la aprecierea statelor instituirea unei astfel de garanții, iar elementul esențial al analizei legitimității restricționării acestuia îl constituie conținutul și scopul reglementării naționale care permite limitarea acestui acces.

4. Caracterul de spaţiu public al reţelelor sociale

Legătura dintre libertatea de exprimare și internet poate fi analizată pe mai multe niveluri și din mai multe perspective: caracterul de spațiu public al diferitelor medii sau spații de pe internet, unde circulă informații, mesaje, discursuri, întinderea libertății de exprimare în medul virtual, garantarea unui drept de acces la informații, ca parte componentă a libertății de exprimare, prin intermediul internetului.

O primă lămurire ce ar trebui realizată are în vedere natura mediului on line, respectiv, dacă acesta poate fi considerat de natură privată sau dimpotrivă, aparține spațiului public. Urmând interpretarea dată în anul 2014 de către Înalta Curte de Casație și Justiție[28] site-urilor de socializare, ca spațiu unde circulă și sunt expuse atât opinii și idei proprii ale persoanelor particulare, cât și informații de interes public, cu conținut variat, provenite de la alte entități juridice, putem susține că atât timp cât conținutul mesajelor este disponibil sau accesibil publicului larg sau unor persoane incluse în categoria de prieteni ai persoanei care afișează un mesaj, idee sau opinie, acest mesaj este transmis în spațiul public, chiar dacă este virtual, urmând a fi aplicate toate condițiile și eventualele restricții generale sau speciale stabilite de cadrul normativ cu privire la exprimarea într-un astfel de spațiu și consecințele lor, în cazul depășirii limitelor admisibile. Cu toate că decizia la care am făcut referire mai sus se referă doar la o anumită rețea de socializare și la efectele pe care le produc mesajele afișate de către un anumit utilizator, apreciem că aspectele reținute de către Înalta Curte de Casație și Justiție pot fi aplicate și în cazul altor rețele de socializare sau alte medii online unde circulă opinii, idei sau mesaje, deoarece în centrul argumentării instanței, s-au aflat criteriul naturii și scopului mesajului sau discursului afișat.

[28] Înalta Curte de Casație și Justiție, Secția de Contencios Administrativ și Fiscal, Decizia nr. 4546/2014, din 27 noiembrie 2014, [Online] la: http://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=131400, accesată la 03 decembrie 2017.

5. Perspectiva Curții Europene a Drepturilor Omului în aprecierea condiţiilor de limitare a exprimării pe internet

Un aspect ce poate fi analizat în legătură cu libertatea internetului este cel referitor la existența și întinderea libertății de informare prin intermediul internetului. Având în vedere caracteristica libertăţii de exprimare de drept al cărei exercitare poate fi supusă unor limitări sau restricţii în anumite situaţii şi aplicarea tuturor principiilor şi clauzelor de limitare a exercitării sale, nu putem susţine ideea unei libertăţi absolute a formelor de exprimare pe internet, în stabilirea caracterului legitim al ingerințelor autorităților naționale, elemente importante fiind reprezentate de conținutul și natura mesajului, discursului sau opiniei exprimate.

5.1. Apărarea moralei

Una dintre primele cauze analizate de către instanța europeană, *Perrin c. Regatului Unit al Marii Britanii*[29], s-a încheiat prin pronunțarea unei decizii de inadmisibilitate și deci de respingere a susținerii de încălcare a articolului 10 din Convenție, în anul 2005, motivat de faptul că sancțiunea aplicată reclamantului, de 30 de zile închisoare, pentru publicarea de articole obscene pe internet, a fost necesară într-o societate democratică pentru apărarea moralei și a drepturilor altora și de asemenea, a fost proporțională cu scopul urmărit. Reclamantul, cetățean francez stabilit în Regatul Unit, administra o companie de internet înregistrată în Statele Unite, care avea conținut sexual explicit.

5.2. Defăimarea și rolul arhivelor disponibile pe internet în privința accesărilor succesive

În privința accesărilor succesive pe internet a unor articole considerate defăimătoare și a antrenării răspunderii celui care le-a publicat și care deține arhivele internet, relevanță prezintă hotărârea din 2009 în cauza *Times Newspapers Ltd c. Regatului Unit* (nr. 1 și 2)[30]. Societatea reclamantă, deținător și editor al ziarului The Times, a invocat în fața Curții Europene a

[29] Curtea Europeană a Drepturilor Omului, decizia asupra admisibilităţii din 18 octombrie 2005, în cauza *Perrin c. Regatul Unit al Marii Britanii*.

[30] Curtea Europeană a Drepturilor Omului, Hotărârea din 10 martie 2009, în cauza *Times Newspapers LTD (Nr. 1 şi 2) c. Regatul Unit al Marii Britanii* (Cererile 3002/03 şi 23676/03).

Drepturilor Omului că regula din Regatul Unit potrivit căreia de fiecare dată când se accesează materiale defăimătoare pe internet apare un nou motiv de acțiune în procesele de calomnie („regula publicării pe internet”[31]) constituie o restricție nejustificată și disproporționată a dreptului său la liberă exprimare și în încălcare a libertății sale de exprimare.

Ca situație de fapt care a generat cauza, este publicarea, în luna decembrie 1999, de către reclamantă, a două articole care au fost considerate defăimătoare de către persoana particulară la care se refereau, astfel că aceasta a inițiat proceduri civile pentru defăimare împotriva ziarului, a redactorului șef și a celor doi jurnaliști, autori ai articolelor.

Ambele articole au fost încărcate și pe site-ul The Times în aceeași zi cu publicarea în versiunea tipărită a ziarului. În timp ce primul proces pentru calomnie era în curs, articolele au rămas pe site-ul de internet al ziarului, fiind accesibile în cadrul arhivei ziarului.

În decembrie 2000, persoana în cauză a introdus o a doua acțiune pentru defăimare din cauza publicării continue a articolelor în arhiva internet. Ziarul a adăugat ambelor articole publicate pe internet un avertisment prin care anunța că acestea făceau obiectul unor litigii de calomnie și nu se permitea să fie reproduse sau invocate fără consultarea departamentului juridic al societății. În cadrul celei de a doua cereri, ziarul s-a apărat invocând regula publicației unice, care prevede că doar prima publicare a unui articol publicat pe internet putea duce la intentarea unei acțiuni în justiție pentru defăimare, și nu descărcările consecutive efectuate de utilizatori. Instanța de apel a confirmat aplicarea „regulii publicării pe internet” și a considerat că întrebarea privind gestionarea arhivelor era un aspect relativ minor al libertății de exprimare și că era de dorit să se publice un avertisment prin care cititorii să fie informați despre caracterul pretins fals al documentelor din arhivă, din moment ce se cunoștea caracterul lor potențial defăimător.

În considerentele hotărârii, Curtea a subliniat că rolul internetului în dezvoltarea accesului publicului la știri și în favorizarea transmiterii informațiilor în general, datorită accesibilității sale și capacității de a păstra

[31] Regula *common law* potrivit căreia publicațiile succesive ale aceleași declarații defăimătoare dau motiv pentru acțiuni distincte, stabilită în cauza Duke of Brunswick v. Harmer [1849], de către High Court.

și comunica mari cantități de informații[32], însă, pe fond, a constatat că nu a avut loc o încălcare a articolului 10.

Instanța europeană a analizat dacă aplicarea regulii privind publicarea pe internet era „necesară într-o societate democratică". Curtea a reținut că arhivele internet constituie o resursă importantă de educare și de cercetare istorică, dar în același timp a constatat că marja de apreciere a statelor este susceptibilă să fie mai mare în ceea ce privește arhivele decât actualitățile și că obligația presei de a veghea asupra exactitudinii este mai strictă pentru acest tip de informații. În analiza cauzei, instanța a apreciat ca semnificativ faptul că, deși cererile pentru defăimare au fost introduse pentru ambele articole în decembrie 1999, nicio rectificare nu a fost adăugată la versiunea arhivată a articolelor înainte de decembrie 2000. Având în vedere că arhivele internet erau gestionate de ziar și că instanțele naționale nu au indicat că articolele trebuie să fie retrase în totalitate, Curtea a considerat că exigența impusă ziarului de a adăuga o calificare adecvată versiunii internet a articolelor, nu a fost disproporționată.

Având în vedere concluzia la care a ajuns, instanța europeană a considerat că nu se impune analiza argumentului societății reclamantei potrivit căruia „regula privind publicarea pe internet" ar avea un efect inhibitor mai larg. În schimb, a analizat problema termenului de prescripție al acțiunilor pentru defăimare și argumentul ziarului conform căruia regula în cauză determină o responsabilitate continuă. Curtea a reținut că în cauză, acțiunile pentru defăimare priveau aceleași articole și ambele au început după cincisprezece luni de la publicarea inițială, astfel încât capacitatea societății reclamante de a-și pregăti apărarea nu a fost afectată de trecerea timpului. Însă, dacă o acțiune pentru defăimare este intentată după o perioadă lungă de timp, ea poate cauza, chiar în absența unor circumstanțe excepționale, o atingere disproporționată libertății presei sub aspectul articolului 10 din Convenție.

5.3. Discriminarea ca limită a libertății de exprimare

În cauza *Willem c. Franța*[33], Curtea a analizat prin prisma articolului 10 din Convenție, apelul adresat de către un primar, prin

[32] Curtea Europeană a Drepturilor Omului, Hotărârea din 10 martie 2009, în cauza *Times Newspapers LTD (Nr. 1 și 2) c. Regatul Unit al Marii Britanii* (Cererile 3002/03 și 23676/03), § 27.

intermediul site-ului web al municipalității, de boicotare a produselor israeliene. Primarul a fost ulterior condamnat pentru provocarea discriminării. Instanța europeană a constatat că nu a existat o încălcare a articolului 10 din Convenție, deoarece motivele prezentate de instanțele franceze pentru a justifica ingerința în libertatea de exprimare a reclamantului au fost „relevante și suficiente" în sensul articolului 10. În plus, amenda aplicată a fost relativ moderată și proporțională cu scopul urmărit.

Urmând linia generală aplicată comunicării în sensul tradițional, în aprecierea legalității restricțiilor aplicate în cazul insultei, în cauza *Renaud c. Franța*[34], Curtea Europeană a constatat încălcarea articolului 10 în cazul condamnării aplicate reclamantului pentru calomnierea pe internet a unui primar, pe site-ul unei asociației al cărei președinte și administrator era acesta, pe motiv că sancțiunea aplicată a fost disproporționată față de scopul legitim al protejării drepturilor altor persoane.

5.4. Răspunderea juridică a deținătorului unui portal internet pentru conținutul comentariilor utilizatorilor

Prima hotărâre pronunțată de Curtea Europeană a Drepturilor Omului în materie de antrenare a răspunderii juridice a deținătorului unui portal internet de știri pentru conținutul comentariilor utilizatorilor, a fost pronunțată în anul 2015, de către Marea Cameră în cauza *Delfi AS c. Estonia*[35]. Plângerea analizată de către Curte, prin prisma încălcării articolului 10 din Convenție, a privit antrenarea răspunderii unei societăți comerciale (Delfi AS) pentru comentarii ofensatoare ale utilizatorilor pe un portal de știri, mesaje ce au fost îndepărtate de pe portalul de știri după șase săptămâni de la afișare.

În speță, reclamanta deținea Delfi, unul dintre cele mai mari portaluri internet de știri din Estonia, pe care se publicau zilnic peste 330 de articole (la data depunerii cererii în fața Curții, în anul 2009). Situația de fapt

---

[33] Curtea Europeană a Drepturilor Omului, Hotărârea din 16 iulie 2009 în cauza *Willem c. Franţa* (Cererea nr. 10883/05).

[34] Curtea Europeană a Drepturilor Omului, Hotărârea din 5 mai 2011, *în cauza Editorial Board of Pravoye Delo and Shtekel c. Ucraina.*

[35] Curtea Europeană a Drepturilor Omului, Marea Cameră, Hotărârea din 16 iunie 2015, în cauza *Delfi AS c. Estonia (Cererea nr. 64569/09).* Textul integral al hotărârii este disponibil la adresa: hudoc.echr.coe.int.

care a determinat formularea plângerii individuale din partea reclamantei a fost generată de publicarea, în anul 2006, pe portalul Delfi, a unei ştiri referitoare la imposibilitatea practicării unui drum de gheață[36], din cauza acțiunilor unei companii de feribot şi de afișarea multor comentarii din partea utilizatorilor cu conținut defăimător, potrivit aprecierii proprietarului companiei de feribot. Instanțele naționale au obligat societatea la plata de despăgubiri în cuantum echivalent cu 320 euro. Instanţa europeană a ajuns la concluzia neîncălcării articolului 10 din Convenţie, deoarece deciziile instanțelor naționale de stabilire a răspunderii societății au constituit o restricție asupra libertății de exprimare pe portalul internet, justificată şi proporțională. Principalele considerente care au determinat au fost în esență, următoarele: comentariile au fost extreme și au fost afișate ca reacție la un articol ce a fost publicat pe portalul internet de ştiri, administrat de manieră profesional şi care funcționează pe o bază comercială; măsurile luate de reclamantă pentru a elimina comentariile ofensatoare în cel mai scurt timp după publicarea lor au fost insuficiente; amenda în cuantum echivalent a 320 de euro nu este excesivă pentru reclamantă, care deține unul dintre cele mai mari portaluri internet de ştiri din Estonia.

5.5. Condiția necesității ingerinței restricțiilor în cazul dreptului de a răspândi informații prin partajarea fișierelor torrent

În opinia instanței europene de contencios al drepturilor omului, din cauza *Neij și Sunde Kolmisoppi c. Suediei*, prin decizia de inadmisibilitate din 2013, transmiterea de fișiere pe internet, chiar dacă ele conțin materiale protejate de dreptul de autor, se încadrează în domeniul de aplicare al dreptului de transmite și primi informații, însă restricționarea acestui drept poate fi necesară, tocmai pentru a proteja drepturile de autor.[37]

Cauza privește plângerea formulată de către reclamanți, doi dintre co-fondatorii „The Pirate Bay", unul dintre cele mai mari site-uri web pentru partajarea fișierelor torrent. În opinia lor, condamnarea pentru complicitatea de a comite infracțiuni prin încălcarea legii drepturilor de autor, a încălcat articolul 10 din Convenție.

---

[36] Drumurile de gheaţă sunt drumuri publice formate pe marea înghețată şi deschise între partea continentală a Estoniei şi unele insule în timpul iernii; *Delfi AS c. Estonia (Cererea nr. 64569/09), parag. 16.*

[37] Curtea Europeană a Drepturilor Omului, decizia cu privire la admisibilitate din 19 februarie 2013, în cauza *Neij şi Sunde Kolmisoppi c. Suedia*.

Curtea a declarat inadmisibilă cererea ca fiind vădit nefondată. Instanța a afirmat că partajarea sau permiterea altor persoane de a partaja fișierele de acest tip pe internet, chiar dacă sunt materiale protejate prin dreptul de autor și în scopuri profitabile, intră în domeniul de aplicare al dreptului de a „primi și de a transmite informații", deci acțiunile întreprinse de reclamanți sunt protejate în temeiul articolului 10 parag. 1 din Convenție și, prin urmare, condamnările reclamanților au afectat dreptul lor la libertatea de exprimare.

În opinia Curții, o astfel de ingerință încalcă articolul 10 dacă nu a fost „prevăzută de lege", a urmărit unul sau mai multe scopuri legitime menționate la articolul 10 parag. 2 și nu a fost „necesară într-o societate democratică" pentru a atinge acest scop sau scopuri. Cu toate acestea, Curtea a considerat că instanțele naționale au echilibrat corect interesele concurente în joc – adică dreptul reclamanților de a primi și transmite informații și necesitatea de a proteja drepturile de autor – în cazul condamnării reclamanților.

Analizând raționamentul Curții, suntem nevoiți să aducem în discuție lipsa de consecvență a acesteia, deoarece, pe de o parte, instanța ajunge foarte rapid la concluzia includerii activității de partajare a fișierelor conținând materiale protejate de dreptul de autor, în domeniul de aplicare a dreptului de a primi informații, fără să prezinte relevanță caracterul legitim sau nu al acestora, în sensul deținerii sau nu a dreptului de autor asupra materialelor sau a dreptului de a le transmite, iar pe de altă parte, la examinarea testului necesității într-o societate democratică, protejarea drepturilor de autor apare ca motiv determinant care justifică aplicarea restricționării dreptului protejat de art. 10 parag. 1, concluzie care este în contradicție cu ipoteza de la care a plecat Curtea în analiza sa. În acest context, este neclară motivarea instanței de a include în domeniul de aplicare al articolului 10 par. 1 o astfel de manifestare a dreptului de a transmite informații, dacă este legitimă restricționarea sa, din perspectiva cerinței necesității.

6. Concluzii

Dezvoltarea internetului a determinat adoptarea unor noi reglementări în anumite domenii cu care acesta interferează, în mod special remarcându-se intercondiționarea cu libertatea de exprimare, informare și de

opinie şi cu alte drepturi fundamentale (cum sunt dreptul la respectarea vieţii private, a dreptului la propria imagine şi protecţia datelor personale), multe dintre reglementările noi făcând parte din instrumentele *soft law*. Cel mai important aspect relevat de existenţa, scopul şi conţinutul acestora este acela că nu au fost create drepturi noi, ci au fost adaptate la situaţiile noi standardele bine stabilite în consacrarea şi garantarea drepturilor şi libertăţilor fundamentale. O altă consecinţă a acestei abordări este faptul că menţionarea în mod expres şi direct a internetului în legătură cu libertatea de exprimare sau de informare în instrumente juridice internaţionale şi în jurisprudenţa internaţională este de dată relativ recentă. Arhitectura juridică a protejării libertăţii de exprimare şi de informare nu s-a modificat, iar raportat la folosirea internetului pe scară largă, elementele sale se adaptează la particularităţile comunicării şi transferului de informaţii pe internet.

În vederea realizării depline a libertăţii de exprimare, informare şi de opinie, fără frontiere şi fără ingerinţe abuzive, acestea nu pot fi însoţite decât de principiul libertăţii internetului, concept ce nu este încă consacrat în mod direct, însă evoluția ulterioară a normelor de reglementare specifice nu poate fi decât în acest sens.

ANALELE ŞTIINTIFICE ALE UNIVERSITATII „AL. I. CUZA" IASI
TOMUL LXIII, ŞTIINTE JURIDICE, 2017, NR. II

DIFICULTĂŢI DE ORDIN CRIMINALISTIC ÎN INVESTIGAREA INFRACŢIUNILOR INFORMATICE

FORENSIC DIFFICULTIES IN INVESTIGATING CYBERCRIME

ANCUŢA ELENA FRANŢ[1]

Rezumat: Societatea actuală îşi desfăşoară majoritatea activităţilor utilizând tehnologia digitală, fapt care aduce numeroase beneficii, dar care, în acelaşi timp, creează premisele unor infracţiuni specifice. Investigarea unor astfel de infracţiuni necesită dezvoltarea unei metodologii criminalistice speciale. Prezenta lucrare îşi propune să identifice modalităţile prin care pot fi descoperite asemenea infracţiuni şi cum pot fi identificaţi infractorii, evidenţiind, în acelaşi timp, dificultăţile cu care se confruntă investigatorii în anchetarea unor astfel de fapte antisociale. Dificultăţile pot apărea, de exemplu, atunci când infractorii îşi ascund adresa de IP, când utilizează o altă adresă de IP sau când îşi atribuie o identitate falsă. De asemenea, este important ca anchetatorii să respecte dispoziţiile legale care prevăd respectarea dreptului la viaţă privată şi să desfăşoare percheziţiile informatice doar în condiţiile prevăzute de lege. Studiul îşi propune să cerceteze şi potenţialul preventiv pe care îl poate avea analiza informaţiilor oferite de internet, în condiţiile în care internetul facilitează comunicarea dintre infractori şi poate oferi indicii despre pregătirea unor activităţi infracţionale.
Cuvinte-cheie: internet, criminalitate informatică, criminalistică, prevenirea infracţiunilor.

Abstract: The modern society carries out most of its activities using digital technology, which brings many benefits but, at the same time, creates the premises of specific crimes. Investigating such crimes requires the development of a special forensic methodology. This paper aims to identify ways in which such offenses can be discovered and how criminals can be identified, while highlighting the difficulties faced by investigators in investigating such antisocial facts. Difficulties may arise, for example, when offenders hide their IP address, use another IP address or assign a false identity. It is also important for investigators to comply with legal provisions regarding the right to privacy and to conduct computer searches only under the

[1] Asistent univ. dr., Facultatea de Drept, Universitatea „Alexandru Ioan Cuza" din Iași, email: ancuta.frant@uaic.ro.

conditions provided by law. The study also aims to examine the preventive potential of internet information analysis, given that the internet facilitates communication between criminals and can provide clues about the preparation of criminal activities.
Key-words: internet, cybercrime, forensic science, crime prevention.

1. Privire generală asupra infracţiunilor informatice

Dezvoltarea tehnologică permanentă reprezintă una din trăsăturile definitorii ale umanităţii.

În prezent, activitatea societăţii se bazează în mare măsură pe tehnologia digitală. Aceasta aduce numeroase beneficii şi facilitează, fără îndoială, viaţa oamenilor, dar, în egală măsură, aduce modificări în modul în care percepem relaţia cu ceilalţi. De asemenea, îi face pe oameni vulnerabili într-un mod care nu fusese cunoscut anterior, deoarece, în paralel cu facilităţile aduse de tehnologie, se dezvoltă şi infracţionalitatea cibernetică.

În special dezvoltarea internetului a modificat radical modul în care se desfăşoară relaţiile sociale în toate domeniile de activitate. Însă această dezvoltare a internetului a atras şi o vulnerabilitate a oamenilor în faţa infracţionalităţii specifice, care s-a dezvoltat în mediul informatic.

Infractorii utilizează internetul în scopuri multiple, de exemplu, pentru a face schimb de informaţii, pentru a-şi ascunde identitatea, pentru a-şi asuma o altă identitate, pentru a descoperi şi a strânge informaţii despre potenţialele victime, pentru a lua legătura cu alţi infractori, pentru a distribui informaţii (adevărate sau false)[2].

Revine criminalisticii, care, prin excelenţă, are rolul de a analiza urmele infracţiunilor, să dezvolte mijloace eficiente pentru a descoperi făptuitorii, astfel încât aceştia să fie pedepsiţi.

Dezvoltarea internetului permite însă şi dezvoltarea laturii preventive a criminalisticii, deoarece pot fi identificate indicii cu privire la pregătirea săvârşirii unor infracţiuni.

În lucrarea de faţă ne propunem să trecem în revistă modalităţile prin care criminalistica poate utiliza caracteristicile specifice mediului informatic, astfel încât să se realizeze combaterea şi prevenirea infracţiunilor cibernetice. Nu avem în vedere neapărat infracţiunile informatice, ci orice

[2] A.R. Gonzales, R.B. Schofield, D.W. Hagy, *Investigations Involving the Internet and Computer Networks*, U.S. Department of Justice, Office of Justice Programs, [Online] la: https://www.ncjrs.gov/pdffiles1/nij/210798.pdf, accesat la data de 18.10.2017, p. 1.

infracţiuni care pot fi sancţionate sau prevenite prin analiza datelor ce pot fi obţinute prin intermediul internetului sau prin alte resurse informatice.

Ceea ce dorim să realizăm este să identificăm şi să clarificăm elementele de bază care permit utilizarea mediului cibernetic pentru a afla informaţii despre comiterea unor infracţiuni şi care permit identificarea autorilor. De asemenea, ne interesează latura preventivă, adică modalitatea în care pot fi prevenite faptele antisociale, prin utilizarea informaţiilor pe care le oferă internetul. Mai ales în ceea ce priveşte infracţiunile săvârşite de grupuri organizate, probabilitatea de a afla informaţii despre pregătirea unor infracţiuni prin intermediul internetului este cu atât mai mare, cu cât membrii reţelelor criminale trebuie să comunice între ei. Însă, evident, nu este uşor de identificat comportamentul infracţional, deoarece persoanele care pregătesc săvârşirea unor infracţiuni şi care comunică prin intermediul internetului în acest scop îşi iau toate măsurile de precauţie pentru a-şi ascunde identitatea şi intenţiile. De exemplu, munca investigatorilor este îngreunată de faptul că persoanele care au intenţii infracţionale utilizează frecvent aşa-numitul „dark web" (internetul întunecat), care este mai greu accesibil, aşa cum vom vedea în prezentul studiu.

În lucrarea de faţă ne propunem să identificăm unele dintre dificultăţile care pot apărea în activitatea de investigare a infracţiunilor informatice, încercând să prefigurăm şi eventuale soluţii, acolo unde este posibil.

2. Modalităţi de utilizare a mediului informatic pentru săvârşirea infracţiunilor

Realitatea arată faptul că sunt foarte multe moduri în care mediul informatic în general şi internetul în special sunt utilizate pentru săvârşirea infracţiunilor. Cunoaşterea acestor modalităţi este un pas important în realizarea activităţii de identificare criminalistică.

Una dintre modalităţile de utilizare a mediului informatic pentru săvârşirea de fapte antisociale este *folosirea internetului pentru a facilita comunicarea între persoanele care pregătesc săvârşirea unor infracţiuni*, inclusiv pentru infracţiuni foarte grave, precum terorism, trafic de persoane, trafic de droguri[3].

[3] A.R. Gonzales, R.B. Schofield, D.W. Hagy, *op.cit.*, p. 1.

De asemenea, internetul este utilizat propriu-zis ca *mediu în care se realizează unele infracţiuni* – de exemplu pornografie infantilă sau trafic de persoane ori de droguri[4].

Larg răspândită este utilizarea internetului pentru realizarea *de fraude fiscale*. Aceste fapte urmăresc fie finanţarea unor organizaţii infracţionale (precum organizaţiile teroriste), fie urmăresc pur şi simplu obţinerea unor bani sau foloase ilicite, pentru uzul personal al infractorilor[5].

Internetul reprezintă mediul ideal pentru *racolarea persoanelor*, în vederea săvârşirii faptelor de trafic de persoane sau de pornografie infantilă.

De asemenea, internetul reprezintă un mediu propice şi pentru săvârşirea faptelor de *spionaj economic*, deoarece permite accesarea sistemelor informatice ale organelor de stat sau ale organismelor private, cu scopul furtului de informaţii[6].

Practica a arătat şi numeroase situaţii în care au fost realizate intruziuni ilegale în sistemele informatice ale unor instituţii cu scopul de a le *îngreuna activitatea*[7].

Nu puţine sunt cazurile hackerilor care săvârşesc fapte ilicite în mediul informatic din *teribilism.* Este mai ales cazul unor hackeri tineri, care săvârşesc faptele doar pentru a arăta că au capacitatea intelectuală de a comite asemenea fapte (de exemplu, cazurile unor hackeri care au spart reţelele NASA ori conturile personale ale unor vedete)[8].

De asemenea, există şi cazuri de hackeri care îşi asumă rolul de *„justiţiari”*, acţionând împotriva celor care săvârşesc infracţiuni (de exemplu, organizaţia Anonymous, care a reuşit destabilizarea unor site-uri care promovau pornografia infantilă)[9].

---

[4] A.R. Gonzales, R.B. Schofield, D.W. Hagy, *op.cit.*, pp. 1-2.

[5] A se vedea C.R. Baker, *An analysis of fraud on the internet*, în Internet Research, Vol. 9, Issue 5, pp. 348-360.

[6] A se vedea K. Davis, *Why Cybercrime Is So Hard To Investigate*, în Computer Crime Research Center, 2015, [Online] la: http://www.crime-research.org/articles/4002/, accesat la data de 20.11.2017.

[7] *Ibidem.*

[8] M. Levinson, *Why Law Enforcement Can't Stop Hackers*, [Online] la: https://www.cio.com/article/2402264/security0/why-law-enforcement-can-t-stop-hackers.html?page=2, accesat la data de 22.11.2017.

[9] A. Cuthbertson, *Anonymous Hacker Takes Down 20 Percent of Dark Web in Child Porn Operation*, 2017, [Online] la: http://www.newsweek.com/anonymous-hacker-dark-web-child-porn-operation-553014, accesat la data de 22.11.2017.

Elementele prezentate mai sus, fără a epuiza totalitatea situaţiilor ce pot fi întâlnite în practică, ilustrează diversitatea modalităţilor în care poate fi utilizat mediul informatic pentru săvârşirea infracţiunilor, ceea ce este de natură să arate amploarea fenomenului infracţiunilor cibernetice. Astfel, devine clar de ce este important demersul de prevenire şi combatere a infracţiunilor informatice.

3. Identificarea dificultăţilor cu care se confruntă anchetatorii în investigarea infracţiunilor de natură cibernetică

Literatura de specialitate arată că, teoretic, identificarea persoanelor care săvârşesc infracţiuni informatice ar trebui să fie relativ simplă, deoarece orice activitate în mediul virtual lasă anumite urme. Astfel, ipotetic vorbind, pornindu-se de la identificarea sistemului atacat (sau accesat), mergând înapoi pe linie temporală, ar trebui să se ajungă la identificarea făptuitorilor[10].

Însă realitatea arată că, din păcate, nu este chiar atât de uşor de identificat infractorii, deoarece apar o serie de dificultăţi care împiedică urmărirea drumului activităţii infracţionale. Dificultăţile referitoare la investigarea criminalistică a infracţiunilor informatice se pot referi fie direct la realizarea anchetei, fie la elemente care, deşi nu ţin efectiv de ancheta penală, au urmări asupra modului în care, în general, este organizată o asemenea investigaţie. În continuare vom prezenta unele dintre problemele cu care se confruntă organele judiciare în demersul de cercetare a infracţiunilor informatice.

O primă piedică este reprezentată de faptul că informaţia din mediul virtual este perisabilă şi foarte uşor se poate altera sau distruge, fie datorită acţiunii intenţionate a infractorilor, fie din neglijenţă în ceea ce priveşte stocarea şi utilizarea datelor[11].

O altă problemă provine din faptul că datele temporale sunt uşor de alterat, ori acestea sunt, de multe ori, esenţiale pentru dovedirea vinovăţiei persoanelor suspectate de săvârşirea infracţiunilor cibernetice[12].

O altă dificultate ţine de faptul că investigarea infracţiunilor informatice necesită personal specializat, cu temeinice cunoştinţe în

[10] M. Levinson, *op. cit*.
[11] A.R. Gonzales, R.B. Schofield, D.W. Hagy, *op. cit.*, pp. 1-2.
[12] *Ibidem*, pp. 1-2.

domeniul informatic. Adesea se observă o veritabilă concurenţă între organele statului care caută specialişti în domeniul cibernetic şi mediul economic privat, care, de asemenea, are nevoie de specialişti în mediul informatic[13]. Cel puţin în România, condiţiile oferite de companiile private sunt de multe ori superioare celor oferite de stat, ceea ce explică de ce specialiştii în informatică preferă să aleagă domeniile private de activitate.

Un alt aspect ţine de percepţia asupra gravităţii infracţiunilor săvârşite în mediul informatic. Astfel, unele infracţiuni care se săvârşesc în mediul virtual şi care sunt considerate mai grave polarizează mult mai multă atenţie din partea organelor de anchetă. De exemplu, infracţiunile de pornografie infantilă sau de trafic de persoane ori de droguri atrag implicarea majorităţii personalului specializat din cadrul poliţiei şi parchetelor, ceea ce, mai ales în lipsa unui număr suficient de cadre, face ca atenţia acordată altor infracţiuni informatice, considerate mai puţin grave, să fie mai mică. De exemplu, faptele prin care se creează fraude financiare sunt considerate de mai mică importanţă, ceea ce face ca atenţia acordată pentru urmărirea şi sancţionarea unor asemenea fapte să fie mai mică, ceea ce duce la un număr mare de infractori nedescoperiţi. Este semnificativ faptul că, în Statele Unite ale Americii, deşi se înregistrează lunar chiar şi sute de mii de plângeri pentru fraude fiscale săvârşite în mediul on-line, foarte multe asemenea fapte rămân nedescoperite[14].

Un alt aspect care îngreunează investigarea infracţiunilor cibernetice este faptul că mulţi hackeri sunt tineri care acţionează din teribilism. Adesea, aceste persoane nu ar săvârşi infracţiuni în afara mediului online, dar tehnologia îi face să nu mai distingă graniţa dintre bine şi rău. De multe ori, ei încep prin a sparge site-uri de pe care descarcă muzică sau filme (care în mod normal sunt contra-cost) şi ajung să săvârşească ulterior fapte mai grave (de exemplu, să spargă conturile NASA). Hackerii care acţionează din teribilism duc la încărcarea agendei investigatorilor, care trebuie să se ocupe şi de anchetarea unor asemenea fapte, în loc să se concentreze asupra altora (precum trafic de persoane sau de droguri). Această dificultate nu ţine propriu-zis de criminalistică, ci mai mult de criminologie, dar trebuie analizată în strânsă legătură cu domeniul criminalisticii, datorită impactului pe care îl are în desfăşurarea anchetelor. S-a arătat în literatura de

[13] K. Davis, *op. cit*.
[14] M. Levinson, *op. cit*.

specialitate că aici este, în primul rând, o problemă de educaţie, deoarece tinerii nu sunt învăţaţi care sunt limitele normale ale utilizării mediului informatic, astfel încât să nu se ajungă la săvârşirea de fapte antisociale. Se vorbeşte chiar despre dezvoltarea unei ramuri a eticii – etica utilizării tehnologiei – care să fie predată în şcoli, pentru a preveni săvârşirea unor asemenea fapte[15].

O altă particularitate a infracţiunilor informatice provine din faptul că, de multe ori, sancţiunile aplicate pentru fapte considerate mai puţin grave (de exemplu, fraude fiscale sau fapte săvârşite din teribilism de hackerii tineri) sunt foarte mici. Mai mult, este important faptul că, dacă nu intervin criptări sau denaturări de date, activitatea desfăşurată de infractori pe internet lasă urme care sunt foarte greu de combătut, iar aceasta deschide calea spre încheierea unui acord de recunoaştere a vinovăţiei, care duce, prin efectul legii, la aplicarea de sancţiuni reduse. Aceste sancţiuni mici creează impresia generală că infracţiunile săvârşite în mediul informatic nu sunt foarte grave, ceea ce încurajează săvârşirea lor în continuare[16].

O altă problemă provine din faptul că investigarea infracţiunilor informatice necesită, de regulă, desfăşurarea unor activităţi complexe şi de durată. De multe ori, infracţionalitatea cibernetică implică făptuitori şi victime aflate în ţări diferite, fiind astfel dificil de obţinut accesul la dispozitivele electronice care pot oferi dovezi cu privire la infracţiunile săvârşite. De asemenea, ancheta poate evidenţia necesitatea de a accesa baze de date deţinute de entităţi care nu au legătură directă cu infracţiunea, precum instituţii de stat sau firme private. În plus, poate fi dificil accesul la servere, routere sau la datele stocate de furnizorii de servicii de internet. Legat de acest aspect, este important de subliniat faptul că unele ţări sunt reticente în ceea ce priveşte cooperarea internaţională referitoare la infracţiunile informatice (de exemplu, Rusia[17]).

[15] M. Levinson, *op. cit*.

[16] *Ibidem*. Autoarea oferă drept exemplu cazul lui Joshua Holly, care a furat datele de la 200 de carduri de credit, dar care nu a făcut nici măcar o zi de închisoare pentru fapta sa.

[17] A se vedea M.A. Vatis, *The Council of Europe Convention on Cybercrime*, în Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 2010, [Online] la: https://www.nap.edu/read/12997/chapter/14, accesat la data de 29.11.2017, p. 218.

O dificultate dificil de înlăturat în cercetarea infracţiunilor informatice este faptul că, de multe ori, infractorii folosesc reţele criptate, ceea ce face aproape imposibilă identificarea adresei de I.P. a utilizatorilor.

De asemenea, o adevărată provocare în activitatea investigatorilor o reprezintă faptul că activitatea lor nu trebuie să încalce dreptul la viaţă privată. Altfel spus, toate activităţile de strângere şi analiză a probelor trebuie să se desfăşoare cu respectarea dispoziţiilor legale care garantează respectarea acestui drept.

În cele ce urmează vom detalia două dintre dificultăţile de anchetare prezentate mai sus, şi anume utilizarea reţelelor criptate şi necesitatea de a păstra echilibrul între obţinerea datelor necesare anchetei şi respectarea dreptului la viaţă privată.

4. Dificultăţi în realizarea anchetei penale datorate utilizării reţelelor criptate de către infractori

Investigarea infracţiunilor cibernetice este de multe ori îngreunată de faptul că unii infractori folosesc pentru desfăşurarea activităţilor lor ilegale aşa-numitul *dark web* („internetul întunecat”). Pentru a înţelege cum funcţionează *dark web* trebuie să facem distincţia dintre *dark net, dark web* şi *deep web,* noţiuni între care, adesea, se face confuzie.

Dark net este o reţea de internet ce se poate accesa numai utilizând anumite softuri şi, de multe ori, având şi o cheie care să permită accesarea. De exemplu, reprezintă o reţea de dark net o reţea peer-to-peer criptată sau parolată, prin care un utilizator trimite altui utilizator un fişier[18]. Utilizatorii de *dark net* pot folosi şi softuri speciale, precum Tor sau I2P, care permit ascunderea adresei de IP. Astfel, cei care utilizează *dark net* îşi păstrează anonimitatea şi sunt protejaţi de o eventuală supraveghere sau cenzură[19].

Dark web este constituit din mai multe *dark net*-uri. Practic, *dark web* reprezintă totalitatea site-urilor şi a serviciilor ce activează în *dark net*[20]. Este important de înţeles că, în esenţă, *dark web* poate fi accesibil oricui, de

[18] G. Stanciu, *Care este diferența dintre Deep Web, Darknet și Dark Web*, [Online] la: https://playtech.ro/2017/care-este-diferenta-intre-deep-web-darknet-si-dark-web/, accesat la data de 25.10.2017.

[19] A. Greenberg, *Hacker Lexicon: What is the Dark Web?*, [Online] la: https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/, accesat la data de 20.10.2017.

[20] G. Stanciu, *op. cit*.

exemplu oricărei persoane care utilizează softul Tor şi cunoaşte adresa url a site-ului pe care doreşte să-l viziteze, însă va fi foarte dificil de identificat adresa de IP a utilizatorilor[21].

Deep web reprezintă colecţia tuturor site-urilor de pe internet care nu pot fi găsite prin utilizarea unui motor de căutare. *Deep web* include, într-adevăr, şi *dark web*, dar este format în principal din pagini cu un conţinut licit. De exemplu, fac parte din *deep web* paginile cu un conţinut dinamic, precum cele care sunt generate de completarea unui formular. Tot din *deep web* fac parte şi conţinuturile video ale unor servicii de streaming (de exemplu, Netflix), deoarece se doreşte ca aceste conţinuturi să poată fi vizualizate doar de către cei care le accesează în mod direct[22]. S-a estimat că *dark web* reprezintă, în esenţă, aproximativ 0,01 din totalul paginilor de internet. Concret, unele studii arată că există aproximativ 10000 de servicii Tor ascunse, faţă de cele câteva mii de milioane de pagini web obişnuite[23].

Utilizarea reţelelor criptate este una dintre cele mai dificile probleme pe care le pot întâlni anchetatorii în investigarea infracţiunilor informatice.

5. Păstrarea echilibrului între dreptul la viaţă privată şi necesitatea obţinerii datelor care să permită cercetarea şi sancţionarea infracţiunilor informatice

O problemă greu de surmontat în investigarea infracţiunilor informatice provine din necesitatea de a păstra echilibrul între oportunitatea unor intervenţii energice pentru accesarea datelor care să permită identificarea infractorilor şi respectarea dreptului la viaţă privată.

Semnificativ în acest sens este textul Convenţiei de la Budapesta[24], prin care s-a încercat trasarea unor reguli menite să faciliteze obţinerea

[21] A. Greenberg, *op. cit*.
[22] G. Stanciu, *op. cit.*
[23] A. Greenberg, *op. cit*.
[24] Convenția Consiliului Europei de la Budapesta, din 23.11.2001, privind criminalitatea informatică, ratificată de România prin Legea nr. 64/2004, publicată în M.Of. nr. 343 din 20.04.2004.

datelor necesare anchetării infracţiunilor cibernetice, în special atunci când este necesară cooperarea judiciară internaţională[25].

Convenţia de la Budapesta a fost primită cu rezervă în multe din ţările semnatare (deşi a fost ratificată de 56 de state), în special de către societatea civilă, care a considerat că prevederile sale duc la o imixtiune nejustificat de mare a statului în viaţa privată[26].

În România, mai multe încercări de a legifera direcţiile trasate de Convenţia de la Budapesta au fost declarate neconstituţionale[27].

Este important de subliniat faptul că Rusia, deşi membră a Consiliului Europei, nu a semnat această Convenţie, considerând că prevederile ei reprezintă o încălcare a suveranităţii sale statale. În special dispoziţiile referitoare la posibilitatea ca anchetatorii din alt stat să poată obţine informaţii doar cu acordul proprietarului computerului sau cu acordul deţinătorului informaţiei au fost considerate de Rusia inadmisibile[28].

Aşadar, este dificil de echilibrat necesitatea anchetatorilor de a obţine informaţii care să ducă la identificarea şi pedepsirea infractorilor cu dreptul cetăţenilor la respectarea intimităţii lor. Apreciem că această dificultate care apare în investigarea infracţiunilor informatice este greu de depăşit, deoarece nu ţine de aspecte tehnice (care pot fi, până la urmă, rezolvate), ci de elemente care implică interpretarea drepturilor. Ori, când este vorba despre interpretarea drepturilor şi despre stabilirea limitelor între

[25] Pentru textul oficial al Convenției de la Budapesta, a se vedea [Online] la: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, accesat la data de 29.11.2017.

[26] A se vedea K. Rodriguez, *Dangerous Cybercrime Treaty Pushes Surveillance and Secrecy Worldwide*, Electronic Frontier Foundation, 2011, [Online] la: https://www.eff.org/deeplinks/2011/08/cybercrime-treaty-pushes-surveillance-secrecy-worldwide, accesat la data de 29.11.2017.

[27] Legea nr. 82/2012 privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului, precum și pentru modificarea și completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice a fost declarată neconstituțională prin Decizia Curții Constituționale nr. 440 din 8.07.2014. Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice (prin care se dorea furnizarea cartelelor telefonice *prepay* doar pe bază de buletin) a fost declarată neconstituțională prin Decizia Curții Constituționale nr. 461 din 16.09.2014. Legea privind securitatea cibernetică a României a fost declarată neconstituțională prin Decizia Curții Constituționale nr. 17 din 21.01.2015.

[28] A se vedea M.A. Vatis, *op. cit.*, p. 218.

care acestea se pot manifesta, discuţiile pot fi interminabile, iar rezultatele concrete pot fi extrem de greu de obţinut.

6. Concluzii

Cele prezentate mai sus susţin ideea că, în domeniul investigării infracţiunilor informatice, previziunile sunt mai degrabă sumbre. Concret, se pare că infractorii sunt întotdeauna cu un pas înaintea anchetatorilor, ceea ce face ca prevenirea, descoperirea şi sancţionarea infracţiunilor cibernetice să fie extrem de dificil de realizat. Mediul informatic oferă condiţii propice pentru manifestarea intenţiilor infractorilor, iar aceştia vor profita de aceste condiţii. Totuşi, realitatea arată că, prin alocarea unor resurse semnificative, umane şi materiale, pot fi obţinute rezultate în lupta contra infracţiunilor informatice. Rămâne doar să sperăm că, în viitor, investigatorii vor reuşi să depăşească dificultăţile de cercetare a acestor infracţiuni şi vor putea să îi aducă în faţa justiţiei pe majoritatea infractorilor din mediul informatic, în paralel cu realizarea unei activităţi eficiente de prevenire a infracţionalităţii cibernetice.

ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

INTERNETUL LUCRURILOR. PERSPECTIVA JURIDICĂ

INTERNET OF THINGS. LEGAL PERSPECTIVE

ANDA CRIȘU-CIOCÎNTĂ[1]

Rezumat: Se pare că într-un viitor nu prea îndepărtat „Internetul lucrurilor", zis și "Internet of Things" (IoT), va deveni un mod de viață pentru mare parte a omenirii. Într-o redare succintă, Internetul lucrurilor presupune conectarea oricărui dispozitiv la Internet și/sau conectarea mai multor dispozitive între ele, cu scopul de a fi monitorizate și controlate de la distanță. Axarea producătorilor pe cercetări menite să descopere cele mai sofisticate modalități de exploatare a lucrurilor conectate la Internet, precum și goana lor după obținerea rapidă a unor profituri cât mai consistente, face ca nivelul de securitate a acestor lucruri să rămână în plan secund. Securitatea scăzută a lucrurilor conectate la Internet va facilita acțiunile celor rău intenționați și, în cele din urmă, va influența criminalitatea. În prezentul material ne-am propus să realizăm o scurtă introducere în ceea ce poartă denumirea de „Internetul lucrurilor", după care să prezentăm o serie de fapte prevăzute de legea penală a căror comitere ar putea fi facilitată de dispozitivele inteligente conectate la Internet și controlate printr-o conexiune la distanță.
Cuvinte cheie: Internetul lucrurilor, securitate, dispozitive inteligente, provocări, criminalitate

Summary: As it seems like in a forthcoming future, "The Internet of things" also called "Internet of Things" (IoT), will become a way of living for most of the people. In a nutshell, the Internet of things implies the connection of every device to the Internet and/or the connection of multiple devices among each other in order to be monitored and controlled from the distance. The fact that manufacturers focused on research with the purpose of discovering the most sophisticated modalities of exploiting thing connected to the Internet, as well as their rush to quickly obtain as much consistent profits as possible determines the level of security of these things to remain on a second plan. The low security of the things connected to the Internet will encourage the actions of those who are malicious and, finally, it will influence the criminality. In this paper, we propose to make a brief introduction of what stands

[1] Doctorand, Universitatea „Alexandru Ioan Cuza" din Iași, Facultatea de Drept.

for “The Internet of things”, and then to present a series of criminal law facts, which, once committed, could be relieved by intelligent devices connected to the Internet and controlled through a remote connection.

Key words: Internet of things, security, intelligent devices, challenges, criminality

1. Introducere

Internetul, una dintre cele mai importante tehnologii a ultimilor aproximativ 60 de ani, care a reușit să ne influențeze modul de viață, a fost creat de oameni pentru oameni. În timp, lucrurile au evoluat, iar cercetările în domeniu au dus Internetul la un alt nivel, unul care presupune conectarea nu doar a oamenilor, ci și a lucrurilor. Spre deosebire de primele lucruri care au fost conectate la Internet - calculatorul și telefonul mobil - în cazul cărora oamenii sunt cei care în ultimă instanță se conectează la Internet, lucrurile din Internet of Things (IOT este prescurtarea uzuală) sunt dispozitive care interacționează mai mult între ele și, mai puțin, cu oamenii.

Internetul lucrurilor este un concept ce presupune conectarea oricărui dispozitiv la Internet și/sau conectarea mai multor dispozitive între ele, cu scopul de a fi monitorizate și controlate de la distanță. Se pare că într-un viitor nu prea îndepărtat se va ajunge la un Internet al tuturor lucrurilor – Internet of Everything – care să conecteze tot mai multe dispozitive ce ne vor asista viața de zi cu zi. Un astfel de lucru este posibil prin implementarea de senzori și abilități de comunicare tuturor dispozitivelor ce ne înconjoară. Prin senzorii implementați, dispozitivele vor culege date din mediul înconjurător, se vor conecta între ele și astfel vor transfera datele obținute care, în cele din urmă, vor ajunge la utilizator, acesta având posibilitatea de a controla activitatea dispozitivelor conform propriilor decizii.

În ultima perioadă, Internetul lucrurilor este într-o continuă expansiune. În acest sens, în anul 2016 erau conectate 6,4 miliarde de dispozitive, iar media zilnică a dispozitivelor nou conectate la Internet este de 10 milioane. Se estimează că până în 2020 vor exista peste 26 de miliarde de dispozitive conectate. Regula pentru viitor este aceea că „orice lucru care poate fi conectat la Internet, va fi conectat”[2].

Este incontestabil faptul că Internetul lucrurilor ne poate schimba viața în sens pozitiv datorită numeroaselor avantaje pe care le aduce. Ne putem imagina cum ar fi ca ceasul să ne trezească dimineața la ora stabilită,

[2] https://alinvelea.wordpress.com/2016/12/12/ce-este-internetul-lucrurilor/.

apoi să anunțe televizorul să pornească pe canalul preferat, expresorul să pregătească cafeaua, toasterul să prăjească pâinea, mașina să fie pregătită în momentul în care ieșim din casă și să ne indice traseul optim pentru a ajunge în cel mai scurt timp la destinația dorită (serviciu/școală). Sau dacă imprimanta știe când se va termina hârtia ori tonerul și va face comandă automat. Toate aceste lucruri sunt aproape posibile și, în mod evident, ne pot ușura viața, lăsându-ne mai mult timp liber pe care să-l petrecem după bunul plac.

Realitatea este că posibilitățile și conexiunile pot fi practic nelimitate, la multe dintre ele nici nu ne putem gândi sau nu putem înțelege pe deplin impactul lor, în acest moment. Internetul lucrurilor este o temă de larg interes întrucât presupune o mulțime de posibilități și de avantaje dar, în același timp, și multe provocări și neajunsuri. Din această din urmă categorie, problema securității credem că este cea mai importantă. Focusați pe ideea de a scoate cât mai repede și la costuri cât mai reduse un produs nou pe piață, producătorii echipamentelor IoT, de cele mai multe ori, lasă în plan secund aspectele ce țin de securitate. Lipsa ori insuficiența măsurilor de securitate fac ca tot mai multe dispozitive inteligente (telefoane, televizoare, camere de supraveghere, etc) să fie implicate în atacuri cibernetice de amploare. Multe companii au analizat sistemele inteligente disponibile în acest moment pe piață și au ajuns la concluzia că securitatea acestora este complet nesatisfăcătoare[3].

Dintre numeroasele probleme ce pot apărea ca urmare a lipsei sau insuficientei securități a IoT, atenția noastră va fi îndreptată asupra modului în care noua tehnologie poate influența criminalitatea sau, altfel spus, modul în care dispozitivele inteligente conectate la Internet pot favoriza fenomenul infracțional.

2. Influența IoT asupra criminalității

Pe lângă numeroasele avantaje pe care Internetul lucrurilor le poate aduce pentru omenire, această tehnologie poate crea și dezavantaje, unul dintre ele fiind acela al favorizării comiterii de fapte prevăzute de legea penală de către persoane rău intenționate. După părerea noastră, Internetul lucrurilor va putea fi folosit de către infractori ca un instrument menit să le

[3] https://cybersecuritytrends.ro/internetul-lucrurilor-vis-frumos-sau-cosmar/.

ușureze și, în același timp, să le favorizeze comiterea de activități infracționale.

Dacă până nu demult, comiterea de fapte prevăzute de legea penală prin intermediul Internetului era limitată la o sferă relativ restrânsă de infracțiuni specifice (avem în vedere infracțiunile privind comerțul electronic și cele de fraude comise prin sisteme informatice), odată cu apariția Internetului lucrurilor aria faptelor penale ce pot fi comise prin folosirea Internetului va cunoaște o extindere în sensul că va putea cuprinde infracțiuni dintre cele mai diverse. Având în vedere paleta extrem de largă a lucrurilor care pot fi conectate la internet și apoi interconectate între ele – obiecte casnice (de exemplu, aparate de cafea, smart Tv-uri, cuptoare electrice, frigidere, mașini de spălat), aparate medicale, autovehicule, instalații de foraj de petrol, etc - valorilor sociale ce pot fi lezate prin fapte comise și cu ajutorul IoT este una largă și diversă, drepturile fundamentale ale persoanei și patrimoniul fiind, în opinia noastră, cele care pot fi cel mai frecvent afectate

În continuare vom prezenta o serie de cazuri care redau legătura strânsă dintre comiterea de fapte prevăzute de legea penală și Internetul lucrurilor, cazuri în care noua tehnologie este un factor ce facilitează comportamentele ilicite.

O primă situație pe care ne-o imaginăm are în prim plan o plită electrică ce are încorporat un computer, iar printr-o aplicație este conectată la telefonul mobil, putând astfel primi comenzi de la distanță. Asta presupune că deținătorul unui astfel de obiect, în timp ce se află la birou de exemplu, poate porni plita electrică pentru ca fiul său minor (aflat în locuință) să-și încălzească laptele. Ne putem imagina că o persoană rău intenționată, prin spargerea contului și/sau a parolei, are acces la comenzile acelei plite electrice și astfel o poate deschide în timp ce în locuința nu se găsește nici o persoană, provocând astfel un incendiu care, în cele din urmă, duce la distrugerea locuinței. În acest caz poate fi reținută infracțiunea de distrugere a unui bun imobil, prin incendiere; infracțiunea fiind comisă fără ca autorul să se fi aflat în preajma bunului distrus în momentul comiterii faptei și nici măcar în momentul imediat premergător. Bineînțeles, infracțiunea de distrugere se va afla în concurs cu o serie de infracțiuni informatice (de exemplu, acces neautorizat).

O altă situație ipotetică pornește de la un aparat medical care monitorizează o persoană bolnavă și care poate fi controlat de pe Internet. Să

presupunem că aparatul medical este programat să controleze administrarea dozelor de medicamente prescrise pacientului, iar o persoană rău intenționată reușește să se conecteze la respectivul aparat și astfel, cu intenția de a ucide sau doar de a vătăma integritatea corporală sau sănătatea pacientului, îl manipulează în așa fel încât să trimită fie o doză mult mai mică, fie una mult mai mare din medicamentul prescris. Doza insuficientă sau supradoza poate fi fatală pentru pacient sau îi produce doar o lezare a integrității corporale sau a sănătății, situație în care putem vorbi de comiterea unor infracțiuni contra vieții sau infracțiuni contra integrității corporale sau sănătății persoanei. Observăm astfel că prin intermediul lucrurilor conectate la Internet pot fi comise și infracțiuni dintre cele mai grave, cum ar fi infracțiunea de omor.

Un alt caz ipotetic este acela în care un frigider este conectat la Internet și programat ca atunci când stocul la anumite produse este aproape epuizat să comande automat on-line acele produse la furnizor având, totodată, atașată o soluție pentru plata contravalorii produselor comandate (card, cont, PayPal, etc). Ca o vulnerabilitate ce poate apărea într-o astfel de situație este faptul că un infractor poate redirecționa comanda în așa fel încât produsele comandate și plătite să ajungă la o altă adresă decât cea unde se găsește obiectul în cauză. Practic beneficiarul produselor achiziționate este o altă persoană decât cea care le-a comandat și le-a plătit. Într-o astfel de situație poate fi reținută comiterea unor infracțiuni din categoria celor de fraudă comise prin sisteme informatice și mijloace de plată electronice. În plus, credem că poate fi pusă în discuție și existența unei infracțiuni de înșelăciune deoarece s-a produs o inducere în eroare prin prezentarea ca adevărată a unei împrejurări mincinoase (adresa de livrare a produselor comandate și plătite), fiind cauzată o pagubă materială. De remarcat faptul că persoana indusă în eroare nu este aceeași cu persoana în patrimoniul căreia s-a produs paguba materială însă această împrejurare nu constituie un impediment în reținerea infracțiunii de înșelăciune.

O altă situație pe care ne-o putem imagina vizează dispozitivele care permit autentificarea după amprentă sau după retină. Ca orice alte date, datele privind autentificarea sunt stocate într-un fișier care, atunci când nu este bine securizat, poate fi spart de un haker care le fură. Să ne imaginăm că respectivele date – amprenta sau retina – sunt folosite la dispozitivul de închidere-deschidere a ușii de acces într-o locuință. Dacă cineva fură cheia de acces în locuință, soluția este schimbarea yalei însă, retina și amprenta nu

mai pot fi schimbate. Dacă o persoană a ales să deschidă ușa la casă cu ochiul sau amprenta pe un dispozitiv slab securizat și un haker fură acele date, e ca și cum ar avea cheia de la casă care poate fi folosită ulterior pentru pătrunderea fără drept în locuință, fiind astfel facilitată comiterea infracțiunilor de violare de domiciliu sau violarea sediului profesional. De această dată, conectarea lucrurilor la Internet (în speță, dispozitivul de deschidere a ușii de acces) este de natură să-l ajute pe infractor, facilitându-i pătrunderea în imobil. Totodată, noul mod de pătrundere în domiciliu/sediu profesional se îndepărtează de modurile clasice, tradiționale de violare de domiciliu/sediu profesional.

Tot așa ne putem imagina cazul ușilor de garaj ce sunt conectate la wireless pentru a fi deschise din mașină și care pot fi folosite de către infractori pentru a intra în casă fără să mai fie nevoiți să apeleze la metodele clasice (spargerea și escaladarea geamului, efractarea sistemului de închidere a ușii de acces) și fără a declanșa sistemul de alarmă. Și într-o astfel de situație acțiunea de pătrundere fără drept în imobil este mult ușurată pentru infractor ca urmare a conectării la Internet a ușilor de garaj. Este facilitată astfel comiterea infracțiunii de violare de domiciliu și, în ipoteza în care pătrunderea se face în scopul sustragerii de bunuri, și a infracțiunii de furt sau, eventual, a celei de tâlhărie.

Însă, de departe cea mai la îndemână infracțiune pe care un infractor ar putea să o comită beneficiind de avantajele pe care le aduce Internetul lucrurilor este infracțiunea de violare a vieții private (art. 226 Cod penal). Multe dintre dispozitivele inteligente au sau pot avea încorporată o cameră Web și/sau microfon prin intermediul cărora putem fi „spionați” atunci când ne aflăm în spațiul nostru privat. Hakerii pot utiliza webcam-ul și microfoanele încorporate într-un Smart TV, de exemplu, pentru a vedea și a auzi tot ceea ce se întâmplă în fața acelui dispozitiv. Evident că în situații de acest gen putem vorbi de atingerea adusă vieții private în mod nelegal prin captarea sau înregistrarea de imagini sau ascultarea cu mijloace tehnice a unei persoane aflată într-un spațiu privat. Practica ne dovedește că în situații de acest fel, conduita ilicită a infractorului nu se oprește la violarea vieții private, ci, de cele mai multe ori, atunci când imaginile/înregistrările sunt compromițătoare pentru persoana vătămată continuă cu săvârșirea unor fapte de șantaj (art. 207 Cod penal). Practic, după ce intră în posesia unor imagini sau înregistrări pretins sau real compromițătoare, infractorul amenință

persoana vătămată cu darea în vileag a imaginilor/înregistrărilor deținute cu scopul de a obține un folos patrimonial.

3. Concluzii

Viitorul va aparține din ce în ce mai mult Internetului lucrurilor care are potențialul să schimbe radical modul în care interacționăm cu tehnologia, între noi și în societate. Dincolo de beneficiile pe care le aduce această nouă tehnologie, considerăm că trebuie conștientizate și riscurile pe care ea le implică.

În opinia noastră, principala problemă a dispozitivelor inteligente este securitatea care de cele mai multe ori este neglijată de producători din dorința de a face cât mai mult profit și a scoate un produs cât mai ieftin pe piață.

După părerea noastră, adoptarea unui cadru legislativ adecvat care să îi oblige pe producătorii de echipamente IoT să instaleze pe aceste echipamente soluții de securitate performante pentru a nu mai fi preluate atât de ușor, ar reprezenta o soluție viabilă pentru rezolvarea, cel puțin parțială, a problemei securității lucrurilor conectate la Internet. De asemenea, o altă soluție ar fi aceea a securizării dispozitivelor inteligente cu ultimele versiuni de software.

Potrivit unui studiu realizat de dată relativ recentă de Pew Internet Project Research, din marea majoritate a experților în tehnologie și utilizatori de Internet care au răspuns, 83% au fost de acord cu ideea că Internet of Things, cu sisteme informatice integrate și portabile (și sistemele dinamice corespunzătoare) vot avea efecte benefice larg răspândite până în 2025 și doar 17% dintre respondenți au susținut că aceasta tehnologie va avea efecte negative. Observăm astfel că opinia majoritară este în favoarea dezvoltării, extinderii Internet of Things, ceea ce presupune asumarea riscurilor pe care această tehnologie le implică și, totodată, identificarea soluțiilor menite să le diminueze pe cât mai mult posibil.

ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

PROTECȚIACORESPONDENȚEI PRIVATE A ANGAJATULUI. ASPECTE DE DREPT PENAL

THE PROTECTION OF THE EMPLOYEE'S PRIVATE CORRESPONDENCE BY CRIMINAL LAW MEANS

MIHNEA VALENTIN STOICESCU[1]

Rezumat: Realitatea arată că persoanele își petrec o foarte mare parte din timp la locul de muncă sau în legătură cu activitatea profesională și dezvoltă cea mai mare parte a relațiilor sociale în acest cadrul profesional, apărând inerente interferențe cu viața privată. Pe de altă parte, creșterea competiției în piață a condus angajatorii în a fi mai atenți cu privire la conduita, fidelitatea angajaților și protejarea informațiilor nepublice. Astfel, se conturează un conflict între dreptul angajatului la protecția secretului corespondenței private desfășurate în raporturile de muncă și interesul legitim al angajatorului în a asigura buna funcționare a organizației. Prezenta lucrare urmărește să analizeze nivelul de protecție acordat de către legiuitorul român corespondenței private a angajatului, având în vedere ultimele evoluții ale jurisprudenței CEDO și punând accentul pe mijloacele de protecție de drept penal. Lucrarea va evidenția criteriile pe care juriștii trebuie să le aibă în vedere în analiza elementelor constitutive ale infracțiunii, făcând trimitere și la categoriile de angajați care, prin natura activității, justifică a suporta un grad mai ridicat de intruziune.
Cuvinte-cheie: angajat, corespondență, viață privată, drept penal, angajator.

Abstract: Reality shows that people spend most of their time at work or engaging in activities regarding their workplace. Also, most of their social ties are created at work. On the other hand, due to always increasing competition, employers pay more attention over the protection of the industrial secrets and on the loyalty of the employees. There needs to be a balance between the employee's right to privacy and the employer's conflicting right to look over the good of the organization. This article aims to analyze the level of protection awarded by Romanian law regarding the employee's right to have his private correspondence protected, taking into consideration the latest ECHR case-law and emphasizing the criminal law means of protection. The article will emphasize the need of a more broad view of the

[1] Doctorand, Universitatea „Alexandru Ioan Cuza" din Iași, Facultatea de Drept.

violation, taking European standards into consideration, and will analyze the particularities of employees who, considering their job, must accept a higher level of intrusion in their private lives.

Key words: Employee, private correspondence, criminal law

În prezent, persoanele dezvoltă cea mai mare parte a relațiilor sociale în acest cadrul profesional, apărând astfel inerente interferențe cu viața privată. Pe de altă parte, creșterea competiției în piață a condus angajatorii în a fi mai atenți cu privire la conduita, fidelitatea angajaților și protejarea informațiilor nepublice. Astfel, se conturează un conflict între dreptul angajatului la protecția secretului corespondenței private desfășurate în raporturile de muncă și interesul legitim al angajatorului în a asigura buna funcționare a organizației. De la bun început, apreciem că se pot identifica două opinii cu privire la acest aspect. Pe de o parte, se poate susține că pe perioada în care salariatul se află la locul de muncă, în timpul orelor de program, acesta nu poate avea așteptarea la protecția vieții sale private. Pe de altă parte, se poate susține că în cazul în care salariatul califică o anumit document sau o anumită adresă de e-mail drept privată, angajatorul nu îi poate verifica sub nicio formă conținutul.

În acest context, considerăm că este oportun să analizăm în ce măsură un angajator are posibilitatea legală de a controla corespondența unui angajat al său iar, în cazul în care identificăm o încălcare a drepturilor angajatului, trebuie să analizăm ce sancțiune se impune a fi aplicată angajatorului.

Din perspectiva sancțiunilor, Curtea Europeană a Drepturilor Omului pune un accent deosebit de important asupra marjei de apreciere a statului în executarea obligației de a legifera, admițând că sunt mai mult moduri prin care se poate atinge o protecție adecvată dreptului la viață privată, recurgerea la mijloace de drept penal nefiind obligatoriu cea mai adecvată soluție[2]. Putem adăuga că există situații în care recurgerea la mijloace de drept penal nu este doar inoportună, ci este chiar incompatibilă cu scopul Convenției, acordarea unei protecții excesive vieții private conducând la încălcarea altor drepturi fundamentale relative sau chiar

[2] CEDO, Hotărârea din 26 martie 1985, *X & Y c. Olandei*, 8978/80, par. 24; Hotărârea din 4 decembrie 2003, *M.C. c. Bulgariei*, 39272/98, par. 150; Hotărârea din 2 septembrie 2010, *Mincheva c. Bulgariei*, nr. 21558/03, par. 81. Hotărârea din 2 iunie 2009, *Codarcea c. României*, 31675/04.

absolute. De asemenea, Curtea a precizat că legislația adoptată trebuie să prevadă atât un mecanism restaurativ eficient cu privire la dreptul lezat, cât și o metodă de sancționare proporțională[3].

Remarcăm că, în materie civilă, legiuitorul nu s-a rezumat doar la a proclama necesitatea protecției dreptului la viață privată, ci a și indicat, cu titlu exemplificativ, o serie de măsuri definitive sau provizorii ce pot fi luate de către instanța de judecată, la solicitarea persoanelor vătămate, pentru o înlăturare efectivă a ingerinței provocate. În acest sens, s-a pronunțat și Curtea Europeană, arătând că pot exista mai multe modalități de a garanta respectarea vieții private, iar natura obligației statului va depinde de aspectul specific al vieții private în cauză, remediile penale neexcluzând *per se* existența unui remediu și în planul dreptului civil[4]. Cu toate acestea, remarcăm că faptele ilicite apte a angaja răspunderea civilă delictuală, descrise potrivit art. 74 C. civ., prezintă un conținut constitutiv asemănător cu cele faptele ce pot constitui una dintre infracțiunile ce protejează diferite aspecte ale vieții private, revenind practicii ca, pe baza pericolului social concret al faptei, să decidă forma de răspundere adecvată.

În executarea obligațiilor sale pozitive, legiuitorul penal român a decis ca prin Noul Cod Penal să extindă și protecția penală a elementelor vieții private creând, pentru prima dată, un capitol separat destinat acestei categorii de infracțiuni. Cu toate acestea, din motive apreciate surprinzătoare de întreaga doctrină, legiuitorul a decis să nu includă și infracțiunea de violare a secretului corespondenței în cadrul acestui capitol.

Având în vedere toate aceste aspecte, în analiza elementelor constitutive ale acestei infracțiuni, pe lângă structura clasică pe care o prezintă orice normă incriminatoare, trebuie avută în vedere dacă, din perspectiva jurisprudenței CEDO, o faptă ce întrunește formal elementele constitutive ale infracțiunii este considerată o încălcare a dispozițiilor art. 8 CEDO iar aplicarea unei sancțiuni în materie penală răspunde principiului minimei incidențe a dreptului penal. Astfel spus, în cazul în care o anumită ingerință în viața privată a persoanei nu a fost apreciată de către Curte ca fiind și o ingerință în drepturile acesteia, nu poate fi vorba despre tragerea la răspundere penală a subiectului activ pentru săvârșirea respective faptei.

---

[3] CEDO, *M&M c. Croația*, op. cit., par. 177.

[4] CEDO, Hotărârea din 22 octombrie 1996, *Stubbings şi alţii c. Regatului Unit*, 22083/93, par. 63-66.

Literatura de specialitate a primit cu reticență opțiunea legiuitorului de a include această infracțiune în capitolul privind infracțiunile contra serviciului, subliniindu-se că obiectul juridic principal al infracțiunii rămâne inviolabilitatea secretului corespondenței, drept subiectiv al persoanei ce ar fi justificat includerea acestei infracțiuni în noul capitol privind atingerile aduse domiciliului și vieții private din cadrul titlului privind infracțiunile contra persoanei.

De asemenea, potrivit normei interpretative prevăzute de art. 244 din Legea nr. 187/2012, fapta constituie infracțiune indiferent dacă a fost săvârșită în cadrul unor relații de serviciu sau în afara acestora, iar în cazul în care fapta a fost săvârșită în afara unor relații de serviciu, ea pierde orice legătură cu sfera infracțiunilor de serviciu[5]. Considerăm că însăși existența normei interpretative reprezintă o recunoaștere a posibilei erori de legiferare, poziționarea normei în respectivul capitol conducând, la prima vedere, la concluzia că legiuitorul a înțeles să protejeze penal doar corespondența schimbată în cadrul relațiilor de serviciu.

Prin incriminarea analizată sunt apărate relațiile sociale referitoare la libertatea persoanei de a comunica cu alte persoane, prin intermediul corespondenței, telefonului sau al oricărui alt mijloc electronic de comunicații, relații care formează obiectul juridic principal al infracțiunii. În forma agravată prevăzută de art. 302 alin. 3, infracțiunea are și un obiect juridic secundar, care constă în relațiile sociale referitoare la asigurarea secretului profesional și a confidențialității informațiilor de către persoanele care au acces la ele în baza atribuțiilor de serviciu[6].

Odată cu dezvoltarea tehnologică, s-a extins și sfera metodelor de comunicare ce se bucură de protecție, esențial fiind să existe un schimb de idei între două sau mai multe persoane. Nu prezintă relevanță în ce măsură informațiile transmise sunt deja publice sau ușor accesibile publicului, ci doar intenția expeditorului și a destinatarului ca transmiterea mesajului să nu fie publică. Trăsătura esențială a corespondenței este că aceasta trebuie să aibă loc mijlocit, presupune utilizarea unei forme de comunicare la distanță.

---

[5] A. Vlăsceanu, A. Barbu, *Noul Cod penal comentat prin raportare la Codul penal anterior*, Editura Hamangiu, București, 2014, p. 698.

[6] A. Crișu-Ciocîntă în T. Toader, M.I. Michinici, R. Răducanu, A. Crișu-Ciocântă, S. Răduleţu, M. Dunea,, *Noul Cod penal. Comentarii pe articole*, Editura Hamangiu, București, 2014, p. 487.

În cazul în care se interceptează o comunicare directă, aceasta are natura juridică a unei convorbiri, devenind aplicabile dispozițiile art. 226 C.pen. privind infracțiunea de violare a vieții private.

Curtea Europeană a subliniat de altfel că viața privată include și protejarea caracterului privat a comunicațiilor persoanei, indiferent de mijlocul prin care acestea se realizează, respectiv corespondență scrisă, telefonică, prin intermediul e-mail sau prin intermediul unui pager[7].

În privința protecției corespondenței profesionale, făcând referire inițial doar la protecția domiciliului, Curtea a precizat pentru prima oară[8] că ar fi mult prea restrictiv ca noțiunea să fie limitată la un cerc intim unde persoana poate să își conducă viața personală după cum dorește, la adăpost de lumea exterioară, arătând că protecția acordată de către art. 8 CEDO trebuie să se extindă și cu privire la activitățile profesionale al individului. În mod firesc, Curtea a statuat ulterior că apelurile telefonice efectuate utilizând mijloacele tehnice de la locul de muncă sunt, la prima vedere, incluse în noțiunea de viață privată și protejate de dispozițiile art. 8 CEDO[9].

De asemenea, pentru a exista o ingerință, nu este strict necesar a se intercepta conținutul corespondenței, fiind suficientă obținerea unei liste de apeluri telefonice efectuate sau de mesaje e-mail transmise[10].În timp, constatăm că a urmat pronunțarea unei decizii privind acordarea aceluiași standard de protecție și corespondenței realizate prin e-mail și a informațiilor derivate din monitorizarea traficului pe Internet la locul de muncă[11]. Astfel, putem spune că potrivit art. 8 CEDO și art. 302 C.pen., se acordă protecție oricărei forme de corespondență profesională ce se poate identifica, neprezentând relevanță mijlocul tehnic prin care aceasta se realizează efectiv.

Subiectul activ al infracțiunii de violare a secretului corespondenței nu este sub nicio formă circumstanțiat, infracțiunea putând fi săvârșită de către orice persoană fizică a cărei răspundere penală poate fi angajată. De asemenea, sub rezerva întrunirii condițiilor prevăzute de art. 135 C.pen., subiect activ al infracțiunii poate fi și o persoană juridică.

---

[7] CEDO, Hotărârea din 22 octombrie 2002, *Taylor-Sabori c. Regatului Unit.*

[8] CEDO, Hotărârea din 16 decembrie 1992, *Niemietz c. Germania*, 13710/88, par. 29; Hotărârea din 25 iunie 1997, *Halford c. Regatului Unit*,20605/92, par. 42-46.

[9] Hotărârea din 25 iunie 1997, *Halford c. Regatului Unit*,20605/92.

[10] CEDO, Hotărârea din 2 august 1984, *Malone c. Regatului Unit*, 8691/79.

[11] CEDO, Hotărârea din 3 aprilie 2007, *Copland c. Regatului Unit*, 62617/00.

În analiza elementelor constitutive ale infracțiunii cu referire la subiectul abordat, apreciem că cele mai multe dezbateri le implică condiția esențială a elementului material, în oricare dintre variantele infracțiunii, respectiv ca aceasta să fie efectuată fără drept, şi cele două cauze justificative prevăzute de art. 302 alin. 5 C.pen.

Spre diferență de alte domenii unde nu se poate identifica, de regulă, niciun interes legitim al subiectului activ pentru a proceda la supravegherea corespondenței subiectului pasiv, în cadrul raporturilor de muncă, angajatorul şi organele sale de conducere au dreptul de a se asigura, cu anumite limitări, că angajații desfășoară activitate profesională în timpul programului de lucru, folosesc echipamentele puse la dispoziție pentru executarea obligațiilor ce decurg din contractul de muncă şi nu transmit către terți informații a căror divulgare ar putea afecta activitatea angajatorului. Astfel, salariatul beneficiază de o expectațiune limitată şî relativă la viață privată, care va depinde, de la caz la caz, de informațiile pe care angajatorul a înțeles să le furnizeze din timp cu privire la nivelul de monitorizare, la mijloacele în care aceasta se realizează şi la modul în care urmează a fi utilizate rezultatele monitorizării.[12]

Astfel, cerința esențială în cazul tuturor modalităților alternative ale elementului material este ca acestea să se desfășoare fără drept de către angajator. Pentru întrunirea acestei cerințe este necesară reținerea încălcării unei dispoziții legale sau a unui standard de protecție şi lipsa incidenței vreuneia dintre cauzele justificative prevăzute de art. 302 alin. (4) C.pen.

De asemenea, considerăm că nu sunt întrunite condițiile de tipicitate în cazul în care angajatul, subiectul pasiv al infracțiunii, își exprimă expres acordul în sensul de a-i fi supravegheată corespondența la locul de muncă**.** Această nuanțare își are temeiul în caracterul de ordine privată al drepturilor protejate prin intermediul acestei incriminări, neapreciind necesară tragerea la răspundere a subiectului activ în cazul în care chiar subiectul pasiv este cel care şi-a exprimat intenția de a-i fi supravegheată corespondența. În cazul în care persoana vizată își dă consimțământul pentru a-i fi reținută şi interceptată corespondența, nu se mai poate reține o încălcare a dispozițiilor art. 8 CEDO. Cu toate acestea, protejarea secretului corespondenței presupune exprimarea consimțământului subiectului nu numai cu privire la

[12] R. Dimitriu, *Respectul vieții private a lucrătorului și al demnității la locul de muncă*, în Revista Română de Dreptul Muncii, nr. 7/2011, București, p. 42.

interceptarea acestora, ci și cu privire la transmiterea sau difuzarea acestora, existența unuia neatrăgând automat concluzia existenței și a celui de-al doilea.În privința acordului angajatului, trebuie să se aibă în vedere în ce măsură acesta a fost real, serios, și exprimat de către o persoană care putea dispune în mod legal de acest drept, potențialul abuz de poziție economică al angajatorului făcând dificilă demonstrarea existenței unui acord serios din partea angajatului. De asemenea, considerăm că trebuie avut în vedere și dacă angajatul, la momentul exprimării consimțământului, de regulă la momentul încheierii contractului de muncă, cunoștea nivelul de monitorizare la care urmează a fi supus.

O altă împrejurare ce atrage lipsa cerinței esențiale a elementului material este existența unei obligații din cadrul fișei postului a subiectului activ. Cu titlu de exemplu, în cadrul întreprinderilor private, precum și în administrațiile publice, deschiderea corespondenței se face de către persoana sau funcționarul însărcinat cu această atribuție, așa că deschiderea corespondenței ce nu-i este adresată celui însărcinat, dar este adresată persoanei juridice sau administrației se face în mod licit[13]. De asemenea, considerăm că în cazul în care este transmisă corespondența personală a unui angajat la locul de muncă, prin intermediul adresei la e-mail a companiei sau prin posta scrisă fără însă a purta o mențiune expresă a caracterului personal, fapta săvârșită de către funcționarul responsabil nu va fi tipică mai ales sub aspectul laturii subiective, secretul corespondenței fiind încălcat accidental, în principal din culpa expeditorului.

Mai mult, apreciem că fapta nu este tipică în cazul în care un angajat este supus unei interceptări permanente justificată de necesitatea asigurării ordinii publice în respectivul spațiu sau inerentă, prin natura funcției deținute. Astfel, cu titlu de exemplu, în cazul asigurării serviciilor de call-center sau costumer assistance, aceste apeluri sunt înregistrate în vederea asigurării calității serviciilor și pentru o eventuală preconstituire de probe, subiect principal al supravegherii fiind persoane din publicul larg care participă la convorbire iar angajații au fost în prealabil informați cu privire la existența măsurilor de supraveghere, nu se poate reține întrunirea condiției esențiale săvârșirii faptei fără drept, fiind realizat un echilibru

[13] A. M. Truichici, *Implicaţii penale referitoarela inviolabilitatea corespondenţei*, în Dreptul nr. 12/2008, p. 255.

corect între interesul general și chiar al angajatului împotriva reclamațiilor și interesul particular al angajatului la viață privată în cadrul locului de muncă.

Pe lângă autorizarea expresă a legii și acordul subiectului pasiv, apreciem că mai există împrejurări care vor atrage lipsa de tipicitate a faptei săvârșite de către angajator. Astfel, orice ingerință în dreptul angajatului la protecția corespondenței nu va fi considerată o încălcare a standardului de protecție stabilit prin dispozițiile art. 8 CEDO, excluzându-se astfel posibilitatea tragerii la răspundere penală a angajatorului, în cazul în care aceasta este prevăzută de lege, urmărește un scop legitim și este proporțională, necesară într-o societate democratică.

Curtea a subliniat că analiza proporționalității ingerinței în dreptul la viață privată al angajatului se poate realiza nu doar prin raportare la un interes general, cum s-a arătat anterior, ci și prin raportare la un interes privat, al angajatorului[14].

Curtea Europeană a Drepturilor Omului a arătat că o ingerință în viața privată a unui salariat poate să nu fie considerată ca disproporționată, în special atunci când trebuie să se răspundă la un motiv imperativ de securitate sau pentru a proteja drepturile altora în cadrul unei întreprinderi[15]. În acest sens, Curtea s-a pronunțat, de exemplu, cu privire la testele impuse salariaților pentru descoperirea consumului de droguri sau de alcool[16].

Reținem că în jurisprudența Curții există o cauză extrem de relevantă, efectuându-se o analiză extrem de detaliată a condițiilor în care argumentul rațiunilor de securitate națională poate fi invocat pentru justificarea anumitor acțiuni intrusive în viața privată[17]. Curtea a reținut, în esență, că o supraveghere generalizată, fără scopuri clare, în lipsa unor indicii care să contureze pericolul pe securitatea națională și lipsa unui mecanism eficient de distrugere a înregistrărilor efectuate în cazul în care acestea se dovedesc a fi excesive sau neconcludente, atrage o încălcare a dreptului la viață privată, indiferent de interesul general sau particular protejat.

---

[14] CEDO, Hotărârea din 12 iunie 2003, *Van Kuck c. Germaniei*.

[15] J.-F. Renucci, *Tratat de drept European al drepturilor omului*, Editura Hamangiu, București, 2009, p. 256.

[16] CEDO, Hotărârea din 7 noiembrie 2002, *Madsen c. Danemarca*, 58341/00.

[17] CEDO, Hotărârea din 5 iulie 2011, *Avram și alții c. Republicii Moldova*, 41588/05.

Doctrina și practica inițială au promovat ideea potrivit căreia, atâta vreme cât angajatul se află la locul de muncă, în timpul programului de lucru utilizând echipamentele angajatorului, acesta se poate aștepta, în mod rezonabil, fără o informare anterioară, că angajatorul controlează întreaga corespondență.

În dreptul american s-a arătat astfel că nu poate exista o așteptare rezonabilă a angajatului la protecția vieții sale private, în contextul corespondenței efectuate prin posta electronică, dacă: a) serverul este deținut de autoritatea publică unde este angajat; b) conturile de poștă electronică pot fi utilizate doar pentru activitatea oficială a instituției şi c) a existat o notificare prealabilă a angajatului cu privire la faptul că poșta electronică este monitorizată de administratorul de sistem al instituției[18].

Considerăm însă că practica actuală a clarificat că simpla existență a dreptului de proprietate al angajatorului asupra elementelor hardware și software puse la dispoziția angajatului nu permite accesarea, fără nicio limitare, a corespondenței purtate de către salariat la locul de muncă.

Este adevărat că, în general, se presupune că un mesaj trimis sau primit de la calculatorul pus la dispoziție de întreprindere are caracter profesional, și fără o indicație specială în ceea ce privește subiectul mesajului, care să indice că acest mesaj este privat, angajatorul nu poate să cunoască faptul că acest mesaj este privat şi că este protejat prin dispozițiile legale privind secretul corespondenței[19]. Aceeași soluție considerăm că este valabilă și în cazul adresele de e-mail profesionale, mai ales cele hostate de către angajator.

În cazul tuturor acestor ipoteze, angajatorul justifică un interes legitim în a accesa corespondența ce se presupune a fi profesională, Curtea Europeană subliniind că organele judiciare au obligația de a verifica în ce măsură angajatorul a avut posibilitatea de a se asigura și s-a asigurat că nu accesează corespondență privată iar, în cazul in care o astfel de ingerință a avut loc, în ce măsură aceasta a fost întreruptă și cum au fost utilizate informațiile private obținute.

---

[18] United States vs. Monroe, 50 M.J. 550 (A.F.C.C.A. 1999), în Revista Pandectele Române nr. 2/2003, p. 126.

[19] C. Gîlcă, *Viața publică și viața privată a salariatului*, în Revista Română de Dreptul Muncii nr. 2/2006, p. 96.

Astfel, luându-se act de dezvoltarea fără precedent a dreptului la viață privată, atât instanțele naționale, cât și Curtea Europeană a Drepturilor Omului au început să traseze linii directoare în baza cărora să se poată stabili un echilibru just între cele două drepturi în conflict. In acest sens, în anul 2006, Curtea de Casație din Franța a subliniat necesitatea menținerii unui echilibru între protecția libertății salariatului la locul de muncă și dreptul legitim al angajatorului de a se asigura că salariații își execută loial obligațiile de care sunt ținuți conform interesului întreprinderii. Astfel, confirmând soluția unei instanțe inferioare, Curtea de Casație a reținut existența unei culpe grave apte a justifica concedierea unui angajat care a procedat în mod voluntar la criptarea computerului său, fără autorizația societății, împiedicând astfel consultarea informațiilor. S-a arătat că datele și fișierele create de către un salariat prin intermediul instrumentelor informatice puse la dispoziția sa de către angajator pentru executarea muncii sale sunt prezumate, cu excepția situației în care angajatul le cataloghează a fi personale, că au caracter profesional, astfel încât angajatorul poate să aibă acces la aceste documente chiar în absența salariatului. S-a reținut că salariatul a fost informat cu privire la împrejurarea că operațiunile de criptare împiedică angajatorul de la a consulta fișierele, făcând astfel imposibilă menținerea relațiilor contractuale[20].

La nivel european, într-o cauză ce privea interceptarea convorbirilor telefonice ale unui ofițer cu rang înalt din cadrul Poliției, Curtea a statuat că maniera de interceptare generalizată, nejustificată temeinic și nelimitată în timp constituie o încălcare a vieții private la locul de muncă[21]. Cu aceeași ocazie, Curtea a respins argument statului reclamat potrivit căruia reclamanta, față de funcția pe care o deținea, nu avea așteptarea rezonabilă de a nu îi fi interceptate toate convorbirile efectuate la locul de muncă[22]. Este de reținut că, în respectiva speță, reclamanta, prin natura funcției sale, avea acces la informații clasificate și o obligație suplimentară de rezervă, putându-se aștepta, în mod rezonabil, la un grad de ingerință mai ridicat în dreptul său la păstrarea secretului corespondenței.

---

[20] Cass. Soc., 18 octombrie 2006, nr. 04-48.025, în Revista Română de dreptul muncii nr. 4/2006, p. 218.

[21] CEDO, Hotărârea din 25 iunie 1997, *Halford c. Regatului Unit*,20605/92.

[22] R.C.A. White, C. Ovey, *The European Convention on Human Rights, Fifth Edition*, Oxford University Press, New York, 2010, p. 369.

Ulterior, într-o cauză foarte relevantă pentru situația specială a angajaților, aplicabilă și în materia secretului corespondenței, Curtea a efectuat o analiză detaliată a criteriilor pe care le are în vedere în analiza proporționalității ingerinței[23]și a echilibrului între drepturile angajaților șicele ale angajatorului. Astfel, Curtea a reținut că în mod corect a fost invocat argumentul descoperirii săvârșirii unei infracțiuni, nefiind vorba de o încălcare nejustificată a dreptului la viață privată al angajatului, reținând următoarele argumente: supravegherea a fost dispusă ulterior constatării unor neregularități contabile; s-a dispus supravegherea video pentru o perioadă determinată de timp, aproximativ două săptămâni; supravegherea a încetat la momentul săvârșirii unei infracțiuni de furt; înregistrările au fost vizionate de către un număr minim de persoane și utilizate doar în cadrul procedurii disciplinare; interesul angajatorului era unul legitim, respectiv aflarea adevărului și excluderea altor angajați dintre persoanele bănuite. Cu toate acestea, din cuprinsul motivării, doctrina[24] a interpretat un avertisment al Curții în sensul că, în viitor, echilibrul dintre cele două drepturi private analizate s-ar putea modifica având în vedere apariția unor metode tehnice din ce în ce mai sofisticate ce permit intruziuni mult mai grave, dar mai subtile.

Cu ocazia pronunțării primei hotărâri cu privire la corespondența electronică a angajatului[25], Curtea a confirmat creșterea anticipată anterior a standardelor de protecție, În fapt, s-a reținut că angajatorul a solicitat comunicarea facturilor desfășurate din partea operatorului de telefonie mobilă cuprinzând numerele de telefon apelate, data apelului și durata acestuia, a procedat la supravegherea paginilor web accesate, data și durata accesării și la supravegherea adresei de e-mail în sensul analizării adreselor către care au fost transmise mesaje. Curtea a respins categoric argumentul statului reclamat potrivit căruia universitatea, angajatorul reclamantei, avea obligația de diligență de a face toate eforturile pentru a asigura un nivel ridicat de pregătire a studenților, aici fiind inclusă și abilitatea de a supraveghea corespondența angajaților pentru a se asigura că resursele universității nu sunt folosite și în scopuri personale. Curtea a identificat

[23] CEDO, Hotărârea din 5 octombrie 2010, *Kopcke c. Germaniei*, 420/07.

[24] D.J. Harris, M O'Boyle, E.P. Bates, C.M. Buckley, *Law of the European Convention on Human Rights*, Third Edition, Oxford University Press, New York, 2014, p. 557.

[25] CEDO, Hotărârea din 3 aprilie 2007, *Copland c. Regatului Unit*, 62617/00.

două argumente principale pentru a concluziona că a existat o încălcare a art. 8 CEDO. În primul rând, a constatat că nu existau la acel moment legislație primară la nivel național sau regulamente interne universitare care să prevadă motivele și procedura prin care se poate proceda la supravegherea corespondenței la locul de muncă. În cel de-al doilea rând, s-a constatat că, în ciuda lipsei reglementării, persoana vizată nu a fost niciodată avertizată cu privire la posibilitatea angajatorului de a supravegherea traficul de Internet și corespondența, aceasta având astfel așteptarea rezonabilă că se bucură de intimitate și la locul de muncă.

Speța cea mai importantă în materie, care exprimă și optica actuală a Curții, este cea recent pronunțată de către Marea Cameră în cauza Bărbulescu c. României[26]. În fapt, s-a reținut că, la cererea angajatorului, salariatul a creat un cont de Yahoo Messenger în scopuri profesionale, pentru a răspunde solicitărilor clienților. Ulterior negării de către angajat a faptului că ar fi folosit contul în scopuri personale, angajatorul a accesat contul și a luat decizia desfacerii contractului de muncă pe motivul încălcării regulamentului intern, care interzicea angajaților utilizarea resurselor societății în scopuri personale. În cadrul procedurii disciplinare, şi ulterior în fața instanței, angajatorul a printat și prezentat pe zeci de pagini corespondența angajatului, aceasta vizând, prin altele, discuții cu logodnica şi cu fratele acestuia și priveau aspecte legate de sănătate și viața sexuală.

În analiza Camerei, s-a statuat că angajatorul a acționat în cadrul competențelor disciplinare, nu fără un motiv întemeiat sau într-o supraveghere generală, accesând contul de Yahoo Messenger sub prezumția că informațiile respective erau legate de activități profesionale. În ceea ce privește folosirea transcriptului comunicațiilor reclamantului pe Yahoo Messenger ca probă în fața instanțelor naționale, Curtea a observat că acestea nu au analizat sau redat conținutul efectiv al corespondenței și nu alte date și documente stocate în computer, stabilind că monitorizarea angajatorului a fost limitată ca scop și proporțională.

Curtea a conchis că în speță nu există nimic care să indice că autoritățile naționale nu au reușit să găsească un echilibru just, în marja lor de apreciere, între dreptul reclamantului la respectarea vieții sale private și

[26] CEDO, Hotărârea din 12 ianuarie 2016 (Secțiunea a patra), Hotărârea din 5 septembrie 2017 (MC), *Bărbulescu c. României*, 61496/08.

interesele angajatorului său deși, spre diferență că cauza Kopcke c. Germaniei , angajatul nu a produs anterior pagube materiale angajatorului.

Ulterior, Marea Cameră a avut în vedere că angajatul a fost informat cu privire la interdicția de a utiliza în scop personal adresa de Yahoo Messenger, dar nu au existat dovezi că ar fi fost informat efectiv cu privire la posibilitatea angajatorului de a verifica și stoca conținutul efectiv al corespondenței sau cu privire la amploarea operațiunii de monitorizare. Marea Cameră a reținut în continuare că instanțele naționale nu au realizat o analiză a scopului pentru care angajatorul a procedat la interceptarea corespondenței și nu s-au preocupat să stabilească dacă ingerința era necesară la acel nivel extrem, de captare, înregistrare și printare a tuturor mesajelor private. Curtea a precizat că motivele indicate de către instanțele naționale, protecția sistemului IT al companiei de intruziuni exterioare și păstrarea secretului industrial, sunt abstracte pentru că nu exista nici o dovadă că reclamantul ar fi întreprins vreo acțiune în acest sens. Curtea a subliniat că nu s-a analizat nici dacă se putea ajunge la același rezultat folosind proceduri mai puțin invazive, arătându-se foarte sceptică la accesarea efectivă a corespondenței.

De asemenea, având în vedere și împrejurarea că nu s-a clarificat în ce moment din cadrul procedurii disciplinare a avut loc accesarea efectivă a conținutului mesajelor, Curtea neacceptând posibilitatea intruziunii la orice moment, a concluzionat că lipsa analizării elementelor prezentate face ca instanțele naționale să fi eșuat în executarea obligației de a asigura un just echilibru între drepturile angajatului și cele ale angajatorului, catalogând concluzia instanțelor drept formală și teoretică, nesusținută de o analiză concretă.

În cazul particular al funcționarilor statului, aceștia au, pe lângă obligațiile generale ale oricărui angajat, o obligație suplimentară de rezervă și o obligație mai restrictivă de a păstra secretul profesional. O asemenea obligație este instituită pentru a proteja "secretele administrației", ale statului în general. Sub rezerva satisfacerii cererilor legitime de informare a administraților, funcționarilor publici le este interzisă divulgarea oricăror fapte, informații sau documente[27].

[27] În acest sens, C. F. Costaș, *Considerații asupra limitării exercițiului unor libertăți publice ale funcționarilor publici*, în Revista Pandectele Române nr. 3/2004.

Cu privire la limitările speciale pe care trebuie să le accepte o persoană ce deține sau urmărește să dețină poziții strategice în organizarea statului, Curtea Europeană a statuat într-o cauză pe care o apreciem încă de actualitate, că utilizarea unor informații stocate pentru o perioadă lungă de timp într-un registru secret al poliție în cadrul unei proceduri de selecție pentru o funcție relevantă pentru siguranța națională și respingerea candidaturii în baza acestora nu constituie o încălcare a art. 8 CEDO, interesele societății trebuind ca în acest caz să prevaleze drepturilor individului[28]. Cu toate acestea, după cum s-a arătat, nici deținerea unei funcții înalte în stat nu poate justifica în sine o supraveghere generalizată, nelimitată în timp și fără un scop precis.

În cazul în care se interceptează corespondența ce reprezintă o dată informatică, doctrina este divergentă cu privire la încadrarea juridică a faptei. Pe de o parte[29], se apreciază că art. 361 C.pen. este normă specială prin raportare la art. 302 C.pen. având în vedere că corespondență purtată printr-un mijloc electronic are la bază o transmisie de date informatice. Pe de altă parte[30], într-o opinie la care ne raliem, se consideră că art. 302 C.pen. este normă specială prin raportare la art. 361 C.pen, corespondența fiind una dintre categoriile de date informatice, obiectul juridic al protecției fiind informația transmisă iar nu natura sa de dată informatică. În final, se apreciază că se va reține săvârșirea ambelor infracțiuni prevăzute de art. 302 alin. 2 C.pen. și art. 361 C.pen..[31]

Potrivit art. 302 alin. 5 C.pen., nu constituie infracțiune fapta dacă făptuitorul surprinde săvârșirea unei infracțiuni sau contribuie la dovedirea săvârșirii unei infracțiuni.

Această cauză justificativă devine operantă doar în cazul în care supravegherea persoanei la momentul relevant a fost punctuală, întâmplătoare sau foarte redusă în timp, neputând fi acceptată excluderea

[28] CEDO, Hotărârea din 26 martie 1987, *Leander c. Suediei*.

[29] În acest sens, S. Bogdan (coord.), D.A. Șerban, G. Zlati, *Noul Cod penal. Partea specială*, Editura Universul Juridic, București, 2014, p 690.

[30] În acest sens I. Kuglay în G. Bodoroncea, V. Cioclei, I. Kuglay, L.V. Lefterache, T. Manea, I. Nedelcu, F.-M. Vasile, *Codul penal. Comentariu pe articole art. 1-446*, Editura C.H.Beck, București, 2014, p.782.

[31] În acest sens, V. Dobrinoiu, M.A.Hotca, M. Gorunescu, M.Dobrinoiu, I. Pascu, I. Chiș, C. Păun,N. Neagu, M.C.Sinescu, *Noul Cod Penal Comentat. Vol. II. Partea specială*, Editura Universul Juridic, București, 2012, p. 899.

răspunderii penale în cazul unei supravegheri generalizate, permanente, efectuate în speranța descoperirii săvârșirii unei infracțiuni. Reținem că în jurisprudența Curții există o cauză extrem de relevantă, efectuându-se o analiză extrem de detaliată a condițiilor în care argumentul rațiunilor de securitate națională poate fi invocat pentru justificarea anumitor acțiuni intrusive în viața privată[32]. Curtea a reținut, în esență, că o supraveghere generalizată, fără scopuri clare, în lipsa unor indicii care să contureze pericolul pe securitatea națională şi lipsa unui mecanism eficient de distrugere a înregistrărilor efectuate în cazul în care acestea se dovedesc a fi excesive sau neconcludente, atrage o încălcare a dreptului la viață privată.

În final, considerăm că această cauză justificativă este dificil a fi invocată de către un angajator, un raport de muncă fiind, în principiu, unul de lungă durată, neputând fi justificată o supraveghere îndelungată prin identificarea, la un moment dat, a indiciilor săvârșirii unei infracțiuni. Apreciem că, în cazul invocării acestei cauze justificative, organelor judiciare le revine sarcina de a efectua o analiză similară celei efectuate de către Curte în Cauza Kopcke c. Germaniei[33].

De asemenea, nu constituie infracțiune fapta dacă surprinde fapte de interes public, care au semnificație pentru viața comunității şi a căror divulgare prezintă avantaje publice mai mari decât prejudiciul produs persoanei vătămate.

Această ultimă cauză de excludere a infracțiunii este şi cea mai discutabilă, formularea cuprinzând expresii cu un grad ridicat de relativitate, fiind dificilă stabilirea unei ierarhii clare între două entități diferite: avantajul public versus prejudiciul personal.[34] Considerăm că această ultimă cauză justificativă va fi cel mai des invocată în practică şi va crea condițiile unei jurisprudențe neunitare, nivelul de generalitate a reglementării neoferind, în opinia noastră, suficiente garanții din perspectiva principiului legalității incriminării. Mai mult, nu putem ignora că legiuitorul a urmărit să trimită la standardul stabilit de către Curtea Europeană a Drepturilor Omului în privința echilibrului dintre drepturile statuate prin art. 8 şi art. 10 CEDO. Or, efectuând o analiză istorică a jurisprudenței Curții, se constată că aceasta

[32] CEDO, Hotărârea din 5 iulie 2011, *Avram şi alții c. Republicii Moldova*, 41588/05.

[33] CEDO, Hotărârea din 5 octombrie 2010, *Kopcke c. Germaniei*, 420/07.

[34] G. Bodoroncea, V. Cioclei, I. Kuglay, L.V. Lefterache, T. Manea, I. Nedelcu, F.-M. Vasile, *op.cit.*, p. 407.

nu este foarte constantă în timp, fiind inițial înregistrată o creștere exponențială a protecției acordate libertății de exprimare în detrimentul vieții private, revenind în prezent și acordând o protecție din ce în ce mai ridicată vieții private. Or, considerăm că în materie penală, aceste fluctuații jurisprudențiale sunt de evitat, putându-se ajunge la soluții diferite în cauze asemănătoare, doar funcție de momentul pronunțării hotărârii judecătorești. *De lege ferenda*, apreciem că această cauză ar trebui reformulată în sensul de a fi împărțită în mai multe cauze justificative, dar mai aplicate, mai concrete.

În concluzie, apreciem că, spre deosebire de alte domenii ale dreptului penal substanțial, în materia protecției vieții private a salariaților, organele judiciare au obligația de a se raporta, anterior constatării întrunirii tuturor elementelor constitutive ale infracțiunii de violare a secretului corespondenței, la standardele și criteriile stabilite de către Curtea Europeană a Drepturilor Omului în jurisprudența sa. În acest fel, considerăm că soluția pronunțată va reflecta nivelul de protecție urmărit al vieții private și va preveni eventuale îngrădiri excesive ale drepturilor angajatorilor. Această analiză urmează a fi efectuată cu ocazia verificării existenței cerinței esențiale a elementului material.

Mai mult, ulterior pronunțării hotărârii în cauza Bărbulescu c. României, considerăm că punerea în balanță a drepturilor aflate în conflict cu referire la toate criteriile trasate constituie o obligație a instanțelor naționale, iar nu doar o facultate a acestora. După cum s-a observat, nu obligatoriu acțiunea angajatorului a condus la încălcarea dispozițiilor art. 8 CEDO, ci lipsa abilității autorităților naționale de a acorda protecția necesară drepturilor încălcate, Curtea subliniind pe parcursul întregii decizii importanțe unei asemenea analize exhaustive.

ANALELE ȘTIINȚIFICE ALE UNIVERSITĂȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

GARANTAREA DREPTULUI LA EDUCAȚIE-ANALIZĂ COMPARATIVĂ ÎNTRE SISTEMUL DE ÎNVĂȚĂMÂNT TRADIȚIONALȘI SISTEMUL E-LEARNING-

GUARANTEEING THE RIGHT TO EDUCATION - COMPARATIVE ANALYSIS BETWEEN THE TRADITIONAL EDUCATIONAL SYSTEM AND THE E-LEARNING-

ANA-MARIA GOLDAN[1]

Rezumat: Încă din vechime, fiecare civilizație a militat, prin intermediul reprezentanților ei de frunte, pentru impunerea unui anumit set de valori și le-a selectat pe acestea în mod conștient, astfel încât să se obțină conturarea unui ideal educațional, condiționat însă de realitatea social-istorică. Astăzi vorbim despre convergența educației cu tehnologia, fapt care a dat naștere unei palete foarte largi de aspecte care trebuie cercetate și studiate, deoarece trebuie să recunoaștem că nu există niciun actor educațional care să nu fi simțit presiunea exercitată de emergența tehnologiilor informaționale și de comunicare în procesul de predare-învățare. Lucrarea de față cuprinde tematizări noi, curajoase, atât pentru cei care fac educația, cât și pentru cei care o primesc. Astfel, vom face referire la scrierile filosofice care susțin metodele tradiționale de educație, la normele cuprinse în Legea educației naționale, dar și la provocările lansate de mediile și comunitățile virtuale de învățare.
Cuvinte-cheie: educație tradițională, e-learning, ideal educațional, dreptul la învățătură, blended learning

Abstract: Since ancient times, each civilization has, through its leading representatives, militated for the imposition of a certain set of values and has chosen them consciously in order to obtain an outline of an educational ideal, conditioned by the socio- historically reality. Today, we are talking about the convergence of the technology with the education, which has given rise to a wide range of issues that needs to be researched and studied, because we have to recognize that there is no educational actor who has not felt the pressure exerted by the emergence of the information and communication technologies in the teaching-learning process. The

[1] Doctorandă, Universitatea „Alexandru Ioan Cuza" dinIași, Facultatea de Drept, email:anne_marie9128@yahoo.com

present paper contains new, courageous themes for those who are teaching and those who receive the education. Thus, we will refer to the philosophical writings that sustain the traditional methods of education, to the norms contained in the National Education Law, but also to the challenges posed by the virtual learning environments and communities.

Keywords: traditional education, e-learning, educational ideal, the right to study, blended learning

1. Considerații preliminare

Dreptul fiecărei persoane la educație, ca drept mixt, ocupă un loc central în sistemul drepturilor omului, acesta fiind garantat doar printr-o acțiune pozitivă a statului. El constituie fundația pe care se poate construi o asumare conștientă și o exercitare liberă a celorlalte drepturi și libertăți fundamentale, pentru împlinirea efectivă a personalității fiecăruia. Carta fundamentală a drepturilor omului definește dreptul la educație la art. 14 astfel: (1) *Orice persoană are dreptul la educație, precum și la accesul la formare profesională și formare continuă*; (2) *Acest drept include posibilitatea de a urma gratuit învățământul obligatoriu*; (3) *Libertatea de a înființa instituții de învățământ cu respectarea principiilor democratice, precum și dreptul părinților de a asigura educarea și instruirea copiilor lor, potrivit propriilor convingeri religioase, filozofice și pedagogice, sunt respectate în conformitate cu legile interne care reglementează exercitarea acestora.*”[2] Pentru a completa întreaga dimensiune socială, economică și culturală a drepturilor omului, Consiliul Europei a adoptat în anul 1961 Carta socială europeană. Protocolul adițional al acestei Carte, adoptat la Strasbourg, pe data de 5 mai 1988 prevede la punctul 1 faptul că „*...toți lucrătorii au dreptul la șanse egale și la un tratament egal în materie de muncă și de profesie, fără discriminare bazată pe sex*.”[3] De asemenea, regăsim articole referitoare la dreptul la educație și în alte acte precum Carta europeană a limbilor regionale sau minoritare[4], Convenția europeană cu

[2] A. V. Nedelcu-Ienei, *Dreptul la învățătură-drept fundamental al omului*, Editura Institutul român pentru drepturile omului, București, 2007, p. 95 și urm.

[3] Adoptată la Strasbourg la data de 30 mai 1996. Carta a fost ratificată de România prin Legea nr. 74 din 3 mai 1999, Monitorul Oficial nr. 193 din anul 1999.

[4] Aceasta a intrat în vigoare la data de 1 martie 1998, iar România a semnat-o la data de 17 iulie 1995.

privire la echivalarea generală a perioadelor de studii universitare[5], Tratatul asupra Uniunii Europene, Tratatul de la Amsterdam, Tratatul instituind o constituție pentru Europa și altele.

În România, Legea educației naționale, transpune aceleași principii incluse în documentele europene, specificându-se faptul că statul asigură cadrul pentru exercitarea acestui drept fundamental, pe tot parcursul vieții, și că învățământul constituie o prioritate națională.[6] Dat fiind faptul că învățământul românesc a pus un accent mai mare pe latura informativă, adică pe cantitate și mai puțin pe latura formativă, adică pe calitate, elevii și studenții români au fost nevoiți să opteze singuri, să analizeze și să își valorifice potențialul personal. În ultimii ani, ca soluție pentru modernizarea învățământului și ca oportunitate pentru învățământul la distanță, au fost propuse tehnologiile e-learning, acestea dovedindu-se a fi formula care corespunde nivelului de dezvoltare tehnologică a epocii contemporane.

E-learning-ul poate fi conceput ca fiind un set de instrucțiuni transmise prin intermediul unui dispozitiv digital, cum ar fi un computer sau o unitate mobilă, fiind destinat să sprijine formarea. În domeniul educațional, e-learning-ul acoperă un set extins de aplicații și procese on-line și off-line. Acestea includ platformele educaționale și învățarea bazată pe web, IAC, clasa virtuală, multimedia, programele educaționale, simulările, jocurile etc[7].

Lucrarea de față își propune să concilieze sau să reconcilieze disputele tradiționale dintre sistemul de învățământ clasic și cel de tip e-learning, prin configurarea premiselor unui sistem mixt, analizând cu mijloacele psihopedagogiei evoluția istorică și filosofică, stadiul actual și orientările de perspectivă ale teoriei și practicii în acest domeniu. În ansamblu, lucrarea identifică prezentul și viitorul realității educaționale românești, marcate de noul cadru legislativ, iar rezultatul constă în creionarea diagnozei pedagogice și în sugerarea unor intervenții.

2. Analiza filosofico-istorică a dreptului la educație

[5] Aceasta Convenție a fost elaborată la Roma, la data de 6 noiembrie 1990. Acest document reprezintă unul dintre cele mai importante acte multilaterale de cooperare în domeniul învățământului semnate de România.

[6] T. Toader, *Legea educației naționale*, Editura Hamangiu, București, 2011, p. 5.

[7] C. Daicu, *E-Learning. Astăzi O Provocare, mâine o normalitate*, Editura Studis, Iași, 2013, p. 37.

Încă din vechime, fiecare civilizație a militat, prin intermediul reprezentanților ei de frunte, pentru impunerea unui anumit set de valori și le-a selectat pe acestea în mod conștient, astfel încât să se obțină conturarea unui ideal educațional, condiționat însă de realitatea social-istorică. Orice incursiune, chiar neprofesionistă, în istoria filosofiei educației, oferă repere importante pentru înțelegerea mai amplă a fenomenelor sociale contemporane. Un asemenea itinerariu este desigur jalonat de nume cu rezonanță pentru spiritul educației europene. Primul care a fundamentat teoretic, printr-un text clasic al filosofiei educației, legătura dintre strategia politică și educație este Platon, iar lucrarea de numește Republica. Pentru acesta, o comunitate ideală trebuie să se ghideze după anumite criterii iar unul dintre aceste criterii este creșterea și educarea copiilor împreună încă de la naștere, privindu-se unul pe altul ca fiind o mare familie ai cărei părinți vor fi cei care fac parte din întreaga generație mai vârstnică[8].

De asemenea, dintre cei vechi, consider de cuviință a-l aminti pe Plutarh, cel care ne oferă o imagine a educației ca sistem coerent, expresie a performanțelor, ori măcar a năzuințelor, dar și a limitelor sociale, ideologice și morale în cadrul cărora s-a conturat. *Despre educarea copiilor*[9]este un scurt tratat didactic, manual practic ancorat în realitatea imediată a veacului, adresat părinților de copii liberi[10], preocupați de formarea caracterului acestora.

În Antichitate, educația se rezuma la a-i învăța pe tineri arta elocvenței, drept pentru care supremația în ceea ce privește învățământul era deținută de retorică și de filosofie. În epoca elenistică, romanii ajung în

[8] Platon, *Republica*, vol. I, Cartea I, trad. din greacă de Vasile Bichigean, Editura Tipografia profesională Dim. C. Ionescu, București, 1923, p. 32: „Statul va fi cu adevărat unul, deoarece fiecare om din el va numi al meu exact ceea ce oricare alt cetățean va numi al meu.

[9] Plutarh, *Despre educarea copiilor*, trad. conf. dr. Ovidiu Pop, Editura Sophia, 2013, p. 17-18: „De bună seamă, ar fi potrivit să se înceapă de la naștere. Eu i-aș sfătui pe cei ce doresc să devină tații unor copii deosebiți să nu stea împreună cu orice femei, și mă refer la hetaire sau concubine (...) Trebuie, după cum aș spune eu, ca mamele însele să-și hrănească copiii și să-i alăpteze. Căci ele-i hrănesc mai cu drag și cu mai multă grijă, pentru că-și iubesc odoarele din interior și, cum se spune, *din unghii*. Doicile și bonele au bunăvoință exterioară și prefăcută, căci iubesc pentru plată."

[10] Ca reflex al admiterii fără rezerve a inegalităților sociale, educația devine apanajul exclusiv al tinerilor liberi și bogați și, poate în anumite limite, chiar al celor săraci, dar liberi. De asemenea, sunt trecute sub tăcere, deci excluse, fetele.

contact cu cultura greacă, ceea ce va duce la transferul principiilor și metodelor grecești în educația romană. Acest transfer va conduce la apariția unui ideal de educație de tip roman, un ideal de factură practică, în opoziție cu idealul estetic al grecilor. Așa se face că înțeleptul grec va fi înlocuit cu cetățeanul pragmatic, iar locul gimnasticii și al muzicii va fi luat de instrucția prin gramatică. Sistemul pedagogic roman urmărea memorarea mecanică a unor date și noțiuni considerate necesare, copiii învățând să citească, să scrie și să socotească pe de rost[11].

Mai târziu, au existat și alți filosofi care au vorbit despre educație, precum: Comenius, cel care ne-a transmis idealul deopotrivă politic și educațional al prețuirii potențialului individual în sine, pansofia[12]; John Locke, indicant al conflictului care se poate stabili la nivel ideatic, între politică și educație; americanul John Dewey, vizionarul pragmatic care a rezumat întreaga teorie a curricumul-ui, sesizând că „o școală ideală trebuie să reflecte o societate ideală”[13]și alții. Deşi obligatorie pentru orice demers în discutarea educației, percepția filosofică nu este suficientă prin ea însăși pentru pedagogie.

Evoluția istorică a sistemelor de învățământ din România a urmărit îndeaproape evoluția sistemului politic și administrativ al formațiunilor statale de pe actualul teritoriu al României. Perioada medievală este caracterizată printr-un interes scăzut și limitat al elitei conducătore, boierești și ecleziastice, de a dezvolta instituții de învățământ de calitate și durabile. Cu câteva excepții de marcă, precum Vasile Lupu, prin înființarea Academiei vasiliene sau Iacob Heraclid Despotul, prin înființarea școlii de la Cotnari, domnii Țărilor Române nu au acordat practic atenție creării de școli și academii pentru educarea tineretului țării[14].În toată această perioadă, populația formațiunilor statale românești a fost practic analfabetă în cvasi-totalitatea ei.

---

[11] Fericitul Augustin, *Mărturisi*, vol. V-VI, în „Scrieri I” (PSB, nr. 64), trad. Prof. Nicolae Barbu, Editura IBMBO, București, 1985, pp.118-119.

[12] R. Mocan, *e-Learning. Introducere și perspective sociologice*, Editura Risoprint, Cluj-Napoca, 2007, p. 21.

[13] C. Crețu, *Politica promovării talentelor. Dreptul la educație diferențiată*, Editura Cronica, Iași, 1995, p. 12.

[14] N. Iorga, *Istoria învățământului românesc*, Editura Științifică și Enciclopedică, București, 1985, p.10 și urm.

Începutul procesului de construcție a unor sisteme naționale educaționale este dat de însăși formarea statului modern român de după revoluția lui Tudor Vladimirescu din anul 1821.Astfel, au apărut și s-au dezvoltat diferitele tipuri de instituții de învățământ (școli elementare, gimnazii, colegii, pensioane, universități etc.). Totodată au apărut o serie de legi de organizare și funcționare a acestui sistem precum Regulamentul Organic[15] sau legea de reformare a învățământului a lui Spiru Haret[16]. Învățământul în această perioadă este unul destul de elitist deoarece accederea în formele sale superioare și chiar în cele de bază presupunea o anumită stare materială, pe care cea mai mare parte a populației nu o avea.

După anul 1990, sistemul de învățământ românesc a fost într-un continuu proces de reorganizare deopotrivă lăudat și criticat. În conformitate cu Legea Educației Naționale nr.1/2011, sistemul educativ românesc este reglementat de către Ministerul Educației, Cercetării și Inovării. Fiecare nivel are propria sa formă de organizare și este subiectul legislației în vigoare. Grădinița este opțională între 3 și 6 ani, școlarizarea începe la vârsta de 6 ani și este obligatorie până în clasa a 10-a (de obicei, care corespunde cu vârsta de 16 sau 17 ani), iar învățământul superior este aliniat la spațiul european al învățământului superior. La finalizarea studiilor, sistemul tradițional oferă diplome de absolvire, de bacalaureat, de licență, de masterat, de doctorat.[17]

Dacă în urmă cu zeci de ani pregătirea din timpul formării inițiale putea să fie, în cele mai multe cazuri, suficientă pentru tot restul vieții, astăzi situația s-a schimbat radical. Omul contemporan este mai însetat de cunoaștere și nu încetează să acumuleze știință și experiență. Datorită acestui fapt, Internetul a ajuns să reprezinte o pasiune a tinerilor, iar conform unui studiu realizat în România, rezultă faptul că aproximativ 31% dintre tinerii integrați în sistemul de învățământ tradițional, utilizează Internetul în mod excesiv[18]. Astăzi, perspectiva asupra educației se extinde de la un mediu de învățare limitat de cei patru pereți ai sălii de clasă până la un mediu de

[15] *Regulamentul organic al Țării Românești*, București, 1832, capitolul VIII, secția 4.

[16] Z. Sandu, *Spiru Haret, organizatorul învățământului național*, Editura Școlii Militare Principele Carol, Sibiu, 1930, p.19.

[17] T. Bănaș, D. Cojocatu, *Legea educației naționale cu comentarii și adnotări*, Editura Pim, Iași, 2011, p.5 și urm.

[18] M. Capriș, *L'internet, espace de l'éducation interculturelle dans l'Union Européenne*, Editura Lumen, Iași, 2009, p. 45.

învățare virtual, având astfel loc și modificarea substanțială a rolului celor doi actori educaționali și anume profesorul și elevul.

Mare parte dintre practicile și dezvoltările educaționale cunoscute astăzi sub numele de e-learning nu sunt noi. Formarea cu ajutorul calculatorului a fost experimentată pentru prima dată cu aproximativ jumătate de secol în urmă, când s-a decis utilizarea unor computere mainframe (de mari dimensiuni) în domeniul evaluării educaționale[19].

Comunitatea științifică leagă începuturile e-learning-ului și ale instruirii asistate de calculator de activitatea profesorului american Patrick Suppes de la Universitatea Stanford. Acesta a fost primul cercetător care a pus la punct, în 1966, un sistem bazat pe utilizarea calculatorului în context educațional: CMI (Computer Managed Instruction) - instruirea gestionată de calculator. În esență, era vorba despre crearea unei serii de sisteme tutoriale care încercau să ofere suport în învățare pentru studenți și elevi. Sistemele tutoriale aveau rolul de a suplimenta și de a îmbogăți instruirea realizată prin forma clasică de profesor. În ciuda entuziasmului, începuturile au fost destul de ezitante și dificile, pe de o parte, din cauza dificultăților tehnologice, iar pe de altă parte, din cauza unui suport pedagogic aflat încă la începuturi[20].

3. Sistemul de învățământ tradițional vs. sistemul e-learning

În şcolile din România se practică într-o proporţie mai mare modelul tradiţional faţă de cel modern. Cu toate acestea, putem afirma și faptul că e-learning-ul a evoluat într-un ritm foarte accelerat în ultimii ani, existâd deja o ofertă amplă de cursuri universitare în acest sistem, marile universități dispunând deja de secțiuni de învățământ virtual sau chiar de campusuri virtuale.

Avantajele învățământului tradițional ar fi, din punctul meu de vedere următoarele: stimulează productivitatea, promovează aspiraţii mai înalte, pregăteşte elevii pentru viaţa competitivă, iar memorarea şi reproducerea cunoştinţelor sunt transmise de cadrul didactic. Limitele învățământului clasic sunt date de faptul că generează uneori conflicte sau agresivitate[21].

[19] C. Ceobanu, *Învățarea în mediul virtual*, Editura Polirom, Iași, 2016, p. 19.

[20] C. Ceobanu, *op. cit.*, p. 24.

[21] S. Bernat, *Tehnica învățării eficiente*, Presa Universitară clujeană, Cluj-Napoca, 2003, p.36.

Pe de altă parte, avantajele unui mediu educațional virtual sunt că acesta este un spațiu social (astfel că educatorii și educații pot interacționa între ei) și că se bazează pe reprezentări ale obiectelor educaționale[22] (de la variante bazate pe text până la reprezentări de tip 3D). Acest aspect contribuie la sporirea curiozității și a motivației cursanților. De asemenea, utilizatorii acestor spații au, în cadrul mediilor virtuale, un rol activ (activitățile de învățare în mediile virtuale se referă la ceva mult mai bogat decât un curs obișnuit, fiind mai aproape de noțiune de proiect). Însă, mediile de învățare virtuală nu se limitează la învățarea la distanță. De fapt diferențele dintre cele două soluții educaționale tind să se estompeze. La aceasta contribuie noile forme și soluții educaționale ce se nasc pe măsura dezvoltării tehnologice, cum ar fi m-learning-ul (învățarea mobilă cu ajutorul tehnologiei wireless și a telefoanelor inteligente). Limitele mediilor virtuale sunt că de multe ori, aplicațiile în mediul virtual sunt centrate mai ales asupra cursurilor și mai puțin asupra cursanților. De asemenea, deși aria de aplicabilitate a unui asemenea tip de învățare pare a fi nelimitată, există unele domenii și discipline a căror învățare în mediul virtual se poate desfășura cu mai mult succes decât în cazul altora. Totodată, învățarea în mediul virtual nu dezvoltă într-o manieră relevantă abilitățile de învățare independente[23].

În concluzie, autonomia oferită cursantului prin intermediul sistemului e-learning reprezintă o sabie cu două tăișuri deoarece, dacă acesta nu este suficient de motivat și nu are voință adecvată, poate abandona cu ușurință o asemenea formă de învățământ. Cursantul devine responsabil pentru propria formare, accentul fiind pus în e-learning mai mult pe învățare și mai puțin pe predare. Paradoxul în cazul învățării mediate de calculator îl reprezintă faptul că, deși comunicarea este facilitată tehnologic, existând posibilitatea de a veni în contact cu persoane din medii total diferite, aflate la distanțe foarte mari, totuși e-learning-ul predispune la izolare. Un alt paradox este dat de faptul că e-learning-ul pune accent pe informare și nu pe formarea unor deprinderi și capacități intelectuale. Introducerea TIC în învățământul tradițional a presupus o schimbare de mentalitate didactică, o depășire a locurilor comune și o permisivitate la nou, ceea ce nu este la îndemâna oricui.

[22] A. Gîju, *e-Learning în România*, Editura Arves, Iași, 2009, p. 8 și urm.
[23] C. Ceobanu, *op. cit*., p. 86.

4. Învățarea prin intermediul mediilor de socializare

În contextul educației școlare, părerile asupra site-urilor de socializare sunt împărțite. Există poziții care minimalizează sau nu iau în calcul deloc potențialul acestui instrument[24]. Argumentele, multiple și deloc de neglijat, merg de la ocuparea timpului celor care sunt fanii acestor rețele de socializare până la imersarea totală în spațiul social virtual, cu neglijarea vieții reale. În plus, autodezvăluirea socială aproape indecentă și promovarea unei culturi cel puțin îndoielnice nu permit luarea în calcul a unui potențial educativ al acestor rețele. Apariția unor fenomene de tip cyberbullying, expunerea la mesaje și conținuturi nepotrivite, descurajarea comunicării de tip față în față sunt alte argumente împotriva utilizării unor astfel de rețele în școală.

Unii autori [25] afirmă faptul că efectul rețelelor de socializare asupra generațiilor tinere, poate contribui la o slăbire intelectuală și științifică a unor generații de elevi Google, incapabili de gândire independentă, iar în general rețelele de acest fel grăbesc debutul unui proces de dez-educare a generațiilor tinere, iar Facebook nu face altceva decât să îi deconecteze pe tineri de la viața reală. Alți autori[26]susțin însă că tinerii ar trebui să distingă între deprinderile necesare pentru a identifica informația on-line și abilitatea de a înțelege corect această informație. Folosirea mediei pentru o învățare temeinică este posibilă, dar presupune o bună focalizare a atenției, ignorarea informației irelevante și îndepărtarea tentației de a naviga on-line fără un scop precis. Tinerii consideră că pot utiliza potențialul acestui instrument pentru a partaja materiale educaționale și pentru a comunica cu colegii și profesorii.

Dincolo de toate studiile, putem trage o conluzie foarte clară-rețelele de socializare au, în ultimă instanță, o valoare instrumentală. Este evident că nu media de socializare în sine contribuie la eficientizarea educației și la

[24] R.J. Light, *Making the most of college*, Editura Harvard University Press, Cambridge, 2001, p. 19.

[25] N. Selwyn, *Faceworking: exploring students education-related use of Facebook, Learning, Media and Technology*, [Online] la http://www.tandfonline.com/doi/abs/10.1080/17439880902923622, accesat 10.10.2017.

[26] M. R. Connolly, *Social networking and student learning: Friends without benefits, Editura* Sterling Stylus, Virginia, 2011, pp.128-129.

susținerea învățării, ci modul în care aceasta este folosită și pusă în slujba actului de instruire îi conferă relevanță în sfera educațională.

5. Blended learning/ Învățarea hibridă

În contextul educațional actual, o soluție de formare ce are tot mai mulți adepți este modelul educațional mixt, numit blended learning environments care îmbină maniera tradițională de abordare a sesiunilor de formare față în față cu oportunitățile oferite de e-learning. Aceste medii de formare mixte definesc o realitate care încearcă să combine beneficiile și să înlăture dezavantajele unor modele diferite, mai precis, formarea tradițională și e-learning-ul într-un mediu de învățare activ[27]. Există studii care au demonstrat că această formă de organizare a învățării este preferată de studenți, iar aceștia au obținut rezultate academice mai bune după ce au parcurs o serie de cursuri organizate conform modelului blended learning[28].

Mediile mixte de învățare nu reprezintă totuși soluția magică la toate problemele privind formarea, ci mai curând o modalitate de optimizare a acesteia. Avantajele învățării hibride sunt că avem de-a face cu o învățare mai eficientă și că reduce timpul petrecut în sala de clasă și în fața calculatorului,câștigându-se astfel timp suplimentar pentru studiu. De asemenea, blended learning oferă oportunități de acces la educație unui număr mare de persoane, chiar și celor care nu se pot înscrie în sistemul educațional tradițional din diverse motive.

Cu toate acestea, la fel ca în orice formă de învățământ on-line, în cadrul cursurilor hibrid,profesorul își modifică rolul tradițional, devenind un colaborator, un partener și un facilitator al actului de învățare. Având în vedere dezvoltarea continuă a tehnologiei, reducerea costurilor legate de aceasta, precum și creșterea posibilităților de acces la Internet, blended learning reprezintă o cale de învățare importantă în viitor.

[27] C. Ceobanu, *op. cit*., p. 121.

[28] V. Demirer, I. Sahin, *Effect of blended learning environment on transfer of learning: An experimental study* în „Journal of Computer Assisted Learning", nr. 29, pp. 518-529, [Online] la http://onlinelibrary.wiley.com/journal/10.1111/(ISSN)1365-2729, accesat 12.10.2017.

Concluzii

Lumea de astăzi pare să fie sufocată de o avalanșă de informații pe care le putem accesa prin intermediul cărților, prin mijloacele de comunicare în masă, dar și din sursele inepuizabile ale tehnicii moderne. Rolul dascălilor în educarea tinerilor a fost și va rămâne fundamental, dar educația nu trebuie să tindă numai la faptul de a transmite o serie de cunoștințe fără conținut. Formarea deprinderilor morale și modelarea caracterului copiilor și tinerilor este de o importanță certă în actul educațional. Prin urmare, profesorul formează și modelează nu numai mintea tinerilor, ci și sufletele lor. E-learning-ul este însă o realitate care se impune de la sine, reprezentând de fapt școala pe care noi o vom construi pentru nepoții noștri. În ochii generației tinere, un motor de căutare pe web se bucură astăzi de mai multă importanță decât pedantul profesor. Cu toate acestea, școala viitorului nu poate fi imaginată fără magistru, însă profesorul reproducător de cunoștințe va dispărea, locul său fiind luat de profesorul coordonator.

ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

PROTECȚIA DATELOR CU CARACTER PERSONAL ÎN CONTRACTELE INTERNAȚIONALE

PERSONAL DATA PROTECTION IN INTERNATIONAL CONTRACTS

CARMEN TAMARA UNGUREANU[1]

Rezumat: Protecția datelor cu caracter personal în contractele internaționale este analizată în linii mari, mai ales în contextul dreptului Uniunii Europene. Sunt tratate, pe rând, reglementarea protecției datelor cu caracter personal, noțiunea de date cu caracter personal, legătura dintre dreptul la protecția datelor cu caracter personal și dreptul la viața privată, titularul dreptului la protecția datelor și titularul obligației corelative. În majoritatea contractelor internaționale, protecția datelor cu caracter personal este necesară, deoarece are loc un transfer transnațional de date. Sunt analizate regulile ce trebuie respectate la transferul transnațional de date și eficiența acestor reguli în contextul evoluției tehnologiei și a omniprezenței Internetului.
Cuvinte-cheie: protecția datelor cu caracter personal, drept la viața privată, contracte internaționale, transfer de date cu caracter personal

Abstract: Personal data protection in international contracts is broadly analyzed, especially in the context of European Union Law. The regulation of personal data protection, the concept of personal data, the link between the personal data protection right and the privacy right, the data protection right holder and the person who is obliged to respect it are approached, one by one. In most of international contracts, the protection of personal data is necessary, because a transnational data transfer takes place. The rules to be respected for transnational data transfer and the effectiveness of these rules in the context of the evolution of technology and the ubiquitousness of the Internet will be analyzed.
Key-words: personal data protection, privacy right, international contracts, personal data transfer

[1] Profesor univ. dr., Universitatea „Alexandru Ioan Cuza" din Iași, Facultatea de Drept, e-mail: carment_ungureanu@yahoo.com.

Introducere. Evoluția tehnologiei și utilizarea Internetului au condus la creșterea substanțială a accesului la informații și la schimbul de informații, la dezvoltarea comerțului electronic internațional, la posibilitatea transferului electronic de date, toate acestea fiind însoțite de riscuri, care privesc, printre altele, încălcarea dreptului la viața privată și a dreptului la protecția datelor cu caracter personal.

Protecția datelor cu caracter personal impune utilizarea de norme de drept public și de drept privat, fiind un subiect care poate fi tratat interdisciplinar, prin prisma drepturilor omului, dreptului administrativ, dreptului penal, dreptului civil, comerțului internațional. Studiul de față va avea ca obiect doar o parte a problemelor pe care le ridică protecția datelor cu caracter personal, fiind orientat spre dreptul privat, mai precis, spre protecția datelor cu caracter personal în cadrul contractelor internaționale.

Vom avea în vedere un plan structurat pe ideea de întrebări ipotetice pe care și le-ar putea pune un jurist nefamiliarizat cu acest domeniu al protecției datelor cu caracter personal, precum: cum este reglementată protecția datelor cu caracter personal, ce reprezintă datele cu caracter personal și care este legătura dintre acestea și dreptul la viața privată. Protecția datelor cu caracter personal se referă doar la persoana fizică? Cum sunt afectate întreprinderile de comerț internațional de legislația în materia protecției datelor cu caracter personal? Protecția datelor cu caracter personal este necesară în toate contractele internaționale? Care sunt regulile ce trebuie respectate la transferul transnațional de date cu caracter personal?Care este eficiența regulilor cu privire la transferul transnațional de date cu caracter personal?

1. Reglementarea protecției datelor cu caracter personal

Protecția datelor cu caracter personal este reglementată în norme internaționale, regionale, *hard law*[2] și *soft law*[3] și în legislații naționale[4].

[2] Normele *hard law* sunt acelea care au caracter obligatoriu, putând fi impuse, la nevoie, prin forța coercitivăa statului.

[3] Normele *soft law* sunt acelea care au caracter de recomandare, sunt neobligatorii și care nu pot fi impuse prin forța coercitivă a statului. Aceste norme pot proveni de la un guvern, de la organizații internaționale, instituții private, profesionale sau asociații profesionale ori de comerț. Pentru detalii, M.G. Desta, *Soft law in international law: an overview*, în A.K. Bjorklund, A. Reinisch (editori), *International Investment Law and Soft Law*, Editura Edward Elgar, UK, 2012, p. 39 și urm.

Singurul instrument internaţional obligatoriu din punct de vedere juridic în domeniul protecţiei datelor este Convenţia nr. 108 a Consiliului Europei din 1981 (în vigoare din 1985) pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal (în continuare, Convenţia 108). Convenția 108 a fost ratificată de 50 de state[5] (majoritatea membre ale Consiliului Europei). România a ratificat-o în 2001[6].

În Uniunea Europeană (în continuare, UE), protecția datelor cu caracter personal este reglementată, în prezent, în art. 16 din Tratatul privind funcționarea Uniunii Europene (TFUE)[7], art. 8 din Carta Drepturilor Fundamentale a UE[8], Directiva 95/46/CE privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date[9], transpusă în legislația națională din România prin Legea nr. 677/2001pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date[10] și în toate legislațiile naționale ale statelor membre.

Din 25 mai 2018, va avea loc unificarea normelor aplicabile în UE, în toate statele membre devenind aplicabil Regulamentul (UE) 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (în continuare, Regulamentul general privind protecția datelor)[11], în vigoare din 25 mai 2016.

---

[4] Pentru o prezentare detaliată, S. Șandru, *Protecția datelor personale și viața privată*, Editura Hamangiu, București, 2016, p. 160 și urm.

[5] În acest sens, [Online] la: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=7gRdN5tT, accesat 10.06.2017.

[6] Legea nr. 682/2001 privind ratificarea de către România a Convenţiei pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg la 28 ianuarie 1981, publicată în M.Of. nr. 830, 21.12.2001.

[7] Publicat în J.O. nr. C 326, 26.10.2012.

[8] Publicată în J.O. nr. C 326, 26.10.2012.

[9] Publicată în J.O. nr.L 281, 23.11.1995.

[10] Publicată în M.Of. nr. 790, 12.12.2001, cu modificările și completările ulterioare. România a transpus directiva europeană înainte de aderarea la UE din 2007, în vederea atingerii acquis-ului comunitar.

[11] Publicat (în ultima ei formă, după intrarea în vigoare a Tratatului de la Lisabona, Tratatul de Funcționare a Uniunii Europene) în J.O. L 119, 4.05.2016.

În Statele Unite ale Americii (în continuare, SUA) protecția datelor cu caracter personal este reglementată, în principal prin: The Fourth Amendment to the US Constitution și Privacy Act din 1974[12].

2. **Ce reprezintă datele cu caracter personal?**

Noțiunea de „date cu caracter personal" are o semnificație largă în majoritatea normelor internaționale, regionale și naționale.

În Convenția 108 [art. 2, lit. a)] *datele cu caracter personal* sunt considerate a fi *orice informaţie* privind persoana fizică identificată sau identificabilă (persoana vizată).

În Directiva 95/46/CE [art. 2, lit. a)], *datele cu caracter personal* au aceeași semnificație ca în Convenția 108. În plus, se explică ce înseamnă o persoană identificabilă, aceasta fiind o persoană care poate fi identificată, direct sau indirect, în special prin referire la un număr de identificare sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale.

În Regulamentul general privind protecția datelor, definiția *datelor cu caracter personal* nu prezintă decât mici diferențe față de directivă, care se referă la elementele de identificare a persoanei fizice, specificându-se numele acesteia, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale[13].

În SUA, spre deosebire de UE, datele cu caracter personal au multiple definiții și explicații[14]. Nu se face distincție între persoana identificată și persoana identificabilă. Noțiunea de date personale este sinonimă cu sintagma „personally identifiable information". În Privacy Act

[12] F. Bignami, *The US Legal System on Data Protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens*, 2015, [Online] la:http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf, accesat 11.06.2017.

[13] A se vedea art. 4.1. din Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), publicat în J.O. L 119, 4.05.2016.

[14] P.M. Schwartz, D.J. Solove, *Reconciling Personal Information in the United States and European Union*, în California Law Review, vol. 102/2014, p. 879 și urm., [Online] la:http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=4252&context=californialawreview, accesată 1.06.2017.

din 1974 [5 U.S.C. § 552a(a)(4)], datele cu caracter personal sunt considerate acele date colectate, utilizate și dezvăluite ce conțin mai multe tipuri de informații cu caracter personal, descrise ca o "înregistrare" ținută asupra unei persoane, incluzând, dar fără a se limita la, educația acesteia, tranzacțiile financiare, istoricul medical, al locurilor de muncă, cazierul judiciar, numele sau numărul de identificare, simbolul sau alte elemente de identificare atribuite individual, cum ar fi amprentele, vocea sau o fotografie[15].

3. Ce este dreptul la protecția datelor cu caracter personal? Care este raportul dintre dreptul la viața privată și dreptul la protecția datelor cu caracter personal?

În UE, persoanelor fizice le este recunoscut *dreptul* la protecția datelor cu caracter personal. Conform art. 16 din TFUE și art. 8 din Carta Drepturilor Fundamentale a UE „(1) Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc.”.

Dreptul la protecția datelor cu caracter personal este un drept fundamental al omului, indisolubil legat de dreptul la viață privată. Nici în literatura juridică, nici în jurisprudență, distincția între cele două drepturi fundamentale nu este clară, chiar dacă în Carta Drepturilor Fundamentale a UE există prevederi separate pentru fiecare dintre acestea (art. 7 și art. 8). În Directiva 95/46/CE, în art. 1, se folosește noțiunea de *drept la viață privată în ceea ce privește prelucrarea datelor cu caracter personal*[16], înțelegându-se că dreptul la protecția datelor este un element al dreptului la viață privată.

Dreptul la protecția datelor cu caracter personal a fost inclus în Carta Drepturilor Fundamentale a UE ca drept fundamental distinct pe baza prevederilor din dreptul UE, în special a Directivei 95/46/CE, și a normelor Consiliului Europei (Convenția 108 și art. 8 din Convenția europeană a

[15] F. Boehm ș.a., Policy Department C: Citizens' Rights and Constitutional Affairs: *A comparison between US and EU data protection legislation for law enforcement purposes*, 2015, p. 52, [Online] la:

http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf, accesat 24.05.2017.

[16] S. Șandru, *op. cit*., pp. 145-146.

Drepturilor Omului, care reglementează dreptul la respectarea vieții private și de familie)[17].

Dreptul la viața privată și dreptul la protecția datelor cu caracter personal sunt drepturi fundamentale ale omului, care sunt inseparabile[18], dar nu se suprapun. Dreptul la viața privată include multe aspecte, printre care și protecția datelor cu caracter personal, dar nu toate datele cu caracter personal intră în sfera dreptului la viață privată. De ex., în cauza T-194/04 *The Bavarian Lager Co. Ltd împotriva Comisiei Comunităților Europene*[19], tribunalul a subliniat că „noțiunea de viață privată este o noțiune largă, conform jurisprudenței Curții Europene a Drepturilor Omului, și că dreptul la protecția datelor cu caracter personal poate constitui unul dintre aspectele dreptului la respectarea vieții private". Dar asta nu înseamnă că„toate datele cu caracter personal intră în mod necesar în sfera noțiunii „viață privată". „*A fortiori*, nu toate datele cu caracter personal pot, prin natura lor, să aducă atingere vieții private a persoanei vizate.".În considerentul (33) al Directivei 95/46/CE, se face referire la datele care pot, prin natura lor, să aducă atingere libertăților fundamentale sau vieții private și care nu ar trebui să fie prelucrate fără consimțământul explicit al persoanei vizate, ceea ce indică faptul că nu toate datele sunt de aceeași natură.

În jurisprudența Curții de Justiție a Uniunii Europene (în continuare, CJUE) nu se face o delimitare precisă între cele două drepturi[20]. Există hotărâri în care dreptul la protecția datelor este o parte a dreptului la viață privată[21], hotărâri în care cele două drepturi sunt considerate distincte, dar dreptul la protecția datelor este tratat ca element al dreptului la viața

[17] M. Brkan, E. Psychogiopoulou, *Introduction: Courts, Privacy and Data Protection in the Digital Environment*, în M. Brkan, E. Psychogiopoulou (editori), *Courts, Privacy and Data Protection in the Digital Environment*, Editura Edward Elgar, 2017, ebook, p. 12.

[18] M. Brkan, *op.cit*., p. 331.

[19] Cauza T-194/04, *The Bavarian Lager Co. Ltd împotriva Comisiei Comunităților Europene*, „Acces la documente – Regulamentul (CE) nr. 1049/2001 – Documente referitoare la o procedură de constatare a neîndeplinirii obligațiilor – Decizie prin care se refuză accesul – Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal – Regulamentul (CE) nr. 45/2001 – Noțiunea de viață privată", [Online] la: http://curia.europa.eu/juris/celex.jsf?celex=62004TJ0194&lang1=en&lang2=RO&type=TXT&ancre, accesată 1.06.2017.

[20] M. Brkan, E. Psychogiopoulou, *op. cit*., pp. 14-16.

[21] Cauza *YS* (C-141/12 și C-372/12), [Online] la:http://curia.europa.eu, accesat 3.10.2017.

privată[22]și hotărâri în care se recunoaște caracterul autonom al dreptului la protecția datelor cu caracter personal[23].

4. Cine este titularul dreptului la protecția datelor cu caracter personal?

Toate definițiile noțiunii de date cu caracter personal se referă doar la persoana fizică. Numai persoana fizică beneficiază de protecția datelor cu caracter personal. Persoana fizică este titularul dreptului la protecția datelor și în toate normele europene și naționale din România, poartă denumirea de „persoană vizată”[24]. Dreptul la protecția datelor cu caracter personal este considerat un drept personal nepatrimonial. În contracte, persoana vizată poate fi parte în așa numitele contracte de consum, având rolul de consumator, utilizator, abonat, în funcție de raportul juridic în care intră[25].

Persoana juridică, în instrumentele internaționale și europene, ca regulă, nu este titular al dreptului la protecția datelor. Totuși, în state europene, precum Austria și Italia sunt protejate și persoanele juridice sau grupuri de persoane fizice[26].

Persoana juridică poate fi expusă riscului încălcării datelor ei de identificare. În asemenea cazuri, poate utiliza prevederile Convenției Europene a Drepturilor Omului (în continuare, CEDO) referitoare la protecția vieții private (art. 8). Astfel, în jurisprudența Curții Europene a Drepturilor Omului (în continuare, CtEDO) se arată că separarea completă a aspectelor legate de viața privată și cea profesională poate fi dificilă; de exemplu, cauza *Amann c. Elveției* (hotărârea CtEDO nr. 27798/95[27]).

În jurisprudența CJUE, în cauza *Volker und Markus Schecke și Hartmut Eifert/Land Hessen* (C-92/09 și C-93/09), CJUE s-a pronunțat asupra proporționalității publicării, impusă de legislația UE, a numelor

[22] Cauza *Digital Rights Ireland* (C-293/12 și C-594/12*);* cauza *Maximillian Schrems împotriva Data Protection Commissioner* (C- 362/14), [Online] la: http://curia.europa.eu, accesat 13.10.2017.

[23] Cauza *The Bavarian Lager Co. Ltd împotriva Comisiei Comunităților Europene* (T-194/04); cauza*Tele2 Sverige AB* (C-203/15 și C-698/15), [Online] la:http://curia.europa.eu, accesat 13.10.2017.

[24] Art. 4.1 din Regulamentul general privind protecția datelor, art. 2 (a) din Directiva 95/46/CE, art. 2 a) din Convenția 108.

[25] S. Șandru, *op. cit*., p. 199.

[26] *Ibidem.*

[27] Hotărârea este disponibilă [Online] la:hudoc.echr.coe.int/app/conversion/, accesată 10.06.2017.

beneficiarilor subvenţiilor agricole ale UE şi a sumelor pe care aceştia le-au primit. Făcând referire la publicarea datelor cu caracter personal ale beneficiarilor de ajutoare pentru agricultură, CJUE a considerat că „persoanele juridice nu se pot prevala de protecţia articolelor 7 şi 8 din Cartă faţă de o astfel de identificare decât în măsura în care denumirea persoanei juridice identifică una sau mai multe persoane fizice. […] Respectarea dreptului la viaţă privată în raport cu prelucrarea datelor cu caracter personal, recunoscută prin articolele 7 şi 8 din Cartă, se raportează la orice informaţie privind o persoană fizică identificată sau identificabilă […]"

5. Cine este titularul obligației la protecția datelor cu caracter personal?

În Regulament, ca și în directiva pe care o va înlocui acesta, răspunderea pentru protecția datelor revine operatorului (în principal) și persoanei împuternicite de operator.

Conform art. 4.7 din Regulament, operatorul este persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește *scopurile și mijloacele de prelucrare* a datelor cu caracter personal. Potrivit art. 4.8 din Regulament, persoana împuternicită de operator este persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

Oricine decide să prelucreze datele cu caracter personal ale altor persoane este un operator în conformitate cu legislaţia privind protecţia datelor; în cazul în care mai multe persoane iau această decizie împreună, acestea pot fi operatori comuni. O persoană împuternicită de către operator este o entitate separată din punct de vedere juridic, a cărei sarcină este prelucrarea datelor cu caracter personal pe seama operatorului. O persoană împuternicită de către operator devine operator în cazul în care utilizează datele în scop personal, fără a respecta instrucţiunile operatorului[28].

Prin urmare, titularul obligației la protecția datelor cu caracter personal este operatorul sau persoana împuternicită de operator. Calitatea de

[28] *Manual de legislație europeană privind protecția datelor*, Agenţia pentru Drepturi Fundamentale a Uniunii Europene, 2014 Consiliul Europei, p. 50, [Online] la: fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-ro.pdf, accesat25.05.2017.

operator nu este dată de exercitarea activității de prelucrare a datelor, ci de puterea de control și decizie asupra acestora[29].

Persoana împuternicită de operator prelucrează date cu caracter personal în numele operatorului, având la bază un contract. De regulă, acest contract este unul de natură comercială de prestări servicii; operatorul are calitatea de beneficiar, iar persoana împuternicită de operator are calitatea de furnizor de servicii[30]. Este posibil ca operatorul să fie o întreprindere mai mică, iar persoana împuternicită de către operator să fie o corporaţie mare, care are puterea de a dicta condiţiile în care îşi oferă serviciile. De exemplu, operatorul de date încheie un contract *cloud computing*[31], cu un furnizor de cloud și stochează date cu caracter personal în cloud. Furnizorul de cloud, în temeiul autonomiei de voință și a libertății contractuale poate subcontracta. În cazul încălcării obligațiilor referitoare la protecția datelor, este dificil de stabilit cine este responsabil.

În materia protecției datelor, întreprinderile de comerț internațional au calitatea de titulari ai obligației la protecție, acestea fiind în toate cazurile operatori de date cu caracter personal sau persoane împuternicite de operatorul de date.

Persoana fizică care prelucrează date cu caracter personal în cadrul unei activități *exclusiv personale sau domestice* nu are calitatea de operator de date [art. 3.2, ultima liniuță din Directiva 95/46/CE și art. 2 alin. (2) lit. (c) din Regulamentul general privind protecția datelor].

În cazul în care, însă, activitatea prin intermediul căreia se prelucrează datele, nu este exclusiv personală sau domestică, persoana fizică

---

[29] S. Șandru, *op. cit*., p. 202.

[30] S. Șandru, *op. cit*., p. 206.

[31] Cloud computing înseamnă distributed computing prin intermediul unui network, Internetul, și constă în abilitatea de a face să funcționeze un program sau o aplicație în același timp, în mai multe computere conectate între ele. Mari furnizori de cloud computing sunt, de exemplu, Google, Amazon, Apple, Dropbox, IBM, Microsoft, Facebook. Faptul că un număr mare de clienți este deservit prin intermediul cloud computing este avantajos din punct de vedere financiar și pentru furnizorul de cloud și pentru clienți: furnizorul folosește baze mari de stocare și prelucrare a datelor clienților, iar clienții nu investesc în tehnologie, externalizând stocarea datelor. Prin utilizarea Internetului, accesarea datelor poate fi făcută de oriunde în lume. (C.T. Ungureanu, *Contractul cloud computing în comerțul internațional*, în Revista moldovenească de Drept Internațional și Relații Internaționale, vol. 37, nr. 3/2015, p. 26, [Online] la:http://rmdiri.md/wp-content/uploads/2015/01/RMDIRI-Nr.-3-20157.pdf, accesată 19.06.2017).

dobândește calitatea de operator de date cu caracter personal. De exemplu, în cauza *Bodil Lindqvist* (C-101/01)[32] CJUE a considerat că referirea, pe o pagină de Internet, la diverse persoane şi identificarea acestora, fie după nume, fie prin alte mijloace, astfel încât aceste date să fie accesibile unui număr nedefinit de persoane, constituie prelucrare de date cu caracter personal, integral sau parţial prin mijloace automate, deoarece această activitate nu poate fi interpretată ca fiind asociată unor activităţi desfăşurate în viaţa privată sau de familie.

6. Când este necesară protecția datelor în contractele internaționale? În ce contracte poate interveni transferul de date cu caracter personal?

Necesitatea protecției datelor în contractele internaționale există atunci când datele sunt *transferate.*

Practic, orice contract internațional/cu element de extraneitate poate presupune transferul de date cu caracter personal. Internaționalitatea este conferită contractului, de regulă, de sediul sau reședința părților, care se află pe teritoriul unor state diferite. Astfel, dacă se utilizează criteriul calității părților[33], datele cu caracter personal se pot transfera în cazul următoarelor contracte:

- contracte încheiate între profesioniști[34]; de exemplu, *contractul de distribuție* (distribuitorul colectează date de la cumpărători și le transferă producătorului, cu sediul în alt stat decât acela al distribuitorului, care le prelucrează în vederea realizării de profiluri, publicitate orientată spre anumite tipuri de cumpărători – *targeting*, ș.a.), *contractul de agenție* (agentul, mandatar profesionist, cu sediul în România, colectează datele clienților pe care le transmite producătorului în numele căruia acționează – în legislația română, comitentului - cu sediul în Canada, în vederea negocierii și încheierii de contracte între producător și clienți), *contractul de vânzare* (un medic cumpără online aparatură medicală pentru dotarea cabinetului său și transmite datele sale cu caracter personal vânzătorului); ș.a.

[32] [Online] la:http://curia.europa.eu, accesat 13.10.2017.

[33] A se vedea și C. T. Ungureanu, *Contractul electronic*, în revista Dreptul, nr. 9/2015, pp. 163-164.

[34] Se are în vedere noțiunea de profesionist în accepțiunea art. 3 C. civ., coroborat cu prevederile art. 8 din Legea nr. 71/2011 pentru punerea în aplicare a Legiinr. 287/2009, privind Codul civil (publicată în M.Of. nr. 409, 10.06.2011).

- contracte încheiate între un profesionist și un consumator[35]/contracte de consum; de exemplu, *contractul de vânzare* (un agent imobiliar cu sediul în Franța, care vinde online case de vacanță în toate statele UE și prelucrează datele clienților săi la filiala din Bulgaria[36]); contractul de vânzare prin care consumatorul achiziționează bunuri de la un magazin online, iar profesionistul îi prelucrează datele în scopul realizării de profiluri, orientării publicității; *contractele de transport* (aerian, rutier, feroviar, maritim) *internaționale de persoane* (la achiziționarea biletului online, consumatorul transferă datele sale cu caracter personal furnizorului de servicii); *contractele bancare*, încheiate între bănci și consumatori (datele sunt transferate băncilor; consumatorul face plăți online cu carduri de credit/debit, de exemplu prin PayPal[37]), *contracte de prestări servicii*, cum sunt contractele *cloud computing*;ș.a.

- contracte încheiate între un consumator și un profesionist; de exemplu[38], Elance-oDesk[39] este o platformă online, unul dintre liderii mondiali pe piața muncii „de acasă", care permite angajatorilor să posteze locuri de muncă, căutând lucrători independenți (*freelancers*[40]); fiecare lucrător independent (care are calitatea de consumator) poate posta CV-ul său și poate face oferte angajatorilor, în anumite condiții;

- în anumite contracte încheiate între consumatori (de regulă, în cazul acestor contracte, chiar dacă se transferă date cu caracter personal, consumatorul nu este considerat operator de date, dacă prelucrează datele în

[35] Consumatorul este, potrivit Codului consumului (O.G. nr. 21/1992 privind protecția consumatorilor, republicată în M.Of. nr. 208, 28.03.2007, cu modificările și completările ulterioare), orice persoană fizică sau grup de persoane fizice constituite în asociații, care acționează în scopuri din afara activității sale comerciale, industriale sau de producție, artizanale ori liberale.

[36] A se vedea și M. Brkan, *Data Protection and Conflict-of-Laws: a challenging relationship*, în European Data Protection Law Review, nr. 3/2016, p.329, [Online] la:http://www.lexxion.de/pdf/edpl/EDPL%20Reading%20Sample_Maja%20Brkan.pdf, accesat 18.06.2017.

[37] Pentru detalii, a se vedea, [Online] la:https://ro.wikipedia.org/wiki/PayPal, accesată 28.06.2017.

[38] M. Tudorache, *Contractul încheiat prin mijloace electronice, în reglementarea din noul Cod civil*, Editura C. H. Beck, București, 2013, pp. 69-70.

[39] [Online] la: http://www.elance-odesk.com/homepage, accesat 15.10.2017.

[40] Lucrător *freelance* este o persoană care lucrează independent, care desfășoară o profesie fără un angajament pe termen lung cu un angajator ([Online] la: http://ro.wikipedia.org/wiki/Freelancer, accesat 2.05.2017).

cadrul unei activități *exclusiv personale sau domestice*); de exemplu, contractele încheiate folosind site-ul și aplicația eBay, prin care un consumator poate cumpăra de la un alt consumator un produs *second hand* (ca la un talcioc online)[41]; în aceste contracte datele cu caracter personal se transferă profesionistului care prestează servicii, facilitând încheierea contractului, adică eBay[42]; eBay este operatorul de date cu caracter personal și nu consumatorii;

- contracte internaționale de muncă;contractele internaționale individuale de muncă, care au elemente de legătură cu mai multe state facilitează transferul de date cu caracter personal; astfel, de exemplu, angajatorii prelucrează datele personale ale angajaților lor, inclusiv când aceștia prestează munca în filiale sau sucursale cu sediul în alte state; există angajați ale căror locuri de muncă sunt, prin natura lor, internaționale, cum sunt aceia care lucrează în transporturile internaționale, agenții comerciali care desfășoară activitatea pe teritoriul mai multor state, ș.a.

- contracte internaționale de asigurare, ș.a.

Dacă se utilizează criteriul *naturii contractului*, datele cu caracter personal pot fi transferate în străinătate în cazul contractelor care presupun un transfer de *know how* în vederea formării personalului, al contractelor de *outsoucing*[43] (atunci când *outsourcing*-ul este *offshore*, adică externalizarea are loc într-o țară străină, exploatându-se, de regulă, costurile reduse ale forței de muncă[44], are loc divulgarea unui volum mare de informaţii personale sau sensibile către furnizorii de servicii externi), al stocării datelor

[41] Pentru detalii, a se vedea, [Online] la:http://ro.wikipedia.org/wiki/EBay, accesat 10.05.2017.

[42] Pentru detalii, a se vedea, [Online] la:http://pages.ebay.com/help/policies/privacy-policy.html#global, accesat 28.06.2017.

[43] *Outsourcing*-ul (externalizarea) este o strategie folosită de întreprinderi mari, prin care acestea externalizează o parte dintre funcțiile lor de management, în special din domeniul marketing-ului, logisticii, resurselor umane și contabilității, în scopul de a reduce costurile. De exemplu, angajarea unei firme de avocatură, ori de contabilitate, în loc de a angaja jurişti ori contabili *in-house*, care să facă parte din personalul întreprinderii.

[44] Pentru detalii referitoare la contractele *outsourcing*, a se vedea, M. M. Blair, E. O'Hara O'Connor, G.Kirchhoefer, *Outsourcing, Modularity, and the Theory of the Firm*, în Brigham Young University Law Review, 2011, p. 263 și urm., [Online] la:http://www.law2.byu.edu/lawreview/articles/1359671093_01blair.fin.pdf, accesat 7.05.2017; J. Almalki, *ICT Offshore Outsourcing: Its Appeals and Impacts*, în International Journal of Computer Science, vol. 9, issue 6, nr. 1, 2012, p. 359 și urm., [Online] la:http://ijcsi.org/papers/IJCSI-9-6-1-359-362.pdf, accesat 7.05.2017.

prin practica *cloud computing*, atunci când se evaluează o societate/corporație în vederea fuziunii/absorbției, ș.a.

7. Care sunt regulile ce trebuie respectate la transferul transnațional de date cu caracter personal?

Încheierea de contracte internaționale de consum, de contracte internaționale de muncă, de contracte de comerț internațional poate conduce la transferul de date cu caracter personal. Operatorii de date care transferă datele (exportatorii de date) trebuie să aibă în vedere legislația din materia protecției datelor, care impune reguli de transfer.

Dacă avem în vedere UE, regulile aplicabile transferului de date diferă după cum acesta are loc între statele membre UE sau între UE și state terțe. Aceste reguli se regăsesc în art. 25 și 26 din Directiva 95/46/CE, aplicabile până la 25 mai 2018, când vor fi înlocuite de regulile din art. 44-50 din Regulamentul general privind protecția datelor.

Între statele contractante la Convenția 108, datele se transferă conform art. 2 din Protocolul adiţional la Convenţia pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, cu privire la autorităţile de control şi fluxul transfrontalier al datelor (2001)[45]. Regulile sunt diferite după cum transferul are loc între statele contractante sau din statele contractante spre state terțe. Întrucât majoritatea statelor contractante la Convenția 108 sunt membre atât ale UE, cât și ale Consiliului Europei, Convenția 108 se află într-un proces de revizuire și modernizare, astfel încât instrumentele juridice de la nivelul acestor două organizații regionale să fie compatibile[46].

Pe teritoriul UE, *între statele membre, datele cu caracter personal se transferă liber*. De asemenea, *transferul transnațional are loc liber între statele contractante la Convenția 108*. De exemplu, dacă o societate multinațională are sedii în mai multe state membre ale UE, printre care România și Ungaria, și transferă date cu caracter personal din România în Ungaria, transferul de date are loc liber (nerestricționat și fără îndeplinirea vreunei formalități).

---

[45] Ratificat de România prin Legea nr. 55/2005, publicată în M.Of., nr. 244, 23.03.2005.

[46] Forma modernizată propusă poate fi accesată [Online] la: http://www.coe.int/en/web/data-protection/modernisation-convention108, accesat la 10.10.2017.

În ceea ce privește transferul de date cu caracter personal din UE către state terțe, se aplică *trei categorii de reguli*, în funcție de statul terț în care se importă datele. Astfel, transferul este liber, dacă în statul terț există un nivel adecvat al protecției datelor cu caracter personal (a), datele se transferă în statul terț în absența unui nivel adecvat de protecție a datelor, în anumite cazuri expres prevăzute și de strictă interpretare (b) și transferul datelor are loc în statul terț în absența unui nivel adecvat de protecție a datelor, atunci când sunt asigurate *garanții adecvate* a protecției acestora (c).

(a) *Transferul este liber, dacă în statul terț există un nivel adecvat al protecției datelor cu caracter personal.*

Conform art. 25 din Directiva 95/46/CE și a art. 45 din Regulamentul general privind protecția datelor, transferul de date cu caracter personal către state terțe este *liber*, cu condiția ca în statul destinatar al datelor protecția acestora să aibă un nivel adecvat.

Cine apreciază caracterul adecvat al nivelului de protecţie a datelor? Conform dreptului UE, caracterul adecvat al protecţiei datelor într-o ţară terţă este evaluat de Comisia Europeană. În acest sens, Comisia poate decide, printr-un act care face parte din legislația secundară UE (printr-o decizie), că un stat terț, un teritoriu sau unul sau mai multe sectoare dintr-un stat terț asigură un nivel de protecție adecvat al datelor cu caracter personal. Decizia Comisiei este obligatorie pentru toate statele membre și în temeiul acesteia datele pot fi transferate liber, fără vreo formalitate.

Decizia Comisiei, deși nu are o aplicabilitate limitată în timp, dacă se schimbă condițiile în care a fost stabilit caracterul adecvat de protecție, poate fi abrogată. Acesta este cazul, de exemplu, al deciziei care a stabilit *Safe Harbour* între UE și SUA[47], care în 2015 a fost abrogată printr-o hotărâre a CJUE, în cauza Schrems (C-362/14)[48]. În Regulamentul general privind protecția datelor există prevederi exprese cu privire la abrogarea, modificarea sau suspendarea deciziei Comisiei prin care se stabilește nivelul adecvat de protecție a datelor într-un stat terț [art. 45 alin. (5)].

Apartenența la *Safe Harbour* („Sfera de siguranță") se obţinea printr-un angajament voluntar declarat în faţa Departamentului de Comerţ al

[47]Decizia Comisiei din 26 iulie 2000 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de principiile „sferei de siguranță" privind protecția vieții private și întrebările de bază aferente, publicate de Departamentul Comerțului al S.U.A (Publicată în J.O. nr. L 215, 25.08.2000).

[48][Online] la:http://curia.europa.eu/, accesat 3.10.2017.

SUA şi înregistrat într-o listă publicată de respectivul departament. *Safe Harbour* reprezenta un cod de conduită, un set de principii pe care întreprinzătorii se obligau să îl respecte[49].

În urma invalidării deciziei Comisiei prin cauza Schrems, în 2016 Comisia Europeană a adoptat o altă decizie[50] prin care s-a stabilit un nou mecanism de protecție a datelor, *Privacy Shield Framework*[51] (Scutul de confidențialitate). Potrivit acestei decizii, SUA garantează un nivel adecvat de protecţie a datelor cu caracter personal transferate din UE către întreprinzători din SUA în temeiul Scutului de confidenţialitate UE-SUA, cu condiţia ca întreprinzătorii să prelucreze datele cu caracter personal în conformitate cu un set puternic de principii şi garanţii pentru protecţia vieţii private şi a datelor cu caracter personal care sunt echivalente cu cele din UE.

În prezent, Comisia consideră că au un nivel de protecție adecvat: Andora, Argentina, Canada (organizațiile comerciale), Insulele Feroe, Guernsey, Israel, Isle of Man, Jersey, Noua Zeelandă, Elveția, SUA **(**dar numai pentru transferul către companii care sunt membre ale înțelegerii Safe Harbour/Privacy Shield Framework) și Uruguay[52].

(b) *Datele se transferă în statul terț, în absența unui nivel adecvat de protecție a datelor, în anumite cazuri expres prevăzute și de strictă interpretare.*

Deşi statul terț în care se transferă datele nu asigură o protecție adecvată a acestora, transferul are loc liber, dacă este necesar pentru interesele specifice ale persoanei vizate sau pentru interesele legitime prioritare ale altor persoane, în special interese publice importante (art. 26 alin. 1 din Directiva 95/46/CE, art. 2 alin. 2 din Protocolul adițional la Convenția 108 și art. 49 din Regulamentul general privind protecția datelor).

---

[49] *Manual..., op.cit.,* p. 140; [Online] la: http://2016.export.gov/safeharbor/eu/, accesat 10.09.2017.

[50] Decizia de punere în aplicare (UE) 2016/1250 a Comisiei din 12 iulie 2016 în temeiul Directivei 95/46/CE a Parlamentului European şi a Consiliului privind caracterul adecvat al protecţiei oferite de Scutul de confidenţialitate (Privacy Schield Framework) UE-SUA, publicată în J.O. nr.L 207, 1.08.2016.

[51] [Online] la: https://www.privacyshield.gov/Program-Overview, accesat 10.09.2017.

[52] [Online] la:

http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm, accesat 21.06.2017.

Astfel, conform art. 26 (1) din Directiva 95/46/CE, transferul de date personale spre state terțe care nu asigură un nivel adecvat de protecție a acestora poate avea loc cu condiția ca: „(a) persoana vizată să își dea consimțământul ferm la transferul avut în vedere sau (b) transferul să fie necesar pentru executarea unui contract între persoana vizată și operator sau pentru aducerea la îndeplinire a măsurilor precontractuale luate ca răspuns la cererea persoanei vizate sau transferul să fie necesar pentru încheierea sau executarea unui contract încheiat sau care urmează să fie încheiat în interesul persoanei vizate între operator și un terț sau (d) transferul să fie necesar sau impus prin lege pentru apărarea unui interes public important, sau pentru constatarea, exercitarea sau apărarea unui drept în justiție sau (e) transferul să fie necesar apărării interesului vital al persoanei vizate sau (f) transferul să fie făcut dintr-un registru public care, în conformitate cu dispozițiile legale sau de reglementare, este destinat informării publicului și este deschis spre consultare publicului sau oricărei persoane care demonstrează un interes legitim, în măsura în care se îndeplinesc condițiile prevăzute prin lege pentru consultări în cazurile particulare.”.

În Regulamentul general privind protecția datelor (art. 49) se păstrează aceleași cazuri.

(c) *Transferul datelor are loc când sunt asigurate garanții adecvate a protecției acestora.*

Potrivit art. 26(2) din Directiva 95/46/CE și art. 46 din Regulamentul general privind protecția datelor, pot avea loc transferuri de date cu caracter personal către o țară terță care *nu asigură* un nivel de protecție adecvat, atunci când operatorul de date/ persoana împuternicită de operator oferă garanții suficiente/adecvate cu privire la protecția acestora și garantează exercitarea drepturilor corespunzătoare.

Asemenea garanții sunt măsuri de protecție a datelor, care nu există în legislația statului terț în care se transferă/exportă datele și care sunt create pentru un anumit caz de transfer de date[53].

Conform Directivei 95/46/CE, *garanțiile adecvate* recunoscute sunt de două tipuri: *clauze contractuale* și *reguli corporatiste obligatorii* (*Binding Corporate Rules*).

[53] Ch. Kuner, *Extraterritoriality and International Data Transfers in EU Data Protection Law*, în International Data Privacy Law, 2015, vol. 5, nr. 4, p. 237.

Clauzele contractuale, la rândul lor, pot fi *clauze standard*, aprobate de Comisia Europeană prin decizie sau clauze *ad-hoc*, redactate de către părțile contractante, pentru fiecare caz în parte, care, de regulă, trebuie aprobate de autoritatea de supraveghere națională a protecției datelor[54], care verifică dacă acestea respectă regulile din dreptul UE referitoare la protecția datelor cu caracter personal[55]. Prin urmare, utilizarea clauzelor standard este voluntară, părțile putând redacta propriile clauze. De exemplu, rețeaua de socializare Facebook folosește clauze contractuale standard[56].

Clauzele contractuale standard se încheie între exportatorul de date şi importatorul de date, ambii asigurând luarea anumitor măsuri pentru protecția datelor. În prezent, operatorul care exportă date are posibilitatea de a alege între două seturide clauze standard pentru transferurile de la operator la operator. Setul I este inclus în anexa la Decizia Comisiei Europene 2001/497/CE privind clauzele contractuale standard pentru transferul de date cu caracter personalcătre ţări terţe în temeiul Directivei 95/46/CE[57]; Setul II este inclus în anexa la Decizia Comisiei Europene 2004/915/CE de modificare a Deciziei 2001/497/CE privind introducerea unui set alternativ de clauze contractuale standard pentrutransferul de date cu caracter personal către ţări terţe.

Pentru transferurilede la operator la împuternicit, există un singur set de clauze contractualestandard, incluse în anexa la Decizia Comisiei Europene 2010/87/UEprivind clauzele contractuale tip pentru transferul de date cu caracter personal către persoanele împuternicite de către operator stabilite în țări terțe în temeiul Directivei 95/46/CE[58].

Clauzele contractuale *ad-hoc* pot fi redactate de părțile contractante sau părțile pot prelua clauze standard, elaborate de organizații internaționale, cum sunt acelea ale ICC (International Chamber of Commerce) de la Paris[59].

---

[54] Autoritatea de supraveghere reprezintă una sau mai multe autorități publice independente, responsabile cu supravegherea protecției datelor cu caracter personal într-un anumit stat. (art. 28 din Directiva 95/46/CE; art. 51-59 din Regulamentul general privind protecția datelor).

[55] Ch. Kuner, *op. cit*., p. 237.

[56] În acest sens, [Online] la:https://ro-ro.facebook.com/privacy/explanation, accesată 28.06.2017.

[57] Publicată în J.O. nr. L 181, 4.07.2001.

[58] Publicată în J.O. nr. L 39, 12.02.2010.

[59] ICC, Department of Policy and Business Practices, *Task Force on Privacy and the Protection of Personal Data. Final Approved Version of Alternative Standard Contractual*

În contextul Convenţiei 108 a fost elaborat unghid privind elaborarea clauzelor contractuale[60].

Regulile corporatiste obligatorii (în continuare, RCO). Deși nu sunt reglementate expres în Directiva 95/46/CE, RCO au fost recunoscute de autoritățile de supraveghere din statele membre ca bază legală pentru exportul de date personale în state terțe[61]. RCO reprezintă reguli de protecție a datelor adoptate de o întreprindere sau de un grup de întreprinderi/societăți multinaționale, care garantează drepturile persoanelor vizate. RCO se aprobă de autoritățile de supraveghere din statele membre. De exemplu, eBay asigură protecția datelor utilizând RCO; eBay Inc. a stabilit standarde globale de confidențialitate pentru toate companiile eBay Inc., cunoscute ca reguli corporatiste obligatorii (BCR – Binding Corporate Rules), aprobate de mai multe autorități de supraveghere din statele Uniunii Europene[62].

În Regulamentul general privind protecția datelor (art. 46), *garanții adecvate* înseamnă:

Garanții adecvate furnizate fără să fie nevoie de *nicio autorizație* specifică din partea unei autorități de supraveghere, prin [art. 46 alin. (2) lit. (a)-(f)]:

- un instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice;

- reguli corporatiste obligatorii;

- clauze standard de protecție a datelor adoptate de Comisie;

- clauze standard de protecție a datelor adoptate de o autoritate de supraveghere și aprobate de Comisie;

- un cod de conduită, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate;

Clauses for the Transfer of Personal Data from the EU to Third Countries (controller to controller transfers), [Online] la:https://www.inforights.im/media/1066/icc-data-controller-to-data-controller-contract-clauses.pdf, accesat 24.06.2017.

[60] [Online] la: search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016804e0476, accesat 1.06.2017.

[61] A se vedea, C. Kuner, *op. cit.*, p. 238.

[62] [Online] la:http://pages.ebay.com/help/policies/privacy-policy.html#global, accesată 27.06.2017.

- un mecanism de certificare, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate.

Garanții adecvate furnizate *sub rezerva autorizării din partea autorității de supraveghere competente*, prin [art. 46 alin. (3) lit. (a)-(b)]:

- clauze contractuale între operator sau persoana împuternicită de operator și operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din țara terță sau organizația internațională;

- dispoziții care urmează să fie incluse în acordurile administrative dintre autoritățile sau organismele publice, care includ drepturi opozabile și efective pentru persoanele vizate.

În Regulamentul general privind protecția datelor, noțiunea de RCO este detaliat reglementată în art. 47.

8. Care este eficiența regulilor cu privire la transferul transnațional de date cu caracter personal?

Regulile descrise se aplică sau urmează să se aplice (Regulamentul general privind protecția datelor) în era Internetului, a *Big Data*, *Internet of Things* (IoT), a rețelelor de socializare (Facebook, LinkedIn ș.a.).Internetul captează o mulțime de date. Cardurile de credit și de debit, cecurile și alte activități financiare implică un flux constant de miliarde de tranzacții financiare. Din ce în ce mai multe rețele de senzori - camere de supraveghere video, computere încorporate în automobile, telefoane mobile - înregistrează locații, mișcări și activități. Colectarea datelor este omniprezentă; aproape tot ceea ce facem are ca rezultat colectarea și stocarea datelor de către una sau mai multe părți, fie operatori de date, împuterniciți de operatorul de date, terți, destinatari. Aceste date sunt digitale. Ele pot fi stocate, partajate, căutate, combinate și duplicate cu o viteză foarte mare și la un cost foarte mic[63]. Prin urmare, toate aceste reguli din dreptul UE referitoare la transferul datelor cu caracter personal în state terțe *au o eficiență practică redusă*. Au

[63] Ch. Kuner, F.H. Cate, Ch. Millard, D. Jerker, B. Svantesson, *The challenge of 'big data' for data protection*, în International Data Privacy Law, vol. 2, nr. 2/2012, p. 48, [Online] la:https://academic.oup.com/idpl/article/2/2/47/755343/The-challenge-of-big-data-for-data-protection, accesat 20.06.2017.

rolul de a crea o *hologramă a protecției datelor*, care, poate, utilizând tehnologia (3D printing?), ar putea deveni realitate.

Există încercări de asigurare a protecției datelor prin acțiuni judiciare, la diferite niveluri (naționale, regionale - CJUE, internaționale – CtEDO)[64], dar Internetul, *IoT*, *Big Data*, evoluția tehnologiei în general, provoacă limitele legislației și controlul protecției datelor apare ca fiind greu de realizat.

Concluzii

Protecția datelor cu caracter personal reprezintă unul dintre subiectele aflate în centrul preocupărilor legiuitorului european, intens dezbătut în literatura de specialitate și destul de frecvent analizat în cauzele cu care sunt sesizate autoritățile de protecție a datelor la nivel regional și național și instanțele europene (CJUE, CtEDO) și naționale.

Deși există o preocupare reală pentru asigurarea protecției datelor cu caracter personal, deși se impun reguli referitoare la transferul transnațional de date, *persoanele vizate* acționează, în marea majoritate a cazurilor, fără a se preocupa de soarta datelor lor cu caracter personal, fiind „vrăjite” de oferta tehnologică a erei Internetului. Astfel, încheie contracte electronice online de diferite tipuri (poate, fără a fi conștiente, întotdeauna, că își exprimă consimțământul la încheierea unui contract), cum sunt cele cu rețelele de socializare, cu alți furnizori de *cloud*, acceptând servicii oferite de aceștia pentru a obține spațiu de stocare a documentelor/fotografiilor/altor creații personale în *cloud*, pentru a obține o adresă de email, „încarcă” (upload) fotografii, dintre cele mai personale, pe diferite pagini de Internet, își dau acordul, prin intermediul telefoanelor mobile, pentru ca diverse aplicații să le afle localizarea, în timp și spațiu, și alte informații cu caracter personal, toate „gratis”, plătind *de fapt* cu datele lor cu caracter personal.

Era Internetului, în care nu există frontiere, și a tuturor mijloacelor tehnice și tehnologice care facilitează circulația datelor într-un ritm greu de imaginat, completate, de multe ori, cu „dispoziția” persoanelor vizate de a permite invadarea vieții lor private, fac deosebit de dificilă protecția datelor cu caracter personal.

[64] Aceste probleme nusunt tratate în prezenta lucrare.

ANALELE ȘTIINȚIFICE ALE UNIVERSITĂȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

DE LA FORMATUL PE HÂRTIE AL CAMBIEI LA CAMBIA ELECTRONICĂ. TITLU DE CREDIT SAU INSTRUMENT DE PLATĂ?

FROM THE FORMAT PAPER BILL OF EXCHANGE TO THE ELETRONIC BILL OF EXCHANGE.CREDIT TITLE OR PAYMENT INSTRUMENT?

SILVIA LUCIA CRISTEA[1]

Rezumat: Prezentul articol conține câteva noțiuni introductive privind istoricul reglementării cambiale (sect. 1), apoi analiza caracteristicilor cambiei ca titlu de credit și instrument de plată (sect. 2), precum și particularitățile reglementării cambiei electronice în România (sect. 4). Concluziile vizează transformările regimului juridic al cambiei odată cu intrarea în vigoare a O.U.G. nr. 39/2008 privind cambia electronică, respectiv trecerea de la regimul juridic de titlu de credit la cel de instrument de plată.
Cuvinte-cheie: cambie informatizată, cambie informatică, trunchiere, titlu de credit, instrument de plată

Abstract: This article contains a few introductory notions on the history of the cambial international regulating (section 1), then the analysis of the bill of exchange juridical regime as a credit title and payment instrument (section 2), as well as the particularities of electronic bill of exchange regulating in Romania (section 3&4). The conclusions aimed at reducing the juridical regime of the bill of exchange-once it enters into force of the Emergency Ordinance no. 39/2008 on electronic bill of exchange and promissory note-namely the transition of bill of exchange from the juridical regime of credit title to the payment instrument status.
Keywords: computerized bill of exchange, electronic bill of exchange, truncating, credit title, payment instrument

[1] Profesor univ. dr., Academia de Studii Economice din București, Departamentul de Drept și cercetător asociat la Institutul de Cercetări Juridice al Academiei Române, email: silvia_drept@yahoo.com.

1. Considerații introductive

Titlurile comerciale de valoare, cambiile şi biletele la ordin au o existență îndelungată în cadrul schimburilor economice internaționale (evul mediu târziu), ulterior, adăugându-se la acestea ca mijloc de plată şi cecul. Ideea unificării reglementărilor referitoare la aceste titluri de valoare ca o consecință a diversificării relațiilor economice internaționale, dar şi ca urmare a apariției unor probleme conflictuale generate de diferențele dintre legislațiile naționale în materie s-a materializat prin adoptarea la 7 iunie 1930 la Geneva a Convenției internaționale care cuprinde legea uniformă asupra cambiei şi biletului la ordin şi la 11 martie 1931 în acelaşi oraş a Convenției internaționale care cuprinde legea uniformă asupra cecului, respectiv 19 martie 1931 a Convenției de reglementare a unor conflicte de legi în materie de cec.

România, deşi nu a semnat şi ratificat Convențiile de la Geneva a considerat oportună adoptarea prevederilor acestora, ceea ce s-a realizat în anul 1934 prin adoptarea Legii nr. 58/1934 asupra cambiei şi biletului la ordin, respectiv a Legii nr. 59/1934 asupra cecului[2].

Aceste două legi nu au fost abrogate în perioada regimului comunist întrucât titlurile de valoare menționate erau utilizate numai în relațiile comerciale externe ale țării noastre[3].

După 1990 în cadrul etapei de tranziție spre economia de piață s-a impus o reevaluare a regimului juridic creat de legile din 1934 în care scop ele au fost modificate prin O.G. nr. 11/1993[4]. Acest act normativ a reinstaurat cu unele corective sistemul procedural consacrat în anul 1934[5].

---

[2] A se vedea comentariile referitoare la aceste legi, S. Ionescu, P. Demetrescu, I.L. Georgescu, *Noua lege asupra cambiei şi biletului la ordin şi legea asupra cecului*, Editura Națională Ciornei SAR, Bucureşti, 1934; respectiv E. Cristoforeanu, *Tratat de drept cambial, Legile asupra cambiei şi biletului la ordin din 1 mai 1934*, vol. I-II, Bucureşti, Editura Curierul Judiciar SA, 1936;

[3] Legile în cauză, după adoptare, au generat nu puține critici, de ex., Gălăşescu-Pyk, *Cambia şi biletul la ordin*, vol. I, Bucureşti, Editura Tiparul Universitar, 1939, pp. 135-136, 720-721 şi 725-727;

[4] M.Of. nr. 201, 23.08.1993, aprobată şi modificată prin Legea nr. 83/1994, M.Of. nr. 119 bis, 14.06.1994;

[5] Un comentariu la O. Căpățână, *Cambia, biletul la ordin şi cecul, noi reglementări procedurale*, în Revista de Drept comercial, nr. 1/1994, Editura Lumina Lex, București, pp. 5-28.

Banca Națională a României a elaborat mai multe reglementări de ordin intern menite să orienteze activitatea băncilor comerciale în legătură cu titlurile de valoare, dispoziții ce au intrat în vigoare începând cu data de 1 aprilie 1995, după cum urmează:

- Normele cadru nr. 6 din 8 martie 1994 privind comerțul făcut de societățile bancare şi celelalte societăți de credit, cu cambii şi bilete la ordin pe baza Legii nr. 58/1934 asupra cambiei şi biletului la ordin, modificată prin Legea nr. 83/1994;
- Normele tehnice nr. 10 din 20 aprilie 1994 privind cambia şi biletul la ordin;
- Normele cadru nr. 7 din 8 martie 1994 privind comerțul efectuat de societățile bancare şi celelalte societăți de credit cu cecuri pe baza Legii nr. 83/1994 asupra ceculuи, modificată prin Legea nr. 83/1994;
- Normele tehnice nr. 9 din 20 aprilie 1994 privind cecul;
- Anexe referitoare la cec din Regulamentul nr. 10 din 14 noiembrie 1994 privind compensarea multilaterală a plăților interbancare fără numerar pe suport de hârtie.

Legea nr. 105/1992 cu privire la reglementarea raporturilor de drept internațional privat, în capitolul IX, consacrat cambiei, biletului la ordin şi ceculuи, preia numeroase soluții promovate de Convențiile de la Geneva privind reglementarea conflictelor de legi în materia acestor titluri de valoare. La intrarea în vigoare a Codului civil[6], când Legea nr. 105/1992 a fost abrogată, dispozițiile respective au fost incluse în noul act normativ.

Întrucât uniformizarea normelor conflictuale în materie realizată de convențiile de la Geneva a fost considerată doar parțial, neținându-se seama de soluțiile promovate de practica anglo-saxonă în materie, s-a adoptat la capătul unor negocieri îndelungate Convenția Națiunilor Unite cu privire la cambiile şi biletele la ordin internaționale la New York în 1988 pe baza proiectului elaborat în cadrul Comisiei Națiunilor Unite pentru dreptul comercial internațional CNUDCI (UNCITRAL – în engleză)[7].

---

[6] Legea nr. 287/2009 privind Codul civil, republicată în M.Of. nr. 505, 15.07.2011, cu modificările şi completările ulterioare.

[7] Rezoluția nr. 43/165 a Adunării Generale a Națiunilor Unite şi textul Convenției în Annuaire CNUDCI, vol. XIX, 1988, pp. 179-195, (Această convenție nu a intrat, încă, în vigoare). Comentarii ample ale convenției la S.L. Cristea, *Cambia în dreptul comparat*, Bucureşti, Editura Lumina Lex, 2001.

Finele secolului XX şi începutul secolului XXI au înregistrat în paralel cu informatizarea la toate nivelurile operaţiuni comerciale prin mijloace electronice aşa-numitul e-commerce. Aceste practici au generat şi impulsionat un ansamblu de preocupări de reglementare a noilor aspecte la nivel internaţional şi intern în plan convenţional şi legislativ neocolind nici domeniul titlurilor de valoare.

Implicaţiile comerţului desfăşurat cu mijloace electronice au generat o serie de practici ce au influenţat şi statutul juridic al cambiei, biletului la ordin, respectiv ceculi, aspecte nereglementate de Convenţia din 1988 şi în raport de care şi normativul intern nu este suficient de acoperit.

2. Cambia pe suport hârtie

Cambia, ca înscris prin care o persoană, numită trăgător sau emitent, dă dispoziţie altei persoane, numită tras, să plătească la scadenţă o sumă de bani unei a treia persoane, numită beneficiar, sau la ordinul acesteia, conţine următoarele menţiuni obligatorii conform legii:

- denumirea de cambie în limba de redactare a înscrisului;
- ordinul necondiţionat de plată a unei sume determinate;
- indicarea numelui trasului;
- indicarea scadenţei;
- indicarea locului de plată;
- indicarea numelui beneficiarului;
- indicarea datei şi locului emiterii;
- semnătura trăgătorului.

2.1. Cambia – instrument de plată

Într-o etapă în care activitatea comercială suferea datorită caracterului rudimentar al comunicaţiilor, insecurităţii transportului, dar şi diversităţii monedelor de plată, cambia a cunoscut o nouă evoluţie[8].

Comerciantul din statul A, în urma afacerilor încheiate în statul B, putea să dobândească o serie de creanţe faţă de comercianţii din statul B (de exemplu să fi vândut o cantitate de marfă pe care cumpărătorul să se oblige să o plătească la o dată ulterioară predării mărfii). Reîntors în statul B pentru alte afaceri, n-ar fi fost posibil cumva ca acel comerciant să se angajeze să-şi

[8] În acest sens a se vedea S. Cristea şi C. Stoica, *Drept comercial*", Editura Lumina Lex, Bucureşti, 2002, pp. 234-238.

plătească propriile datorii folosindu-se de creanța ce o avea împotriva cumpărătorului pentru care scadența plății nu se împlinise (care în dreptul cambial corespunde raportului fundamental ce stă la baza emiterii cambiei)?

Mecanismul ce face posibilă legătura între creanțe şi datorii este următorul: comerciantul din statul A (numit trăgător) în loc să-şi plătească în moneda din statul B, propriile datorii față de un creditor personal din statul B (numit beneficiar, iar raportul juridic dintre beneficiar şi trăgător se numeşte valoare furnizată) va invita să plătească în locul lui pe cumpărătorul-debitor al plății prețului (numit tras).

Operațiunea juridică va îmbrăca următoarea formă: comerciantul din statul A (numit trăgător) redactează (trage) o cambie (înscris) pe care, predându-l unei persoane numită beneficiar, dă dreptul acesteia din urmă să obțină plata unei sume de bani de la tras, la data consemnată în titlu[9].

Acesta este profilul cambiei din zilele noastre. Avantajele operațiunii juridice prezentate sunt colosale:

- trăgătorul nu mai trebuia să efectueze schimbul de monedă pentru că trasul plătea beneficiarului în aceeaşi monedă, respectiv a statului B;
- trăgătorul nu mai trebuia să transporte moneda necesară plăților dintr-un stat în altul;
- beneficiarul urmărea la plată un comerciant (pe tras) de pe teritoriul pe care el însuşi domicilia, deci putea apela pentru eventualele constrângeri la instanțele naționale.

Rămâneau însă o serie de inconveniente ce nu puteau fi, la acea dată, depăşite, şi anume:

- ce se întâmpla dacă trasul refuza să plătească;
- de ce n-ar fi posibil ca beneficiarul, până la scadență, să transmită cambia unor alte persoane, proprii creditori, stingându-şi astfel datoriile fără o plată în numerar.

Pentru a fi sigur de plata trasului, beneficiarul trebuia să aibă aceleaşi drepturi cu ale transmițătorului-trăgător.

Două ar fi aspectele ce se impun a fi analizate pentru a înțelege importanța circulației cambiei:

---

[9] Pentru detalii a se vedea D. Galașescu - Pyk,*"Cambia și biletul la ordin"* vol I, Editura Tiparul Universitar, București, 1939, pp.163-181.

1) pe de o parte că transmiterea titlului (cambiei) presupune existența unui interval de timp suficient de lung între momentul tragerii cambiei şi cel al scadenței acesteia;

2) pe de altă parte, care ar trebui să fie tehnica juridică cea mai potrivită pentru transmiterea cambiei. Această problemă a fost soluționată prin recurgerea la procedura cesiunii de creanță, instituție existentă în dreptul civil, dar care, pentru a fi preluată în materie comercială necesita o serie de corective.

2.2. Cambia – instrument de credit

Prin aceea că plata urmează a se face la o dată ulterioară, cambia constituie un instrument de credit.

În ipoteza prezentată la începutul secțiunii 2.1. a prezentului capitol, cea a vânzării-cumpărării încheiate între trăgătorul-vânzător şi trasul-cumpărător, acesta din urmă, debitor pentru plata prețului mărfii, are suficient timp să revândă marfa, să încaseze prețul şi să-şi plătească datoria la împlinirea scadenței cambiei.

În ceea ce-l priveşte pe beneficiar (ca titular al unei creanțe față de trăgător) ca posesor al titlului, fie aşteaptă ca titlul să devină exigibil (să ajungă la maturitate prin împlinirea scadenței), fie transmite cambia unui bancher, ce, la rândul lui, o poate resconta.

Cambia prezintă avantajul de a reprezenta creanța, iar posesia (deținerea) titlului îi conferă dobânditorului garanția plății, aşa încât operațiile de scontare şi rescontare de cambii sunt frecvente în practica bancară. Ceea ce caracterizează în mod fundamental titlurile de credit față de celelalte titluri documentare utilizate în relațiile civile şi comerciale este încorporarea creanței, a creditului, în însuşi titlul, de unde şi denumirea de titlu de credit.

2.3. Caracterele cambiei

Pentru a întări statutul juridic al deținătorului titlului, legea a consacrat caracterul comercial, de o rigoare accentuată, literal, autonom şi abstract al obligației cambiale. Toate acestea nu sunt decât consecințe sau, mai bine zis, manifestări ale formalismului cerut pentru existența valabilă a titlului (exista opt condiții de formă obligatorii, pe când existența raportului fundamental – corespunzând provizionului din dreptul francez, nu este

absolut necesară pentru valabilitatea cambiei în dreptul român); îndeplinirea condițiilor de formă prevalând de cele mai multe ori asupra celor de fond[7].

Obligația va fi comercială indiferent care este natura raportului fundamental care l-a determinat pe semnatar să se oblige cambial, deci chiar când acesta este un necomerciant; va fi caracterizată de un rigorism accentuat al executării, în sensul că este exclusă stipularea vreunui termen de grație (nu este permisă amânarea scadenței; dacă termenul de plată este, să presupunem, 01.10.2001, acesta nu poate fi prelungit), constatarea refuzului de acceptare sau de plată al debitorului (precizam anterior că trasul nu devine obligat cambial decât prin acceptarea cambiei) se face în formă solemnă (dresarea protestului), iar exercitarea regresului (când trasul-acceptant, debitor direct, nu plătește, devin obligați să plătească debitorii indirecți: trăgătorul, avaliștii lui, giranții anteriori sau avaliștii lor, iar acțiunea îndreptată împotriva acestora poartă denumirea de acțiune în regres) se face printr-o procedură simplificată.

- Caracterul literal rezidă în aceea că existența şi întinderea obligației sunt fixate numai prin mențiunile inserate în titlu.

Reamintim că însăşi dobândirea calității de semnatar presupune manifestarea voinței de a se angaja cambial (prin depunerea semnăturii pe titlu ca: tras-acceptant, beneficiar, girant, giratar sau avalist).

Caracterul literal este evident dacă menționăm următorul exemplu: giratarul-mandatar are, în temeiul unui contract de mandat cu titlu oneros, o creanță împotriva beneficiarului-mandant în valoare de 10 milioane lei, iar pe cambie suma înscrisă este de 9 milioane lei; la întrebarea care va fi suma ce trebuie plătită giratarului, trebuie să înțelegem că, deşi raporturile directe mandant-mandatar dau naştere unei creanțe mai mari (de 10 milioane lei), în temeiul raporturilor cambiale, singura sumă valabil a fi cerută este cea de 9 milioane lei. Ceea ce prevalează în cambie este ceea ce este înscris în ea şi poate fi cunoscut astfel de orice semnatar (şi nu raporturile juridice extra-cambiale dintre semnatari; în cazul nostru nu 10 milioane lei, ci 9 milioane lei, cât datora trasul trăgătorului când a fost trasă cambia).

- Totodată, obligația cambială este autonomă, adică angajamentul cambial al fiecărui semnatar deține o poziție juridică de-sine-stătătoare; validitatea lui nu poate fi afectată nici de nulitatea, nici de viciile obligațiilor altor semnatari.
- Este, în fine, abstractă, în sensul că este independentă de raportul fundamental care a generat-o.

Aşadar, cambia se prezintă ca un titlu complet. Dacă lipseşte vreuna dintre menţiunile considerate esenţiale, obligaţia cambială nu poate fi salvată prin recurgerea la alte documente, chiar dacă în însuşi titlul cambial se face trimitere la acestea.

Adoptând o definiţie pur formală, vom considera cambia ca fiind titlul care, predat (remis) de către trăgătorul beneficiarului, conferă acestuia din urmă, sau aceluia la al cărui ordin a fost emis, dreptul de a face să se plătească, la o dată determinată, o anumită sumă de bani sau, după Vivante este "un titlu de credit formal şi complet, conţinând obligaţiunea de a plăti, fără contraprestaţiune, o sumă de bani, la scadenţă şi în locul care sunt menţionate în ea".

3. Cambia. Informatizarea cambiei. Cambia electronică.

3.1. Informatizarea cambiei

Băncile utilizează operaţiunile electronice ca mijloace de perfecţionare a tehnicilor de prelucrare a titlurilor de credit, mai ales a cambiilor, prin procedura telematica. Telematica reprezintă o tehnologie de transmitere la mare distanţă a informaţiilor în sistem digital, combinând informatica cu comunicaţiile prin satelit şi reţele web publice şi private. S-a urmărit, printre altele, eliminarea unui volum uriaş de manipulări reprezentând un cost ridicat pentru instituţiile bancare [10] şi scumpind substanţial creditul. Dar simplificarea procedurilor de încasare a cambiei şi biletului la ordin utilizând mijloace electronice chiar dacă ar duce la crearea unui veritabil titlu de credit ridică unele probleme ce au impus pentru început, conservarea cambiei pe suport de hârtie la începutul şi la sfârşitul circuitului, circulând interbancar numai informaţiile referitoare la titlul de credit pe suport magnetic. Sub această formă, documentul reprezintă o cambie informatizată. Documentul conţine toate menţiunile impuse de legea cambială, plata realizându-se prin utilizarea tehnicilor informatice. Astfel, practic, menţiunilor obligatorii prevăzute de lege li se adaugă menţiunile menite să permită circulaţia cambiei în format electronic. Lipsa acestor date

[10] De exemplu, înregistrări contabile, completarea de borderouri, operaţiuni de triere, semnături, întreţinerea unor calendare de scadenţe etc. Costul acestor manipulări reprezintă, potrivit unei opinii, cca. 40% din cheltuielile generale ale unei bănci fără a mai discuta despre implicarea unei părţi considerabile din personal. I. Turcu, *Operaţiuni şi contracte bancare*, Bucureşti, Editura Lumina Lex, 1997, p. 163.

nu afectează validitatea titlului, ci doar circulația sa informatică. Nulitatea titlului se aplică doar dacă mențiunile obligatorii conform normelor cambiale nu sunt respectate. Originalitatea cambiei informatizate provine din îmbinarea unui titlu de credit veritabil pe suport hârtie, cu un procedeu informatic de prezentare la plată și încasare[11].

Banca trăgătorului păstrează cambia pe hârtie, transpune informațiile din cambie în format digital şi le transmit în sistemul automat de compensări interbancare numai formatul electronic, şi, după triere transpuse în banca trasului. Computerul acesteia întocmeşte un extras pe care îl predă trasului – deci reapare suportul de hârtie – prin intermediul instituției ce deține contul acestuia. După verificare, trasul detaşează o parte a extrasului pe care o semnează la rubrica acceptare comunicând băncii sale aceasta conservând cealaltă parte a extrasului identică cu prima.

Cambia informatizată deşi întocmită conform cerințelor legale, se deosebeşte de cambia obişnuită întrucât nu circulă conform dispozițiilor legale referitoare la gir, acceptare sau aval. Procedeele informatice utilizate în cazul acestui tip de cambie nu sunt prevăzute de lege, motiv pentru care utilizarea ei este supusă acordului de voință expres sau tacit al trăgătorului şi trasului.

Cambia informatizată este emisă cu mențiunea „fără protest", care preia modelul de reglementare francez al cambiei electronice; ea poate fi remisă băncii numai cu titlu de mandat de încasare reprezentând, deci, un credit comercial consimțit de trăgător în favoarea trasului pe perioada de timp cuprinsă între data exigibilității cambiei şi scadența acesteia. De asemenea, cambia informatizată poate fi utilizată în cadrul contractului de cont curent dintre trăgător şi bancă, caz în care calificarea juridică este de remitere.

De regulă, girul cambiei informatizate se efectuează în favoarea băncii trăgătorului pentru încasare sau pentru scont - așadar circulația prin gir este restrânsă datorită faptului că în momentul prelevării imaginii informatice de către bancă, titlul urmează să fie transmis la Casa de Compensare şi numai poate circula prin gir. Avalul cambiei informatizate, posibil, se efectuează, de regulă, înainte de a fi girat băncii, întrucât această cambie nu este menită să circule, avalul se dă numai în favoarea trăgătorului sau a trasului acceptant. Cambia informatizată este păstrată de bancă pe

[11] M. Jeantin, P. Le Cannu, *op.cit.*, p. 272.

perioada de timp prevăzută de prescripția extinctivă a dreptului acțiunii comerciale şi nu a celei cambiale. În ceea ce privește scadența, tot după modelul francez, cambia informatizată nu poate fi trasă decât ,,la vedere" sau la ,,o dată fixă", iar pe titlu este obligatorie menționarea domiciliului trăgătorului (clauza de domiciliere).

Avizarea trasului înainte de scadență şi predarea către acesta a unui extras al cambiei poate face să reapară suportul de hârtie, caz în care el se înfățişează cu un document cu două părți:

- partea dreaptă (păstrată de tras) unde se înscriu datele privind mențiunile din cambie, respectiv toate informațiile utile pentru plată (cuantum, scadență etc.);
- partea stângă se repetă mențiunile amintite şi se adaugă semnătura trasului pentru acceptare şi, eventual, instrucțiunile acestuia privind cambiile refuzate la plată. Partea stângă se restituie băncii trasului.

Refuzul de plată, expres sau tacit, este comunicat de banca trasului prin ordinatorul Casei de compensare băncii trăgătorului în termenul stabilit de regulamentul sistemului interbancar de telecompensații. De subliniat faptul că în caz de refuz la plată, banca trăgătorului nu va protesta cambia întrucât aceasta se emite „fără protest", dar îl informează pe client, restituindu-i cambia la cererea acestuia pentru ca în continuare să poată să uzeze de acțiunile cambiale prevăzute de condițiile înscrise în legea pentru cambia clasică.

Dovada plății efective a cambiei rezultă din bonul de plată validat de debitor şi existent la instituția de credit a trasului, precum şi din rulajul de cont al trasului, în al cărui debit a fost înregistrată plata[12].

Întrucât circulația şi plata cambiei informatizate diferă de procedura cambiei clasice prevăzute de Legea nr. 58/1934, cu modificările ulterioare, a apărut necesitatea adoptării de noi reglementări completatoare în materie la care ne vom referi mai jos.

Deşi este vorba despre o cambie veritabilă, cambia informatizată prezintă deci, anumite caracteristici proprii[13]:

---

[12] A. Bulearcă *„Regimul juridic al instrumentelor de plată în dreptul comerțului internațional"*- teză de doctorat nepublicată, București, 2017, p. 224;

[13] O. Crauciuc în volumul coordonat de S.L. Cristea, *Tehnici de finanțare în dreptul afacerilor*, Editura ASE, București, 2009, p. 216.

- În primul rând, cambiile informatizate sunt emise cu mențiunea „fără protest”. Aceasta este o mențiune utilizată frecvent în cambiile obişnuite. Este de remarcat că o clauză denumită „fără cheltuieli” este sistematic utilizată în cambia informatizată; ceea ce implică consecințe importante în caz de incidente de plată;
- În al doilea rând, este indispensabil ca pe această cambie să fie menținută o clauză de domiciliu;
- În al treilea rând, dispozițiile de determinare a scadenței cambiei nu sunt aplicabile cambiei informatizate, practica, influențată de constrângerile impuse de tratamentul informatic al titlurilor de credit a limitat libertatea de stipulare a scadenței recunoscută părților. Astfel, cambia informatizată este fie trasă la vedere, fie la termen (la o zi fixă). În acest ultim caz, părțile nu au libertatea de a fixa liber ziua scadenței.
- În al patrulea rând, cambia electronică conține mențiuni suplimentare necesare tratamentului informatic.

3.2. Cambia informatică

După cum s-a menționat, cambia informatizată a rămas tributară exigențelor Legii nr. 58/1934, iar avantajele prelucrării informatice funcționează numai în ceea ce priveşte circulația şi plata. A devenit posibilă redarea integrală a cambiei direct pe suport magnetic şi transmiterea ei mai întâi băncii şi apoi, în continuare, Casei de compensare interbancare. Emiterea materială a titlului este evitată şi astfel se obține cambia informatică, prin procedeul numit de trunchiere, obținându-se un produs informatic similar celui realizat prin reglementarea specială din dreptul francez. Denumirea de trunchiere se datorează faptului că imaginii informatice a cambiei, prelevate de bancă odată cu prezentarea titlului la plată, i se asociază o serie de informații prevăzute de legislația informatică în materie, care conțin detalii privind identitatea trăgătorului, a trasului, dar şi pe cele privind conturile bancare ale acestora.

Doctrina admite că o cambie informatică nu este nici titlu de credit, nici cambie veritabilă[14], dar are un pronunțat caracter de instrument de plată, motiv pentru care este utilizată pe scară largă, fapt ce va determina, într-un viitor apropiat, amendarea reglementărilor în materie, cel puțin la nivel

[14] S. L. Cristea, *op.cit*., p. 38.

comunitar[15]. Convenţiile de la Geneva sunt formale când menţionează exigenţa absolută a unui titlu pe hârtie cu menţiuni obligatorii. Dar acest suport este suprimat în cambia informatică. Nici una din regulile ce se aplică cambiilor tradiţionale nu se pot aplica cambiei informatice. Deci nu se poate vorbi de girare, acceptare, nici chiar de aval în sensul cambial al termenului.

4. **Ordonanţa de urgenţă a Guvernului nr. 39 din 26 martie 2008 pentru modificarea şi completarea Legii nr. 58/1934 asupra cambiei şi biletului la ordin**[16] a fost adoptată pentru a veni în întâmpinarea exigenţelor amplului proces de reformă, modernizare, dezvoltare şi diversificare a sistemului de plăţi şi decontare, proces a cărui finalizare impune modificarea Legii nr. 58/1934 cu modificările ulterioare. Considerentele explicative din expunerea de motive a acestui act normativ se referă la pregătirea noului mod de procesare preconizat de Banca Mondială prin Programul de convergenţă care, în esenţă, cere trecerea de la modul de procesare actual, manual, la modul de lucru bazat pe transmiterea de imagini în cadrul unei perioade de tranziţie, deja întârziate. Banca Mondială este conformă cu tendinţa europeană în domeniul plăţilor, iniţiativa de modernizare fiind considerată de Banca Centrală Europeană (BCE) ca fiind „salutară".

Banca Naţională a României a adoptat Norma nr. 6/2008 din 5 iunie 2008 pentru aplicarea O.U.G. nr. 39/2008[17].

Noutatea reglementării constă în promovarea tipului de cambie denumit „**trunchiată**" căreia i se stabileşte:

- formatul electronic;
- reproducerea electronică;
- transmiterea informaţiei electronice obţinute;
- procedurile de utilizare a cambiei sub formă trunchiată.

---

[15] A. Bulearcă, *op.cit.*, p. 254.

[16] M.Of. nr. 284, 11.04.2008. Actul normativ a intrat în vigoare la 12 mai 2008. Textul O.U.G. şi norma B.N.R. de aplicare inserate în cadrul legii a se vedea în *Titluri de credit şi instrumente de plată* actualizat 1 septembrie 2008, Editura Hamangiu, 2008;

[17] Norma nr. 7/2008 din 5 iunie 2008 pentru modificarea şi completarea Normelor cadru ale Băncii Naţionale a României nr. 6/1994 privind comerţul făcut de societăţile bancare şi celelalte societăţi de credit, cu cambii şi bilete la ordin pe baza Legii nr. 58/1934 asupra cambiei şi biletului la ordin, modificată prin O.G. nr. 11/1993, aprobată şi modificată prin Legea nr. 83/1994, M.Of. nr. 512, 8.07.2008.

Coroborând cele două acte normative constatăm:

Prezentarea unei cambii la plată se poate face în original (cambia clasică) sau prin trunchiere. În sensul legii prin trunchiere se înțelege procedeul informatic care constă în următoarele operațiuni succesive:

a) transpunerea în format electronic a informațiilor relevante de pe cambia originală;

b) reproducerea imaginii cambiei originale în format electronic şi

c) transmiterea informației electronice obținute prin operațiunile de mai sus, de către instituțiile de credit plătitoare.

Observăm că se au în vedere două situații: doar transpunerea în format electronic sau pur şi simplu reproducerea imaginii cambiei originale.

Situațiile menționate au în vedere doar cambiile acceptate întrucât numai acestea pot fi trunchiate.

Se precizează că sub aspectul efectelor juridice, prezentarea la plată a unei cambii trunchiate există identitate ca şi prezentarea la plată a cambiei originale, dar conținutul cambiei trunchiate şi emiterea acesteia să se efectueze conform legii.

Condițiile procedeului trunchierii, informațiile relevante pentru trunchiere ca şi imaginea cambiei originale în caz de copie electronică a acesteia se stabilesc de instituțiile de credit care sunt ținute să încheie convenții prealabile în acest sens.

Atât informațiile relevante pentru trunchiere, cât şi imaginea electronică a respectivei cambii trebuie transmise sub condiția respectării autenticității şi integrității acestuia prin utilizarea oricăror procedee tehnice admise însă de lege. În acest sens, instituțiile de credit care aplică trunchierea vor agrea prin convenții, precizate de art. 46 alin. 5 din Legea nr. 58/1934 (articol nou introdus de O.U.G. nr. 39/2008), procedeele tehnice admise de lege, utilizate pentru a asigura autenticitatea şi integritatea imaginii cambiei şi ale informațiilor transmise.

În continuare avem trei seturi de reglementări în materie:

a) unele consacrate controlului şi garanțiilor cambiilor prin trunchiere prezentate la plată;

b) altele referitoare la modalitățile (procedurile) de prezentare la plată şi efectuarea plății, circulația cambiei trunchiate şi

c) refuzul de plată al cambiei trunchiate.

Potrivit art. 46^2 introdus prin O.U.G. nr. 39/2008 în Legea nr. 58/1934 cu modificările şi completările ulterioare, când prezintă la plată o cambie prin trunchiere, instituția de credit este obligată:

- să verifice dacă acea cambie în original respectă în formă şi conținut prevederile legale, inclusiv regularitatea succesiunii girurilor, cu excepția autenticității semnăturilor trăgătorului şi giranților;
- să garanteze acuratețea şi conformitatea informațiilor relevante pentru trunchiere transmise electronic, cu datele din cambia în original, precum şi conformitatea imaginii cambiei cu cambia în original. Este angajată şi răspunderea instituției de credit pentru orice pierdere suferită ca urmare a nerespectării obligațiilor de mai sus.

Care ar fi condițiile de formă şi conținut ce trebuie întrunite şi verificate la o cambie prezentată la plată prin trunchiere? Potrivit pct. 264^7, nou, din Normele nr. 7/2008, instituția de credit va verifica respectarea condițiilor de formă şi conținut, îndeosebi cele referitoare la valabilitatea titlului, cazurile de nulitate, eventualele modificări, completări sau alterări ale mențiunilor obligatorii, precum şi identitatea clientului şi dreptul acestuia de a cere plata sumei înscrise în cambie. Aceasta nu exonerează instituția de credit care plăteşte titlul sau pe tras de obligațiile sale, cu excepția celor care pot fi îndeplinite numai dacă se află în posesia cambiei originale.

Potrivit pct. 264^8 din aceleaşi Norme, instituția de credit care prezintă cambia la plată nu are obligația de a verifica sau de garanta valabilitatea semnăturilor înscrise pe cambie. În fine, când prezintă la plată o cambie prin trunchiere, instituția de credit are obligația să verifice acuratețea şi conformitatea cu cambia, ale informațiilor şi imaginii, înainte de a le transmite către instituția de credit care plăteşte cambia.

Majoritatea celor 11 noi puncte introduse după punctul 264 (264^1 – 264^{11}) din Norma nr. 7/2008 se referă la procedura de prezentare la plată a cambiilor prin trunchiere. Ansamblul reglementărilor este conținut de noile norme şi nu de O.U.G. nr. 39/2008. Se au în vedere următoarele aspecte:

- modalitățile de prezentare la plată a cambiilor prin trunchiere;
- rolul şi modul de aplicare a convențiilor încheiate între instituțiile de credit care recurg la procedeul trunchierii;

- în emiterea informațiilor relevante pentru trunchiere şi cele privind imaginea electronică a cambiei se respectă condițiile prevăzute de Legea nr. 58/1934 cu modificările şi completările ulterioare.

Astfel, cambiile pot fi prezentate la plată prin trunchiere în conformitate cu Regulile sistemului SENT, iar în cazul în care operațiunea de trunchiere nu se poate realiza, prin prezentarea acesteia la încasare, în original direct la instituția de credit trasă sau, după caz, la instituția de credit beneficiară conform procedurilor existente în convențiile încheiate între instituțiile de credit implicate (pct. 264^1 din Norma 7/2008) .

Atât Banca Națională a României, cât şi instituțiile de credit vor prezenta la plată prin trunchiere numai cambii acceptate de către tras pentru întreaga sumă înscrisă pe cambie. Nu se vor accepta de instituțiile menționate pentru prezentarea la plată prin trunchiere cambii care prezintă alterări, îndoiri, pete sau alte asemenea elemente care pot afecta vizibilitatea mențiunilor aflate pe titlul în cauză (pct. 264^2, Norma 7/2008).

Informațiile şi/sau imaginea cambiei trebuie să respecte condițiile stipulate de convențiile prevăzute la art. 46^1 alin. 5 din Legea nr. 58/1934, introdus prin O.U.G. nr. 39/2008. Aplicarea acestor convenții încheiate între instituțiile de credit fie în contextul unui aranjament de plată sau în vederea aderării lor la un sistem de plată, va fi adusă la cunoştința clienților săi de către fiecare instituție de credit, mai ales cât priveşte durata operațiunilor de prezentare la plată şi de efectuare a plății (pct. 264^3, Norma 7/2008).

Prevederile Legii nr. 58/1934 cu modificările şi completările ulterioare trebuie să fie respectate cât priveşte următoarele aspecte:

- producerea de informații relevante pentru trunchiere şi a imaginii electronice a cambiei;
- momentul recepționării informațiilor şi imaginilor este momentul în care acestea sunt puse la dispoziția instituției de credit care plăteşte cambia sau sunt înregistrate în sistemul de plăți.

În cazul prezentării la plată prin trunchiere, circulația cambiei originale pe suport hârtie se opreşte la instituția de credit care efectuează trunchierea, toate operațiunile care au loc între instituțiile de credit referitoare la prezentarea la plată, adică plată sau refuz de plată, având loc în cazul trunchierii numai în formă electronică.

b) Cât priveşte refuzul la plată a unei cambii prezentate cu trunchiere se coroborează prevederile art. 46^3, nou introdus în Legea nr. 58/1934 prin

O.U.G. nr. 39/2008 cu prevederile punctelor 264^{10} – 264^{11} din Norma nr. 7/2008 care completează normele cadrul nr. 6/1994 a B.N.R. în materie.

Astfel, refuzul total sau parțial la plată a unei cambii prezentate la plată prin trunchiere se face în formă electronică de către instituția de credit plătitoare.

Refuzul total sau parțial la plata cambiei este întocmit şi transmis în formă electronică de către instituția de credit căreia i-a fost cerută plata cambiei instituției de credit care a prezentat titlul la plată, fie direct, fie prin intermediul unui sistem de plăți, caz în care se apelează la convențiile prevăzute la art. 46^1 alin. 5 din Legea nr. 58/1934 cu modificările şi completările ulterioare.

Odată înregistrat refuzul la plată, instituția de credit care deține cambia originală va înscrie pe aceasta:

- data prezentării acesteia la plată spre a se constata dacă prezentarea s-a efectuat în cadrul termenului prevăzut la art. 41 din Legea nr. 58/1934 aşa cum a fost modificat prin O.G. nr. 11 din 4 august 1993 şi care fixează termene diferite după cum avem în vedere o cambie cu scadență fixă la o zi fixă sau la un termen de la data emisiunii sau cambia cu scadență la vedere;
- declarația de refuz datată şi semnată de către reprezentanții legali sau împuterniciți ai acestora. Mențiunile de mai sus înscrise pe cambia originală constituie dovada refuzului de plată.

O inovație a reglementărilor noi are în vedere şi regimul juridic al biletelor la ordin. Şi aceste titluri de valoare pot fi prezentate la plată prin trunchiere dacă îndeplinesc condițiile prevăzute de art. 104 şi 105 din Legea nr. 58/1934, respectiv cele pentru cambie de la art. 46^1 – 46^3 din O.U.G. nr. 39/2008, mai puțin condiția referitoare la acceptare prevăzută la art. 46^1 alin. 3^{18}, producând toate efectele pe care legea le recunoaşte biletului la ordin original.

Modificările legislației în materia cambiei şi a biletului la ordin, mai sus comentate, acoperă deci operațiunile ce urmează a se efectua cu titlurile de valoare cambia şi biletul la ordin prin mijloace electronice. Dispozițiile tranzitorii şi finale ale Normei nr. 7/2008 fixează termenele şi modalitățile de procesare a cambiei şi biletelor la ordin. Sistemul dualist cambie în

[18] Art. 46^1 din O.U.G. nr. 39/2008 şi pct. 262 din Norma nr. 7/2008;

original sau cambie trunchiată există, condițiile de procesare fiind clar precizate.

Concluzii

Convenția CNUDCI/UNCITRAL privind cambiile internaționale şi biletele la ordin internaționale – New York 1988 nu tratează cambia electronică, iar în termenii utilizați noțiunea de „înscris" nu este explicitată, doctrina considerând că este posibil orice mod de reproducere a cuvintelor, fie prin scriere de mână, dactilografiere sau imprimare[19]. Dar legislația națională în materie nu face această precizare. Și atunci se pune întrebarea dacă în condițiile unei cambii informatice nu cumva este incidentă nulitatea titlului pe motivul lipsei formatului de hârtie, ca sinonim al noțiunii de înscris, așa cum era conceput acesta la momentul intrării în vigoare a Legii nr. 58/1934, respectiv la data de 1 mai 1934[20]?

O altă problemă ce rezultă din emiterea unei astfel de cambii este aceea a semnăturii olografe a trăgătorului ca o condiție de validitate a titlului. Nu cumva este incidentă nulitatea titlului pe motivul lipsei semnăturii olografe a trăgătorului, așa cum era concepută aceasta la momentul intrării în vigoarea a Legii nr. 58/1934, respectiv la data de 1 mai 1934? Un nou răspuns nu a fost posibil decât odată cu intrarea în vigoare a Legii privind semnătura electronică, nr. 455/2001, care, în art. 5 pune semnul egal între forța juridică a semnăturii electronice extinse, cu cea olografă. Menționăm că dacă în materia cardurilor de plată sau de credit se recunoaşte valabilitatea semnăturii informatice prin tastarea codului personal pe un terminal, în domeniul cambial, semnătura informatică nu este posibilă decât cu modificarea Legii cambiei, situație care nu s-a realizat nici prin intrarea în vigoare a O.U.G. nr. 39/2008, care, potrivit art. 8 lit. b) reiterează obligativitatea semnăturii olografe a oricărui semnatar cambial[21].

---

[19]Art. 46^3 alin. 3 „Menţiunile înscrise pe cambia originală potrivit alin. 2 cu respectarea dispoziţiilor art. 49 alin. 1;

[20] Publicarea în M.Of. nr 100 și intrarea în vigoare a Legii 58/1934 privind cambia și biletul la ordin a avut loc la data de 1 mai 1934.

[21] Pentru opinia potrivit căreia titlul își păstrează valabilitatea pentru ca odată cu introducerea cambiei în sistemul automat de compensări interbancare identificarea trăgătorului devine certă, prin procedurile instituite de reglementările bancare și ale casei de compensări automate, a se vedea A. Bulearcă, *op.cit.*, p. 253;

În concluzie o cambie informatică nu este nici titlu de credit, nici cambie, dar constituie un instrument de plată, care, prin definiție este un înscris, pe suport hârtie sau electronic, prin intermediul căruia se urmărește efectuarea plăților și implicit stingerea obligațiilor[22].

[22] Pentru opinia potrivit căreia instrumentele de plată încorporează în structura lor o valoare exprimată în bani și permite titularului să primească o plată imediată, la cerere, a se vedea O. Căpățână, B. Ștefănescu, *Tratat de drept al comerțului internațional*, vol. I, Ed. Academiei RSR, București, 1987, p...; pentru deosebiri între instrumentele de plată și mijloacele de plată, a se vedea A. Bulearcă, *op.cit.*, p. 37.

I ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA” IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

UBER, CONTRACTUL DE ANTREPRIZĂ ȘI CĂLĂTORIA ÎN TIMP

UBER, SERVICE CONTRACT AND TIME TRAVEL

CODRIN MACOVEI[1]
MIRELA CARMEN DOBRILĂ[2]

Rezumat: Uber este o platformă tehnologică dezvoltată pentru a funcționa pe internet și care utilizează o aplicație *smartphone* care pune în legăturășoferi cu pasageri. Este un fenomen al afacerilorde astăzi. Uber (prescurtare pentru Uber Technologies Inc.) este o companie americană de închiriere a vehiculelor private cu sediul în San Francisco, California, Statele Unite ale Americii, care operează în peste 650 de orașe din întreaga lume. Ea creează piețe și operează aplicațiile mobile de transport și de livrare a alimentelor Uber. Șoferii de la Uber folosesc propriile mașini pentru a transporta pasageri, deși șoferii pot șiînchiria o mașină cu Uber. Uber susține că șoferii nu sunt angajați printr-un contract de muncă, ci că firma încheie cu aceștia un contract de antrepriză. Simplificând, Uber pretinde că vinde software și nu curse/deplasări cu autovehicule. Dacă ar fi adevărat, Uber tocmai a reușit revoluția de a întoarce contractul de antrepriză în perioada romană, când era cunoscut ca *locatio conductio operis faciendi*. La acea vreme, o varietate a contractului de locațiune –*conductiolocatio*. Dacă ar fi adevărat, atunci Uber tocmai a inventat modalitatea de a opera călătoria legii în timp... Acest articol își propune să afle dacă acest lucru este cu adevărat posibil.
Cuvinte cheie: Uber, antrepriză, contract de muncă, locațiune

Abstract: Uber is a internet technology platform using a smartphone app that connects driver-partners and riders. It is a modern business phenomenon.Uber (that is short for Uber Technologies Inc.) is an American private hire company headquartered in San Francisco, California, United States, operating in more than 650 cities worldwide. It develops markets and operates the Uber car transportation and food delivery mobile apps. Uber drivers use their own cars, although drivers can rent a car to drive with Uber. Uber claims that the drivers are not hired by an

[1] Lector univ. dr., Universitatea „Alexandru Ioan Cuza” din Iași, Facultatea de Drept, email: mcodrin@uaic.ro
[2]Asistent univ. dr., Universitatea „Alexandru Ioan Cuza” din Iași, Facultatea de Drept, email: mirela.dobrila@uaic.ro

employment contract but that the firm relates to them through a contract of service. Simply put, Uber pretends it sells software and not rides. If that were to be true Uber just succeeded the revolution of turning the service contract back in the roman times when it was known as the *locatio conductio operis faciendi*. At the time, a variety of the *locatio conductio* contract. Thus Uber just succeded in inventing the legal time travel *operarum*…This article is set to find out if this is really possible.
Keywords: Uber, employment contract, service contract, *locatio conductio*

1. Preliminarii – techviziunea asupra lumii anilor 2000

În secolul al XX-lea lumea era extrem de încrezătoare în continuarea avansului tehnologic și, chiar mai mult, în noi descoperiri care vor schimba cu totul fața planetei noastre[3]. Noile generații erau încurajate de sistemele de învățământ din statele dezvoltate și în curs de dezvoltare să își imagineze cum va arăta lumea anilor 2000 pentru a le dezvolta viziunea care urma să concretizeze inovația tehnologică. Omenirea spera că până în anii 2000 tehnologii cu totul noi vor fi descoperite și aplicate. Între ele un loc aparte îl ocupă cele care vizează transportul. De la navete spațiale, colonizarea altor planete și până la teleportare sau măcar mașini zburătoare, totul părea posibil. Astăzi, în anul 2017 știm, prea bine, că acest avans tehnologic nu s-a concretizat. Chiar dimpotrivă, în ceea ce privește transportul aeronautic, de la care se așteptau cele mai notabile progrese, înregistrează astăzi timpi de realizare a curselor inferiori anilor 1950[4]. Astfel, de exemplu,durata unui zbor de la New York la Los Angeles este astăzi cu aproape 40 de minute mai lungă decât în anii 1967[5], deși tehnologia motoarelor avioanelor a suferit două transformări majore (propulsie cu elice, propulsia prin reacție,

[3]A se vedea și L. Davis, *How our predictions for the Year 2000 changed throughout the 20th Century*, articol publicat pe site-ul Gizmodo, 5 decembrie 2012, [Online] la: https://io9.gizmodo.com/5908600/how-our-predictions-for-the-year-2000-changed-throughout-the-20th-century; A. Swanson, *What people in 1900 thought the year 2000 would look like?*, articol publicat în ziarul Washington Post, 4 octombrie 2015, [Online] la: https://www.washingtonpost.com/news/wonk/wp/2015/10/04/what-people-in-1900-thought-the-year-2000-would-look-like/?utm_term=.2b65110b35c5,accesat 30.11.2017.

[4] H. Morris, *Why are flight times longer than they were 40 years ago?*, articol publicat în ziarul The Telegraph, 6 ianuarie 2017, [Online] la: http://www.telegraph.co.uk/travel/news/why-flight-times-are-getting-longer-fuel-flying-slower/,accesat 30.11.2017.

[5] Un documentar care explică aceste diferențe și sub aspect tehnic sub titlul *Why dont planes fly faster* poate fi accesat pe Youtube [Online] la:https://www.youtube.com/watch?v=n1QEj09Pe6k, accesat 30.11.2017.

turboventilatorul) de la cel de-al doilea război mondial până astăzi[6]. Una dintre cauzele vehiculate pentru a explica acest rezultat este că progresul tehnologic a fost folosit de companiile aeriene pentru maximizarea profitului (aceeași viteză sau viteză inferioară cu consum mai mic de combustibil rezultă în eficientizarea costurilor) și nu pentru reducerea timpului de zbor, ceea ce, de altfel, a permis și apariția companiilor ce oferă curse aeriene *low cost*[7].

Cu toate acestea, ceva este pe cale să se schimbe în modul în care funcționează lumea în care trăim. Doar că nu este vorba neapărat despre evoluția *hardware*-ului, ci, mai ales, despre revoluția *software*-ului[8]. Iar aceasta se întâmplă, în primul rând, datorită expansiunii internetului.

Se susține de cel puțin 10 ani că „*Software*-ul devorează lumea”[9]. Această afirmație extraordinară a devenit mantra antreprenorilor din industria IT de oriunde de pe glob, codificând o nouă filozofie de tech-antreprenoriat și o nouă eră de îndrăzneață creație. Analiza sloganului indică următoarele: ingineri de software sunt constructorii lumii noi în care trăim și mai ales vom trăi. Ultima generație de antreprenori tech sunt creatorii sistemelor de operare sociale pentru societățile și economiile viitorului. Reconfigurând relațiile dintre bunuri, consumatori și furnizori de servicii, aceste noi sisteme de operare socială înghit piețe întregi cum ar fi recrutarea, companiile de taximetrie, lanțurile hoteliere, agenții imobiliari etc.

Un sistem de operare este un software de nivel scăzut, care rulează pe un computer și direcționează operațiunile sale. La fel cum sistemul de

[6]A se vedea și S. Dowling, *The Soviet Unions Flawed Rival to Concorde*, 20 octombrie 2017, articol publicat pe site-ul BBC Future, [Online] la: http://www.bbc.com/future/story/20171018-the-soviet-unions-flawed-rival-to-concorde,accesat 30.11.2017.

[7]A se vedea J. Glancey, *Concorde: The Rise and Fall of the Supersonic Airliner*, Atlantic Books, London, 2015, *passim*;S. Dowling, *How Do You Bring An Aircraft Back From The Dead*, 25 septembrie 2015, articol publicat pe site-ul BBC Future, [Online] la: http://www.bbc.com/future/story/20150925-how-do-you-bring-an-aircraft-back-from-the-dead,accesat 30.11.2017.

[8]A se vedea și raportul *Deep Shift: 21 Ways Software Will Transform Global Society*, realizat de World Economic Forum în anul 2015, [Online] la: http://www3.weforum.org/docs/WEF_GAC15_Deep_Shift_Software_Transform_Society.pdf, accesat 30.11.2017.

[9]M. Andreessen, *Why Software Is Eating the World*, articol publicat în ziarul The Wall Street Journal, 20 august 2011, [Online] la: https://a16z.com/2016/08/20/why-software-is-eating-the-world/, accesat 30.11.2017.

operare al calculatorului organizează resursele hardware ale unității de calculator, creând o mașină funcțională, sistemele de operare socială rearanjează „hardware-ul“ realității umane, legând oameni și lucruri în moduri noi și productive.

Câteva exemple: Airbnb pune oameni care au camere de închiriat în contact cu turiștii ce caută cazare pe termen scurt. Uber și Lyft pun pasagerii în căutarea unei plimbări în contact cu șoferi în căutarea unui câștig. TaskRabbit leagă oameni la un univers de micro-antreprenori care sunt gata ca pentru a încasa comisioane lor să curețe casele, să cosească peluza lor, să repare țevile etc., etc.

Structurile sociale și economice construite peste secole sunt reproiectate rapid de pasionații și curajoșii tineri din domeniul IT.

Poate suna tentant pentru beneficiarii direcți și, în spiritul justiției sociale, pentru publicul larg, dar este totodată un proces început de mai mult timp.Internetul și comunicațiile au făcut poșta clasică aproape irelevante când a devenit largrăspândit e-mailul, antrenând și acuzații de șomaj, taxe mai mici încasate la buget, „concurență neloială”. Sigur, nu mai trimite nimeni scrisori, însă a apărut comerțul online iar comenzile nu pot fi livrate tot online. Așa s-au dezvoltat companiile de curierat, care au ajuns la volume de afaceri de neimaginat înainte, în timp ce serviciile poștale clasice se zbat în pragul falimentului. În mod identic, munca voluntară și colaborarea celor cu resurse imaginative a făcut ca în zona internetului lucrurile să se ducă încă de la început în direcția asta. Așa a apărut Linux, un sistem de operare care a ocupat mai întâi piața serverelor. Azi, peste 80% din internet funcționează pe baza unui soft care nu costă nimic. Pe piața utilizatorilor finali, Linux părea să nu aibă nici o șansă în fața Windows-ului de la Microsoft. Însă totul s-a schimbat când tehnologia a migrat spre mobil. Google a simțit trendul, a adoptat Linux-ul și l-a ramificat în ceea ce cunoaștem azi drept Android. Windows mobil e acum o chestie exotică, pentru care prea puțini doresc să scrie aplicații.

Există motive deci să ne simțim încântați de această nouă generație de start-up-uri. Acestea creează noi oportunități. Acestea permit persoanelor care au nevoie de servicii să găsească oameni gata să le ofere. Acestea activează resursele latente ale unei comunități –locuințe la schimb, mașini nefolosite, unelte uitate în boxe - crearea de noi piețe pentru închirierea și utilizarea în comun, precum și noi linii de venit pentru micro-antreprenori. Sigur, ele perturbează status quo-ul:companiile care dețin sistemele de

operare sociale sunt deja evaluate în milioane și miliarde. Aceia dintre ei care și-au dat seama cum să monetizeze invențiile lor au creat motoare extrem de profitabile de creștere economică. Iar acest lucru a schimbat piața bursieră din SUA. Dacă până la finalul anilor 1990 vedetele pieții erau General Electric, General Motors, companiile petroliere, Wallmart, astăzi ele sunt Apple, Alphabet (Google), Facebook, Twitter, Microsoft, Airbnb, Uber, Lyft, Whats Up. Din punctul de vedere al capitalizării de piață, majoritatea acestor exemple reprezintă nu un succes, ci un adevărat miraj financiar pe care puține persoane l-au putut intui[10].

Totuși, din dialogul contemporan asupra acestor evoluții viziunea critică pare a lipsi, sau măcar a se califica ca retrogradă în raport cu noua așezare a lumii. Noile sisteme de operare socială demolează industrii deja existente, precum distrug și locuri de muncă și vieți în acest proces. În timp ce creează noi locuri de muncă, putem observa că acestea nu sunt aceleași locuri de muncă în aceleași industrii. Având o perspectivă mai largă cu privire la implicațiile acestor evoluții, ne-am putea întreba dacă experți tech tineri sunt într-adevăr cei mai buni oameni pentru a fi reformularea sistemelor sociale. Ne îndreptăm rapid într-o lume care este configurată de proiectare *software*. Noi nu am experimentat o astfel de lume înainte. Nu avem nici o idee despre ce fel de probleme de aceste noi modele vor crea. Vor servi sistemele de reputație socială ca substitute de încredere pentru protecția de consumatorilor? Răspunsul este neclar. Același lucru este valabil și pentru protecția lucrătorilor.

Poate doar atunci când noile sisteme de operare sociale vin în conflict cu deciziile politice se poate observa o îngrijorare mai mare în privința efectelor nedorite. De exemplu, audierile comisiei Congresului american care anchetează modul în care alegerile pentru președintele țări ar fi putut fi influențate prin intermediul Facebook, Twitter și Google au dezvăluit întregii lumi răspunsuri ezitante din partea celor trei companii și concluzia subiectivă că nici una dintre ele nu este în poziția de a controla în mod efectiv softul pe care l-a dezvoltat[11].

În ceea ce ne privește însă, o anumită viziune asupra dreptului și eticii ne-a atras în mod deosebit atenția. Este vorba despre soluția *software*pe

[10]M. Andreessen, *op. cit., passim.*

[11]A se vedea, pentru dezvoltări, S. Matei, *Puterea dumneavoastră ne lasă fără respirație*, articol publicat pe blogul personal în 8 noiembrie 2017, [Online] la: http://sorinamatei.ro/puterea-dumneavoastra-ne-lasa-fara-respiratie/,accesat 30.11.2017.

care Uber a dezvoltat-o pentru a „revoluționa” modul în care transportul individual se desfășoară. În plus, la această dată Uber reprezintă cel mai valoros *start-up* al planetei fiind evaluată la o valoare de piață de 70 miliarde de dolari! Prezentul articol încearcă să înțeleagă acest model din perspectiva creatorului său și nu își propune o analiză exhaustivă a activității Uber, care ar trebui să investigheze și perspectiva juridică, cel puțin, a clienților transportați prin aplicația dezvoltată de Uber.

2. Uber – un fenomen al lumii moderne

Uber a fost înființat în Statele Unite ale Americii în anul 2009, iar aplicația *smartphone* - instrumentul prin care operează serviciile sale („aplicația”) - a fost lansată în 2010 în SUA. În anul 2016 directorul executiv al lui Uber de la acel moment, dl. Travis Kalanick, a descrie afacerea sa în următorul mod: „Uber a început activitatea ca un serviciu de limuzine de lux pentru 100 de prieteni în San Francisco - șoferulpersonal al tuturor. Astăzi suntem o rețea de transport care acoperă 400 de orașe din 68 de țări care transportă alimente și pachete, precum și oameni, totul fiind posibil prin atingerea unui buton ;am evoluat de la un serviciu de lux la un lux accesibil, la o opțiune de transport zilnică pentru milioane de oameni”.

Uber oferă o gamă largă de servicii, pentru un singur călător sau pentru un grup de persoane, de la mașini simple și până la un serviciu de limuzine executiv. Uber oferă, în principiu, cinci niveluri de servicii:

- UberX este cea mai ieftină și cea mai comună formă de Uber;automobilele sunt obișnuite și pot transporta până la patru pasageri; vehiculele trebuie să fie nu mai vechi de anul 2000;tarifele sunt de obicei jumătate din tarifele unui taxi în același oraș;
- UberPOOL, oferit în unele orașe, permite călătoria cu o altă (alte) persoană și împărțirea costului;
- UberXL este un serviciu care poate transporta 6 pasageri cu un SUV sau un minivan; este mai scump decât UberX;
- UberSelect oferă sedanuri de lux cu interior din piele, inclusiv mărci precum Audi, Mercedes, BMW;tariful este premium;
- UberBLACK este serviciul de limuzină de lux cu vehicule dedicate serviciilor de nivel executiv.

De la lansarea sa mondială în 2012, Uber a devenit cea mai recunoscută alternativă la serviciile de taxi tradiționale. Conducătorii auto Uber nu dețin licențe speciale de transport; ei folosesc vehiculele lor

personale pentru a oferi curse ieftine. Comenzile curselor și plata lor sunt toate manipulate printr-o aplicație *smartphone*, iar clientul nu are nevoie să plătească cu numerar (banii sunt luați automat de pe cardul său bancar) sau să ofere sfaturi pentru conducătorul auto Uber privind traseul de urmat (aplicația determină traseul care trebuie urmat strict de șofer sub pedeapsa penalităților).

Șoferii Uber nu pot accepta curse solicitate în direct de pe stradă, ci doar comenzi făcute prin aplicație, motiv pentru care Uber susține că nu este exact un furnizor de servicii tip taxi. În schimb, Uber susține că este un fel de serviciu de închiriere auto care se bazează pe tehnologia *smartphone*, serviciu care are în plus responsabilitatea alegerii traseuluișia încasăriicontravalorii cursei efectuate.

Uber solicită titularilor de cont (celor care își descarcă aplicație pe *smartphone*) să aibă vârsta de 18 ani sau mai mult.

Uber este gândit să fie mai ușor de utilizat decât serviciile de taxi.

Practic, procesul Uber constă în următorii pași:

- se instalează aplicația pe telefonul *smartphone* și se creează un cont online Uber; o carte de credit este obligatoriu să fie atașată contului, astfel încât clientul nu are nevoie să gestioneze niciun fel de numerar;
- când clientul are nevoie de o deplasare cu autovehiculul, utilizează aplicația pentru a comunica către Uber locația de preluare; telefonul cu GPS poate prelua automat această sarcină; există, de asemenea, alternative de mesaje text și de site-uri mobile pentru utilizarea aplicației;
- Uber trimite un text pentru a confirma câte minute trebuie clientul să aștepte; în general curseleau în mod frecvent un timp de așteptare de 3-10 minute în centrul orașelor unde Uber operează;
- Uber trimite un mesaj text când șoferul sosește la locul indicat pentru preluarea clientului; aplicația Uber va afișa, de asemenea, detalii despre șofer, numele și fotografia acestuia și tipul de mașină pe care o conduce;
- clientul Uber are opțiunea de a partaja cursa cu oricare alte persoane sau alți utilizatori Uber cu care poate, de asemenea, împărți electronic tariful;
- plata se face automat, la finalul cursei, fără să fie nevoie o acțiune a clientului, Uber luând costul cursei din contul cardului bancar;

- după efectuarea cursei, clientul evaluează șoferul pe o scară de la 1 la 5 pentru calități precum politețe, siguranță, curățenie;în mod similar, șoferul evaluează la rândul său clientul pe o scară de la 1 la 5 pentru politețea sa; clienții au acces la ratingul Uber al șoferului și pot gestiona cursele pe baza acestuia; șoferii nu au un drept similar în privința ratingului clienților.

Experiența Uber este proiectată să fie foarte simplă și convenabilă, având și opțiunea de urmărire a feedback-ul clientului.

Succesul Uber se datorează prețului practicat pentru curse, standardelor de calitate și comodității oferite de utilizarea aplicației *software*.

Uber își reduce tarifele cu până la 50% față de serviciile taxi. Acesta este unul dintre motivele majore pe care clienților le place să le folosească Uber.

În plus, clienții comentează că mașinile Uber sunt mai curate, mai noi și au mirosuri mult mai plăcute decât mașinile pe care le folosesc frecvent șoferii de taxi.

Clienții Uber susțin că le place confortul plății automate, că nu pot fi păcăliți prin alegerea unui traseu mai lung și că beneficiază și de curse gratuite din partea Uber. Acest lucru le este mult mai plăcut decât să se confrunte cu șoferii de taxi nepoliticoși care cer bani cash, astfel încât să poată ocoli taxele bancare aferente utilizării cărților de credit.

Uber se ocupă de toate aceste detalii printr-o aplicație convenabilă pentru *smartphone*, totul costând numai o fracțiune din costul curselor companiilor de taxi tradiționale.

Astfel, modelul Uber de a transporta pasageri este foarte amenințător pentru companiile tradiționale de taxi, care până acum au avut monopolul pieții călătorilor.

În timp ce tarifele variază în funcție de oraș și de ora din zi, există date publice substanțiale care arată că o călătorie cu UberX poate fi cu 25% până la 50% mai ieftină decât luarea taxiului local. Cu toate acestea subliniem că Uber impune prețuri majorate (*surge pricing*) pentru evenimentele de vârf, cum ar fi meciurile sportive importante și Revelionul, când taxele de călătorie pot crește de două până la cinci ori pentru anumite

intervale orare[12]. De regulă, însă, cursele de la Uber sunt mai ieftine decât cele de taxi.

De asemenea, Uber nu acceptă și nu încurajează bacșișul; orice sumă cu titlu gratuit adăugată de clientul binevoitor peste costul călătoriei determinat de aplicație este considerată de aceasta ca făcând parte din costul călătoriei plătită cu cardul de credit.

Deoarece Uber este atractiv și pentru șoferi, numărul de șoferi disponibili este mare iar aceștia are au de obicei un timp de răspuns foarte rapid. În timp ce acest lucru variază cu siguranță de la oraș la oraș, șoferii de la Uber descriu că își iau clienții în 3-10 minute de la apelare, în timp ce taxiurile au un timp mai mare de răspuns.

Deoarece șoferii Uber sunt evaluați de fiecare pasager în fiecare zi, există stimulentul să fie atât prompți cât și politicoși.

Clienții citează, de obicei, printre motivele pentru care aleg Uber timpul scurt de așteptare și plățile facile fără elemente personale[13].

Uber este un model de afaceri excelent[14]; o evoluție rapidă pentru monopolul de calitate scăzută al taxiurilor. Uber dorește să ofere clienților o experiență convenabilă, la prețuri accesibile și curate, și să înlăture dificultatea efectuării plăților în numerar și bacșișului.

Totuși analiza financiară a modelul de afaceri oferă anumite surprize. Uber nu a făcut nici un profit pe toată durata existenței sale. Mai mult decât atât,pierderile anuale ale companiei sunt imense, iar majoritatea analiștilor economici nu înțeleg cum această companie reușește să convingă investitorii să contribuie la ... o gaură neagră: doar pentru anul 2016 pierderile sunt mai mari de 2,8 miliarde de dolari, iar pentru 2017 ele se anunță și mai mari[15]. Pe baza înregistrărilor evoluțiilor tuturor companiilor

[12]Presa semnalează și tarife mai mari, a se vedea, de exemplu, R. Felton, *Uber Charges Passenger Clueless About Surge Pricing $925 For Ride*, articol publicat pe site-ul Jalopnik în 10 februarie 2017, [Online] la: https://jalopnik.com/uber-charges-passenger-clueless-about-surge-pricing-92-1819053368,accesat 30.11.2017.

[13]J.P. Pullen, *Everything You Need to Know About Uber*, articol publicat în revista Times, 4 noiembrie 2014, [Online] la: http://time.com/3556741/uber/, accesat 30.11.2017.

[14]Valoarea de piață de 70 miliarde de dolari o confirmă indubitabil.

[15]Pentru analiza modelul de bussines al companiei și șansele sale de reușită, a se vedea următoarele articole și bibliografia indicată de acestea: R. Felton, *Uber Is Doomed*, articol publicat pe site-ul Jalopnik în 24 februarie 2017, [Online] la: https://jalopnik.com/uber-is-doomed-1792634203; E. Newcomer, *Uber, Lifting Financial Veil, Says Sales Growth Outpaces Losses*, articol publicat pe site-ul Bloomberg în 24 februarie 2017, [Online] la:

americane din 1950 până în prezent și a nivelurilor de venituri ale Uber, probabilitatea ca Uber să realizeze vreodată câștiguri din prezenta sa activitate se situează între 0,1% și 25%, folosind tabele statistice de la Credit Suisse[16].

3. Uber - calificarea juridică a raporturilor sale cu șoferii

Uber pretinde că este o companie care produce *software* iar conducătorii auto sunt antreprenori. Această calificare juridică a raporturilor dintre Uber și șoferi a dat naștere unor controverse juridice.Mai întâi în SUA, unde în 2015, un judecător din California[17] nu a fost de acord cu acest lucru și a hotărât că șoferii Uber sunt într-adevăr angajați care merită beneficii și drepturica angajați.Această decizie este actualmente urmată de alte decizii în alte state americane și în întreaga lume, reprezentându-n obstacol major pentru Uber ale cărui operațiuni se bazează pe costuri reduse și pe șoferi independenți. Calificarea Uber ca angajator și nu ca antreprenor general, ar putea să obliga compania să cheltuiască milioane de dolari pentru a oferi beneficii sociale și asigurări de sănătate șoferilor săi.

În privința viziunii juridice a Uber o altă cauză, mai recentă este însă mai relevatoare. Este vorba despre Aslam, Farrar & others vs. Uber BV, Uber London Ltd. și Uber Britannia Ltd., cauză judecată de Tribunalul muncii din Londra[18].Reclamanții au cerut instanței să constate că au calitatea de angajați ai Uber și că beneficiază de drepturile minimale garantate de legislația engleză aplicabilă (Employment Rights Act 1996, National Minumum Wage Act 1998 și Working Time Regulations 1998).

---

https://www.bloomberg.com/news/articles/2017-04-14/embattled-uber-reports-strong-sales-growth-as-losses-continue,accesat 30.11.2017.

[16]Pentru mai multe amănunte, a se vedea, B. Ryder, *Firms that burn up $1bn a year are sexy but statistically doomed*, articol public în ziarul The Economist, 21 octombrie 2017, [Online] la:https://www.economist.com/news/business/21730446-five-outliers-chesapeake-energy-netflix-nextera-energy-tesla-and-uber-have-collectively,accesat 30.11.2017.

[17]Uber vs. Berwick, Superior Court of California, State of San Francisco, case number CGC-15-546378/16.07.2015, textul hotărârii este disponibil [Online]la: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1988&context=historical,accesat 30.11.2017.

[18]Aslam, Farrar & others vs. Uber BV, Uber London Ltd. și Uber Britannia Ltd, Employment Tribunals, London, Case number 2202550/2015, soluționat pe dat de 26 octombrie 2016, [Online] la: https://www.judiciary.gov.uk/wp-content/uploads/2016/10/aslam-and-farrar-v-uber-reasons-20161028.pdf; mai multe amănunte despre proces și hotărârea tribunalului londonez sunt disponibile pe site-ul: https://www.judiciary.gov.uk/judgments/mr-y-aslam-mr-j-farrar-and-others-v-uber/.

Instanța engleză a reținut că șoferii Uber din Marea Britanie nu aveau nicio obligație să activeze aplicația și chiar reclamanții au acceptat că nu există niciun contract cadru încheiat cu Uber. Totuși, instanța engleză a considerat că din momentul în care aplicația a fost pornită de către șofer următoarea calificare juridică a raporturilor dintre părți trebuie să se aplice: „... orice conducător auto care (a) are aplicația pornită, (b) se află pe teritoriul în care este autorizat să lucreze ... și (c) este capabil și dispus să accepte curse, este, pentru atâta timp cât aceste condiții sunt îndeplinite, angajat Uber pe baza unui contract de muncă..."[19]

Pentru a ajunge la această concluzie, ET a comentat că orice organizație: „... (a) în centrul căreia se regăsețeobligația de a transporta persoane în autoturisme de la locul unde sunt acolo unde doresc și (b) operează parțial prin intermediul unei societăți care îndeplinește responsabilitățile reglementate ale unui operator de transport, dar (c) solicitând conducătorilor auto și pasagerilor să consimtă pe o bază contractuală că nu furnizează servicii de transport și (d) recurgând în contractele sale la ficțiuni, limbaj răstălmăcit și chiar terminologie inventată, … trebuie tratată cu un anumit scepticism"[20].

Mai precis, instanța engleză a respins poziția Uber că nu este în afaceri ca furnizor de servicii de transport, concluzionând că produsele sale vorbesc de la sine. Astfel, Uber oferăo varietate de servicii de transport pe care reclamanții cu siguranță nu le pot oferi ei înșiși, iar marketingul Uber, în mod evident, nu se face în beneficiul unui conducător auto individual. La fel de evident a fost pentru instanța engleză că marketing Uber se face pentru a promova numele Uber și pentru ca acesta să își poată vinde serviciile de transport.

În acest sens, instanța engleză a făcut referire la cauza Douglas O'Connor împotriva Uber Technologies Inc (cauza 3: 13-cv-034260EMC), din 11 martie 2015, în care Tribunalul Districtual din Carolina de Nord a respins afirmația Uber că este o societate care produce tehnologie și nu activează în domeniul furnizării de servicii de transport[21].

[19]Considerentul nr. 86 din Aslam, Farrar & others vs. Uber, *loc. cit.*

[20]Considerentul nr. 87 din Aslam, Farrar & others vs. Uber, *loc. cit.*

[21]Considerentul nr. 89 din Aslam, Farrar & others vs. Uber, *loc. cit.* - „Uber does not simply sell software; it sells rides. Uber is no more a *tehnology company* than a Yellow Cab is a *tehnology company* because it uses CB radios to dispatch taxi cabs".

Instanța engleză a mai concluzionat că Uber a redactat un contract cu șoferii săi în care termenii generali contractuali pe care se bazează nu corespund cu realitatea practică:„Ideea că Uber din Londra este un mozaic de 30.000 de întreprinderi mici legate de o platformă comună este în mintea noastră o susținere ușor ridicolă”[22].

Pentru instanța engleză următoarele puncte au fost relevante pentru stabilirea calității de angajați a șoferilor:

- șoferului i se face cunoscut numele pasagerului, dar nu șiprenumele;
- șoferul nu cunoaște destinația pasagerului până când pasagerul nu a intrat în mașină;
- Uber se așteaptă ca șoferul să urmeze ruta așa cum este sugerată de aplicație, iar orice deviere de la această rută trebuie să fie justificată de șofer;
- calculul tarifului se face de către Uber, deși șoferul poate percepe o taxă mai mică, dar nu mai mare decât cea sugerată;
- Uber poatediminua plățile șoferilor dacă pasagerii se plâng că au fost supratаxați;
- conducătorii auto trebuie să se prezinte în persoanăîmpreună cu documentele lor la Uber înainte de a fi acceptați ca șoferi Uber, ceea ce echivalează cu susținerea unui interviu de angajare;
- conducătorii auto furnizează propriile vehicule și le întreține;
- șoferii nu au libertatea de a schimba date de contact cu pasagerii;
- conducătorii auto care refuză 3 călătorii la rând, pot fi deconectați forțat din aplicație timp de 10 minute;
- conducătorii auto pot lucra pentru alte organizații, precum și pentru Uber;
- Uber nu oferă nici o îmbrăcăminte sau uniformă.

În final, tribunalul englez a decis că reclamanții șoferi sunt angajați ai Uber reținând următoarele argumente principale:

- nici un șofer nu era în poziția de a-și dezvolta propria afacere și nici nu primea de la Uber un astfel de ajutor;
- contractul presupus a se derula între conducătorul auto și pasager este o pură ficțiune care nu avea nicio legătură cu realitățile juridice și relația dintre părți;

[22]Considerentul nr. 90 din Aslam, Farrar & others vs. Uber, *loc. cit.*

- nu este îndreptățit să considerăm că Uber funcționează pentru a servi interesele șoferilor - singura interpretare posibilă este că relația funcționează invers;
- șoferii au oferit munca lor pentru Uber în temeiul unei relații contractuale; șoferii și-au pus la dispoziție serviciile pentru a transporta pasagerii de la Uber spre destinația lor pentru o plată în bani.

În final, interesant este faptul că instanța londoneză a reținut că niciunul dintre raționamentele Uber nueste în sine fals și că pe baza lor ar putea fi conceput un model în care șoferii nu sunt angajați însă tocmai acest model nu a atins prin relațiile contractuale concretizate de Uber cu șoferii.

Ceea ce transpare din decizia tribunalului londonez este, fără putință de tăgadă, că Uber a creat propria realitate juridică, complet desprinsă de realitatea a ceea ce cere de la șoferi. În plus, de-a lungul timpului a modificat cu bună știință terminologia juridică pentru a zădărnici orice calificare juridică facilă a raporturilor cu șoferii. Astfel, termenii de antreprenor și client, independență și control al activității au fost în totalitate îndepărtați din contracte pentru a fi înlocuiți cu termeni ajuridici.

Împotriva acestei decizii a fost admis apelul Uber, un an mai târziu. Decizia din apel menține neschimbată prima decizie a instanței[23] deși se poate observa o schimbare de tactică a apărării Uber în sensul argumentării calității de agent a sa față de șoferi. Instanța a respins vehement această apărare. Se mențin și aprecierile instanței de fond care caracteriza contractele Uber ca fiind: „dense legal documents couched in impenetrable prose”[24].

Din perspectiva dreptului român ceea ce dorește Uber să realizeze din punct de vedere juridic este confundarea contractului de muncă cu conținutul contractului de antrepriză.

Principalul element care diferențiază contractul de antrepriză de contractul de muncă este acela că, în timp ce în baza contractului de muncă se naște un raport de prepușenie, în temeiul căruia angajatorul răspunde față

[23]Uber B.V. and Others v Mr Y Aslam and Others, Employment Appeal Tribunals, London, case number UKEAT/0056/17/DA, soluționat pe data de 10 noiembrie 2017, [Online] la: https://assets.publishing.service.gov.uk/media/5a046b06e5274a0ee5a1f171/Uber_B.V._and_Others_v_Mr_Y_Aslam_and_Others_UKEAT_0056_17_DA.pdf; mai multe amănunte despre proces și hotărârea tribunalului londonez [Online] la: https://www.gov.uk/employment-appeal-tribunal-decisions/uber-b-v-and-others-v-mr-y-aslam-and-others-ukeat-0056-17-da.

[24]Considerentul nr. 73 din Uber B.V. and Others v Mr Y Aslam and Others, *loc. cit.*

de terți pentru faptele păgubitoare ale persoanelor încadrate în muncă precum un comitent pentru prepușii săi, în cazul contractului de antrepriză nu se naște un astfel de raport, antreprenorul având independență juridică în executarea lucrării, iar clientul nerăspunzând de prejudiciile create de antreprenor terților. Antreprenorul poate, deci, să angajeze lucrători și subantreprenori, fără consimțământul clientului, situație care nu ia în vedere cazul salariatului, care își desfășoară activitatea doar în limitele celor permise de angajator și nu poate lua decizii de ordin administrativ fără acordul acestuia, așa cum poate antreprenorul, fără acordul beneficiarului.

De asemenea, în cazul contractului de muncă, salariul angajatului se plătește după cantitatea și calitatea muncii depuse, conform fișei postului pentru meseria, profesia sau funcția respectivă. În situația antreprizei, antreprenorul va primi prețul numai în funcție de rezultatul muncii sale, predat clientului.

Un alt element care diferențiază cele două contracte este acela că în timp ce, în contractul de muncă, munca reprezintă cauza contractului, în cazul contractului de antrepriză, munca prestată de antreprenor este accesorie scopului stabilit cu clientul, adică rezultatul lucrării. Având în vedere aceste divergențe între cele două contracte, spre deosebire de contractul de antrepriză care are sediul de drept comun în C.civ., la care se adaugă reglementările legale speciale, contractul de muncă este supus regulilor speciale ale dreptului muncii, făcând obiectul de reglementare al Codului muncii și al altor acte normative speciale.

În ceea ce privește antreprenorul, acesta poate avea calitatea de profesionist sau de simplu subiect de drept civil, în timp ce salariatul nu are, prin definiție, calitatea de profesionist.

Se mai impune a fi reliefat elementul care diferențiază cele două contracte, desprins și din literatura de specialitate[25], respectiv riscul în cele două contracte. Astfel, în privința salariatului nu se pune niciodată în discuție problema răspunderii pentru riscuri.

În lumina acestor precizări credem că devine evident Uber dorește să aibă toate drepturile din contractul de muncă (în calitate de angajator) și toate obligațiile din contractul de antrepriză (în calitate de client). În fapt, ceea ce dorește să realizeze Uber din punct de vedere juridic este nesocotirea

[25]M.-L. Belu Magdo, *Reglementarea contractului de antrepriză în actualul Cod civil*, în R.D.C. nr. 5/2012, p. 12.

cu totul a elementelor de distincție între antrepriză și contractul de muncă. Uber, practic, a întors contractul de antrepriză la originile sale romane, când acesta era o varietate a locațiunii (*locatio conductio operis faciendi*). Tot o varietate a locațiunii era, de altfel și contractul de muncă (*locatio conductio operarum*), diferența dintre cele două stabilindu-se astfel: contractul de muncă prevedea pentru locatar o obligație de mijloace (prestarea unei munci), iar antrepriza un contract care prevedea pentru locatar o obligație de rezultat – realizarea unei lucrări determinate. Cum efectuarea unui transport însemna și pentru romani dificultăți de calificare între cele două contracte a apărut *Lex Rhodia de jactu* (aprox. 475 î. d. Ch.) care organizează contractul de transport într-o manieră modernă și mai ales valabilă până în zilele noastre. Când atât antrepriza, cât și contractul de muncă nu mai sunt varietăți ale locațiunii fiindcă nu mai putem folosi nici serviciile și nici munca unei persoane[26]. Pur și simplu societatea a evoluat și odată cu ea și concepțiile juridice care îl pun pe antreprenor sau pe *locator operis* în puterea folosinței locatorului…Din acest punct de vedere, putem spune că demersul Uber a reușit întru-totul călătoria în timp: a plasat termenii juridici oferiți șoferilor doritori de înrolare pe platforma sa prin anul 1.000 î. d. Ch.

4. Uber – calificarea etică a viziunii sale

În măsura în care suntem de acord cu calificarea juridică a raporturilor dintre Uber și șoferi mai sus efectuată, ne putem întreba în ce măsură reprezintă manipularea acestora doar un banal exemplu de lăcomie, fie el și experimentat la scară planetară. În ce ne privește lucrurile ar putea fi observate într-un orizont mai larg. Ontologia Silicon Valley poate fi însumată în fraza: „Hack totul!“. Potrivit CEO-ului Facebook, Mark Zuckerberg, „Hackerii cred că ceva poate fi întotdeauna mai bun, și că nimic nu este niciodată complet. Ei trebuie doar să găsească versiunea mai bună – demulte ori în fața oamenilor care spun că este imposibil sau sunt mulțumiți cu *status quo*-ul”[27]. Aparent, calea hackerului este atrăgătoare. Cine nu vrea să se joace cu alternative creative și să exploreze posibilitatea de a face

[26]Pentru mai multe amănunte, a se vedea, V.M. Ciucă, *Drept roman. Lecțiuni*, vol al II-a, Editura Universității „Alexandru Ioan Cuza”, Iași, 2014, p. 479 și urm.

[27]T. Rayner, *Heidegger In Silicon Valley: Technology And The Hacker Way*, articol publicat pe blogul PHILOSOPHY FOR CHANGE, 1 septembrie, 2014, [Online] la: https://philosophyforchange.wordpress.com/2014/09/01/heidegger-in-silicon-valley-social-operating-systems-technological-enframing-and-the-hacker-way/,accesat 30.11.2017.

lucrurile mai bine? Modul hacker are sens perfect atunci când este aplicat la piese de mașini, plăcile cu circuite și cod. Aplicat la realitatea socială are implicații ontologice alarmante. Tratarea realității ca materie primă ce urmează a fi piratată schimbă modul în care ne gândim la ea. Realitatea apare ca un câmp neutru de resurse care pot fi mișcate, decuplate, recuplate, exploatate, redefinite. Este ca și cum lumea ar fi doar un câmp n-dimensional de obiecte-resurse. Nimic nu are valoare intrinsecă,totul este manipulabil[28].

Modul hacker, aplicat la realitatea socială, reflectă o viziune alienată a lumii. De fapt, acesta a fost descrisă cu mai mult timp în urmă de Martin Heidegger. El numește procesul„înrămare tehnologică". Din punctul de vedere al înrămării tehnologice, realitatea apare ca un câmp de resurse abstracte care pot fi supuse la manipulare. Dacă software-ul devorează lumea, aceasta se datorează faptului că lumea a fost încadrată într-o lumină tehnologică, recreată ca un set de circuite, fire și diode gata să fie piratat[29].

Perspectiva lui Heidegger, introdusă în lucrarea „Ființă și timp" (1927), este că ființele umane sunt entități care „dezvăluie lumea"[30]. Noi dezvăluim lumea în moduri diferite, în funcție de modul în care ne interacționăm cu oameni și lucruri. Când „lăsăm lucrurile așa cum sunt", respectând dreptul lor de a exista în mod independent de conceptele și preocupările noastre, realitatea apare ca domeniu de profunzime și mister infinit. Dar când ne raportăm la lucruri cu cererea ca acestea să ne satisfacă nevoile noastre și să se potrivească cu conceptele și sistemele noastre, lumea apare diferit. Realitatea apare ca oglinda propriei noastre activități, plină de lucruri mai mult sau mai puțin utile, dar la dispoziția noastră.

Aceasta este „înrămarea tehnologică". Heidegger face apel la antichitate pentru a înțelege modul în care înrămare tehnologică a ajuns să domine societățile moderne. În cele mai vechi timpuri, Heidegger susține, ființele umane au avut un alt mod de a trata lucrurile. Ei lăsau ființele să fie. Artizanii și antreprenorii doreau să surprindă esența lucrurilor. Să le înțeleagă însăși rațiunea lor de a fi. Fermierii au învățat să lucreze cu clima și anotimpurile; artizanii cu lemnul și piatra; vânători cu fluxurile migratoare de animale, păsări și pești. Această atitudine receptivă față de natură continuă și astăzi în societățile indigene. Cu toate acestea, ea apare ciudată și

[28]T. Rayner, *op. cit.*.
[29]*Ibidem*.
[30]M. Heidegger, *Ființă și timp*,Editura Humanitas, București, 2012, trad. în limba română,*passim*.

demodată în lumea harnică a tehnologiei. În lumea europeană, Heidegger susține, modificarea a venit odată cu apariția științei și tehnologiei. Cadrele conceptuale științifice au permis oamenilor să clasifice lumea, în timp ce tehnologia industrială le-a dat instrumentele de care au nevoie să o domine. Astfel, a demarat înrămare tehnologică a naturii, care continuă până astăzi. În loc contempla lumea și a ne acomoda la realitate, suntem provocați să descoperim bogăția ascunsă a lumii. Astfel, natura devine un scop, natura devine resursă[31].

Discursul Uber, *ride-sharing*, pune într-o lumină favorabilă societatea tehnologică și bunăstarea. Prin sublinierea rolului schimbului de bunuri și resurse, suntem capabili să creăm sisteme de operare prin care oamenii sunt puși pe primul loc și au beneficii sociale extrem de favorabile. Dacă însă Heidegger are dreptate, există, de asemenea, o linie de continuitate profundă care ne leagă de economia „veche“ pe care încearcă să-o înlocuiască. Susținătorii Uber ne spun că sunt în căutarea soluției de a face lumea un loc mai bun. Cu toate acestea, încercarea de a pirata structura societății contribuie la stare generală de rău pe care capitalismul industrial l-a adus pe lume, prin tratarea ființelor umane ca lucruri gata să fie manipulate și exploatate pentru profit.

Critica lui Heidegger aruncă atitudinea „să piratăm totul“ într-o lumină neonorantă. În loc de a fi un mod simplu, pragmatic de a privi lumea, modul în care piratăm poate fi văzut ca o atitudine ontologic-transformatoare, care înrămează realitatea ca domeniu de resurse manipulabile. În lumina hotărârilor instanțelor britanice analizate șoferii și clienți-călători sunt supuși unui astfel de experiment de „înrămare tehnologică”, de manipulare fără un scop deocamdată foarte clar – Uber nu face profit și economiști spun că nici nu va reuși să producă altceva decât pierderi uriașe – activitatea sa pare mai mult un pariu al unor persoane care și-l permit.

5. Uber – viitorul transportului fără șoferi (în loc de concluzii)

[31]M. Heidegger, *Ființă și timp*,Editura Humanitas, București, 2012, trad. în limba română,*passim*.

Din păcate, Uber, cel mai valoros *start-up* al planetei, este afectat de o gestionare defectuoasă și de opțiuni de afaceri discutabile[32]. În timp ce experiența este în mare parte pozitivă din partea clienților săi, Uber trebuie să câștige încrederea și respectul pentru municipalități și autoritățile de aplicare a legii și să arate mai multă prudență în strategiile sale de marketing și răspunsurile la feedback-ul părților interesate.

În ceea ce ne privește cea mai controversată chestiune care însoțește modelul de business Uber este cea juridică.

Uber susține că poate oferi tarife reduse deoarece îi plătește pe șoferii săi ca antreprenori, nu ca angajați cu normă întreagă și alte drepturi salariale. Asta este în întregime fals. Uber atrage bani ca să suporte această diferență de tarife cu pierderi monstruoase. Scopul este obținerea unei însemnate cote de piață. Calificarea Uber ca angajator nu atrage decât înnorarea planului de afaceri.

În egală măsură nu suntem de acord că aceste probleme juridice ale Uber sunt expresia conflictelor de legi și a diferențelor dintre legislațiile naționale. Așa cum am arătat la punctul precedent, filozofia Uber este posibil să nu fie pe calea cea mai onorantă.

Dar Uber pare a avea deja răspunsuri la aceste probleme: în data de 20 noiembrie a anunțat că va achiziționa de la Volvo o flotă impresionantă de autovehicule autonome: 24.000[33]. Înțelegem din declarațiile noului CEO al Uber că viitorul deja arată altfel pentru firmă și că s-a găsit soluția pentru problemele legale: se renunță la șoferi pentru robotaxiuri. Dar asta înseamnă că Uber nu va mai vinde software? Deocamdată acest tip de anunțuri par croite pentru cei doritori să investească în continuare în Uber, fiindcă Uber are doar în SUA 600.000 de șoferi…

[32]A se vedea și M. Ehrenkranz, *A Running List of Uber's (Predictably Lukewarm) Apologies*, articol publicat pe site-ul Gizmodo la data de 17 august 2017, [Online] la: https://gizmodo.com/a-running-list-of-ubers-predictably-lukewarm-apologie-1818524273.

[33]R. Felton, *Uber's Buy Of 24,000 Autonomous Volvos Doesn't Seem To Reconcile Its Inability To Turn A Profit Yet*, articol publicat pe site-ul Jalopnik în data de 20 noiembrie 2017, [Online] la: https://jalopnik.com/ubers-buy-of-24-000-autonomous-volvos-doesnt-seem-to-re-1820616446.

ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

PROIECTUL DE FUZIUNE ÎN CAZUL SOCIETĂȚILOR COMERCIALE. ÎNREGISTRARE ON-LINE SAU PE HARTIE ?

THE PROJECT ACT OF MERGER. ONLINE REGISTRATION OR REGISTRATIONON PAPER?

VIOREL BĂNULESCU[1]

Rezumat: Fuziunea reprezintă un proces complex ale cărui efecte pot prejudicia creditorii societăților comerciale implicate, precum și pe terți. Legea societăților prevede publicarea proiectului de fuziune pentru o mai buna cunoaștere a operațiunilor preconizate de fuziune și în același timp a condițiilor de realizare a acesteia. Actul constitutiv modificat se înregistrează la Registrul Comerțului în a cărui circumscripție își are sediul societatea absorbantă. Apoi, actul, vizat de judecătorul delegat de la Registrul Comerțului se publică în Monitorul Oficial-pe suport hârtie, sau electronic, prin publicarea pe site-ul societății sau pe alte site-uri(de ex. al unei asociații profesionale). Prezentul articol va analiza comparativ cele două modalități de realizare a publicității proiectului de fuziune, cu scopul de a reliefa avantajele și dezavantajele fiecăreia.
Cuvinte-cheie: fuziune, act constitutiv modificat, proiect de fuziune, publicare online/electronică/digitală

Abstract: Merger is a complex process whose effects can harm the creditors of the involved companies as well as third parties. The Companies Act provides for the publication of the merger project for a better understanding of the expected merger operations and, at the same time, the conditions for its completion. Thethe constituent act amended must be registered at the Trade Register in whose jurisdiction the acquiring company is headquartered. Then, the document endorsed by the empowered judge of the Trade Register shall be published in the Official Gazette, on paper or electronically, by publishing on the company's website or other sites (e.g. a professional association). This study will compare the two ways of realizing the publicity of the merger project, with a view to highlight the advantages and disadvantages of each one.

[1]Doctorand, Academia de Studii Economice din București.

Keywords: merger, the constituent act amended, merger project, online/electronic/digital publishing

1. Considerații introductive

Fuziunea reprezintă un proces complex ale cărui efecte pot prejudicia creditorii societăților comerciale implicate, precum și pe terți;de aceea legea impune anumite măsuri de publicitate aplicabile proiectului de fuziune[2]. Doctrina subliniază faptul că, prin publicarea[3] proiectului de fuziune, se urmărește facilitarea cunoașterii operațiunii preconizate și în același timp a condițiilor de realizare a acesteia[4]. De asemenea, prin această operațiune se fundamentează dreptul creditorilor sociali deținători de creanțe anterioare datei publicării proiectului de fuziune, de a-l atac acu acțiune în opoziție[5]. În acest sens, putem cita o decizia a Curții Supreme de Justiție[6] secția comercială, care este coerentă cu opinia citată mai sus. Putem observa că această soluție este fundamentată pe faptul că dispozițiile art. 153 din Legea nr. 31/1900 au fost adoptate cu scopul protejării drepturilor creditorilor, care au calitatea juridică de terți în raport cu societatea intrată în reorganizare și care urmează a fi lichidată[7].

2. Cadrul general de reglementare a formalităților de publicitate

[2] I. Schiau, *Drept Comercial*, Editura Hamangiu, 2009, p. 199; A. Hinescu, *Fuziunea societăților*, Editura Hamangiu, 2016, p. 95.

[3] De la momentul înregistrării și publicării proiectul devine opozabil terților în baza principiului dublei publicități.

[4] M. Șcheaua, *Legea societăţilor comerciale nr. 31/1990 – comentată şi adnotată*, Editura Rosetti, București, 2002, p. 490; S. Angheni, C. Stoica, M. Volonciu, *Drept Comercial*, Ediția a 4-a, Editura C.H. Beck, București, 2008, p. 210; S. Bodu, *Legea societăților, comentată și adnotată*, Editura Rosetti Internațional, 2017, p. 1229.

[5] I. Adam, C.N. Savu, *Legea societăților comerciale. Comentarii și explicații*, Editura C.H. Beck, București, 2010, p. 886; I. Schiau, T. Prescure, *Legea societăților comerciale nr. 31/1990*, Editura Hamangiu, 2007, p. 698.

[6] C.S.J. Secția comercială, decizia nr. 500 din 11 februarie 1998; Instanța a precizat:„este adevărat că pentru fuzionarea societăţilor comerciale se cer îndeplinitecumulativcondiţiile prevăzute de dispoziţiile art. 174 şi 175 din Legea nr. 31/1990 privind societăţile comerciale, precum şi cele cuprinse în art. 153 din lege dar analizând condiţiile speţei, se constată că acestea au fost îndeplinite, întrucât faţă de împrejurarea că aceleaşi persoane fizice cumulau calitatea de asociaţi în cele două societăţi comerciale, întocmirea formelor de publicitate privind modificarea actelor constitutive nu mai era necesară’’.

[7] S.P. Gavrilă, *Legea societăţilor comerciale nr. 31/1990. Practică judiciară*, Editura Hamangiu, București, 2009, p. 566.

Articolul 242 din Legea nr. 31/1990, privind societățile comerciale

În legislația românească, cadrul general de reglementare a formalităților de publicitate îl constituie Legea 31/1990 privind societățile comerciale, respectiv prevederile conținute de art. 242[8]. Prin dispozițiile articolului mai sus citat, se prevăd o serie de obligații de natură procedurală precum și de publicitate legală, ce trebuie îndeplinite de către organele de administrare ale societăților implicate, pe care le vom analiza în continuare[9].

În doctrină, se subliniază faptul că, publicarea proiectului de fuziune, are ca obiectiv facilitarea cunoașterii operațiunii preconizate și în același timp a condițiilor de realizare a acesteia[10]. De asemenea, prin această operațiune se fundamentează dreptul creditorilor sociali, care dețin creanțe anterioare datei publicării proiectului de fuziune, de a face opoziție[11]. În acest sens, putem cita o decizia a Curții Supreme de Justiție[12] secția comercială care este coerentă cu opinia citată mai sus. Această soluție este fundamentată pe faptul că dispozițiile art. 153 din Legea nr. 31/1900 au fost adoptate cu scopul protejării drepturilor creditorilor, care au calitatea juridică de terți în raport cu societatea intrată în reorganizare și care urmează a fi lichidată[13].

Prin dispozițiile acestui articol se instituie un control de legalitate asupra proiectului de fuziune, ce urmează a fi publicat[14].

Astfel, observăm că art. 242 prevede în mod expres că judecătorul delegat controlează îndeplinirea condițiilor legale[15] pentru întocmirea

[8] S. Angheni, C. Stoica, M. Volonciu, *op.cit.*, p. 210.

[9] I. Adam, C.N. Savu, *op.cit.*, pp. 882-886; I. Schiau, T. Prescure, *op.cit.*, p. 699.

[10] M. Șcheaua, *op.cit.*, p. 490; S. Angheni, C. Stoica, M. Volonciu, *op.cit.*, p. 210; S. Bodu, *op.cit.*, p. 1229.

[11] I. Adam, C. N. Savu, *op.cit.*, p. 886; I. Schiau, T.Prescure, *op.cit*., p. 698.

[12] C.S.J. Secția comercială, decizia nr. 500 din 11 februarie 1998; Instanța a precizat:„este adevărat că pentru fuzionarea societăţilor comerciale se cer îndeplinite cumulativ condiţiile prevăzute de dispozițiile art. 174 şi 175 din Legea nr. 31/1990 privind societățile comerciale, precum și cele cuprinse în art. 153 din lege dar analizând condiţiile speţei, se constată că acestea au fost îndeplinite, întrucât faţă de împrejurarea că aceleași persoane fizice cumulau calitatea de asociaţi în cele două societăţi comerciale, întocmirea formelor de publicitate privind modificarea actelor constitutive nu mai era necesară’’.

[13] S.P. Gavrilă, *op.cit.*, p. 566.

[14] S. Popa, *Drept comercial. Teorie și practică judiciară*, Universul juridic, 2009, p. 197.

[15] În sensul că procedura de control realizată de judecător în temeiul art. 242 are caracter grațios rezumându-se la o verificare a„dosarului’’societății fără să poată viza fondul, a se

proiectului de fuziune[16]. În realizarea acestui control, judecătorul delegatare obligația de a verifica existența hotărârii Adunării generale, conținutul proiectului și dacă sunt îndeplinite condițiile legale detaliate de dispozițiile art. 242 din Legea 31/1990[17].

Dacă în urma realizării controlului, sunt evidențiate anumite încălcări ale legii, judecătorul delegat trebuie să dispună respingerea cererii de avizare pentru publicarea proiectului de fuziune[18,19]. Putem cita, în acest sens, din practica judiciară, o decizie[20]civilă a Curții de Apel Cluj.

În cauză, instanța constatând îndeplinirea condițiilor prevăzute de lege admite recursul, dispune modificarea încheierii judecătorului delegat, publicarea în M. Of. și înregistrarea operațiunii de fuziune. Tot în același sens[21], putem cita o decizie civilă pronunțată de Curtea de Apel Timișoara.

Legea societăților impune depunerea unei declarații de către societatea, care se dizolvă în care să se specifice modalitatea în care se va realiza stingerea pasivului patrimonial (apreciată ca inutilă de către un

---

vedea Bodu S., *op.cit.*, p. 1229; St. D. Cărpenaru, S. David, Gh. Piperea, *op.cit.*, p. 820;I. Schiau, T. Prescure, *op.cit.*, p. 698; S. Angheni, C. Stoica, M. Volonciu, *op.cit.*, p. 210.

[16] Tot în sensul că procedura de control realizată de judecător este una necontencioasă a se vedea Î.C.C.J., s. com., dec. nr. 3634/16.11.2006 în S.Petrina Gavrilă, *op.cit.*, p. 584.

[17] Trib. Alba, încheierea nr. 377/2008 în A.C. Târșia, *op.cit.*, p. 138; A se vedea și I. Adam, C. N. Savu, *op.cit.*, p. 878.

[18] Trib. Satu Mare, s. a-II-a civ. cont. admin. și fiscal, sent. nr. 235/10.05.2012;Încheierea judecătorului poate fi atacată numai pe calea apelului așa cum rezultă din interpretarea dispozițiilor Noului Cod de procedură civilă respectiv art. 60 din Legea societăților nr. 31/1990; În sensul că judecătorul delegat poate decide respingerea înmatriculării societății dar nu are competența de a decide suspendarea fuziunii prerogativă care aparține tribunalului, a se vedea C.T. Ungureanu, M. Afrăsinei, M.L. Belu-Magdo., A. Bleoancă, *Noul Cod civil. Comentarii, doctrină și jurisprudență*. București, Editura Hamangiu, 2012, p. 278.

[19]A. Hinescu, *op.cit.*, p. 119;I. Adam, C.N. Savu, *op.cit.*, pp. 878, 884;C. Cucu, M.V. Gavriș, C-G Bădoiu, C. Haraga, *Legea societăților comerciale nr. 31/1990. Repere bibliografice. Practică judiciară. Decizii ale Curții constituționale. Adnotări*, Editura Hamangiu, București, 2007, p. 566. A se vedea și C.S.J., s. cont. adm., dec. nr. 1255/1997 în Dreptul nr. 3/1998, p. 138; În sensul că încheierea de respingere poate fi atacată cu apel și nu cu recurs a se vedea C. A. București, s. a. V-a civ., dec. nr. 279/09. 09. 2013 definitivă, nepublicată în A. Hinescu, *Fuziunea și divizarea societăților. Practică judiciară adnotată*, Editura Hamangiu, 2015, p. 6.

[20] C.A. Cluj, dec. civ. nr. 2984/2009, [Online]la: http://www.avocatura.com/spețа.

[21] C.A. Timişoara., dec. civ. nr. 289/23.08.2008,[Online] la: http://www.avocatura.com/spețа.

autor)[22]. De asemenea, va fi depusă și o declarație privind modul de realizarea publicității proiectului de fuziune[23].

Apreciem că pasivul patrimonial se poate stinge în două moduri: fie anterior fuziunii, fie ulterior acesteia, caz, în care obligațiile societății, care își încetează existența vor fi preluate de societatea beneficiară[24]. Menționăm, de asemenea, că, întrucât fuziunea este o operațiune de concentrare economică, proiectul de fuziune trebuie vizat și de Consiliul Concurenței[25]. Proiectul de fuziune, semnat de reprezentanții societăților implicate, se depune la Oficiul Registrului Comerțului în raza căruia este înmatriculată fiecare societate în conformitate cu dispozițiile art. 242 din Legea societăților 31/1990[26]. În doctrină[27], se susține că deținerea de sedii secundare/sucursale, precum și faptul că datoriile sunt născute ca urmare a

[22] O-M. Corsiuc, E-C. Giurgea, *Drept comercial. Legislație. Doctrină. Jurisprudența.*, Editura Universitară, București, 2015, p. 149;S. Angheni, C. Stoica, M. Volonciu, *op.cit.*, p. 210;S. Popa, *op.cit.*, p. 193; I. Adam, C. N. Savu, *op.cit.*, p. 878; C.Cucu, M.V.Gavriș, C-G.Bădoiu, C. Haraga, *op.cit.*, p. 566; I. Schiau, T. Prescure, *op.cit.*, p. 698; C. Gheorghe, *Drept comercial român*, Editura C.H. Beck, București, 2013, p. 504; S. Bodu, *op.cit.*, p. 1267;St.D. Cărpenaru, *op.cit.*, pp. 252, 261.În sensul că asupra modului de stingere a pasivului trebuie să decidă tot Adunarea generală a se vedea S. Angheni, C. Stoica, M. Volonciu, *op.cit.*, p. 210; L. Tuleașcă, *Drept comercial. Întreprinderile comerciale*, Editura Universul juridic, București, 2016; În sensul că declarația are ca scop stingerea pasivului deoarece fuziunea este condiționată de absența datoriilor societății absorbite, a se vedea E. Precupețu, M. Danil, art. cit. p. 51;St.D. Cărpenaru, S. David, Gh. Piperea, *Legea societăților. Comentariu pe articole*, Ediția a 5-a, Editura C.H. Beck, București, 2014, p. 820;Gh. Piperea, *Societăți comerciale, piața de capital. Aquis comunitar*, Editura All Beck, București, 2005, p. 199.

[23] St.D. Cărpenaru, S. David, Gh. Piperea, *op.cit.*, p. 818;C. Gheorghe, *op.cit.*, p. 504; St.D. Cărpenaru, *op.cit.*, p. 252; L. Tuleașcă, *op.cit.*, p. 338.

[24] St.D. Cărpenaru, S. David, Gh. Piperea, *op.cit.*, p. 820; I. Adam, C. N. Savu, *op.cit.*, p. 886; C. Cucu, M. Gavriș, C. Bădoiu,C. Haraga, *op.cit.*, p. 566.

[25] Gh. Piperea, *Societăți comerciale, piața de capital. Aquis comunitar*, Editura All Beck, București, 2005, p. 295.

[26] S. Angheni, C. Stoica, M. Volonciu, *op.cit.*, p. 210; În sensul că formalitățile de publicitate se realizează în două, inițial se depune la Registrul comerțului proiectul de fuziune în original pentru a fi publicat în M.Of., iar ulterior celelalte documente necesare înregistrării fuziunii a se vedea C.A. București, s. a V-a civ., dec. nr. 2065/20.11.2012, irevocabilă, nepublicată în A. Hinescu, *Fuziunea și divizarea*, *op.cit.*, p. 15;St. D. Cărpenaru, *op.cit.*, p. 252;I. Adam, C. N. Savu, *op.cit.*, p. 886;S. Popa, *op.cit.*, p. 193; S. Angheni, *op.cit.*, p. 251;Gh. Piperea, *op.cit.*, p. 271; A.C. Târșia, *Reorganizarea persoanei juridice de drept privat*, Editura Hamangiu, 2012, p. 138;

[27]C. Cucu, M. Gavriș, C. Bădoiu, C. Haraga, *op.cit.*, p. 567.

încheierii de acte juridice cu aceste dezmembrăminte, nu implică depunerea proiectului de fuziune la sediile Registrului Comerțului în raza cărora se găsesc aceste dezmembrăminte.

Analizând dispozițiile legale citate anterior și comparându-le cu cele privind dubla înregistrare a sediilor secundare, dezmembrăminte ale societății (exclusiv sucursala conform art. 43, alin. (1) și (3), apreciem că, următoarele aspecte, trebuie avute în vedere pentru modificarea, *de lege ferenda*, a legislației societăților.

Astfel, considerăm că ar fi util ca terții cocontractanți ai sediilor secundare să fie informați despre fuziunea societății-mamă. Acest fapt ar impune publicarea proiectului de fuziune și la Registrul Comerțului de la sediul secundar, chiar dacă aceasta poate aglomera activitatea Oficiului Registrului Comerțului printr-o dublă înregistrare (atât la sediul societății mamă, cât și la sediul secundar).

Proiectul de fuziune al societăților implicate vizat de către judecătorul delegat, se publică cu cel puțin 30 de zile înainte de datele ședințelor, în care Adunările generale vor decide asupra fuziunii conform art. 113, lit. (h) din Legea societăților nr. 31/1990[28]. Conform art. 242 din Legea nr. 31/1990, proiectul de fuziune se publică pe cheltuiala părților, integral sau în extras în M.Of. partea a IV-a potrivit dispozițiilor judecătorului delegat sau a cererii părților[29].

3. Tipuri de fuziune. Actul juridic de modificarea a actului constitutiv al societății beneficiare

Legea societăților 31/1990 prevede în art. 248, care sunt *obligațiile de publicitate* referitoare la actul modificator al actului constitutiv al societății beneficiare a fuziunii prin absorbție[30]. Observăm, însă, că nu există prevederi cu privire la cerințele de publicitate în cazul realizării

[28]S. Popa, *op.cit.*, p. 197;I. Schiau, *op.cit.*, p. 199;În forma anterioară a legii proiectul de fuziune era vizat de directorul Oficiului registrului comerțului sau de persoană desemnată să realizeze această activitate.

[29]D-M. Șandru, *Dreptul societăților în România*, Editura Universitară, București, 2017, p. 362;S. Bodu, *op.cit.*, p. 1227; St.D. Cărpenaru, S. David, Gh. Piperea, *op.cit.*, p. 820; I. Schiau, T. Prescure, *op.cit.*, p. 698; S. Bodu, *op. cit.*, p. 362; S. Popa, *op.cit.*, p. 197;S. Angheni, C. Stoica, M. Volonciu, *op.cit.*, p. 210; I. Adam, C. N. Savu, *op.cit.*, p. 886;St. D. Cărpenaru, *op.cit.*, p. 261.

[30]I. Adam, C. N. Savu, *op. cit.*, pp. 714-715, 905.

fuziunii prin contopire[31]. În doctrina[32], se justifică această lipsă de reglementare dat fiind că, în cazul acestui tip de fuziune, se naște o nouă societate și în consecință nu vor fi incidente prevederile acestui articol, ci regulile generale cuprinse în art. 50 din Legea societăților nr. 31/1990.

Din analiza dispozițiilor art. 248, putem observa că obligațiile de publicitate sunt prevăzute distinct atât pentru societatea absorbantă cât și pentru societatea absorbită[33]. Precizăm că,pentru societățile absorbite, publicitatea poate fi efectuată de societatea absorbantă, în cazul în care societățile absorbite nu au efectuat-o, în termen de 15 zile de la vizarea actului modificator al actului constitutiv al societății absorbante de către judecătorul delegat[34].

Menționăm că art. 248, alin. (1)din Legea societăților reglementează procedura specifică de publicitate a actului modificator al actului constitutiv al societății beneficiare a fuziunii prin absorbție[35]. Astfel, actul modificator se înregistrează la Registrul Comerțului în a cărui circumscripție își are sediul societatea absorbantă apoi, actul vizat de judecătorul delegat la Registrul Comerțului se publică în Monitorul Oficial[36].

În măsura, în care se depășește termenul prevăzut de art. 248, alin. (1), se poate aplica o amendă atât societății absorbite cât și societății absorbante[37]în conformitate cu dispozițiile art. 44 din Legea 26/1990[38].Observăm că această sancțiune diferă de cea reglementată de legislația franceză în materie după cum vom preciza în cele ce urmează. Astfel, în dreptul francez societățile, implicate în operațiunea de fuziune, au obligația de a redacta, a semna și de a depune o declarație de

[31] *Ibidem*, p. 714.

[32] *Ibidem*, p. 905;I. Schiau, T. Prescure, *op. cit.*, p. 714.

[33] I. Adam, C. N. Savu, *op.cit.*, p. 906

[34] C. Cucu, M. Gavriș, C. Bădoiu, C. Haraga, *op.cit.*, p. 579; I. Adam, C. N. Savu, *op.cit.*, p. 906;C. Gheorghe, *op.cit.*, p. 512; St.D. Cărpenaru, S. David, Gh. Piperea, *op.cit.*, p. 834; S. Bodu, *op.cit.*, p. 1252.

[35] St.D. Cărpenaru, *op.cit.*, p. 261.

[36] C. Cucu, M. Gavriş, C. Bădoiu, C. Haraga, *op.cit*, p. 579; I. Schiau, T. Prescure, *op.cit.*, p. 714.

[37] C. Cucu, M. Gavriş, C. Bădoiu, C. Haraga, *op.cit.*, p. 581.

[38] Legea nr. 26/1990 privind Registrul comerțului, republicată și actualizată.

conformitate la grefa tribunalului comercial[39]. Nerespectarea acestei obligații legale poate avea ca efect nulitatea operațiunii de fuziune. Declarația de conformitate cuprinde informații privitoare la:

- conformitatea operațiunii de fuziune cu legea și regulamentele în vigoare;

- prezentarea tuturor actelor efectuate pentru realizarea fuziunii.

Din analiza comparată a cele două soluții legale observăm că în timp ce în reglementarea românească accentul cade pe răspunderea asumată de Oficiul Registrului Comerțului (ca autoritate de stat) pentru respectarea dispozițiilor legale privind realizarea fuziunii, în dreptul francez răspunderea și-o asumă societățile în cauză, iar sancțiunea nulității absolute garantează respectarea dispozițiilor imperative.

Recomandăm, *de lege ferenda*, modificarea reglementări românești, în sensul asumării exprese a răspunderii realizării actelor fuziunii și a publicității în conformitate cu dispozițiile legale de către administratori/directorilor societățile implicate, similar situației din dreptul francez prin depunerea unei declarații de conformitate**.** Apreciem că, promovând o astfel de modificare legislativă, activitatea Registrului Comerțului va cunoaște o creștere calitativă.

În plus, apreciem faptul că, în legislația franceză, declarația de conformitate trebuie semnată de cel puțin un director/administrator al societăților angrenate în procedura fuziunii, ceea ce reprezintă dovada desfășurării unei acțiuni de auto-evaluare și control din partea reprezentanților societăților implicate. În dreptul francez, organele de administrare ale societății, care au semnat declarația de conformitate, vor răspunde solidar pentru prejudiciile cauzate prin omisiunile sau neregularitățile, ce afectează actul modificator al societății.

În doctrină, se apreciază că procedura reglementată de art. 248 din Legea societăților se completează cu dispozițiile art. 204, astfel încât la Registrul Comerțului trebuie depus împreună cu actul modificator textul complet al actului constitutiv al societății absorbante, în formă actualizată[40]. În ceea ce privește forma actului modificator, menționăm că acesta poate îmbrăca forma unui înscris sub semnătură privată sau

[39] G. Guez, *Déclaration commune de conformité*, Rev. francophone des laboratoires (RFL), juin 2011, p. 77.

[40] C. Cucu, M. Gavriș, C. Bădoiu, C. Haraga, *op.cit*, p. 376;St.D. Cărpenaru, S. David, Gh. Piperea, *op.cit.*, p. 834.

autentică.

Precizăm, astfel, că actul constitutiv va îmbrăca formă autentică în situațiile prevăzute de art. 204, alin. (2) și (6) din Legea societăților nr. 31/1990[41].

4. Dispoziții impuse de armonizarea cu legislația europeană

În legislația românească, a fost implementată Directiva 2009/109/CE a Parlamentului European și a Consiliului din 16 septembrie 2009 privind obligațiile de raportare și întocmire a documentației necesare în cazul fuziunilor și divizărilor[42].Conform dispozițiilor Directivei citate mai sus, publicitatea fuziunii se poate realizași electronic, prin publicarea pe site-ul societății sau pe un alt site (de ex. al unei asociații profesionale).

Menționăm, de asemenea, că Legea societăților nr. 31/1990 a fost modificată, în acest sens, permițând societăților să aleagă între publicitatea obișnuită și cea realizată utilizând mijloace electronice[43]. Potrivit alin. (2^1)art. 242 din Legea privind societăților, în cazul, în care, societatea deține o pagină proprie web, poate înlocui publicitatea în M. Of. cu publicarea proiectului de fuziune pe această pagină.

Conform dispozițiilor legale publicitatea se va realiza pe o perioadă continuă de cel puțino lună înaintea Adunării Generale, ce decide asupra fuziunii și care nu poate fi încheiată mai devreme de închiderea Adunării Generale respective[44]. Societatea, care a optat să facă publicitatea prin intermediul paginii web, are obligația de a asigura pe durata acestei perioade, condițiile tehnice pentru afișarea continuă și

[41] St. D. Cărpenaru, S. David, Gh. Piperea, *op.cit.*, p. 713; I. Schiau, T. Prescure, *op.cit.*, p. 714; În practica judiciară există soluții care tind să susțină ideea că forma autentică a proiectului de fuziune este general obligatorie, C.A. București, s. civ. dec. nr. 544/2013 în S. Bodu, *op.cit.*, p. 1228; Forma autentică a actului constitutiv este obligatorie în cîteva ipoteze din care amintim majorarea capitalului social prin subscripție publică, cînd se majorează capitalului social prin subscrierea ca aport a unui bun imobil, modificarea formei juridice a societății în societate în nume colectiv sau în comandită simplă.

[42] A. Hinescu, *op.cit.*, p. 94.

[43] A. C. Târșia, *op.cit.*, p. 139; St. D. Cărpenaru, S. David, Gh. Piperea, *op.cit.*, p. 820; C. Gheorghe, *op.cit.*, p. 505; A. Hinescu, *op.cit.*, p. 94; L. Tuleașcă, *op.cit.*, p. 338; S. Angheni, *op. cit.*, p. 252.

[44] C. Gheorghe, *op.cit.*, p. 505; S. Popa, *op.cit.*, p. 192.

neîntreruptă și cu titlu gratuit a tuturor documentelor prevăzute de lege[45].

Concluzii

Potrivit Legii societăților comerciale, societatea, care a optat pentru publicitatea pe Internet are obligația de a dovedi continuitatea publicității precum și de a asigura securitatea informațiilor și autenticitatea documentelor publicate[46]. Precizăm că, atunci, când, se alege publicitatea alternativă a proiectului de fuziune, societatea trebuie să menționeze pe site data publicării proiectului de fuziune. Această informație este utilă pentru a se asigura protecția creditorilor ale căror creanțe sunt anterioare datei publicării proiectului de fuziune și nescadente la această dată, sau a altor prevederi, ce reglementează efectele, ce se declanșează de la data publicării.

Considerăm că este necesar ca acționarii, să fie informați cu privire la adresa site-ului, unde pot consulta documentele publicate în ipoteza în care societatea a ales forma alternativă de publicitate. Precizăm că legislația românească nu a asimilat și posibilitatea ca societatea să poată realiza publicitatea pe un alt site, aceasta nedispunând de un site propriu, prin care să garanteze respectarea dispozițiilor legale prezentate mai sus. Considerăm că nu există un impediment ca societatea în cauză să poată cumula cele două forme de publicitate utilizând concomitent atât site-ul Registrului Comerțului, cât și un site propriu, în măsura în care o astfel de decizie îi este utilă și fezabilă.

În cazul, în care publicitatea se realizează în condițiile alin. (2^1) art. 242 Oficiul Registrului Comerțului, la care este înmatriculată societatea va publica pe site-ul său, cu titlul gratuit, proiectul de fuziune transmis de societate[47].

Apreciem că, față de prevederile legislației românești legea franceză conține în mod expres dispoziția potrivit căreia Comitetul de

[45] În sensul că punerea la dispoziția asociaților/acționarilor interesați la sediul societăților în cauză a rapoartelor administratorilor sau cenzorilor conduce la prezumția că cei interesați au luat la cunoștință de conținutul acestor documente în Î.C.C.J. secț. com., dec. 2410/7. 04. 2005, www.scj.ro.A se vedea și C.A. Ploiești, s. a II-a civ., cont. admin. și fisc., dec. civ. nr. J129/08.02.2013, irevocabilă, nepublicată, în A.Hinescu, Fuziunea și divizarea, *op.cit.*, p. 17.

[46] C.A. București, s. a. VI-a civ. dec. nr. 940/03.11.2014, [Online] la: http://www.avocatura.com/speța.A se vedea și: C. Gheorghe, *op.cit.*, p. 505; A. Hinescu, *op. cit.*, p. 94.

[47] S. Angheni, *op.cit.*, p. 252.

întreprindere din societățile implicate în operațiunea de fuziune are dreptul să consulte proiectul de fuziune.

Considerăm că dispozițiile legale din Legea societăților privind publicitatea electronică a proiectului de fuziune sunt binevenite, avantajând atât creditorii sociali anteriori fuziunii, dar și societățile implicate în fuziune, care dobândesc astfel o cale rapidă, eficientă de publicitate. Utilizând site-ul personal societățile comerciale sunt stimulate în a externaliza informațiile privind deciziile din viața internă, asigurând o transparența a acestora, dar și o rapiditate a diseminării informațiilor, garantând protecția creditorilor sociali, fie ei asociați ai societăților angrenate în procesul fuziunii, fie ei terțe persoane.

ANALELE ȘTIINȚIFICE ALE UNIVERSITĂȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

DREPTUL LA UITARE. CINE CONTROLEAZĂ PREZENTUL CONTROLEAZĂ TRECUTUL

THE RIGHT TO BE FORGOTTEN. HE WHO CONTROLS THE PRESENT CONTROLS THE PAST

ANDREEA VERTEȘ-OLTEANU[1]
CODRUȚA GUZEI-MANGU[2]

Rezumat: Într-o decizie istorică deja (*cauza C-131/12*), Curtea de Justiție a Uniunii Europene a hotărât că operatorul unui motor de căutare pe internet răspunde juridic pentru prelucrarea datelor cu caracter personal care apar pe paginile web publicate de terți. Dreptul la uitare, creație pretoriană, care își va găsi ulterior consacrarea în Regulamentul general privind protecția datelor (Regulamentul (UE) 2016/679), cu aplicare din 25 mai 2018, a declanșat o serie întreagă de reacții. Prezentarea noastră va încerca să explice aceste reacții, să expună avantajele și riscurile implicate, să facă o trecere în revistă a legislației privind prelucrarea datelor cu caracter personal din Europa și să analizeze implicațiile juridice, politice și sociale ale dreptului nou-creat, teritoriu virgin pentru toate părțile implicate și care necesită o atentă punere în balanță a mai multor drepturi fundamentale, precum libertatea de exprimare, dreptul la viață privată, dreptul la demnitate, dreptul la propria imagine sau dreptul publicului la informare.
Cuvinte-cheie: dreptul la uitare, date cu caracter personal, libertate de exprimare, dreptul la viață privată

Abstract: In a landmark decision (case C-131/12), the Court of Justice of the European Union ruled that an Internet search engine operator is legally responsible for the processing of personal data appearing on third-party web pages. The right to be forgotten, a praetorian creation, which would later be enshrined in the General Data Protection Regulation (Regulation (EU) 2016/679), with effect from 25 May 2018, triggered a series of reactions. Our presentation will attempt to explain these reactions, to discuss the benefits and risks involved, to review the data protection legislation in Europe and to explore the legal, political and social implications of the

[1] Lector univ. dr., Facultatea de Drept, Universitatea de Vest Timişoara.
[2] Lector univ. dr., Facultatea de Drept, Universitatea de Vest Timişoara.

newly emerged right, a virgin territory for all parties involved, which requires careful balancing of several fundamental rights, such as freedom of speech, the right to privacy, the right to dignity, the right to one's own image or the right to be informed.
Keywords: right to be forgotten, personal data, freedom of speech, privacy

Ce este uitarea?

În 1944, Jorge-Luis Borges scria *Funes el memorioso*, în care povestește despre un personaj care își amintește absolut totul, fiecare frunză văzută în fiecare pom, fiecare nor de pe cer, fiecare cuvânt auzit de-a lungul vieții, fiecare frază citită. Funes este un om schilodit de incapacitatea de a uita, nu face diferența între banal și important, nu poate generaliza, nu poate prioritiza, e incapabil de idei generale, sumedenia de detalii acumulate în mintea sa aducându-l în imposibilitatea de a abstractiza. Uitarea deci, și nu amintirea, concluzionează Borges, este ceea ce ne definește ca oameni. „Pensar es olvidar (…)"[3]. „A gândi înseamnă a uita".

În epoca Internetului, mai este oare posibilă uitarea? Internetul este Funes, o serie colosală de conținuturi dezordonate, nefiltrate și neorganizate, transferând „blestemul" neuitării și înspre utilizatorii lui. Iar uitarea, pe lângă toate celelalte valențe ale sale, poate fi – în sfera Dreptului – unul dintre instrumentele non-juridice de apărare a dreptului la demnitate al omului. A uita se poate traduce cu a îi îngădui celuilalt să se bucure de demnitate, aceasta putând presupune și dreptul la un trecut imperfect.

În 2007, Harry Surden scrie despre conceptul de „drepturi structurale" în domeniul protecției dreptului la viață intimă. În opinia sa, „privacy" sau dreptul persoanei de a fi lăsată în pace, este protejat atât prin instrumente juridice cât și altele, non-juridice, el referindu-se mai exact la barierele fizice sau tehnologice care reglementează o anumită conduită, cu un accent special acordat costurilor tranzacționale. Constrângerile structurale, scrie Surden, fac ca anumite conduite să fie imposibile sau costisitoare, uneori chiar absurd de costisitoare. Aceste obstacole acționează ca o reglementare non-juridică, oferind un „drept" non-juridic, un drept structural, împotriva conduitelor pe care le împiedică[4]. Dar schimbările

[3] J.-L. Borges, *Funes el memorioso*, în Ficciones, 1944, [Online] la: http://users.clas.ufl.edu/burt/spaceshotsairheads/borges-funes_el_memorioso.pdf, accesat 15.11.2017.

[4] H. Surden, *Structural Rights in Privacy*, în SMU Law Review, vol. 60, 2007, pp. 1605-1629, [Online] la: http://scholar.law.colorado.edu/articles/346, accesat 15.11.2017.

rapide din tehnologie pot elimina aceste drepturi, pe care oamenii se bazau, în special în legătură cu viața privată. Soluția sa: diminuarea drepturilor structurale trebuie echilibrată prin adăugarea de protecții juridice sau prin impunerea unor costuri care să compenseze scăderea celor actuale. Surden continuă și dezvoltă linia de gândire a judecătorului Richard Posner, „Progresul tehnologic reprezintă o amenințare la adresa vieții private, întrucât înlesnește un nivel de supraveghere care, anterior, ar fi fost dezarmant de costisitor, oferind poliției acces la tehnici de supraveghere tot mai ieftine și tot mai eficiente”[5].

Opiniile lor se regăsesc, în 2012, în cauza *United States v. Jones*[6], în care judecătorii Curții Supreme a Statelor Unite au trebuit să decidă dacă fapta poliției de a fixa un dispozitiv GPS pe o mașină a suspectului și de a folosi acel instrument pentru a monitoriza drumurile făcute de mașina respectivă timp de 28 de zile constituie sau nu „percheziție”, în conformitate cu al patrulea amendament al Constituției americane.

> *„În era pre-digitală, cea mai mare protecție a vieții private nu era una garantată nici de constituție, nici de vreo lege anume, ci de practică. Supravegherea tradițională era dificilă și costisitoare și, prin urmare, rar se recurgea la ea. Monitorizarea prin GPS ar fi avut ca echivalent echipe întregi de agenți, vehicule, poate chiar și asistență aeriană. Adică o mulțime de resurse. Toate acestea ar fi presupus o investigație de mare anvergură (...) Când este posibilă supravegherea în masă a tuturor cetățenilor (și a activităților lor) pentru câțiva cenți pe zi, avem nevoie de o mai strictă aplicare a legii. Altfel, e ca și cum am fi urmăriți zilnic de nenumărați agenți minusculi și invizibili, care ne monitorizează fiecare mișcare”*[7].

[5] R. Posner, *United States v. Garcia*, 474 F.3d 994, 998, al 7-lea circuit, 2007, în K. S. Bankston și A. Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, în The Yale Law Journal, vol. 123, 2014, p. 335, [Online] la: https://www.yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones, accesat 15.11.2017.

[6] *United States v. Jones*, 615 F. 3d 544, Curtea Supremă a Statelor Unite ale Americii, 2012.

[7] Opinia judecătorului S. Alito, *United States v. Jones*, 615 F. 3d 544, Curtea Supremă a Statelor Unite ale Americii, 2012, [Online] la: https://www.law.cornell.edu/supct/pdf/10-1259.pdf, accesat 15.11.2017 [traducerea ne aparține].

Soluția *Google Spain v. Costeja*

Oare nu am putea cataloga și uitarea, ca fenomen intrinsec și absolut firesc al ființei umane, printre aceste bariere structurale care apără – sau cel puțin apărau, înaintea apariției internetului – dreptul la viață intimă al persoanei? Internetul ne-a luat unul dintre cele mai prețioase drepturi: dreptul la uitare. În viață, o persoană poate trece prin experiențe teribile, traumatizante, pe care apoi încearcă să le uite, cu mai mult sau mai puțin succes. În prezent, însă, internetul nu îți mai îngăduie să uiți nimic. Soluția în fața acestei imposibilități de a mai uita într-o epocă profund tehnologizată, cu informații disponibile la orice oră, prin intermediul unui simplu clic, vine prin deja celebra decizie *Google Spain v. Costeja*, în care Curtea de Justiție a Uniunii Europene (Marea Cameră) a stabilit, pe data de 13 mai 2014, că operatorul unui motor de căutare pe internet răspunde pentru prelucrarea pe care o efectuează în ceea ce privește datele cu caracter personal care apar pe pagini web publicate de terți.[8]

Contextul legal care întemeiază dreptul la uitare și pe care se bazează hotărârea Curții de Justiție a Uniunii Europene este cel oferit de Directiva 95/46[9] care, potrivit art. 1, are obiectul de a proteja drepturile și libertățile fundamentale ale persoanelor fizice și, în speță, dreptul lor la viață intimă, familială și privată, cu privire specială asupra prelucrării datelor cu caracter personal și a liberei circulații a acestora.

Nu vom realiza o prezentare detaliată a acestei hotărâri, speța fiind deja de notorietate, ci ne vom mărgini la o prezentare succintă a acesteia.

În acest sens, pe 5 martie 2010, domnul Costeja Gonzales, cetățean spaniol, a înaintat Agenției Spaniole a Protecției Datelor (AEPD) o plângere împotriva publicației La Vanguardia și împotriva Google Spain și Google Inc. Plângerea a fost determinată de faptul că, în momentul în care un utilizator internet introducea numele Costeja Gonzales în motorul de căutare Google, acesta obținea link-uri către două pagini web ale publicației La Vanguardia, din ianuarie 1998 și, respectiv, martie 1998, mai precis către un

[8] Cauza C-131/12, *Google Spain SL, Google Inc. Împotriva Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Curtea de Justiție a Uniunii Europene, 13 mai 2014, [Online] la: http://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:62012CJ0131&from=RO, accesat 15.11.2017.

[9] Directiva 95/46/CE a Parlamentului European și Consiliului Uniunii Europene privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, din 24 octombrie 1995.

anunț în care numele domnului Costeja Gonzales apărea în legătură cu o licitație publică organizată cu scopul de a recupera o serie de datorii ce se aflau în sarcina lui la acea dată.

În primul rând, domnul Costeja Gonzales solicită instanței ca publicația La Vanguardia fie să înlăture, fie să modifice paginile sale web de așa natură încât datele personale despre domnul Costeja Gonzales să nu mai poată fi accesate. În cel de-al doilea rând, petentul solicită ca Google Spain și Google Inc. să înlăture sau să ascundă datele personale în legătură cu el, așa încât acestea să nu mai fie incluse în rezultatele căutării și să nu mai apară în legătură cu link-urile publicației La Vanguardia. În motivarea celor solicitate, domnul Costeja Gonzales arată că procedurile cu privire la licitația publică și situația debitelor sale au fost pe deplin rezolvate cu mulți ani în urmă și că, în prezent, informațiile cu privire la acestea nu mai prezintă relevanță.

Cu privire la primul capăt de cerere, AEPD respinge solicitarea domnului Costeja Gonzales și nu obligă publicația La Vanguardia să înlăture informațiile despre domnul Costeja Gonzales. Agenția a procedat în acest sens luând în considerare faptul că ziarul La Vanguardia a publicat informațiile personale ale petentului ca urmare a ordinului Ministerului Muncii și Protecției Sociale, cu scopul de a face cunoscută procedura licitației și de a strânge cât mai multe persoane interesate să participe la aceasta.

Referitor la cel de-al doilea capăt de cerere, AEPD admite solicitarea domnului Costeja Gonzales și obligă Google Spain și Google Inc. să înlăture link-urile ce conduc la informațiile personale ale domnului Costeja Gonzales ce apar pe pagina web a publicației La Vanguardia. AEPD își motivează hotărârea pe argumentul că operatorii motoarelor de căutare trebuie să respecte legislația cu privire la protecția datelor personale, dat fiind faptul că aceștia realizează o prelucrare a datelor, operațiune pentru care sunt responsabili. Pentru această rațiune, AEPD apreciază că obligația de a retrage datele și accesul la anumite link-uri ce conțin referințe cu privire la datele personale ale unui subiect de drept poate fi impusă direct în sarcina operatorilor motoarelor de căutare, fără să fie necesar ca informațiile să fie șterse de pe site-ul pe care apar, incluzând în această categorie și situația în care informațiile trebuie să rămână pe site ca urmare a unei norme legale în acest sens.

Esența hotărârii de care facem vorbire constă în faptul că aceasta conturează o definiție a însuși dreptului la uitare. Astfel, în lumina celor expuse de Curtea de Justiție a Uniunii Europene, în cazul în care se constată, ca urmare a unei cereri formulate de persoana vizată în temeiul art. 12 lit. (b) din Directiva 95/46, că includerea pe lista de rezultate, afișată în urma unei căutări efectuate plecând de la numele acesteia, a unor link-uri către pagini de internet publicate legal de către terți și care conțin informații adevărate referitoare la persoana sa este incompatibilă cu art. 6 alin. (1) lit. (c)-(e), întrucât informațiile se dovedesc a fi inadecvate, nu sunt sau nu mai sunt pertinente ori sunt excesive în raport cu scopurile prelucrării în cauză, realizate de motorul de căutare, informațiile și link-urile vizate trebuie înlăturate.

Interpretarea CJUE fiind punctul de plecare al elaborării Regulamentului UE 679/2016[10], definiția dreptului la uitare în viziunea acestuia se desprinde din conținutul art. 17. Potrivit acestuia, *„Persoana vizată are dreptul la ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a șterge datele cu caracter personal, fără întârzieri nejustificate, în cazul în care se aplică unul dintre următoarele motive: datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate; persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea, în conformitate cu articolul 6 alineatul (1) litera (a) sau cu articolul 9 alineatul (2) litera (a), și nu există niciun alt temei juridic pentru prelucrarea; persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (1) și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea sau persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (2); datele cu caracter personal au fost prelucrate ilegal; datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se află operatorul; datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale menționate la articolul 8 alineatul (1).”* Același articol

[10] Regulamentul (UE) 2016/679 *al Parlamentului European și al Consiliului din 27 aprilie 2016* privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal *și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Reg*ulamentul general privind protecția datelor), publicat în Jurnalul Oficial al Uniunii Europene, L 119 din 4 mai 2016.

trasează și limitele aplicării dreptului la uitare, respectiv, acesta „*nu se aplică în măsura în care prelucrarea este necesară: pentru exercitarea dreptului la liberă exprimare și la informare; pentru respectarea unei obligații legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul; din motive de interes public în domeniul sănătății publice, în conformitate cu articolul 9 alineatul (2) literele (h) și (i) și cu articolul 9 alineatul (3); în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), în măsura în care dreptul menționat la alineatul (1) este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective; sau pentru constatarea, exercitarea sau apărarea unui drept în instanță*."

Dreptul la uitare. Origini.

Cu referire la izvoarele dreptului la uitare, o primă sursă poate fi identificată și dedusă din modul în care a fost motivată hotărârea pronunțată de Curtea de Justiție a Uniunii Europene în cauza C-131/12. În acest sens, dreptul la uitare izvorăște, pe cale de interpretare, din dreptul persoanei la respectarea vieții private[11], a dreptului la demnitate și la imagine, cu cele două conotații, dreptul la onoare și la bună reputație. În acest caz, interpretarea este una realizată de către instanța de judecată în procesul jurisdicțional, dreptul la uitare fiind o creație pretoriană[12], care, asemeni modului în care indicațiile obligatorii pe care le dădea judecătorul roman ce se pronunța asupra unui conflict dedus judecății erau cuprinse în cadrul edictelor pretorilor[13], este cuprins și consacrat într-un act de legislație

[11] S. D. Şchiopu, *Dreptul la ştergerea datelor şi dreptul la aducerea ultimului omagiu: a fi uitat sau a fi ţinut minte*, în Revista Universul Juridic nr. 2/2017, p. 86, [Online] la: http://revista.universuljuridic.ro, accesat 15.11.2017.

[12] S. D. Şchiopu, *Dreptul la delistare: trimiterile preliminare formulate de Consiliul de Stat al Franţei (cauza C-136/17)*, în Revista Universul Juridic, 27 septembrie 2017, [Online] la: http://revista.universuljuridic.ro/dreptul-la-delistare-trimiterile-preliminare-formulate-de-consiliul-de-stat-al-frantei-cauza-c-13617/, accesat 15.11.2017.

[13] M. D. Bob, *Despre precedentul judiciar şi valoarea sa de izvor de drept*, 24 martie 2009, [Online] la: https://www.juridice.ro/39497/despre-precedentul-judiciar-si-valoarea-sa-de-izvor-de-drept.html, accesat 15.11.2017.

secundară a Uniunii Europene, cu aplicare directă[14], respectiv Regulamentul general privind protecția datelor, ce va intra în vigoare la 25 mai 2018.

La o analiză mai atentă, vom observa însă că dreptul la uitare nu este neapărat o creație cu totul nouă sau originală a CJUE. În Europa, dreptul la uitare a fost recunoscut de mai mult timp – sau cel puțin din momentul în care curțile europene au început să recunoască un drept de autodeterminare informațională. Termenul de „autodeterminare informațională" a fost folosit pentru prima dată în contextul unei decizii a Curții Constituționale germane referitor la datele personale colectate cu ocazia recensământului din 1983, termenul german fiind *informationelle Selbstbestimmung*. Dreptul obiectiv al protecției datelor pare fundamentat în ideea de autodeterminare informațională care, la rândul ei, își găsește rădăcinile în ideea de liber arbitru. Filosofia protecției datelor presupune următoarele: orice persoană ar trebui să aibă dreptul să nu fie obiectul unei prelucrări a datelor sale decât dacă această prelucrare este făcută într-unul dintre temeiurile legale și dacă prelucrarea este supusă unor garanții adecvate. Cu ocazia deciziei respective[15], Curtea Constituțională Federală din Germania a statuat următoarele: „*În contextul modern al prelucrării datelor, protecția persoanei față de colectarea, stocarea, utilizarea și dezvăluirea nelimitate a datelor sale personale este cuprinsă în drepturile personale generale ale Constituției germane. Acest drept fundamental garantează, în acest sens, capacitatea persoanei de a determina, în principiu, divulgarea și utilizarea datelor sale personale. Limitările aduse acestei autodeterminări informaționale sunt permise numai în caz de nesocotire a interesului public*".

Dreptul la autodeterminare informațională reprezintă o realizare uriașă în recunoașterea drepturilor utilizatorilor. Acesta a fost inclus în art. 12 lit. (b) a Directivei privind protecția datelor prin regula care îi permite persoanei vizate (subiectului datelor) să solicite de la operator „rectificarea, ștergerea sau blocarea datelor a căror prelucrare nu respectă dispozițiile prezentei directive, în special datorită caracterului incomplet sau inexact a datelor". Dreptul la uitare nu a făcut decât să translateze dreptul la

[14] S. D. Șchiopu, *Dreptul la delistare*, *loc.cit*.

[15] BVerfGE 65, 1 vom 15.12.1983 (Volkszahlungs-Urteil) în E. Riedel, *New Bearings in German Data Protection–Census Act 1983 Partially Unconstitutional*, în 5 Human Rights Law Journal, 1984, p.94. [traducerea ne aparține].

autodeterminare informațională în domeniul digital, constatând că motoarele de căutare realizează un control al datelor și, prin urmare, trebuie considerate „operatori" în sensul art. 2 lit. (d) din Directiva 95/46/CE, ele supunându-se astfel prevederilor directivei. Dreptul la autodeterminare conferă putere persoanelor fizice împotriva operatorilor de prelucrare a datelor, precum agenți de publicitate, asiguratori, supermarketuri, brokeri de date etc, garantând autoritatea persoanei fizice, subiect al datelor, de a decide de una singură dacă datele sale pot fi divulgate sau prelucrate. Curtea germană a investit acest drept cu forță constituțională.

Rămânând în același registru, anume cel al surselor dreptului la uitare, ne vom îndrepta atenția către cea care poate fi regăsită în dreptul francez. În acest sens, avem în vedere, pe de o parte, Recomandarea R(84)10 a Comitetului de miniștri al Consiliului Europei, din 21 iunie 1984, iar, pe de altă parte, decizia CNIL nr. 01-057 din 29 noiembrie 2001[16]. Contextul ce a generat Recomandarea și decizia CNIL este cel al efectelor instituției juridice a reabilitării subiectului de drept care a primit și executat o condamnare penală. Menirea celor două documente este aceea de a încuraja o colaborare între autoritățile judiciare și presă, cu scopul de a identifica și conștientiza riscurile presupuse de rememorarea antecedentelor penale ale subiectului de drept care îndeplinește condițiile reabilitării și care încearcă o reintegrare socială[17]. Cu alte cuvinte, este recomandat organelor de presă ca, odată ce subiectul de drept se califică pentru a-i fi aplicate efectele reabilitării, de drept sau judiciare, să nu mai dea spre publicare informațiile cu caracter personal ce privesc persoana în cauză și infracțiunea în legătură cu ale cărei consecințe intervine instituția reabilitării[18].

Din analiza obiectivului urmărit de cele două documente deducem că, în realitate, dreptul la uitare se prezintă ca un instrument juridic necesar și util pentru ca instituția juridică a reabilitării să își producă efectele în mod

[16] *Le droit a l'oubli*, [Online] la: http://www.prison.eu.org, accesat 15.11.2017.
[17] *Ibidem.*
[18] În prezent, pentru o aplicare eficace a acestei recomandări s-ar putea apela, printr-o interpretare extensivă și în sensul de a produce efecte juridice, la prevederile art. 226-20 Cod penal francez, care fac vorbire despre sancțiunile aplicabile în situația în care datele personale cu privire la o anumită persoană sunt păstrate cu depășirea termenului prevăzut de lege, termen care, în acest caz, ar putea fi interpretat ca fiind cel ulterior intervenirii reabilitării persoanei care a suferit o condamnare penală. Acestea ar putea fi privite ca un mijloc eficient pentru ca obiectul recomandării în discuție să fie respectat.

eficient și de așa natură încât reintegrarea socială a persoanei care a executat o pedeapsă penală să fie una realizabilă.

Așadar, reabilitarea, ca mijloc juridic prin care, în condițiile prevăzute de lege, sunt înlăturate pentru viitor consecințele unei condamnări, respectiv interdicțiile, incapacitățile și decăderile ce rezultă din condamnare[19], nu este altceva decât ștergerea trecutului penal al subiectului de drept cu privire la consecințele infracțiunii în legătură cu care a intervenit reabilitarea. În acest sens, ca efect al reabilitării, va fi înlăturată, din oficiu sau ca urmare a unei hotărâri judecătorești, în funcție dacă facem vorbire despre reabilitarea de drept sau despre cea judecătorească, din cuprinsul certificatului de cazier judiciar, condamnarea cu privire la subiectul de drept în cauză[20].

Principalul scop pentru care sistemul de drept a creat beneficiul reabilitării persoanei care a fost subiectul unei condamnări penale, sub rezerva condițiilor prevăzute de lege, anume caracteristicile infracțiunii ce urmează a fi reabilitată, termenul de reabilitare și conduita persoanei condamnate, în sensul ca aceasta să nu mai fi săvârșit nicio infracțiune și să nu mai fi suferit nicio condamnare, este ca persoana condamnată să aibă o reală posibilitate de fi reintegrată din punct de vedere social.

Așadar, pentru ca efectele reabilitării să poată să se producă în mod eficient și, în consecință, reintegrarea socială a persoanei condamnate să fie una realizabilă, este de înțeles și pe deplin justificată poziția înfățișată în recomandare și în decizia CNIL, anterior menționate. Dacă această recomandare nu este urmată, respectiv informațiile cu caracter personal și referitoare la detaliile cu privire la infracțiunea săvârșită de către subiectul de drept pot fi găsite în continuare, deși subiectul de drept îndeplinește condițiile cerute de lege pentru reabilitare printr-o simplă căutare nominală a persoanei în cauză în link-urile afișate de motoarele de căutare Google, reabilitarea devine o instituție juridică ineficientă și inutilă, persoana condamnată fiind nevoită să se confrunte în continuare cu consecințele condamnării penale, demersul său de reintegrare socială dovedindu-se cu siguranță mai anevoios. În concret, prin imaginarea unui exemplu, chiar dacă persoana condamnată penal, în momentul când participă la un interviu pentru

[19] Pentru detalii asupra reabilitării şi a efectelor acesteia, în sistemul de drept românesc, a se vedea N. Volonciu şi colectivul, *Noul Cod de procedură penală*, Editura Hamangiu, Bucureşti, 2015.

[20] *Le droit a l'oubli*, *ibidem*, p. 7.

a obține o slujbă, prezintă dosarul de angajare, cuprinzând certificatul de cazier judiciar, din care a fost înlăturată mențiunea cu privire la condamnarea penală suferită, dacă angajatorul dorește să realizeze o proprie informare în legătură cu potențialul său angajat, printr-o simplă căutare pe internet, motoarele de căutare Google îi vor deschide link-urile unde se găsesc informații cu privire la condamnarea penală aplicată persoanei respective, caz în care, în mod evident, instituția reabilitării este lipsită de esența efectelor sale, și anume ștergerea informațiilor cu privire la condamnare din evidența destinată publicului[21] și facilitarea unei reintegrări sociale.

În acest context, supraviețuirea informațiilor cu caracter personal, și anume detaliile cu privire la infracțiunea și condamnarea penală în legătură cu o anumită persoană, ulterior momentului în care aceasta se califică pentru a se bucura de efectele reabilitării, se prezintă ca o încălcare a dreptului la demnitate, la imagine și la viață intimă și privată, cauzând, astfel, un prejudiciu celui în cauză.

Nu în ultimul rând, în tradiția juridică britanică, esența dreptului la uitare ține mai degrabă de dreptul de proprietate: „dacă informația este proprietatea mea privată, eu sunt cel care decide cât anume din ea se poate dezvălui publicului". Dreptul a fost catalogat drept unul care ține de demnitatea umană și, respectiv, servește drept fundament dreptului la viață privată. Recentul GDPR, la art. 88 referitor la Prelucrarea în contextul ocupării unui loc de muncă, face trimitere expresă la faptul că aceste norme „*includ măsuri corespunzătoare și specifice pentru garantarea demnității umane, a intereselor legitime și a drepturilor fundamentale ale persoanelor vizate*"[22]. Și, în plus, pentru întreaga Europă post-89, posibilitatea de a fi uitat este văzută ca o măsură suplimentară în consolidarea democrației și a pluralismului, iar colectarea de informații personale este încă percepută ca un instrument puternic în mâna regimurilor totalitare.

[21] N. Volonciu și colectivul, *op. cit.*

[22] *Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE* (Regulamentul general privind protecția datelor), publicat în Jurnalul Oficial al Uniunii Europene, L 119 din 4 mai 2016.

Criteriile stabilite de *Google Spain*

Raportat la cadrul legislativ și jurisprudențial care întemeiază dreptul la uitare, ne vom îndrepta atenția asupra înțelesului unor noțiuni cu ajutorul cărora poate fi încercată o delimitare a domeniului de aplicare a dreptului la uitare și a persoanelor vizate de aplicarea acestuia.

Astfel, „date cu caracter personal", în sensul Regulamentului (GDPR), înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

Prin „prelucrare a datelor cu caracter personal" se înțelege orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea datelor cu caracter personal.

Din reglementarea GDPR, coroborată cu interpretarea dată de CJUE acestei noțiuni regăsite în Directiva 95/46, rezultă că prin „operator"/„controlor" se înțelege persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern.

Prin „persoană împuternicită de operator" se înțelege persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

În considerarea înțelesului acestor noțiuni este esențial de menționat că, din motivarea Curții de Justiție a Uniunii Europene, reiese faptul că motoarele de căutare Google sunt calificate ca fiind controlori care efectuează procesare de date personale, motorul de căutare fiind cel care

determină scopul și mijloacele procesării de date cu caracter personal[23]. Ca urmare a acestei interpretări, activitatea motorului de căutare atrage răspunderea operatorului Google pentru prelucrarea informațiilor cu caracter personal și, în consecință, îl califică pe acesta ca subiect de drept căruia îi este opus dreptul la uitare, în sensul realizării operațiunii de delistare, de înlăturare a link-ului ce conține datele cu caracter personal ale persoanei care se califică, în sensul prevederilor GDPR, să formuleze o cerere în acest scop.

Ca urmare a calificării motorului de căutare ca fiind controlor/operator se prezintă și noutatea legislativă conținută în Regulamentul pentru protecția datelor cu caracter personal, respectiv cea care privește inversarea sarcinii probei. Așadar, dacă în temeiul Directivei 95/46 sarcina probei revine petentului, odată ce Regulamentul va fi aplicat, sarcina probei va fi inversată, operatorul fiind cel care va trebui să justifice necesitatea păstrării și prelucrării datelor[24]. Potrivit noii reglementări, persoana care solicită dreptul la uitare nu va mai fi ținută să justifice „motive întemeiate și legitime" raportate la situația sa particulară, ci va trebui să arate doar „motive" [25] în legătură cu situația particulară în care se află, operatorul fiind cel care va trebui să probeze că se află în una dintre situațiile expres prevăzute de Regulament în baza cărora îi este permis să continue păstrarea și prelucrarea datelor cu caracter personal[26].

Pe lângă importantele reguli stabilite și prezentate deja, *Google Spain* mai are și meritul de a preciza, chiar dacă de o manieră destul de generală, care sunt categoriile de informații pe care motoarele de căutare care operează în Europa trebuie să le șteargă sau să le delisteze/dezindexeze din rezultatele căutării, și anume informațiile *„inexacte (…) inadecvate, nepertinente sau excesive în raport cu scopurile prelucrării"* sau acele informații care nu *„sunt actualizate sau sunt păstrate pentru o perioadă mai lungă decât cea necesară, cu excepția cazului în care păstrarea lor se impune în scopuri istorice, statistice sau științifice"*[27]. La această excepție se mai adaugă una, precizată în chiar ultimul alineat al dispozitivului *„Nu aceasta ar fi însă situația dacă ar reieși că, din motive speciale, precum*

[23] În acest sens, a se vedea pct. 32 și urm. din cauza C-131/12.

[24] E. Chelaru, M. Chelaru, *Right to be forgotten*, în Annales Universitatis Apulensis-Seria Jurisprudentia, nr. 16/2013, p. 6.

[25] *Regulamentul (UE) 2016/679,* art. 21 alin. (1).

[26] S.-D. Șchiopu, *Efectivitatea dreptului de a fi uitat*, în I. Alexe, N.-D. Ploeșteanu, D.-M. Șandru, *Protecția datelor cu caracter personal*, Editura Universitară, București, p. 198.

[27] Cauza C-131/12, 92.

rolul jucat de persoana respectivă în viața publică, ingerința în drepturile sale fundamentale este justificată de interesul preponderent al publicului menționat de a avea acces, prin intermediul acestei includeri, la informația în cauză".

Interesul public, sau „interesul preponderent al publicului", așa cum se exprimă *Google Spain*, este o noțiune care poate ridica probleme în implementare, dată fiind natura sa prea generală. Noțiunea de interes public este definită în Legea nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public. Conform art. 2, lit. (b), *„prin informație de interes public se înțelege orice informație care privește activitățile sau rezultă din activitățile unei autorități publice sau instituții publice, indiferent de suportul ori de forma sau de modul de exprimare a informației"*. Iar conform art. 14 din aceeași lege, *„Informațiile cu privire la datele personale ale cetățeanului pot deveni informații de interes public numai în măsura în care afectează capacitatea de exercitare a unei funcții publice"*. Definiția este însă incompletă și, oricum, aceasta este prevăzută în Legea nr. 544/2001, referitoare la obligațiile de transparență ale autorităților și instituțiilor publice. Sfera informațiilor de interes public este însă mult mai largă, acestea cuprinzând orice informație legată de interesele generale ale societății. „O informație de interes public trebuie să urmărească conștientizarea publicului cu privire la interesele sale generale, într-un context social existent la un moment dat și la modul în care acestea pot fi satisfăcute. De asemenea, dacă justiția nu merge bine, presa are rolul de a evidenția cauzele într-o manieră accesibilă, prin exemplificări, interviuri, astfel încât publicul să le poată evalua și să acționeze în consecință"[28].

În plus, această justificare a unei ingerințe în dreptul la viață privată al unei persoane prin recurgerea la interesul preponderent al publicului nu este doar prea generală ci și, potrivit unor opinii, discutabilă. Într-un stat liberal, „o libertate de bază nu poate fi limitată sau refuzată decât pentru a proteja una sau mai multe alte libertăți de bază și niciodată (…) în numele binelui public sau al valorilor perfecționiste"[29], ceea ce echivalează cu a spune că niciuna dintre cauzele ce duc la restrângerea exercițiului drepturilor sau libertăților nu poate fi invocată în sine și pentru sine, ci doar pentru apărarea drepturilor și libertăților celorlalți. În opinia profesorului Dan-

[28] C. M. Cercelescu, *Regimul juridic al presei. Drepturile și obligațiile jurnaliștilor*, Editura Teora, 2002, p. 98.

[29] J. Rawls, *Libéralisme politique*, PUF, Quadrige, Paris, 2007.

Claudiu Dănișor, această necesitate a restrângerii exercițiului drepturilor ori libertăților într-o societate liberală, distinctă de necesitatea într-o societate democratică, presupune îndeplinirea cumulativă a cel puțin patru categorii de condiții de invocare: „respectarea de către stat a priorității libertății, respectarea priorității justului asupra binelui, respectarea priorității autodeterminării individului, și menținerea neutralității statului în cursul procedurii”[30].

Pentru a răspunde acestei probleme și altor întrebări ridicate de implementarea deciziei *Google Spain*, pe 26 noiembrie 2014, în cadrul reuniunii plenare a Grupului de lucru „Art. 29”, format din reprezentanții autorităților de supraveghere a prelucrării datelor personale din statele membre ale Uniunii Europene, s-a adoptat un ghid privind implementarea hotărârii CJUE. Ghidul conține interpretarea hotărârii, precum și criterii ce urmează să fie folosite de autoritățile naționale de supraveghere în soluționarea plângerilor care le sunt înaintate. Potrivit Grupului de lucru, trebuie să se mențină un echilibru între natura și sensibilitatea datelor și interesul publicului de a avea acces la aceste informații. Cu toate acestea, dacă subiectul joacă un rol în viața publică, interesul publicului va fi semnificativ mai ridicat. Prin urmare, concluzionează ghidul, impactul delistării asupra libertății de exprimare a individului și asupra dreptul de acces la informație va fi limitat. Atunci când autoritățile naționale de supraveghere evaluează circumstanțele relevante, delistarea nu va fi adecvată dacă interesul publicului aduce atingere drepturilor subiectului ale cărui date personale sunt prelucrate. Ghidul conține și 13 criterii principale pe care autoritățile naționale să le aplice plângerilor cu care se confruntă ca urmare a refuzului motoarelor de căutare de a delista.

În ciuda ghidului Grupului de lucru, cum consacrarea dreptului la uitare digitală are o origine pretoriană, limitele acestuia au rămas relativ difuze, ceea ce a condus la solicitarea unor clarificări ale acestora pe calea unei cereri de decizie preliminară introdusă de Consiliul de Stat francez la 15 martie 2017[31]. Întrebările preliminare provin dintr-o serie de litigii între CNiL (Commission Nationale de l’Informatique et des Libertés) și patru

[30] D.C. Dănișor, *Justificarea necesității restrângerii exercițiului drepturilor ori libertăților într-o societate liberală*, în Revista Română de Drept Privat, nr. 1, 2014, p. 50.

[31] *Cerere de decizie preliminară* introdusă de Conseil d’État (Franța) la 15 martie 2017 – *G. C., A. F., B. H., E. D./Commission nationale de l’informatique et des libertés (CNIL)*, cauza *C-136/17*, publicată în Jurnalul Oficial al Uniunii Europene C 168/24 din 29 mai 2017.

persoane care fiecare în parte au adresat plângeri[32] autorității franceze de supraveghere pentru a obține delistarea unor link-uri care duceau către diverse pagini web ce figurau în lista de rezultate obținută în urma unei căutări efectuate pe baza numelor lor pe motorul de căutare al societății Google Inc.

În încheiere, ne vom opri asupra unuia dintre criteriile stabilite de *Google Spain*, și anume importanța trecerii timpului. Ideea de trecere a timpului nu este străină domeniului juridic, aceasta fiind invocată chiar de domnul Costeja Gonzalez în cauza C-131/12 *Google Spain și Google Inc*., care afirmă că, dat fiind faptul că au trecut 16 ani de la momentul care a determinat prelucrarea datelor sale cu caracter personal, timp în care situația care a presupus această prelucrare a fost pe deplin rezolvată, păstrarea acestor informații nu mai prezintă relevanță.

---

[32] „În cazul primei persoane vizate este vorba de un fotomontaj satiric publicat pe Youtube la data de 18 februarie 2011 ce o înfățișează lângă primarul localității a cărei directoare de cabinet fusese și în care este evocată în mod explicit relația intimă care ar fi existat între ei, precum și incidența acestei relații asupra propriului ei parcurs politic. Acest fotomontaj a fost publicat online cu ocazia campaniei electorale pentru alegerile cantonale la care a candidat persoana vizată. La momentul când cererea de dezindexare i-a fost refuzată, persoana vizată nu era nici aleasă, nici candidată la alegerile locale și nici nu mai exercita funcția de directoare de cabinet a primarului comunei.

În cazul celei de-a doua persoane vizate, este vorba de un articol din data de 9 septembrie 2008 publicat în cotidianul Libération, articol reprodus pe site-ul Centrului contra manipulărilor mentale (Centre contre les manipulations mentales) și care privește sinuciderea unui adept al Bisericii scientologice în decembrie 2006, persoana vizată fiind menționată în acest articol în calitate de responsabil cu relațiile publice al Bisericii scientologice, profesie pe care a încetat să o mai exercite între timp. Autorul articolului menționează că a contactat persoana vizată pentru a obține versiunea acesteia a faptelor și relatează informațiile culese cu această ocazie.

În cazul celei de-a treia persoane vizate este vorba de articole, în principal de presă, privind declanșarea cercetării penale în iunie 1995 cu privire la finanțarea Partidului Republican, procedură în cadrul căreia a fost cercetat împreună cu mai mulți oameni de afaceri și personalități politice. În cazul persoanei vizate s-a decis neînceperea urmării penale, majoritatea linkuri-lor ducând către articole contemporane declanșării cercetării penale și care prin urmare nu prezintă modul în care s-a finalizat aceasta.

În cazul celei de-a patra persoane vizate este vorba de două articole publicate în Nice Matin și le Figaro care prezintă ședința de judecată în cadrul căreia a fost condamnat la pedeapsa de 7 ani închisoare și o pedeapsă complementară de 10 ani de supraveghere socio-judiciară pentru fapte de agresiune sexuală comise asupra minorilor de 15 ani. Una din aceste cronici judiciare menționează, printre altele, mai multe detalii intime relative la persoana vizată ce au fost revelate cu ocazia procesului." [traducerea S.-D. Șchiopu, *Dreptul la delistare: trimiterile preliminare formulate de Consiliul de Stat al Franței (cauza C-136/17)*, în Revista Universul Juridic, 27 septembrie 2017, [Online] la: https://www.universuljuridic.ro/dreptul-la-delistare-trimiterile-preliminare-formulate-de-consiliul-de-stat-al-frantei-cauza-c-136-17/, accesat 15.11.2017].

Argumentul bazat pe trecerea timpului a fost unul decisiv în hotărârea pronunțată de Curtea Europeană a Drepturilor Omului în cauza *Plon c. Franței*[33]. Vom realiza o scurtă prezentare a acestei hotărâri CEDO pentru a arăta relevanța trecerii timpului și în ce măsură raționamentul aplicat în cazul acestei hotărâri își poate găsi aplicare în ceea ce privește lămurirea înțelesului celor patru criterii trasate în legătură cu caracteristicile informațiilor cu caracter personal ce fac obiectul unei cereri de delistare.

Reclamanta, editura Plon din Franța, atacă la instanța europeană hotărârea Curții de Casație Franceze, din data de 14 decembrie 1999. Prin această hotărâre, Curtea de Casație respinge recursul formulat de către reclamantă, societatea Plon. Hotărârea pe care societatea Plon a atacat-o viza obligația acesteia de a achita daune-interese pentru publicarea unei cărți, *Le Grand Secret*, și interzicerea dispusă de către instanțele franceze de a difuza această carte. Cartea ce a format obiectul interdicției are ca subiect boala de care a suferit fostul președinte al Franței, François Mitterand, diagnosticarea și tratamentul aplicat. În fapt, inițial, cartea a fost publicată la 11 zile după decesul fostului președinte.

Difuzarea cărții a fost atacată de familia lui Mitterand. Ca urmare a acestui lucru, instanța națională franceză, mai întâi, printr-o ordonanță judiciară, dispune măsura suspendării difuzării cărții, iar apoi, pronunțându-se pe fond, la 9 luni de la momentul suspendării difuzării, confirmă această măsură și dispune interzicerea definitivă a difuzării cărții și obligarea societății Plon la daune-interese pentru prejudiciul provocat. În motivarea hotărârii au fost invocate argumentele că publicarea acestei lucrări nu a respectat principiul proporționalității și secretul confidențialității informațiilor medicale și, de asemenea, faptul că avut loc o încălcare a dreptului la respectarea memoriei fostului președinte și a dreptului la viață privată, raportat la familia acestuia.

În fața acestei hotărâri, societatea Plon, invocând că se încalcă dreptul său la libertate de exprimare, se adresează Curții Europene a Drepturilor Omului.

În acest sens, Curtea Europeană apreciază că prin interdicția definitivă de difuzare a cărții, dispusă de instanța națională, a avut loc o încălcare a dreptului la libertate de exprimare în ceea ce îl privește pe reclamant. Curtea afirmă că, dacă măsura provizorie de suspendare a

[33] Hotărârea CEDO nr. 58148/00, *Plon c. Franței*, 18 mai 2004.

difuzării cărții a fost una corectă și proporțională cu scopul urmărit, și anume respectarea memoriei persoanei decedate și a secretului profesional cu privire la istoricul medical al persoanei și dreptul la viață intimă și privată a familiei fostului președinte, François Mitterand, cea prin care interzicerea difuzării cărții a fost dispusă cu caracter definitiv nu mai este apreciată ca fiind una justificată și proporțională cu scopul urmărit. Curtea consideră că la momentul în care instanța națională s-a pronunțat pe fond, la 9 luni de la momentul în care a avut loc publicarea cărții, a trecut deja destul timp și drept urmare impactul, atât cu privire la memoria fostului președinte, cât și cu privire la familia acestuia, nu mai este același, devenind prioritar interesul public cu privire la datele istorice în legătură cu fostul președinte Mitterand. Așadar, așa cum se poate observa, argumentul trecerii timpului a fost decisiv, simpla trecere a timpului fiind cea în temeiul căreia măsura interzicerii difuzării cărții este recalificată din una corectă și proporțională în una nejustificată și care determină o încălcare a dreptului la libertate la exprimare ce aparține petentului, societatea Plon.

În considerarea acestei abordări a Curții Europene, aducem în discuție întrebarea în ce măsură ideea de trecere a timpului poate sau trebuie să fie luată în considerare ca punct de reper în delimitarea întinderii și înțelesului celor patru criterii avute în vedere de CJUE în cauza C-131/12 *Google Spain și Google Inc*. și, de asemenea, ca un argument autonom în vederea unei soluții favorabile cu privire la o cerere de delistare.

Ne referim în acest sens la faptul dacă cel care înaintează o cerere de delistare ar putea să o întemeieze pe ideea că, datorită trecerii timpului, informațiile cu caracter personal, care poate la momentul apariției prezentau importanță, ajung să nu mai fie relevante și păstrarea lor să nu mai fie astfel justificată. Să înțelegem de aici că, dacă inițial o cerere de delistare a fost respinsă, după ce a trecut o perioadă de timp, aceasta ar putea fi reluată și, dacă da, răspunsul de această dată ar putea fi unul diferit?

În sprijinul unui răspuns afirmativ, în sensul că ideea trecerii timpului poate constitui un argument convingător în această materie, se prezintă chiar motivarea CJUE în cauza C-131/12 *Google Spain și Google Inc*., care afirmă că, în considerarea trecerii timpului, păstrarea informațiilor a căror delistare se solicită se dovedește a fi inadecvată, irelevantă sau

excesivă[34]. Așadar, chiar dacă inițial prelucrarea și publicarea datelor cu caracter personal a fost una licită și justificată, în fața trecerii timpului, ele devin incompatibile cu condițiile normative stipulate în legătură cu prelucrarea datelor cu caracter personal, respectiv cu prevederile Directivei 95/46.

Critici și probleme ridicate de dreptul la uitare

În continuare ne vom îndrepta atenția către problemele ce ar putea să apară în situația aplicării în concret a dreptului la uitare, probleme ce vizează diferite domenii, de la cele cu caracter antropologic, la cele cu valențe juridice și până la cele de ordin tehnic.

Ștergerea istoriei

O primă problemă ce ar putea să survină este una de natură antropologică, respectiv ștergerea istoriei ca urmare a unei aplicări abuzive și discreționare a dreptului la uitare, de așa manieră încât scopul pentru care a fost creat să fie depășit.

Această problemă ar putea să apară în special în contextul globalizării aplicării dreptului la uitare, chestiune pendinte la Curtea de Justiție a Uniunii Europene.

În legătură cu acest aspect, se apreciază că ștergerea istoriei ar putea fi cauzată ca urmare a unei aplicări abuzive, mult prea largi, a dreptului la uitare de către statele cu un regim politic totalitar și în care libertatea de exprimare este mult mai restrânsă[35]. Astfel, aceste state ar putea să vadă în dreptul la uitare un mijloc prin care să controleze opinia publică din punct de vedere social, politic și moral, respectiv dreptul la uitare să devină în mâna acestora un instrument de cenzură politică și socială, istoria devenind astfel una conturată și favorabilă regimului politic totalitarist. Pe această linie de gândire, aplicarea globală a dreptului la uitare, respectiv înlăturarea globală a

[34] Cauza C 131/12 *Google Spain și Google Inc*, „Rezultă din aceste cerințe, prevăzute la articolul 6 alineatul (1) literele (c)-(e) din Directiva 95/46, că și o prelucrare inițial licită a unor date exacte poate deveni cu timpul incompatibilă cu această directivă în cazul în care datele respective nu mai sunt necesare în raport cu scopurile pentru care au fost colectate sau prelucrate. Aceasta este situația în special atunci când ele sunt inadecvate, atunci când nu sunt sau nu mai sunt pertinente ori sunt excesive în raport cu scopurile amintite și cu timpul care s-a scurs".

[35] A. Hern, *ECJ to rule on whether „right to be forgotten" can strech beyond EU*, [Online] la: https://www.theguardian.com/technology/2017/jul/20/ecj-ruling-google-right-to-be-forgotten-beyond-eu-france-data-removed, accesat 15.11.2017.

link-urilor, ar determina un grav precedent care ar permite figurilor și guvernelor autoritare, cum ar fi China, Pakistan, Rusia, Turcia să încerce o cenzură globală a internetului, putându-se ajunge până la înlăturarea unor evenimente esențiale dintre cele care ar trebui să constituie istoria unei națiuni, cum ar fi, de pildă, referințele cu privire la cele întâmplate în Piața Tiananmen[36].

Ca o confirmare a acestei temeri este modul în care Rusia a decis să abordeze aplicarea dreptului la uitare. Ca urmare a hotărârii CJUE, Rusia legiferează dreptul la uitare printr-o lege[37] cu același nume, în iulie 2015, actul normativ intrând în vigoare la data de 1 ianuarie 2016. În temeiul acestei legi, persoanele fizice din Rusia au dreptul să solicite înlăturarea din motoarele de căutare a informațiilor cu caracter personal, care se dovedesc a fi irelevante sau inadecvate. În ceea ce privește conținutul prevederilor acestei legi, deși pe de o parte, respectă optica și criteriile prezente în cauza C-131/12 și în Regulamentul privind protecția datelor cu caracter personal, pe de altă parte, apar numeroase deosebiri. Aceste diferențe, de substanță și cu un impact major în maniera în care dreptul la uitare este înțeles și aplicat, rezultă din faptul că actul normativ rus nu prevede o delimitare clară și criterii suficiente care să contureze limitele de aplicare a acestei legi ci, din contră, acordă persoanelor publice posibilitatea expresă de a solicita dreptul la uitare[38]. Așadar, ceea ce în prevederile Regulamentului pentru protecția datelor și în considerentele cauzei C-131/12 constituie o limită, respectiv faptul că persoanele publice nu se pot bucura de dreptul la uitare, prioritatea fiind acordată dreptului la informare publică și la libertate de exprimare, în Rusia, persoanelor publice le este oferită în mod expres această prerogativă, libertatea de exprimare, cu cele două valențe ale sale, dreptul la exprimarea unei opinii și dreptul de a fi informat, în consecință, aflându-se într-un real pericol, neexistând un echilibru între aceste libertăți fundamentale și dreptul

[36] G. Sterling, *Two major changes potentially coming to EU's Right to Be Forgotten with global implications*, [Online] la: https://searchengineland.com/two-major-changes-potentially-coming-eus-right-forgotten-global-implications-275047, accesat 15.11.2017.

[37] Federal law 264-FZ, 13 iulie 2015.

[38] R. Nurullaev, *Right to be forgotten în the European Union and Russia: Comparison and Criticism*, în *Law in the Modern World Journal*, [Online] la: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2669344, accesat 15.11.2017; V. Shaftan, *Russia signs controversial "right to be forgotten" bill into law*, [Online] la: https://www.dataprotectionreport.com/2015/07/russia-signs-controversial-right-to-be-forgotten-bill-into-law/, accesat 15.11.2017.

la viață privată și intimă, interesele petentului prevalând în fața celor presupuse de interesul public[39].

Așadar, în considerarea modului în care Rusia a ales să reglementeze dreptul la uitare, este lesne de observat că, în lipsa limitei impuse cu privire la persoanele publice și dreptul acestora de a beneficia de uitare prin cereri de delistare, granițele unei abordări raționale și judicioase pot fi foarte ușor încălcate înspre o aplicare abuzivă, discreționară și care să contravină scopului pentru care dreptul la uitare a fost creat.

Libertatea de exprimare

O altă problemă este cea ridicată de faptul că prin dreptul la uitare și, mai exact, o apărare excesivă a sa, s-ar ajunge la încălcări nepermise ale libertății de exprimare.

În realitate, dreptul la uitare este despre punerea în balanță a protecției datelor și a intereselor economice, și mai puțin despre un conflict între protecția datelor și libertatea de exprimare. *Google Spain* și, cu atât mai mult, Regulamentul european nu au uitat de libertatea de exprimare. CJUE a precizat, în dispozitivul său, că dreptul la viață privată al persoanei *„prevalează în principiu nu numai asupra interesului economic al operatorului motorului de căutare, ci și asupra interesului acestui public de a avea acces la informația respectivă cu ocazia unei căutări referitoare la numele acestei persoane”*. Acest lucru nu este deloc surprinzător, având în vedere că dreptul la viață privată reprezintă, prin însăși esența sa, o formă de cenzură și se opune libertății de exprimare, dificultatea constând în a găsi justul echilibru dintre cele două. Dreptul la demnitate, ca parte integrantă a dreptului la viață privată, presupune tocmai să nu diseminezi anumite informații despre o persoană anume. Drepturile personalității sunt cele care definesc limitele libertății de exprimare, și nu invers. Cu toate acestea, dovedind că nu a intenționat o încălcare a libertății de exprimare, CJUE a precizat, în plus, că această regulă generală nu se va aplica în cazul în care *„ar reieși că, din motive speciale, precum rolul jucat de persoana respectivă în viața publică, ingerința în drepturile sale fundamentale este justificată de interesul preponderent al publicului menționat de a avea acces, prin intermediul acestei includeri, la informația în cauză”*.

[39] R. Nurullaev, *op. cit*., p. 190.

Mai mult decât atât, pentru o protecție și mai consolidată a libertății de exprimare, decizia stabilește și situația specială „*numai în scopuri jurnalistice*”, care exonerează paginile web care publică știri de la implementarea dreptului de a fi uitat, prevedere ce se regăsea și în Directiva privind protecția datelor. CJUE precizează: „nu poate fi exclus ca persoana vizată să poată în anumite împrejurări să își exercite drepturile prevăzute la articolul 12 litera (b) și la articolul 14 primul paragraf litera (a) din Directiva 95/46 în raport cu operatorul menționat, însă *nu* și în raport cu editorul paginii web respective”.

Considerăm că nu libertatea de exprimare este pusă în pericol, ci mai degrabă însăși eficiența dreptului la uitare, având în vedere că regulamentul conține prevederi mult mai stricte decât o făcea Directiva privind protecția datelor sau dispozitivul *Google Spain*. Dreptul la uitare nu se aplică atunci când datele sunt comunicate *„în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice (…) în măsura în care dreptul menționat la alineatul (1) este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective”*[40]. În plus, și excepția privind activitățile jurnalistice este mai largă decât echivalentul său din directivă. Excepția nu mai este limitată la prevederea din Directiva 95/46/CE *„Statele membre prevăd exonerări și derogări de la dispozițiile prezentului capitol, ale capitolului IV și ale capitolului VI pentru prelucrarea datelor cu caracter personal efectuată numai în scopuri jurnalistice, artistice sau literare, în măsura în care se dovedesc necesare pentru a pune dreptul la viață privată în acord cu normele care reglementează libertatea de exprimare”*[41]. Mai degrabă, excepția își propune să asigure un echilibru „*între dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament și dreptul la libertatea de exprimare și de informare, inclusiv prelucrarea în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare”*[42].

Nu în ultimul rând, în cazul „dreptului la restricționarea prelucrării”, un drept nou introdus de Regulament, la articolul 18, operatorul are obligația să restricționeze prelucrarea și, astfel, să blocheze accesul la date imediat

[40] *Regulamentul (UE) 2016/679*, art. 17 alin. (3).

[41] Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date.

[42] *Regulamentul (UE) 2016/679*, art. 85, alin. (1).

după solicitare, *„pentru o perioadă care îi permite operatorului să verifice exactitatea datelor”*. Legiuitorul a introdus o prevedere care înclină balanța în favoarea dreptului la viață privată, restrângând accesul la conținut până la verificarea exactității datelor. Nu există consecințe îngrijorătoare pentru libertatea de exprimare. În primul rând, situația aceasta este cu totul diferită de dreptul la uitare pentru că nu se aplică decât în acele cazuri în care exactitatea datelor personale este contestată. În plus, restricționarea aceasta este de scurtă durată. Restricția urmează să fie ridicată imediat după ce operatorii au efectuat verificarea exactității datelor. Durata procedurii ar trebui să fie egală cu cea folosită la procesarea cererilor privind dreptul la uitare, redusă în ultimii doi ani la mai puțin de 20 de zile per cerere[43].

Imposibilitate tehnică

O altă problemă care s-ar putea pune în discuție în legătură cu aplicarea în concret a dreptului la uitare este cea determinată de dificultățile presupuse de implementarea din punct de vedere tehnic a acestui drept.

Dificultatea a fost sesizată de Google în statisticile[44] realizate după momentul pronunțării CJUE în cauza C-131/12. Potrivit acestora, implementarea dreptului la uitare determină o povară din punct de vedere administrativ, costuri semnificative, dat fiind faptul că fiecare cerere trebuie procesată manual și apreciată din punct de vedere al admisibilității acesteia, procedură laborioasă și care presupune acordarea unei perioade de timp semnificative[45].

Cu privire la aceste probleme ce ar putea să survină în vederea aplicării dreptului la uitare au fost sugerate câteva posibile soluții, precum cea în care munca de cântărire a admisibilității și relevanței cererii de delistare să revină unei autorități publice sau cea în care această sarcină este acordată unor organizații colective de management, care în prezent sunt utilizate în procesul de soluționare a cererilor privind încălcarea dreptului de autor[46].

---

[43] G. Sterling, Report: *2 Years in, 75 Percent of Right to Be Forgotten Asks Denied by Google*, în Search Engine Land, 12 mai 2016, [Online] la: http://searchengineland.com/report-2-years-75-percent-right-forgotten-asks-deniedgoogle-249424, accesat 15.11.2017.

[44] Google Transparency Report, *European privacy requests for search removals*, [Online] la: https://www.google.co/transparencyreport/removals/europeprivacy, accesat 15.11.2017.

[45] E. Bougiakiotis, *The Enforcement of The Google Spain Ruling*, International Journal of Law and Information technology, 2016, pp. 318-319.

[46] Idem, p. 319.

Cu privire la această dificultate ridicată de implementarea dreptului la uitare a fost exprimat și un punct de vedere[47] care a încercat să minimalizeze importanța acesteia. În motivarea acestei opinii a fost realizată o comparație între numărul cererilor privind încălcarea dreptului de autor depuse spre soluționare raportat la numărul de cereri de delistare, având în vedere că procesul de decizie cu privire la cele dintâi este la fel sau chiar mai dificil decât cel presupus de cele din urmă.

Astfel, pe de o parte, Google a anunțat că a primit 12.000 de cereri de la persoane fizice pentru a elimina datele lor personale din motorul de căutare în chiar prima zi în care a acceptat astfel de solicitări, iar, pe de altă parte, cifrele cu privire la copyright arată că au fost primite mai mult de 23 de milioane de cereri de eliminare de URL-uri din cauza acuzațiilor de încălcare a drepturilor de autor pe parcursul unei luni, rezultând un număr de 787.000 de astfel de solicitări în fiecare zi. Așadar, din analiza acestei comparații rezultă că, în realitate, această problemă despre care facem vorbire și pe care Google o invocă este până la urmă o falsă problemă sau, cel puțin, una care nu prezintă relevanță.

Extrateritorialitatea implementării dreptului la uitare

O altă presupunere falsă ține de întinderea aplicării recent câștigatului drept, în sensul că este aproape imposibil să se realizeze, online, o blocare totală a unui anumit conținut, odată ce acesta a fost publicat[48]. Instituțiile europene susțin ideea că delistarea (dezindexarea) ar trebui să aibă o acoperire extrateritorială. Astfel, Grupul de lucru „Art. 29” a subliniat faptul că limitarea delistării la domeniile (internet) din cadrul Uniunii Europene nu poate fi considerată o măsură suficientă pentru a garanta în mod satisfăcător protejarea drepturilor persoanelor vizate, în conformitate cu dispozitivul *Google Spain* și, mai recent, cu prevederile GDPR. Mai exact,

[47] V. Reding, *Right to Be Forgotten Is No Harder to Enforce than Copyright***,** [Online] la: https://www.theguardian.com/technology/2014/jun/04/eu-commissioner-right-to-be-forgotten-enforce-copyright-google, accesat 15.11.2017.

[48] „Mă tem că într-o «infosferă» ce nu cunoaște limitele geografice, obligația impusă motoarelor de căutare de a bloca accesul la un conținut nu va fi niciodată soluția optimă. Dacă un anumit conținut este dăunător, acesta ar trebui să fie blocat la sursă, pentru orice motor de căutare, de oriunde, sau eliminat complet, așa cum se procedează în cazul pornografiei infantile. Aceasta ar fi singura implementare eficientă a dreptului la uitare”, L. Floridi, *We Dislike the Truth and Love to Be Fooled* , în CYCEON, 21 noiembrie 2016, [Online] la: https://cyceon.com/2016/11/21/luciano-floridi-oxford-uk-google-interview, accesat 15.11.2017.

aceasta ar presupune ca delistarea să producă efecte pe toate domeniile *.com* relevante.

Urmând ghidul Grupului de lucru, CNiL (Commission Nationale de l'informatique et des Libertés), autoritatea franceză de control în materia protecției datelor cu caracter personal, a cerut Google să aplice dreptul de a fi uitat pe toate numele de domenii ale motorului de căutare Google, inclusiv domeniul *.com* și asta pentru că, inițial, Google a aplicat delistarea doar domeniilor europene din motorul său de căutare. În consecință, rezultatele care încălcau dreptul la uitare (deși câștigat deja) rămâneau accesibile, chiar și pe teritoriul Franței, pe domeniul Google.com și alte extensii non-europene. CNiL a precizat că, „pentru ca dezindexările intervenite să fie efective, ele trebuie să fie puse în operă pe toate versiunile motorului de căutare, fără a fi limitate doar la numele de domenii europene"[49] și a acordat Google 15 zile pentru dezindexarea de pe toate versiunile motorului de căutare. Având în vedere că Google Inc. nu s-a conformat, a pronunțat împotriva sa o sancțiune pecuniară în cuantum de 100.000 de euro[50]. Decizia a fost motivată prin faptul că Google Inc. nu și-a îndeplinit obligația de a respecta drepturile de opoziție și de suprimare a datelor[51]. Google Inc., pe de altă parte, a invocat că măsura are o aplicare extrateritorială și că o dezindexare la nivel mondial ar contraveni de o manieră disproporționată libertății de exprimare și dreptului de acces la informație, iar ulterior a atacat această decizie în fața Consiliului de Stat.

CNiL v. Google se află încă pe rolul instanței franceze. Pe 9 decembrie 2016, Peter Fleischer, consilierul Google în domeniul

[49] CNiL, *Décision n°2015-047 du 21 mai 2015 mettant en demeure la société Google Inc*., [Online] la: https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000030746525, accesat 15.11.2017.

[50] CNiL, *Délibération de la formation restreinte n° 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société Google Inc*., [Online] la: https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000032291946, accesat 15.11.2017.

[51] „Dreptul de a fi dezindexat este derivat din dreptul la viață privată, un drept fundamental recunoscut pe plan mondial. Numai o delistare de pe toate extensiile motorului de căutare, indiferent de extensia utilizată sau originea geografică a persoanei care efectuează căutarea poate proteja în mod efectiv acest drept. Soluția care constă în diferențierea respectului față de drepturile persoanelor pe baza originii geografice a celor care vizualizează rezultatele căutării nu oferă oamenilor o protecție eficientă și deplină a dreptului de a fi dezindexați.", CNiL, *Délibération de la formation restreinte n° 2016-054 du 10 mars 2016 prononçant une sanction pécuniaire à l'encontre de la société Google Inc, op.cit.* [traducerea ne aparţine].

informațiilor confidențiale, a exprimat din nou poziția companiei în legătură cu cauza CNiL:

> *„Ce ați spune dacă link-urile către informații despre trecutul cuiva – informații despre fraudarea unei afaceri internaționale sau malpraxis în turismul medical – ar fi eliminate din căutarea Google în țara dvs. nu pe baza legislației locale, ci pentru că cineva a reușit să folosească legislația unui alt stat. Ce părere ați avea? […] Dreptul la uitare poate părea uneori complex, iar discuțiile despre jurisdicțiile online sunt cu siguranță foarte complicate. Dar chestiunea este simplă: ar trebui echilibrul dintre libertatea de exprimare și dreptul la viață privată să fie decis la nivelul fiecărui stat în parte – pe baza culturii, tradiției și instanțelor sale – sau ar trebui ca tuturor să li se aplice o perspectivă unitară?”*[52].

Ba mai mult, el afirmase anterior și că: „Dacă abordarea propusă de CNiL ar fi adoptată ca un regulament standard pentru Internet, am intra într-o cursă care nu va duce nicăieri. În cele din urmă, Internetul va fi la fel de liber precum cel mai puțin liber loc al lumii”[53]. Răspunsul CNiL este unul simplu: „decizia aceasta nu demonstrează niciun fel de intenție a CNiL de a impune extrateritorialitatea dreptului francez. Ea pur și simplu pretinde respectarea legislației europene de către operatori non-europeni care își oferă serviciile în Europa.”[54]

Soluția propusă de Google, chiar anterior pronunțării sancțiunii, a fost geo-localizarea, în sensul implementării unui filtru care împiedică pe cei din țara de origine a persoanei care a cerut dezindexarea și consultă motorul de căutare să vadă în lista de rezultate pagina eliminată, chiar și atunci când accesează o versiune non-europeană a motorului de căutare. Cu toate acestea, în prezent, grație anumitor mijloace tehnice ușor de întrebuințat, încă mai avem acces gratuit la versiunea listelor de rezultate a motoarelor de căutare neafectată de exercitarea dreptului la uitare, chiar dacă ne aflăm în

---

[52] P. Fleisher, *Reflecting on the Right to Be Forgotten*, în Google Blog, 9 decembrie 2016, [Online] la: https://blog.google/topics/google-europe/reflecting-right-be-forgotten, accesat 15.11.2017 [traducerea ne aparține].

[53] P. Fleischer, *Implementing a European, Not Global, Right to Be Forgotten*, în Google Europe Blog, 30 iulie 2015, [Online] la: https://europe.googleblog.com/2015/07/implementing-european-not-global-right.html, accesat 15.11.2017.

[54] CNiL, *Décision n°2015-047 du 21 mai 2015 mettant en demeure la société Google Inc*, în G.F. Frosio, The *Right to Be Forgotten: Much Ado about Nothing*, în Colorado Technology Law Journal, vol. 15, 2017, p.332.

țara de origine a persoanei care a solicitat dezindexarea, deși informația a devenit, teoretic, indisponibilă publicului larg[55]. Acest lucru ne face, evident, să ne gândim cât de eficient este, până la urmă, dreptul la uitare așa cum este el implementat în prezent de motoarele de căutare.

În continuare, o altă problemă ce ar putea să survină este cea determinată de situația în care link-ul în legătură cu care se solicită delistarea permite accesul la informații cu caracter personal ce aparțin mai multor persoane. O astfel de ipoteză generează o serie de întrebări cu privire la cum va funcționa, în concret, dreptul la uitare. O primă întrebare este cum va fi soluționată problema dacă în legătură cu acest link, care conține informații cu caracter personal cu privire la două persoane. Ambele trimit câte o cerere de delistare raportată la link-ul în discuție și o cerere este admisibilă, iar cealaltă nu. Va fi înlăturat link-ul și, dacă da, această situație nu ar fi, de fapt, o ipoteză în care persoana a cărei cerere nu este admisibilă să ocolească prevederile legale și rigorile în materie sau, cu acest scop, persoana a cărei cerere ar fi admisibilă să acționeze și în calitate de persoană interpusă? Este o astfel de soluție posibilă sau chiar în conformitate cu legea, cu privire specială asupra cazului în care cererea uneia dintre persoanele ce apar în link-ul respectiv nu este admisibilă, pentru că aceasta este o persoană publică și menținerea informațiilor este de interes public? Vor fi respinse ambele cereri, prevalând interesul public ce justifică respingerea uneia dintre ele? Nu ar însemna acest lucru faptul că, într-o astfel de situație, deși toate condițiile de admisibilitate a cererii de delistare ar fi îndeplinite, persoana respectivă nu va putea să își valorifice dreptul la uitare, deși ar fi îndreptățită la acesta? S-ar putea alege o variantă în care ar fi admisă una dintre cereri, iar cealaltă respinsă, dar fără ca link-ul să fie înlăturat, ci să se ascundă, prin mijloace tehnice, numai referințele personale cu privire la subiectul de drept a cărui cerere a fost admisă? Se poate recurge la o anonimizare parțială a datelor?

Toate acestea sunt întrebări inerente procesului de implementare a dreptului la uitare prin cererea de delistare, întrebări la care încă se caută

[55] Dacă se va ajunge vreodată la eficientizarea implementării dreptului la uitare, va deveni interesant de obținut accesul la informația ce nu va mai fi disponibilă atât de facil cum este astăzi, astfel că cererea va genera și oferta, adică o dezvoltare a serviciilor ce furnizează, contra cost, informații privind nu doar persoanele juridice, cum se întâmplă în prezent, ci și asupra persoanelor fizice, informația devenind un „bun" valoros, S.-D. Șchiopu, *Efectivitatea dreptului de a fi uitat*, *op.cit*., p. 203.

răspunsuri pentru o aplicare echitabilă, optimă și eficientă a recent creatului drept.

ANALELE ŞTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IASI
TOMUL LXIII, ŞTIINȚE JURIDICE, 2017, NR. II

CARE ESTE RELAȚIA DINTRE SECURITATE, CONFIDENȚIALITATE ŞI INTERNETUL LUCRURILOR?

WHAT IS THE RELATION BETWEEN SECURITY, CONFIDENTIALITY AND THE INTERNET OF THINGS?

MIRCEA GEORGESCU[1]
ROXANA IBĂNESCU

Rezumat: În urma cercetărilor realizate asupra rețelelor a luat naştere o nouă tehnologie numită Internetul Lucrurilor ce îşi propune să creeze noi valori prin realizarea schimbului de informații şi cunoştințe dintre oameni şi obiecte. Acesta este diferit față de predecesori săi (Internetul tradițional, Internetul Mobil, rețeaua de senzori etc.), axându-se în special pe modele de servicii omniprezente, arhitecturi de rețea eterogene şi acces universal pentru oameni, lucruri, obiecte şi procese. Inovațiile şi cercetările viitoare realizate asupra aplicațiilor şi serviciilor IoT sunt impulsionate de potențialul mare de piață şi de profit. Cu toate acestea, IoT propune noi domenii de studiere a vulnerabilității în securitatea sistemelor şi probleme mai dificile de confidențialitate. Industria din ziua de astăzi şi organizațiile guvernamentale subliniază securitatea cibernetică şi asigurarea confidențialității ca fiind priorități de top al domeniului IT. Amenințările online sunt prezentate atât de persoane fizice, cât şi de grupuri organizate cu intenții de realizare a unor furturi de secrete comerciale, acțiuni de perturbare şi invazie a sistemelor în scopuri activiste şi de spionaj.
Cuvinte cheie: Internetul Lucrurilor, securitate, confidențialitate

Abstract: As a result of future research on networks, a new technology called the Internet of Things has been created, which aims to create new values through the exchange of information and knowledge between people and objects. This technology is different from its predecessors (Traditional Internet, Mobile Internet, Sensor Network etc.), focusing in particular on ubiquitous service models, heterogeneous network architectures and universal access for people, things, objects and processes. Innovations and future research on IoT applications and services are

[1] Universitatea „Alexandru Ioan Cuza" Iaşi, Facultatea de Economie şi Administrare a Afacerilor, Iaşi, Romania, mirceag@uaic.ro, roxana_hucanu@yahoo.com

driven by the high potential for market and profit. However, IoT proposes new areas to study vulnerability in system security and more difficult confidentiality issues. Today's industry and government organizations underline cyber security and privacy as top IT priorities. Online threats are presented by both individuals and groups organized with intent to commit commercial theft, disturbance actions and invasion of systems for activist and espionage purposes.
Keywords: Internet of Things, Security, Data Privacy

1. Introducere

„Internet of Things" (abv. IoT), în traducere din limba engleză, Internetul Lucrurilor sau Internetul Obiectelor, reprezintă o lume fascinantă în care lucruri obişnuite din viața de zi cu zi sunt conectate la Internet. În cadrul acestei lumi digitale, senzorii şi dispozitivele de comunicații sunt integrate în lucruri fizice cu scopul de a facilita comunicarea între lucruri sau între lucruri şi ale dispozitive precum servere cloud, calculatoare, telefoane inteligente şi tablete. Potrivit companiei Cisco Internet Business Solutions Group (IBSG), Internetul Lucrurilor reprezintă acea perioadă de timp în care există mai multe obiecte conectate la Internet decât oameni[2].

Termenul „Internet of Things" a fost utilizat pentru prima dată în cadrul laboratorului MIT[3] în anul 1999, de către Kevin Ashton, cu scopul de a ilustra puterea de conectare a etichetelor RFID[4] utilizate în lanțuri de aprovizionare pentru a controla stocurile de bunuri fără a fi nevoie de intervenție umană[5]. În contextul actual, Internetul Lucrurilor se referă la dispozitive care au un grad înalt de conectivitate, la sisteme şi servicii care interacționează unele cu altele şi acoperă o gamă largă de protocoale, domenii şi aplicații. Putem aduce în discuție o multitudine de arii de aplicabilitate, printre care se numără: energia, transport, clădiri, locuințe, sănătate, oraşe, vânzări, agricultură şi altele. De exemplu, ne putem gândi la o casa inteligentă din viitor, ce presupune pornirea automată a televizorului pe un canal preferat sau a muzicii ambientale atunci când telefonul inteligent al proprietarului sau utilizatorului înregistrat în aplicațiile inteligente specifice casei inteligente, va părăsi automobilul sau va intra pe uşa casei.

[2] D. Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, s.l.: Cisco Internet Business Solutions Group (IBSG), 2011.
[3] MIT – Massachusetts Institute of Technology.
[4] RFID – Radio Frequency Identification.
[5] K. Ashton, *That 'Internet of Things' Thing*, 2009, [Online] la: http://www.rfidjournal.com/articles/view?4986, accesat la 30.08.2017.

Telefonul va fi în permanență conectat la Internet şi va comunica cu sistemul automatizat de acasă. Acesta poate iniția anumite protocoale, precum deschiderea uşilor sau iluminarea automată prin aprinderea becurilor din încăperi. Sau, de exemplu, am putea folosi unele dispozitive precum brățările de fitness pentru măsurarea frecvenței cardiace şi a temperaturii şi să comunicăm mai apoi sistemului automatizat al casei toate aceste informații pentru a crea o temperatură ideală în camere, în funcție de informațiile obținute. Informațiile obținute pot fi împărtăşite cu diferite părți interesate şi folosite în luarea deciziilor sau pentru îmbunătățirea informațiilor de afaceri.

Utilizarea acestei tehnologii a condus către o îmbunătățire a vieții noastre de zi cu zi, ajutându-ne la şi uşurându-ne totodată realizarea sarcinilor zilnice. Însă folosirea acestei tehnologii vine şi cu părți mai puțin bune, printre care se numără invizibilitatea colectării datelor, fapt ce poate conduce la o sacrificare a confidențialității utilizatorilor tehnologiei Internetului Lucrurilor[6]. Prin utilizarea acestei tehnologii viața ne este îmbunătățită şi realizarea sarcinilor de zi cu zi este cu mult uşurată. Însă odată cu toate aceste beneficii, ea vine şi cu părți mai puțin bune, printre care se numără şi invizibilitatea colectării datelor, rezultând o sacrificare majoră a confidențialității[7]. Odată cu utilizarea aplicațiilor şi serviciilor se aşteaptă de la furnizorii serviciilor o livrare automată a serviciilor personalizate pe baza informațiilor colectate de la aplicațiile utilizate, protejarea informațiilor de acces neautorizat şi nedistribuirea acelor date cu persoane terțe[8].

Existența şi utilizarea aplicațiilor IoT determină crearea unor provocări privind securitatea întregului ecosistem al IoT, din motive legate de extinderea „Internetului" prin rețeaua tradițională (Internet, rețea de date celulare, rețea de senzori), conectarea la rețea a obiectelor datorită faptului că fiecare obiect va fi conectat la Internet şi a comunicării dintre obiecte. Compania Gartner plasează securitatea în fruntea listei sale de top 10 tehnologii IoT pentru 2017 şi 2018, afirmând faptul că securitea IoT va fi complicată de faptul că multe „lucruri" utilizează procesoare simple şi

[6] G.A. Fink, D.V. Zarzhitsky, T.E. Carroll, E.D. Farquhar, *Security and privacy grand challenges for the internet of things. In Collaboration Technologies and Systems (CTS)*, International Conference on, 2015, pp. 27–34.

[7] Ibidem.

[8] G. Sun, S. Huang, Y. Yang, Z. Wang, *A privacy protection policy combined with privacy homomorphism in the Internet of Things. Computer Communication and Networks (ICCCN)*, 23rd International Conference on, 4-7 08, 2014, pp. 1-6.

sisteme de operare care nu ar putea să sprijine abordări sofisticate[9]. Prin urmare, ar trebui acordată o mai mare atenție către chestiunilor de cercetare privind confidențialitatea, autenticitatea şi integritatea datelor în Internetul Lucrurilor.

2. Considerații privind securitatea şi confidențialitatea datelor generate de IoT

Întrucât ne bazăm pe dispozitive conectate pentru a ne face viața mai uşoară, trebuie să luăm în considerare un aspect foarte important şi anume, securitatea. Securitatea este definită ca fiind un set de mecanisme întreprinse pentru a proteja datele sensibile la atacuri cibernetice şi pentru a garanta confidențialitatea, integritatea şi autenticitatea datelor. Toți participanții din ecosistemul IoT trebuie să-şi asume responsabilitatea privind securitatea datelor, a dispozitivelor şi serviciilor oferite prin implementarea şi respectarea celor mai bune practici[10].

2.1. Elemente arhitecturale specifice securității

Înaintea altor discuții privind securitatea, se impune realizarea unei descrieri şi analize a arhitecturii securității. Arhitectura este compusă din patru niveluri: aplicație, rețea, suport şi percepție (vezi Figura 1). În unele sisteme, nivelul de procesare este reprezentat de tehnologiile de suport ale rețelei, cele precum middleware, computing, network processing[11].

[9] O. David, *Gartner Identifies the Top 10 Internet of Things Technologies for 2017 and 2018*, [Online] la: https://www.iotcentral.io/blog/gartner-identifies-the-top-10-internet-of-things-technologies-for.

[10] K. Sarah, *9 IoT Security Threats To Watch*, [Online] la: http://www.crn.com/slide-shows/internet-of-things/300089496/black-hat-2017-9-iot-security-threats-to-watch.htm/pgno/0/2, accesat la 30.09.2017.

[11] K. Zhao, L. Ge, *A survey on the internet of things security*, în Proceedings – 9th International Conference on Computational Intelligence and Security, CIS 2013, 14 12, pp. 663-667.

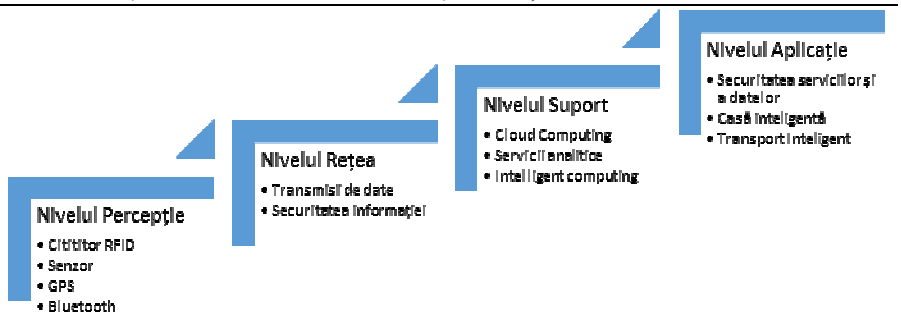


Figura 1. Arhitectura securității IoT

A. *Percepție*

Toate informațiile din lumea reală sunt colectate prin intermediul nivelului percepție utilizând dispozitive fizice ce au integrate senzori, etichete RFID, sisteme GPS și echipamente bluetooth. Datele colectate conțin informații cu privire la proprietățile obiectelor, condițiile de mediu și altele. Senzorii reprezintă factori cheie pentru acest nivel, fiind utilizați în capturarea datelor și transformarea lumii reale, fizice într-o lume digitală.

- *Caracteristici de securitate:* Nivelurile de percepție sunt foarte simple, cu capacități de stocare mici și putere de calcul relativ mică. Din acest motiv este foarte greu să se creeze un sistem de securitate prin care să se realizeze o protecție eficientă a acestuia, determinând apariția unor probleme de comunicare și imposibilitatea aplicării unor algoritmi de criptare a cheilor publice. Datele obținute de la senzori necesită protecție din punct de vedere al integrității, confidențialității și autenticității.
- *Cerințe de securitate:* La acest nivel, autentificarea este folosită cu scopul de a asigura confidențialitatea transmiterii datelor dintre nivele și pentru a preveni accesul ilegal, în acest fel procesul de criptare al datelor devenind necesar.

B. *Rețea*

Împreună cu procesarea inițială a datelor preluate din stratul de percepție este realizată transmiterea fiabilă a datelor, clasificarea informațiilor și polimerizarea. Transmiterea informațiilor se bazează pe câteva rețele de bază, esențiale pentru schimbul de informații realizat dintre

dispozitive, rețele (precum internet, acele rețele „fără fir”, sateliți, comunicații mobile), infrastructura de rețea şi protocoale de comunicații.

- *Caracteristici de securitate:* Mecanismul de securitate al acestui strat este unul de mare importanță pentru Internetul Lucrurilor. Chiar dacă rețeaua centrală este relativ sigură, atacurile de interceptare de genul „Man-In-The-Middle”, mesajele contrafăcute, mail-uri de tip spam şi viruşii de calculator încă cauzează pagube mari ce nu pot fi ignorate, întrucât numărul mare de trimiteri de date provoacă aglomerație în rețea.
- *Cerințe de securitate:* Mecanismele de autentificare (pentru a preveni noduri ilegale), confidențialitatea şi integritatea sunt utilizate pentru a asigura securitatea la acest nivel. Un atac special care este foarte grav şi reprezintă o problemă care trebuie rezolvată la acest nivel este atacul DdoS[12] [13].

C. Suport

După ce informațiile trec prin nivelul rețea, acestea urmează să fie preluate de către nivelul percepție al cărui scop este de a oferi o gamă largă de competențe computerizate inteligente, organizându-le cu ajutorul rețelelor grid network şi cloud computing, cu scopul de a crea o platforma fiabilă pentru sprijinirea nivelului aplicație. Acest nivel joacă un rol de punte între nivelul de sus şi cel de jos.

- *Caracteristici de securitate:* Recunoaşterea informațiilor rău intenționate reprezintă o provocare pentru acest strat, datorită faptului că stratul de suport lucrează cu prelucrarea în masă a datelor şi deciziile inteligente.
- *Cerințe de securitate:* Acest strat trebuie să lucreze cu o varietate de aplicații ale arhitecturii securității, plecând de la cloud computing şi până la computere securizate multi-party, colaborând cu aproape toate protocoalele şi toți algoritmii puternici de criptare, tehnologii de securitate ale sistemului puternice şi soluții anti-virus.

[12] DdoS – Distributed Denial of Service reprezintă o încercare de a face indisponibil un serviciu online prin copleşirea acestuia cu trafic din mai multe surse. Acestea vizează o gamă largă de resurse importante, de la bănci la site-uri de ştiri şi reprezintă o provocare majoră pentru asigurarea faptului că omenii accesează şi publică informații importante.

[13] Digital Attack Map, 2017, [Online] la: https://www.digitalattackmap.com/understanding-ddos/, accesat la 20.10.2017.

D. *Aplicație*

Nivelul aplicație este cel mai înalt nivel, fiind un nod terminal. Datorită nevoilor utilizatorilor ce pot accesa această tehnologie IoT folosind televizorul inteligent, calculatorul personal, laptop-ul sau tableta, la acest nivel de aplicație sunt oferite servicii personalizat[14].

- *Caracteristici de securitate:* Datorită faptului că nevoile de securitate sunt diferite, în funcție de aplicația și schimbul de date ce reprezintă principala caracteristică a acestui nivel, pot apărea probleme privind confidențialitatea, controlul accesului și divulgarea informațiilor[15].
- *Cerințe de securitate:* Problemele de securitate apărute la acest nivel pot fi rezolvate prin protejarea confidențialității utilizatorului, utilizând protocoale de autentificare[16] și key-agreement[17]. De asemenea, gestionarea tuturor parolelor și a dispozitivelor ar trebui să se facă într-un mod adecvat.

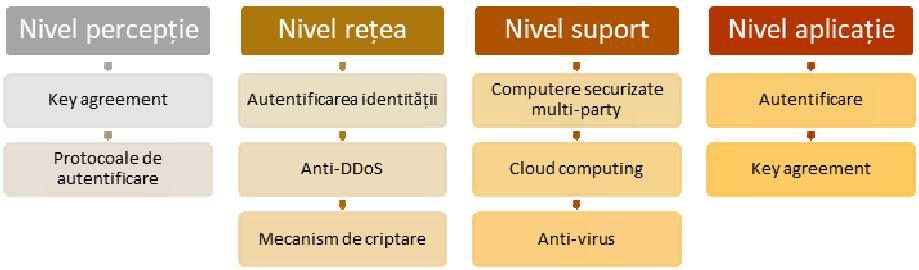


Figura 2. Cerințe specifice nivelurilor arhitecturale

2.2. Servicii de securitate

În arhitectura de securitate a procesului de transmitere a informațiilor trebuie acordată o atenție sporită pentru asigurarea garanției

[14] C. Ding, L. Yang, M. Wu, *Security architecture and key technologies for IoT/CPS*, în ZTE Technology Journal, 2017(1).

[15] Y. Geng și alții, *Security Characteristic and Technology in the Internet of Things* în Journal of Nanjing University of Posts and Telecommunications (Natural Science), 2010, 30(4).

[16] Autentificare – reprezintă procesul prin care o persoană pretinde identificarea în sistem pe baza informațiilor confidențiale stabilite la crearea contului. Acest proces mai poartă denumire de login/log in sau logon/log on.

[17] Key-agreement – reprezintă un protocol prin care două sau mai multe părți implicate pot conveni asupra unei chei partajate către toate dispozivele care vor accesa rețeaua fără fir.

confidențialității, integrității, intimității, autenticității şi instantaneității datelor şi informațiilor ce fac referire în principiu la securizarea rețelelor de telecomunicații şi corespund securității ierarhiei de transmisie a datelor în Internetul obiectelor[18]. Aceste cerințe pot fi observate în Figura 3.

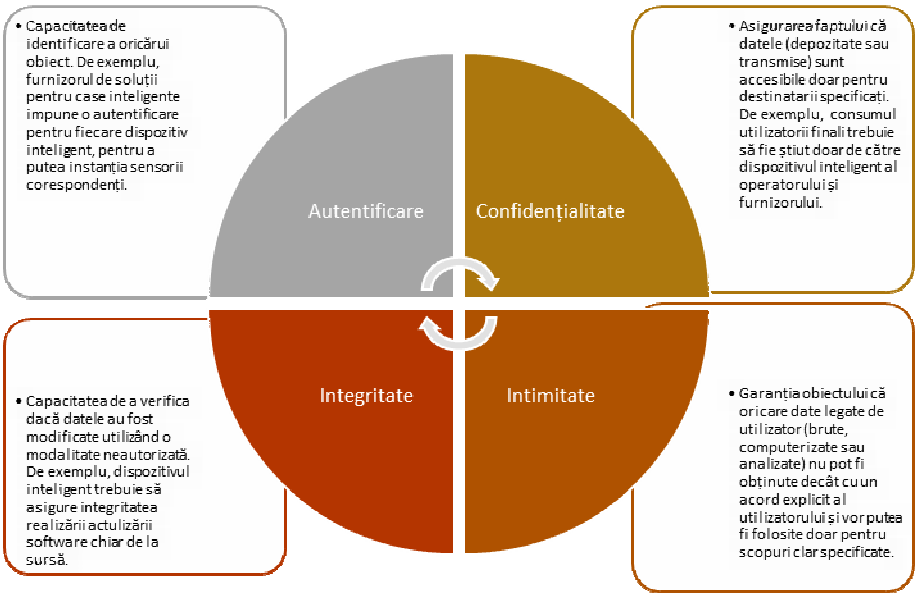


Figura 3. Servicii de securitate ale Internetului Lucrurilor

În acest context, confidențialitatea reprezintă un set de reguli care limitează accesul la informații, integritatea fiind o asigurare a faptului că informațiile sunt exacte şi de încredere, intimitatea – garanția pe care utilizatorii o întreține pentru datele lor sensibile, iar autentificarea este o garanție a accesului fiabil la informații a persoanelor autorizate. Dintre toate cerințele descrise anterior, considerăm că ar trebui să primeze respectarea confidențialității, întrucât aceasta reprezentă un mijloc de protecție a informațiilor care se desfăşoară prin orice mijloc între două părți.

2.3. Provocări privind confidențialitatea

Unele dispozitive inteligente sunt dezvoltate cu scopul de a crea, colecta sau partaja date. Prin urmare, aceste date nu pot fi considerate a fi „date cu caracter personal” şi nu au nici un impact asupra confidențialității

[18] L. Li, *Study on security architecture in the Internet of Things. Measurement, Information and Control (MIC)*, 2012 International Conference on, Volumul 1, pp. 374-377.

sau intimității consumatorilor, nefăcând legătură la legile privind protecția confidențialităților și a datelor. De exemplu, pot fi incluse în această categorie date ce fac referire la starea fizică a mașinilor, la metrici privind starea rețelei sau de diagnosticare internă[19].

Majoritatea serviciilor folosite în Internetul Lucrurilor fac însă referire la crearea și distribuirea datelor cu caracter personal legate de consumatori individuali și care pot avea un impact asupra confidențialității consumatorului, fiind legate de legislația generală de protecție a datelor și confidențialității (vezi Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date). De exemplu, se pot crea analize privind starea de sănătate sau profilul consumatorului în funcție de obiceiurile de cumpărături și de supermarket-urile preferate, cele mai vizitate.

Toți participanții din ecosistemul IoT au obligația de a respecta confidențialitatea persoanelor și de a păstra în siguranță datele personale de identificare. O provocare majoră pentru furnizorii de aplicații IoT este cauzată de legi multiple și adesea inconsistente, legate de confidențialitate și protecția datelor, legi care pot fi aplicate în mod diferit în funcție de sectorul industrial, servicii și tipuri de date implicite în diferite țări. Să luăm exemplul unei mașini inteligente ce călătorește în diferite țări, prin urmare transferurile de date asociate pot fi guvernate de fiecare țară în care mașina trece, folosind diferite jurisdicții legale. Datele obținute de la senzorii instalați în mașină (folosiți pentru a urmări locația mașinii) pot fi folosite pentru a deduce o serie de informații despre locurile frecventate și preferate de către șofer, stilul de viață al acestuia sau hobby-urile, date care pot fi considerate informații personale despre utilizatorul. De asemenea, aceste informații obținute prin intermediul senzorilor de „diagnoză la bord” ar putea fi împărtășite cu societățile de asigurări ce pot utiliza aceste informații pentru a impune o primă mai mare și, prin urmare, să discrimineze conducătorul auto fără cunoștința lui.

O altă provocare este reprezentată de faptul că cele mai multe legi privind protecția datelor solicită societăților (care colectează datele consumatorilor) să obțină consimțământul consumatorului afectat (cunoscut și sub denumirea de „persoana vizată”) înainte de a procesa anumite

[19] T. Victor, *Internet of Things future forecasts: focus on IoT security*, [Online] la: https://www.i-scoop.eu/internet-of-things-guide/iot-security-forecasts/, accesat la 10.10.2017.

categorii de „date cu caracter personal” – cum ar fi datele referitoare la sănătate. Majoritatea legilor definesc „datele personale” ca fiind orice informație ce se referă la o persoană fizică vie (identificată) sau „identificabilă”[20]. Pe măsură ce tot mai multe dispozitive sunt conectate la Internet şi numărul acesta este în creştere[21], tot mai multe date despre persoane vor fi colectate şi analizate şi eventual vor afecta intimitatea lor, fără a fi în mod necesar considerate „date cu caracter personal” prin lege. Se pot obține profiluri detaliate ale utilizatorilor prin combinarea volumelor masive de date, a datelor mari, a stocării în cloud şi a analizelor predictive.

3. Analiza cerințelor de securitate a aplicațiilor din domeniul medical

În acest caz, ne propunem să studiem un Dispozitiv de Monitorizare a ritmului cardiac portabil (dispozitiv de punct final) ce reprezintă un dispozitiv simplu folosit pentru măsurarea şi înregistrarea frecvenței cardiace a utilizatorului, cu scopul de a oferi unele indicații pentru o mai bună securizare a dispozitivului.

Figura 4. Dispozitiv de monitorizare a ritmului cardiac

Dispozitivul a fost dezvoltat cu intenția de urmărire de către utilizatorul final a pulsului pe parcursul zilei, stocându-l atât în aplicație, cât şi în baza de date back-end. Intenția este de a permite utilizatorilor să-şi

[20] S. Gib, *Upcoming IoT regulations and laws: How to survive and stay compliant*, [Online] la: http://www.ioti.com/security/upcoming-iot-regulations-and-laws-how-survive-and-stay-compliant, accesat la 20.10.2017.

[21] E. Rob, *8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016*, [Online] la: https://www.gartner.com/newsroom/id/3598917, accesat la 02.09.2017.

revizuiască valorile ritmul cardiac în timp pentru a-şi urmări sănătatea generală. Utilizatorii pot viziona îmbunătățirea sau agravarea sănătății lor în timp, în funcție de menținerea unui stil de viață sănătos. Acest lucru permite utilizatorilor să se stimuleze prin evaluarea atât a tendințelor pozitive, cât şi a celor negative citite din datele lor stocate în dispozitivul de monitorizare. Datele pot fi de asemenea utilizate de parteneri pentru a interveni în cazul apariției unor evenimente legate de sănătatea utilizatorului, precum atac de cord sau accident vascular cerebral.

3.1. Privire de ansamblu asupra dispozitivului

În Figura 4 se poate observa care este structura generală, precum şi componența unui dispozitiv simplu de urmărire a ritmului cardiac[22].

Dispozitivul simplu de urmărire a ritmului cardiac este compus din următoarele componente:

- Un emițător cu emisie redusă de energie Bluetooth (BLE) – ce asigură conectivitate fără fir (wireless);
- Microcontroler (MCU) activat pentru BLE – ce are obligația de a analiza datele emise de senzor şi de a alege ce date trebuie transmise prin transmițătorul BLE;
- Un senzor fotografic de lumină ambientală – folosit pentru a captura datele privind frecvența pulsului.

În acest exemplu, folosim o baterie de tip monedă pentru a facilita transmiterea datelor între dispozitive, de la dispozitivul portabil la tabletă, laptop sau smartphone.

3.2. Privire de ansamblu asupra serviciilor

Din perspectiva serviciilor, aplicația poate fi disponibilă pe telefonul inteligent, calculatorul personal sau tabletă, cu scopul de a transmite valorile capturate de la punctul final (în cazul nostru, dispozitivul de monitorizare) către punctul de serviciu final folosind orice conexiune de rețea disponibilă. Punctul de serviciu final pentru aplicație asociază pur şi simplu proprietarul dispozitivului cu valorile capturate şi le stochează într-o bază de date locală a serverului de aplicații. Datele pot fi vizualizate utilizând aplicația mobilă sau utilizând un browser pentru a accesa site-ul

[22] V. Mark, *Wearables Technology Components*, [Online] la: https://www.digikey.com/en/product-highlight/p/panasonic/wearable-technology, accesat la 15.10.2017.

web al serviciului. Pe site-urile furnizorului de servicii, utilizatorii pot vizualiza şi utiliza valorile capturate pentru a efectua mai multe acțiuni (Figura 5).

Figura 5. Fluxul de date al punctului de serviciu final

3.3. Model de securitate

Din ce am observat mai sus, la dispozitivul urmărit, cele mai comune probleme pot apărea atât datorită produsului, cât şi a serviciului utilizat.

Din perspectiva produsului, probleme pot apărea datorită următorilor factori:

- Clonare;
- Personalizarea produsului;
- Personalizarea serviciului;
- Asigurarea confidențialității.

Din perspectiva produsului, probleme pot apărea datorită următorilor factori:

- Clonare;
- Atacarea serviciilor;
- Identificarea comportamentului anormal al punctului final;
- Limitarea compromisului;
- Reducerea pierderii datelor;
- Reducerea exploatării;

- Gestionarea confidențialității utilizatorilor;
- Îmbunătățirea disponibilității datelor.

Având în vedere faptul că dispozitivul de monitorizare are foarte puține funcționalități, putem implementa o securitate minimă asupra punctului final, atât pentru securitatea aplicațiilor, cât și pentru comunicare. Deoarece aplicația specifică sistemului de monitorizare a ritmului cardiac este afișată pe un singur dispozitiv, atât timp cât firmware-ul dispozitivului este blocat, nu există nicio amenințare reală de atac împotriva punctului final în cazul utilizării de date. Deoarece confidențialitatea reprezintă o problemă, trebuie să luăm în considerare cel puțin utilizarea unei autentificări, cu o versiune PSK[23] personalizată a unei baze de calcul de încredere. Acest lucru ar asigura faptul că cheile de criptare sunt unice pentru fiecare punct final, astfel încât un punct final compromis nu poate compromite toate celelalte punctele finale. Dacă cheile personalizate (unice) au fost codificate în microcontrolerul încuiat, ar fi rezonabil să credem că acest caz de utilizare a fost asigurat în mod adecvat de amenințarea cu clonarea, personalizare și problemele de confidențialitate.

Din perspectiva infrastructurii de server, lucrurile sunt diferite, deoarece trebuie să ne asigurăm că:

- Există o securitate front-end care să diminueze efectele unui atac Denial of Service;
- Se impune exercitarea unor controale pentru a limita traficul către sau de la servicii;
- Datoriile din straturile de servicii sunt bine delimitate;
- Asigurăm crearea unei baze de date securizate cu jetoane personalizate PSK;
- Sunt definite măsuri de securitate în sistemul de operare al serviciului;
- Sunt definite valorile pentru evaluarea comportamentul anormal al punctului final.

Sistemul poate fi mai sigur dacă luăm în considerare considerațiile expuse și poate aduce unele modificări simple și eficiente din punctul de vedere al obiectivului, asigurând astfel tehnologia fără a schimba arhitectura. Confidențialitatea este asigurată prin acordarea fiecărui jalon criptografic unic.

[23] Pre-Shared key (PSK) – Cheie de criptare pre-partajată

Concluzii

Internetul obiectelor reprezintă un salt important către o conexiune globală şi generalizată folosită de către orice obiect/dispozitiv de comunicație şi de calcul, indiferent de tehnologia lui de acces, resurse şi locație disponibilă. Securitatea este principala preocupare pentru IoT, împreună cu confidențialitatea datelor, deoarece punerea în aplicare a internetului on-line la scară globală afectează miliarde de persoane şi dispozitive.

În această lucrare am analizat pe scurt principalele probleme de securitate şi provocări pentru Internetul obiectelor cu exemplificare pe domeniul medical şi am analizat din punct de vedere teoretic şi practic un dispozitiv inteligent cu scopul de a furniza unele indicații privind asigurarea unui dispozitiv de tip punct final.

ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

O PRIVIRE SUCCESORAL-MEMORIALĂ ASUPRA CONTURILOR DE PE REȚELELE DE SOCIALIZARE

A LEGAL PERSPECTIVE ON THE LEGACY AND THE MEMORY OF SOCIAL NETWORKS ACCOUNTS

CODRIN MACOVEI[1]
VLAD VIERIU[2]

Rezumat: Create în spațiile private ale "părinților" lor, cele mai populare rețele de socializare ale prezentului se întind astăzi peste întreg mapamondul și însoțesc prezența omului în spațiul cosmic. Nenumărate personalități ale lumii în care trăim și-au creat conturi pe rețelele de socializare, veritabile prelungiri ale persoanei, activității și operei lor. *Post mortem*, existența conturilor de socializare generează o suită de necunoscute ale căror soluții vor fi descoperite la confluența dintre cursul voințelor operatorilor și ale utilizatorilor rețelelor de socializare, pe de o parte, și albia dreptului nostru, izvorât din surse internaționale și autohtone, pe de altă parte. Perspectiva noastră caută precedentele și potențialele situații conflictuale născute în siajul deschiderii succesiunii titularilor conturilor de pe rețelele de socializare.
Cuvinte-cheie: cont memorial, profil memorial, contact de moștenire, Facebook, Instagram, Twitter.

Abstract: Born in the private spaces of their "fathers", the most popular social networks of our days extend today over the entire world and follow the human presence out of space. Many peronalities of our days world have their own social networks accounts, genuine extensions of their persons, activity and work. *Post mortem*, the subsistence of social networks accounts generates some questions and the answer to these questins must be discovered at the confluence of the will of the social networks accounts operators and users, on the one hand, and the provisions of our law, on the other hand. Our perspective looks after the former and the potential contentious situations that could appear after the death of the social networks users.

[1] Lector univ. dr., Universitatea „Alexandru Ioan Cuza" din Iași, Facultatea de Drept, e-mail: mcodrin@uaic.ro.

[2] Dr., Universitatea „Alexandru Ioan Cuza" din Iași, Facultatea de Drept, e-mail: vieriuvlad@gmail.com.

Keywords: memorial account, memorial profile, legacy contact, Facebook, Instagram, Twitter.

Interesul creatorilor spațiului online pentru imortalizarea profilului persoanei umane după decesul acesteia s-a intensificat recent, ca un așteptat răspuns al furnizorilor de experiențe digitale la apetența publicului pentru păstrarea memoriei persoanei prin intermediul creațiilor sale stocate pe suport informatic. Cu titlu de exemplu, putem aminti portalul eterni.me, care ne invită să devenim „nemuritori, în mod virtual”[3], pentru a se îngriji ulterior, *sine die*, de gândurile, poveștile și amintirile noastre prin crearea unor avatare inteligente care să ne reprezinte cu fidelitate. Ideea creatorilor platformei eterni.me nu a fost însă o noutate, ci s-a născut natural dintr-o provocare apărută în momentul în care moartea a afectat prelungirile virtuale ale personalității umane, materializate în aplicații ce au devenit, în timp, comune. De la arhicunoscuta adresă de poștă electronică la ultimele inovații în domeniul rețelelor de socializare, moartea titularului a adus cu sine, nu de puține ori, sensibile probleme de drept, instanța fiind, în unele dintre aceste cazuri, chemată să se pronunțe.

Într-un remarcabil editorial, Brandon Ambrosino se întreba cum „prezența noastră în spațiul digital ne schimbă felul în care murim”[4].Putem duce mai departe această reflecție, întrebându-ne, la rândul nostru, cum sunt influențate memoria și respectul datorat ființei umane după moartea sa, prin prisma continuării sau nu a existenței conturilor memoriale de pe rețelele de socializare. Întreținerea, *post mortem*, a unui spațiu virtual în care omul a imprimat o substanțială parte din gândirea și, poate, opera sa, spre anamneză și diseminare în timp, pentru perioade nedeterminabile, aleatorii, poate pentru totdeauna, aduce cu sine, *a fortiori*, provocări incipiente. Facebook, Instagram, Twitter, Google+, Odnoklassniki au o singură certitudine: utilizatorii niciuneia dintre aceste rețele de socializare nu sunt nemuritori.

Privind printr-o prismă a abstracțiunilor juridice, a utiliza rețeaua de socializare Facebook, în cea mai comună accepțiune a acestei expresii, nu reprezintă altceva decât executarea unui contract de prestări servicii, cu titlu gratuit, încheiat odată cu acceptarea online a condițiilor speciale impuse de

[3] eterni.me, accesat 24.10.2017.

[4] B. Ambrosino, *Facebook is a growing and unstoppable digital graveyard*, [Online] la: http://www.bbc.com/future/story/20160313-the-unstoppable-rise-of-the-facebook-dead, accesat 24.10.2017

cealaltă parte, un veritabil contract de adeziune a cărui modificare nu poate interveni decât în formă scrisă, materialmente, fiind dependentă de existența semnăturii reprezentantului[5]. Pentru utilizatorii din România, persoana morală cocontractantă este Facebook Ireland Limited, însă acest aspect nu aduce atingere legii aplicabile convenției, aceasta fiind impusă și fiind reprezentată de dreptul statului California[6]. De altfel, toți utilizatorii din întreaga lume trebuie să-și asume această lege aplicabilă, singura excepție admisă de Facebook fiind convențiile încheiate de utilizatorii germani, care sunt supuse dreptului german[7].Sunt de asemenea aplicabile prevederile dreptului irlandez cu privire la protecția datelor cu caracter personal[8] – Data Protection Act 1988[9]. Dincolo de toate acestea, rămânând în vigoare și în discuție principiile ce guvernează, pentru fiecare cultură juridică națională în parte, ordinea publică în dreptul internațional privat al forului. Legea română, spre exemplu, impune regula potrivit căreia *aplicarea legii străine se înlătură dacă încalcă ordinea publică de drept internațional privat român sau dacă legea străină respectivă a devenit competentă prin fraudarea legii române*[10]. În același spirit, *aplicarea legii străine încalcă ordinea publică de drept internațional privat român în măsura în care ar conduce la un rezultat incompatibil cu principiile fundamentale ale dreptului român ori ale dreptului Uniunii Europene și cu drepturile fundamentale al omului*[11].

Unilateral și în spiritul convenției cu titlu gratuit, administratorii rețelei de socializare Facebook și-au configurat ideal întinderea obligațiilor și a răspunderii. Așadar, aderând la declarația de drepturi și responsabilități ce nu poate fi evitată de niciun utilizator, utilizatorii Facebook consimt și limitele și neajunsurile eventuale ce afectează prestația celeilalte părți. Astfel, existența site-ului însăși este sub un minim semn al întrebării,

---

[5] Facebook, *Declarația de drepturi și responsabilități*, 18.5 (data ultimei revizuiri: 30 ianuarie 2015), [Online] la: https://www.facebook.com/legal/terms/update, accesat 20.10.2017.

[6] *Ibidem*, 15.1.

[7] *Ibidem*, 16.3.

[8] D. McCallig, *Facebook after death: an evolving policy in a social network*, în International Journal of Law and Information Technology, vol. 22, nr. 2/2014, p. 113.

[9] Forma consolidată a acestui act normativ poate fi consultată la adresa http://www.lawreform.ie/_fileupload/RevisedActs/WithAnnotations/EN_ACT_1988_0025.PDF, accesat 25.10.2017.

[10] Art. 2564 alin. (1) C.civ.

[11] Art. 2564 alin. (2) C.civ.

angajamentul administratorilor fiind exclusiv de mijloace, iar utilizarea rețelei de socializare se face sub riscul utilizatorului. Serviciul este oferit fără nicio garanție expresă sau implicită, cu atât mai puțin cu privire la faptul că Facebook va fi întotdeauna un site sigur, securizat sau fără erori, sau că Facebook va funcționa întotdeauna fără întreruperi, întârzieri sau imperfecțiuni[12].În arhitectura complexă a regulilor ce stabilesc drepturile și obligațiile utilizatorilor rețelei Facebook și nu numai, au fost cuprinse și un număr deloc neglijabil de clauze*mortis causa.* Din punctul nostru de vedere, acestea sunt expresia nu doar a unei prelungiri, *sine die*, a serviciilor specifice, de această dată în favoarea apropiaților de-al treilea, ci și aconsiderației pentru memoria utilizatorului persoană decedată.Naturi juridice interesante apar în aceste noi orizonturi create de evoluția tehnologiei informației, precum o idee de contract pentru cauză de moarte, un alt fel de „amintiri de familie", păstrate în servere transoceanice, o nouă dimensiune a „succesorilor" în drepturi sau un nou „testament" întocmit fără respectarea clasicelor condiții de formă și al cărui obiect este nepatrimonial. Toate aceste realități recente înmagazinează nuclee conflictuale în stare latentă, unele dintre ele activate în fața instanțelor din întreaga lume, conturându-se astfel o timidă jurisprudență.

Una dinte paginile acestei noi opere de rafinare a dimensiunii virtuale a existenței omului, după moartea sa, este rezervată conceptelor. Creație a administratorilor rețelelor de socializare, noile tipare ale existenței conturilor de pe rețelele de socializare după moartea utilizatorilor lor se cristalizează treptat într-un veritabil quasidrept consensual succesoral, construit pe o osatură juridică de o admirabilă complexitate, în care voința oamenilor întâlnește dinamica în evoluție a garanțiilor de ordine publică. Analiza acestei creații este dependentă de luarea în considerare a dimensiunii diacronice, de conștientizarea faptului că suntem doar la începutul unei evoluții a unor noi interfețe ale vieții umane și ale regulilor care le guvernează. Cercetarea inițială privește stadiul actual al rețelelor de socializare, cu ale lor norme și posibilități rezervate conduitelor sociale.

În lumina convenției încheiate între rețeaua de socializare Facebook și utilizatorii acesteia, opțiunea *mortis causa* cu privire la soarta conturilor

[12] Facebook, *Declarația de drepturi și responsabilități*, 15.3 (data ultimei revizuiri: 30 ianuarie 2015), [Online] la: https://www.facebook.com/legal/terms/update, accesat 24.10.2017.

de socializare aparține, de principiu, celor din urmă. Utilizatorii sunt invitați a dispune încă din timpul vieții cu privire la continuarea existenței sau, dimpotrivă, a încetării definitive a existenței conturilor de socializare[13]. Angajamentele pe care Facebook le asumă în mod unilateral față de utilizatorii săi nu diferă substanțial dacă utilizatorul mai este sau nu în viață, în unele cazuri rețeaua de socializare preferând confidențialitatea utilizatorilor decedați, în detrimentul intereselor succesorilor acestora. Într-unul dintre cazurile mediatizate la nivel mondial[14], instanța de apel din Berlin a statuat faptul că părinții unei minore ce s-a sinucis, aruncându-se în fața unui tren, nu au dreptul să obțină acces la conținutul contului rețelei de socializare al fiicei lor decedate, pentru că altfel ar aduce o nepermisă atingere secretului telecomunicațiilor garantat printr-o veche reglementare în dreptul german. Această soluție a venit împotriva celei pronunțate, în primă instanță, de o instanță regională germană, care a considerat că succesorii sunt îndreptățiți să dobândească inclusiv conținutul dialogurilor purtate prin serviciul de mesagerie al Facebook, acesta nefiind cu nimic deosebit de corespondența obișnuită.

Conceptul fundamental ce descrie continuarea existenței unui cont pe rețeaua de socializare Facebook, după moartea utilizatorului este cel al contului memorial. Conturile memoriale sunt definite ca fiind spații în care prietenii și familia se pot întruni pentru a împărtăși amintiri despre persoanele care au decedat. Numele persoanei în profil va fi însoțit de cuvintele „*In memoriam*”. În funcție de setările de confidențialitate ale contului, prietenii pot împărtăși amintiri în cronologia memorială. Conținutul pe care l-a distribuit persoana respectivă – fotografii, postări, etc. – rămâne pe Facebook și este vizibil audienței pentru care a fost distribuit. Profilurile memoriale nu apar în spații publice, cum ar fi sugestiile din secțiunea „Poate îi cunoști”, în reclame sau în notificări despre aniversări. Nimeni nu se poate conecta la un cont memorial și, în afara unui contact de moștenire, conturile memoriale nu vor putea fi modificate.[15]

În logica Facebook, succesiunea în gestionarea conturilor de socializare este fie *ab intestat*, fie cu unic moștenitor, denumit „contact de

[13] https://www.facebook.com/help/103897939701143, accesat 24.10.2017.

[14] *Parents lose appeal over acces to dead girl's Facebook account*, [Online] la: https://www.theguardian.com/technology/2017/may/31/parents-lose-appeal-access-dead-girl-facebook-account-berlin, accesat 26.10.2017.

[15] *Ibidem.*

moștenire" (*legacy contact*), persoană ale cărei posibilități sunt limitate. Astfel, aceasta are posibilitatea de a scrie o postare fixată pentru profilul contului memorial, să răspundă noilor solicitări venite din partea terțelor persoane, să actualizeze fotografiile reprezentative, de profil și de copertă și, în ultimă instanță, să solicite ștergerea contului memorial. De asemenea persoana contact de moștenire poate avea dreptul de a solicita o copie a tot ce a distribuit pe Facebook utilizatorul decedat, cu condiția ca acesta din urmă să fi dispus în acest sens în timpul vieții. Pe de altă parte, persoana contact de moștenire nu are posibilitatea de a se conecta la contul memorial, de a șterge sau a modifica postări, fotografii, etc., să acceseze mesajele, să facă noi cereri pentru terțe persoane sau să transmită calitatea de contact de moștenire unei alte persoane. Persoana desemnată contact de moștenire trebuie să aibă minim 18 ani[16]. Apreciind disponibilitatea administratorilor Facebook de a ameliora continuu serviciile, observăm unele deficiențe ale formatului actual. Restrângerea persoanelor ce pot avea calitatea de contact de moștenire la una aduce cu sine riscul ca însăși instituirea unui astfel de contact să rămână ineficientă, precum în cazul comorienților. De asemenea, restrângerea opțiunii utilizatorului de a desemna numai persoana contact de moștenire pentru a obține o copie a conținutului profilului, după moartea acestuia, este nejustificat de restrictivă. Ne putem întreba dacă, odată obținută o astfel de copie la cererea persoanei contact de moștenire, aceasta va face obiectul indiviziunii în care se află moștenitorii, în lumina dispozițiilor art. 1141 alin. (2) C. civ. De altfel, în literatura de specialitate a fost observată iminența conflictelor ce vor apărea pe fondul contradicțiilor între drepturile succesorilor legali sau testamentari și prerogativele altor persoane oferite în virtutea regulilor Facebook[17]. Un caz de notorietate în Regatul Unit al Marii Britanii și Irlandei de Nord a fost cel al lui Hollie Gazzard, ucisă de partenerul ei de viață, Asher Maslin. După moartea acesteia, membrii familiei au descoperit un cont de Facebook înghețat, un cont memorial astfel cum l-am descris anterior, depozitar al unui număr de imagini în care ucigașul și victima sa erau surprinse împreună. Deși inițial au refuzat să elimine aceste fotografii din contul memorial, ulterior

[16] https://www.facebook.com/help/1568013990080948?helpref=faq_content, accesat la data de 26.10.2017.

[17] D. Mangan, Lorna E. Gillies, *The Legal Challenges of Social Media*, Edward Elgar Publishing, 2017, p. 198.

administratorii rețelei de socializare au acceptat să facă aceasta, în urma unor pretenții formulate în temeiul drepturilor de autor asupra fotografiilor[18], cazul nefăcând astfel obiectul vreunei judecăți.

Odată exprimată voința într-un sens sau altul, eficiența manifestării de voință pare a fi inatacabilă. Subzistă întrebarea dacăsuccesorii utilizatorului decedat mai păstrează vreo șansă în a solicita și a obține anularea unei manifestări de voință, fie într-un sens, fie în altul, pentru toate motivele consacrate în sfera nulității actului juridic.Disponibilitatea de principiu a administratorului rețelei de socializare Facebook, pentru a soluționa o astfel de cerere, tinde a elimina, *ab inito,* orice eventual litigiu, de vreme ce din partea acestuia există angajamentul de a desființa un cont de socializare al unei persoane care suferă de o boală mintală[19]. În altă ordine de idei, lipsa discernământului unui utilizator la momentul în care acesta solicită fie transformarea contului într-un cont memorial, *post mortem,* fie desființarea contului de pe rețeaua de socializare poate fi invocată, pe calea amiabilă deschisă de administratorul rețelei de socializare însuși.

Regulile rețelei de socializare Instagram nu sunt substanțial diferite de cele ale rețelei Facebook. Astfel, invitația de a aduce la cunoștința administratorului faptul decesului unui utilizator este adresată oricui. Transformarea unui cont activ într-un cont memorial al unei persoane decedate are loc în urma primirii unei cereri valabile în acest sens. Formularea cererii este condiționată de utilizarea unei adrese web speciale[20], fiind solicitate unele minime date cu caracter personal precum și dovada decesului, fie aceasta un necrolog, un articol media sau chiar o fotocopie a actului de stare civilă ce atestă decesul.Dreptul de a solicita desființarea contului de pe Instagram este recunoscut de administrator doar rudelor de gradul I[21].Regulile Instagram nu statuează în mod expres posibilitatea utilizatorului de a solicita ca, *post mortem,* cererea rudelor de gradul I să fie

---

[18] *What happens to your Facebook profile after you die,* [Online] la: http://www.bbc.co.uk/newsbeat/article/34790918/what-happens-to-your-facebook-profile-after-you-die, accesat 25.10.2017.

[19] https://www.facebook.com/help/480409628639043?helpref=related, accesat 24.10.2017.

[20] https://help.instagram.com/contact/452224988254813?helpref=faq_content, accesat 24.10.2017.

[21] https://help.instagram.com/264154560391256?helpref=faq_content, accesat 24.10.2017.

respinsă, dar nici nu respinge această posibilitate. Transformarea contului unui utilizator în cont memorial nu aduce nicio minimă atingere aspectului contului respectiv, iar conturile memoriale de pe Instagram nu pot fi modificate în niciun fel, aspect valabil inclusiv pentru aprecieri, urmăritori, etichete, postări sau comentarii. Postările distribuite de persoana decedată rămân vizibile pentru cei care au fost distribuite[22].

În perspectiva declanșării unor eventuale litigii între succesorii utilizatorilor decedați și administratorii rețelelor de socializare, se impun unele minime mențiuni privind aspecte procesuale, iar între acestea ne atrag atenția cele privind competența. Astfel, potrivit punctului 15.1. din Declarația de drepturi și responsabilități a utilizatorului rețelei Facebook, acesta, prin acceptarea declarației amintite, își asumă o convenție de alegere a forului, limitându-și opțiunile la Tribunalul Districtual S.U.A. pentru Districtul de Nord al Statului California sau la oricare instanță de judecată statală aflată în districtul San Mateo[23].În lumina dispozițiilor art. 1081 C.proc.civ., o atare convenție de alegere a forului nu este inoperantă, eventualele litigii nefiind de natură a se înscrie în sfera restrânsă a celor ce atrag competența personală exclusivă a instanțelor române sau competența exclusivă în materia unor acțiuni patrimoniale a aceloraşi. Sub acest aspect, Curtea Supremă a Canadei a reținut o altă filosofie juridică, rafinată într-o serie de considerente ce fac parte dintr-o hotărâre recentă. Analizând mai întâi eficiența unei clauze privind alegerea forului, Curtea a statuat faptul că aceasta este condiționată de inexistența vreunui *„forum non conveniens”*, privite în ansamblul echilibrului contractual, referindu-se la aspecte precum ordinea publică, frauda la lege sau alte anomalii. În privința clauzei având ca obiect alegerea forului impusă de Facebook, Curtea, plecând de la faptul că Declarația de drepturi și responsabilități este un act juridic de adeziune, a statuat faptul că este împotriva ordinii publice a da eficiență unei clauze privind alegerea forului într-un contract de consum care are ca efect lipsirea părții la accesul la o instanță învestită prin lege. De asemenea, clauza amintită anterior este ineficientă și prin prisma a ceea ce *common law* cunoaște sub denumirea de *doctrine of unconscionability*, dat fiind

[22] https://help.instagram.com/231764660354188, accesat 24.10.2017.

[23] Facebook, *Declarația de drepturi și responsabilități*, 15.1 (data ultimei revizuiri: 30 ianuarie 2015), [Online] la: https://www.facebook.com/legal/terms/update, accesat 20.10.2017.

dezechilibrul extrem între părți la momentul încheierii convenției[24]. Aceste repere jurisprudențiale, privite în spirit comparatist, sunt salvatoare în momentele de început ale noilor raporturi sociale, chiar în ciuda reticenței anumitor culturi juridice naționale față de unele izvoare ale dreptului contemporan.

În concluzie, putem afirma că noile experiențe umane în emergentele spații virtuale deschid treptat calea spre o nouă dimensiune a dreptului, în care elemente fundamentale ale gândirii noastre juridice vor fi cu atât mai mult relativizate. Vocația anamnetică a tehnologiei ne va ține în „viață" tot mai mult timp, poate cel puțin cât va exista această tehnologie. Poate pentru totdeauna. Considerăm că ne aflăm la începutul unei noi ere în evoluția relațiilor dintre oameni și, pe cale de consecință, a unei noi ere în istoria dreptului.

[24]Supreme Court of Canada, *Douez v. Facebook, Inc*., cae number 36616, [Online] la: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16700/index.do, accesat 29.11.2017.

ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

RĂSPUNDEREA CIVILĂ PENTRU ÎNCĂLCAREA DREPTULUI LA REPUTAŢIE AL SOCIETĂŢILOR REGLEMENTATE DE LEGEA NR. 31/1990 PRIVIND SOCIETĂŢILE SĂVÂRŞITĂ PRIN INTERMEDIUL INTERNETULUI

CIVIL LIABILITY FOR VIOLATION ON THE INTERNET OF THE RIGHT TO REPUTATION OF COMPANIES REGULATED BY LAW NO. 31/1990 ON TRADING COMPANIES

MARIA DUMITRU[1]

Rezumat: Pornind de la premisa că persoanelor juridice ar trebui recunoscute câteva dintre drepturile personalităţii – printre care şi dreptul la bună reputaţie – ne-am propus să abordăm câteva aspecte particulare ale condiţiilor răspunderii civile, particularităţi generate de mijlocul specific prin care este săvârşită fapta ilicită cauzatoare de prejudicii şi anume internetul. În acest context, vom încerca să creionăm criteriile de care instanţa ar putea ţine seama în evaluarea prejudiciului material. În privinţa prejudiciilor nepatrimoniale ar fi de clarificat dacă societăţile reglementate de Legea nr. 31/1990 privind societăţile sunt îndreptăţite a obţine repararea prejudiciilor nepatrimoniale – daune morale – şi, în caz afirmativ, care ar fi cerinţele probatorii ce incumbă societăţii prejudiciate.
Cuvinte-cheie: daune morale persoane juridice, prejudiciu nepatrimonial, drept la reputaţie persoană juridică, încălcare dreptul personalităţii prin internet

Abstract: Assuming that legal persons should also be recognized some of the personality rights – including the right to a good reputation – we intend to address some particularities of the civil liability generated by the specific mean in which the damaging action is committed, the internet. In this context, we will try to outline the criteria a court could use in evaluating the pecuniary damages. Regarding the non-pecuniary damages, it is still to be clarified whether companies under the provisions of Law no. 31/1990 on trading companies are entitled to reparation of non-pecuniary

[1] Conf. univ. dr., Facultatea de Drept şi Administraţie Publică, Universitatea „Ştefan cel Mare" Suceava.

damages – moral damages – and if this is the case, what are the requirements in the burden of proof of the injured company.

Keywords*:* moral damages legal person, non-pecuniary damages, a legal person's right to reputation, personality rights infringement on the internet

1. Prezentarea temei. Dezvoltarea internetului a transformat difuzarea şi receptarea informaţiilor într-un fenomen global, ceea ce are un impact deosebit asupra dreptului. Ca urmare, în prezent, există numeroase categorii juridice care solicită cel puţin o nuanţare, dacă nu o reformare, a conceperii atunci când sunt avute în vedere în raport cu relaţii care se desfăşoară prin internet. Este şi cazul condiţiilor răspunderii civile care dobândesc particularităţi atunci când mijlocul specific prin care este săvârşită fapta ilicită cauzatoare de prejudicii este internetul. În acest context, vom încercam să creionăm criteriile de care instanţa ar putea ţine seama în evaluarea prejudiciului material suferit de persoanele juridice – victime ale unor asemenea fapte. În privinţa prejudiciilor nepatrimoniale ar fi de clarificat mai întâi dacă persoanele juridice, în general, şi societăţile reglementate de Legea nr. 31/1990 privind societăţile[2], în particular, sunt îndreptăţite a obţine repararea prejudiciilor nepatrimoniale prin acordarea de daune morale şi – în caz afirmativ – care ar fi cerinţele probatorii ce incumbă societăţii prejudiciate prin încălcarea dreptului la reputaţie.

2. Realitatea. În ultimul timp ni se întâmplă frecvent să citim pe Facebook postări ce cuprind aspecte negative, critici cu privire la conduita în afaceri a unui anumit comerciant sau la calitatea produselor acestuia; eventual ne exprimăm acordul/dezacordul cu privire la conţinutul mesajului sau îl distribuim ori adăugăm un comentariu. Foarte des întâlnite sunt şi „listele negre" publicate pe internet, în care sunt menţionaţi anumiţi comercianţi ca fiind răi platnici, „ţepari" etc., iar pe forumul de discuţii al acestor pagini de internet se regăsesc numeroase comentarii.

Exemplele de mai sus au elemente comune: afirmaţiile sunt făcute prin intermediul internetului, în diverse variante, iar persoana despre care se afirmă, persoana posibil a fi prejudiciată este o persoană juridică – un comerciant de cele mai multe ori – şi nu o persoană fizică. Sunt cele două aspecte particulare care ne-au suscitat interesul şi care vor contura limitele

[2] Legea nr. 31/1990 privind societăţile, publicată în M.O. nr. 126-127 din 17 noiembrie 1990, cu ultima modificare prin Legea nr. 152/2015, publicată în M.O nr. 519 din13 iulie 2015.

demersului nostru juridic, pornind de la premisa că persoana juridică titulară a dreptului referitor la personalitate susţine că reputaţia sa a fost prejudiciată.

3. Dar o persoană juridică are un drept la reputaţie, un drept la demnitate, un drept la imagine? Poate fi ea titulară a drepturilor personalităţii?

Încălcări ale drepturilor personalităţii al căror titular este o persoană fizică au constituit obiectul unei jurisprudenţe ample, atât la nivelul instanţelor din România, cât şi la nivelul Curţii Europene a Drepturilor Omului (CEDO) ori al Curţii de Justiţie a Uniunii Europene (CJUE), existând abordări şi pentru situaţia în care prejudicierea s-a produs prin mijlocirea internetului.

Persoanele juridice însă se află într-o postură dificilă, existând opinii foarte variate privind aptitudinea lor de a fi titulare de drepturi ale personalităţii: fie se neagă o asemenea vocaţie, fie se recunoaşte o asemenea aptitudine, însă aceste drepturi ale personalităţii sunt excluse din categoria drepturilor fundamentale, fie se pune semn de egalitatea între persoanele juridice şi persoanele fizice[3]. Chestiunea este de foarte importantă pentru a şti care va fi situaţia prejudiciilor produse în statele care nu recunosc drepturile personalităţii persoanelor juridice având în vedere că din cauza caracterului global al internetului informaţiile defăimătoare pot fi accesate de oriunde şi prejudiciile se pot produce în dauna unui comerciant oriunde pe mapamond.

Fără a ne lăsa antrenaţi în dezbaterea aprinsă care există pe această temă, vom încerca să aflăm dacă persoanelor juridice le sunt recunoscute drepturile referitoare la personalitate. Pentru persoanele juridice sunt acestea drepturi fundamentale şi, implicit, se bucură ele de protecţia Convenţiei Europene a Drepturilor Omului („Convenţia”) sau de protecţie la nivelul sistemului de drept din UE, CEDO respectiv CJUE?

4. Poziţia doctrinei. Răspunsurile date întrebărilor de mai sus sunt contradictorii. S-a afirmat că este dificil a accepta o asemenea extindere,

[3] Discuțiile nu sunt limitate la cele două sisteme europene. Pentru exemple din cealaltă parte a Atlanticului, a se vedea, de exemplu, Hotărârea Citizens United/Federal Election Commission 558 U. S. 310 (2010), referitoare la libertatea discursului politic al persoanelor juridice și, mai recent, Hotărârea Burwell/Hobby Lobby Stores 573 U. S. (2014), unde Curtea Supremă a SUA a recunoscut că societățile cu scop lucrativ pot să susțină convingeri religioase.

chiar dacă unele atribute ale persoanei juridice pot evoca o oarecare analogie cu argumentul că aceste drepturi sunt intim ataşate persoanei fizice.[4]

Alţi autori au recunoscut drepturile referitoare la personalitate ale persoanelor juridice, însă le-au catalogat ca drepturi inferioare celor ale persoanelor fizice, întrucât „dacă este vorba despre bani, atunci nu este demn de protecţie a drepturilor fundamentale".[5]

5. Aspecte de drept comparat. Drepturile personalităţii sunt recunoscute la nivel naţional prin legi organice, prin coduri sau chiar prin constituţie.

În dreptul german, protecţia drepturilor referitoare la personalitate se realizează pentru persoanele fizice, cât şi pentru cele juridice, începând de la nivel constituţional. Dreptul referitor la personalitate al întreprinderii protejează reputaţia unei întreprinderi şi libertatea garantată constituţional a acesteia de a desfăşura o activitate comercială[6]. În Franţa, se pare că s-a acceptat faptul că persoanele juridice beneficiază de anumite drepturi referitoare la personalitate, în special atunci când onoarea sau reputaţia acestora este pusă în discuţie[7]. În dreptul englez, conceptele de defăimare şi aserţiuni false rău intenţionate protejează reputaţia şi interesul economic al entităţilor juridice[8]. În Spania, instanţa supremă a admis existenţa onoarei şi a intimităţii persoanelor juridice încă din 1939, menţinându-şi poziţia şi printr-o sentinţă din 1995[9], care statua că, în anumite împrejurări, poate exista o recunoaştere expresă sau tacită a drepturilor fundamentale şi persoanelor juridice. În hotărâre se arată că deşi dreptul la onoare şi la intimitate se găseşte într-o strânsă legătură cu persoana fizică, acestea nu trebuie să fie excluse din domeniul protecţiei persoanei juridice: „persoana

[4] O. Ungureanu, C. Munteanu, *Dreptul la propria imagine, în noul Cod civil*, în *Liber amicorum Liviu Pop. Reforma dreptului privat roman in contextul federalismului juridic European*, Editura Universul Juridic, București, 2015, pp.914-933.

[5] *Ibidem.*

[6] A. Koreng, *Das «Unternehmenspersönlichkeitsrecht» als Element des gewerblichen Reputationsschutze*, în GRUR 2010, pp. 1065-1070, [Online] la https://www.juris.de/jportal/prev/SBLU000850410.

[7] L. Dumoulin, *Les droits de la personnalité des personnes morales*, în *Revue des sociétés nr.1/*2006, spéc., pp. 3-12.

[8] O. Ungureanu, C. Munteanu, *op. cit.*, pp.914-933.

[9] Decizia Tribunalului Constituţional nr. 139 din 26 sept. 1995 citată în O. Ungureanu, C. Munteanu, *op. cit*., pp.914-933.

juridică poate şi ea să fie vătămată în onoarea sa atunci când este defăimată sau când, din pricina altuia, decade din considerarea de care s-a bucurat”[10].

6. Jurisprudenţa CEDO, jurisprudenţa CJUE. Drepturile personalităţii sunt recunoscute la nivel european prin dispoziţiile Convenţiei şi ale Cartei Europene a Drepturilor Fundamentale („Carta”). De altminteri, între Cartă şi Convenţie există convergenţă. În hotărârea Rotaru vs. România, referitor la drepturile fundamentale din Cartă se face trimitere la Convenţie, arătându-se că înţelesul dreptului fundamental consacrat de Cartă este acelaşi cu cel conferit de Convenţie, fără ca aceasta să împiedice dreptul UE să îi acorde limite mai largi. Dreptul la viaţa privată[11] din Cartă este un drept corespunzător celui din art. 8 al Convenţiei [12], textele – alineatul 1 – celor două articole fiind identice.

Iniţial, în cadrul sistemului Convenţiei, doar articolul 1 din Protocolul adiţional nr. 1 la Convenţie privind dreptul de proprietate prevedea *în mod expres* aplicarea acestuia în cazul persoanelor juridice. Cu toate acestea, ulterior, atât CEDO, cât şi CJUE au extins în mod gradual protecţia drepturilor fundamentale la persoanele juridice în cazurile în care o astfel de abordare părea adecvată cu privire la dreptul fundamental în cauză. În ambele sisteme, extinderea drepturilor fundamentale la persoanele juridice s-a produs în mod natural şi spontan. De exemplu, a fost acceptată extinderea în ceea ce priveşte libertatea de expresie, dreptul la respectarea domiciliului şi a corespondenţei şi dreptul la un proces echitabil[13].

Punctual, în ceea ce priveşte drepturile referitoare la personalitate ale persoanelor juridice, recunoaşterea indirectă a acestora poate fi regăsită în Hotărârea Fayed împotriva Regatului Unit[14]. CEDO a afirmat că, în ceea ce priveşte dreptul la o bună reputaţie, limitele unor critici acceptabile sunt mai

[10] O.Ungureanu, C. Munteanu, *op.cit*., pp.914-933.

[11] Art. 7 din Cartă – *„Respectarea vieții private și de familie”* – prevede că: *„Orice persoană are dreptul la respectarea vieții private și de familie, a domiciliului și a secretului comunicațiilor (...)”*.

[12] Art. 8 din Convenție – *„Dreptul la respectarea vieţii private şi de familie”* – are următorul conținut *„1. Orice persoană are dreptul la respectarea vieţii sale private şi de familie, a domiciliului său şi a corespondenţei sale. 2. Nu este admis amestecul unei autorităţi publice în exercitarea acestui drept decât în măsura în care acesta este prevăzut de lege şi constituie, într-o societate democratică, o măsură necesară pentru securitatea naţională, siguranţa publică, bunăstarea economică a ţării, apărarea ordinii şi prevenirea faptelor penale, protecţia sănătăţii, a moralei, a drepturilor şi a libertăţilor altora”*.

[13] P. Oliver, *Companies and their Fundamental Rights: a comparative perspective*, în *International and Comparative Law Quarterly*, vol. 64, ediția a treia, iunie 2015, pp. 661-696.

[14] Hotărârea CEDO în cauza *Fayed împotriva Regatului Unit* din 21 septembrie 1990.

largi cu privire la oamenii de afaceri implicaţi în companii publice decât pentru persoane private[15]. În plus, CEDO a apreciat că statutul unei părţi din proces de a fi companie multinaţională nu înlătură dreptul acesteia de a se apăra împotriva unor acuzaţii calomnioase.

Pe de altă parte însă, CEDO a admis că, în ceea ce priveşte limitarea drepturilor fundamentale, părţile semnatare ale Convenţiei ar putea să dispună de o marjă de apreciere mai mare pentru situaţiile referitoare la activităţile profesionale ale persoanelor implicate.

În mod similar, CJUE[16] a confirmat faptul că persoanele juridice beneficiază de dreptul de proprietate[17], dar şi de libertatea de a desfăşura o activitate comercială[18]. Drepturile referitoare la personalitate pot fi concepute şi ca instrumente pentru protecţia efectivă a altor drepturi fundamentale de care beneficiază persoanele juridice, cum ar fi libertatea de a desfăşura o activitate comercială. Pe cale de consecinţă, încălcarea drepturilor referitoare la personalitate ale unei societăţi care constă într-un prejudiciu adus reputaţiei acesteia se va traduce în mod direct în încălcarea drepturilor economice ale acesteia. Ca urmare, protecţia efectivă a acestor drepturi economice (de care se bucură, cu siguranţă, persoanele juridice) impune şi protecţia drepturilor referitoare la personalitate ale acestora.

În prezent, CJUE este învestită printr-o cerere de decizie preliminară formulată de Riigikohus (Curtea Supremă, Estonia) cu o cauză care, conex, ridică tocmai problema recunoaşterii drepturilor personalităţii şi în favoarea persoanelor juridice. Este vorba despre cauza C-194/16, Bolagsupplysningen OÜ, Ingrid Ilsjan împotriva Svensk HandelAB – „Regulamentul nr. 1215/2012 – Competenţa în materie delictuală şi cvasidelictuală – Publicarea de informaţii pe internet – *Drepturile referitoare la personalitate ale persoanelor juridice* – Centru de interese – Ordin de a şterge şi de a corecta informaţiile într-un alt stat membru – Cerere de despăgubiri”.[19]

---

[15] A se vedea de asemenea și Hotărârea CEDO *Steel și Morris împotriva Regatului Unit* din 15 mai 2005 și Hotărârea CEDO în cauza *Markt intern Verlag GmbH și Klaus Beermann împotriva Germaniei* din 20 noiembrie 1989.

[16] Curtea a stabilit că persoanele juridice au dreptul la o cale de atac efectivă și de dreptul la asistență juridică și că acestea beneficiază de prezumția de nevinovăție.

[17] A se vedea, Hotărârea *Berlington Hungary* și alții din 11 iunie 2015.

[18] A se vedea Hotărârea *AGET Iraklis* din 21 decembrie 2016, C-201/15.

[19] Cauza este pendinte, fiind depuse Concluziile avocatului general Michal Bobek la data de 13 iulie 2017. În speță este vorba despre o societate estoniană care desfășoară activități în Suedia și care a fost inclusă pe o listă neagră, pe pagina de internet a unei federații a

7. În Romania, în prezent, fără să distingă, art. 58 C.civ. cu denumirea marginală *„Drepturi ale personalităţii”* consacră: *„(1)Orice persoană are dreptul la viaţă, la sănătate, la integritate fizică şi psihică, la demnitate, la propria imagine, la respectarea vieţii private, precum şi alte asemenea drepturi recunoscute de lege”*.

După ce în această parte generală sunt enumerate drepturile personalităţii, într-o secţiune subsecventă – secţiunea 2 – sunt reglementate dreptul la viaţă, la sănătate şi la integritate fizică şi psihică, care sunt drepturi inerente calităţii de fiinţa umană şi pot aparţine exclusiv persoanei fizice.

De-abia ulterior, într-o altă secţiune – secţiunea 3 – în art. 72 C. civ. este definit dreptul la demnitate în cuprinsul căruia este inclus expres şi dreptul la reputaţie: *„(1) Orice persoană are dreptul la respectarea demnităţii sale. (2) Este interzisă orice atingere adusă onoarei şi reputaţiei unei persoane, fără consimţământul acesteia ori fără respectarea limitelor prevăzute la art. 75”*.[20]

În Titlul V cu denumirea *„Apărarea drepturilor nepatrimoniale”*, după ce consacră în art. 252 C..civ. cu titlu de principiu că orice persoană fizică are dreptul la ocrotirea valorilor intrinseci fiinţei umane – printre care şi demnitatea – şi indică mijloacele juridice de apărare concrete puse la îndemâna persoanelor prejudiciate, în art. 257 C..civ – *„Apărarea drepturilor nepatrimoniale ale persoanei juridice”* – se prevede că *„Dispoziţiile prezentului titlu se aplică prin asemănare şi drepturilor nepatrimoniale ale persoanelor juridice”*.

---

angajatorilor din Suedia, pentru presupuse practici comerciale îndoielnice, constând în „acte de fraudă și înșelăciune”. Pagina de internet a atras comentarii ostile din partea cititorilor săi, iar pe forumul de discuții al paginii de internet se regăseau aproximativ 1 000 de comentarii, inclusiv apeluri la acte de violență împotriva societății din Estonia și a angajaților acesteia.

Societatea estoniană a introdus o acțiune în fața instanțelor estoniene împotriva federației suedeze acuzând-o că informațiile publicate i-au afectat onoarea, reputația și renumele. Aceasta a solicitat instanțelor estoniene să oblige federația suedeză la rectificarea informațiilor și la ștergerea comentariilor de pe pagina sa de internet. De asemenea, aceasta a solicitat despăgubiri pentru prejudiciul pretins suferit ca urmare a informațiilor și a comentariilor care au fost publicate online.

[20] Art. 75 C.civ. cu denumirea marginală *„Limite”* prevede că: *„(1) Nu constituie o încălcare a drepturilor prevăzute în această secţiune atingerile care sunt permise de lege sau de convenţiile şi pactele internaţionale privitoare la drepturile omului la care România este parte. (2) Exercitarea drepturilor şi libertăţilor constituţionale cu bună-credinţă şi cu respectarea pactelor şi convenţiilor internaţionale la care România este parte nu constituie o încălcare a drepturilor prevăzute în prezenta secţiune”*.

8. O primă concluzie. În considerarea celor mai sus expuse apreciem că, la nivel de principiu, nu există motive întemeiate pentru care persoanele juridice să nu fie înzestrate, în măsura în care analogia permite în mod rezonabil acest lucru, cu drepturi referitoare la personalitate. Este adevărat că referitor la persoana fizică se face vorbire şi se reglementează „personalitatea *umană*", iar în privinţa persoanei juridice expresia utilizată este „personalitate *juridică*", dar apreciem că dreptul fundamental în cauză poate fi recunoscut unei persoane juridice dacă, printr-o analogie rezonabilă, el poate fi aplicat unei persoane juridice. Apreciem că drepturile personalităţii – inclusiv dreptul la reputaţie – sunt aferente şi calităţii de persoană juridică, intră în categoria drepturilor fundamentale şi se bucură de protecţie la nivel european, în măsura în care acestea nu sunt indisolubil legate de calitatea de fiinţă.

9. Potrivit Dicţionarului explicativ al limbii române, reputaţia reprezintă „părere publică, favorabilă sau defavorabilă, despre cineva sau ceva; felul în care cineva este cunoscut sau apreciat; renume, faimă, celebritate".

În doctrină, se apreciază că graniţa dintre onoare şi reputaţie este destul de greu de stabilit, ele putând fi considerate două faţete ale dreptului la demnitate. Onoarea este un sentiment complex, determinat de percepţia pe care fiecare persoană o are despre demnitatea sa, în timp ce reputaţia înseamnă felul în care o persoană este considerată în societate.

Reputaţia nu este înnăscută, ci este, de cele mai multe ori, dobândită, prin modul exemplar în care persoana se comportă în viaţa privată sau în cea socială. Afirmaţia este valabilă atât referitor la persoanele fizice, cât şi în privinţa societăţilor reglementate de Legea nr. 31/1990 privind societăţile. Maniera în care comerciantul persoană juridică se comportă în viaţa de afaceri încă de la constituirea ei generează în piaţă un renume, care are caracteristica de a atrage sau, dimpotrivă, de a respinge clientela sau partenerii contractuali ori potenţialii investitori. Nu este de neglijat că o condiţie cerută până de curând pentru ca o persoană să poată fi numită administrator al unei societăţi era onorabilitatea acesteia – administratorul fiind considerat că reprezintă imaginea societăţii.

10. Fapta ilicită cauzatoare de prejudicii. Pentru a se antrena răspunderea civilă este necesar sa existe o faptă care aduce atingere dreptului la reputaţie, faptă săvârşită în cazul de faţă printr-un mijloc specific –

internetul – ceea ce îi conferă o serie de trăsături care se reflectă şi asupra consecinţelor, adică asupra prejudiciului.

La stabilirea caracterului prejudiciabil al faptei trebuie găsit un just echilibru între libertatea de exprimare şi dreptul la reputaţie, întrucât conform 30 alin. 6 din Constituţia României, *„libertatea de exprimare nu poate prejudicia demnitatea, onoarea, viaţa particulară a persoanei şi nici dreptul la propria imagine”*, existând doctrină amplă şi jurisprudenţă bogată atât naţională, cât şi la nivelul CEDO pe această temă.

Criteriile de apreciere a caracterului prejudiciabil de care instanţa ar putea tine seama sunt: reputaţia persoanei juridice despre care se fac afirmaţiile denigratoare, forma, stilul şi contextul mesajului critic, contextul în care este redactată informaţia (cauza Niculescu Dellakeza împotriva României), interesul public pentru informaţia postată (cauza Bugan împotriva României), buna sau reaua credinţă a celui care a furnizat informaţia (cauza Ileana Constantinescu împotriva României).

Este necesar ca presupusele informaţii prejudiciabile să fie susceptibile să afecteze activităţile profesionale, comerciale ale persoanei juridice.[21]

11. Prejudiciul. În ceea ce priveşte existenţa şi întinderea prejudiciului cauzat prin încălcarea drepturilor personalităţii prin intermediul internetului, ar trebui făcută distincţia dintre persoane fizice şi juridice? Pentru că pentru cele dintâi există o oarece practică, atât în ceea ce priveşte prejudiciului patrimonial, cât şi prejudiciul moral.

În cazul persoanelor juridice, a societăţilor (comerciale), cel mai probabil este ca prejudiciul să se producă în mod specific în legătură cu activitatea profesională a acestora. În privinţa societăţilor considerăm că despăgubirile solicitate ca răspuns la informaţiile prejudiciabile publicate pe internet corespund, în realitate, pierderilor comerciale ale acestora.

Acest lucru ridică probleme diferite faţă de cele care apar în cazul unei persoane fizice a cărei reputaţie este afectată.

De ce este dificil de cuantificat prejudiciul în cazul încălcării dreptului la reputaţie al persoanelor juridice săvârşită prin internet?

---

[21] Decizia nr. 1044/8.08.2017 a Curții de Apel București, [Online] la https://www.clujust.ro/trimis-judecata-pentru-ca-creat-pagina-de-facebook-icepworld-o-mare-teapa-achitat-definitiv/, accesată la data de 25.10.2017.

Internetul este o metodă de difuzare a informaţiei complet diferită de cea realizată prin intermediul suporturilor convenţionale, deoarece presupune accesul universal la informaţie. După cum bine se ştie, informaţia se poate consulta în orice loc al lumii în care există acces la internet. Gravitatea prejudiciului care poate fi suferit de titularul dreptului fundamental este sporită de faptul că informaţiile denigratoare sunt disponibile în orice punct al planetei. Chiar şi mijloacele care presupun plata unei taxe pentru accesarea informaţiei se diferenţiază de formatele tradiţionale de difuzare prin faptul că, în general, achiziţionarea acestora presupune acoperirea întregului mapamond. Pe de altă parte, pentru că informaţiile sunt accesate în diferite state şi pentru că informaţia poate prezenta un interes particular într-un anumit loc, tot în acel loc eventuala atingere adusă drepturilor referitoare la personalitate va putea produce prejudiciul cel mai grav.

Nici impactul aspectului temporal nu poate fi trecut cu vederea. Internetul conferă accesul instantaneu la conţinutul informaţiei şi potenţial de permanenţă informaţiilor. Odată ce un conţinut circulă pe internet, prezenţa sa pe internet este, în principiu, nelimitată în timp, chiar dacă informaţia, în aparenţă, este ştearsă.

Din toate aceste motive măsurarea impactului informaţiei care în cadrul mijloacelor de informare în masă tradiţionale se întemeiau pe tehnici oarecum sigure, se transformă într-o sarcină imposibil de îndeplinit atunci când informaţia circulă pe internet, iar evaluarea prejudiciului este foarte dificilă.

12. La stabilirea prejudiciului patrimonial în cazul unei persoane juridice cu scop lucrativ – de exemplu, o societate reglementată de Legea nr. 31/1990 privind societăţile –, un criteriu de care se va ţine seama este scăderea a cifrei de afaceri. Dacă reputaţia comercială a fost vătămată, consecinţa este pierderea partenerilor de afaceri, pierderea actualei clientele şi imposibilitatea cooptării de noi clienţi – elemente care vor fi luate în considerare la cuantificarea prejudiciului patrimonial. Se poate ca prin publicarea de informaţii incorecte să se ajungă la paralizarea activităţii societăţii denigrate. În special în domeniul afacerilor reputaţia unei societăţi, „imaginea” pe care o are aceasta constituie un adevărat capital (moral). Atingerea adusă reputaţiei va avea consecinţe pecuniare importante, uneori hotărâtoare pentru societatea comercială, dar şi pentru administratorul sau

asociaţii săi, oamenii de afaceri, mergând până la compromiterea bussinesului ca o consecinţă a repudierii lor din viaţa lor de afaceri.

13. Existenţa unui prejudiciu nu se poate presupune, ci trebuie dovedită. Simpla postare a unor informaţii despre activitatea unei persoane nu duce automat la existenţa unui prejudiciu. În lipsa unor dovezi clare, din care să rezulte îndeplinirea cumulativă a condiţiilor răspunderii civile delictuale – şi mai ales a raportului de cauzalitate – nu poate duce la obligarea la plata unor despăgubiri civile.

Scăderea cifrei de afaceri sau a numărul de clienţi ori a altor contacte profesionale se va avea în vedere doar dacă acestea sunt consecinţa postării respectivei informaţii pe internet, chestiune aferentă problematicii raportului de cauzalitate. Împrejurarea diminuării încasărilor, a cifrei de afaceri, a clientelei societăţii, a profitului poate fi explicată în egală măsură şi prin circumstanţe obiective care au afectat piaţa specifică obiectului de activitate al societăţii respective. Ar putea fi vorba de un management defectuos, de o schimbare în structura acţionariatului, de modificări legislative la nivelul fiscalităţii sau de orice altă cauză care nu are legătură cu informaţiile denigratoare publicate şi care nu va antrena obligarea postacului la plata de daune. Altfel spus, dacă nu se va face dovada raportului de cauzalitate între informaţiile postate şi diminuarea încasărilor societăţii nu se vor datora daune. Iar stabilirea raportului de cauzalitate între postarea denigratoare şi diminuarea unor indicatori economici cuantificabili, dar care nu reprezintă prejudiciul suferit, este foarte greu de probat.

Chiar dacă se va constata că diminuarea indicatori economici este consecinţa directă a postărilor contestate, instanţa nu va obliga la plata unor sume egale cu aceste scăderi, întrucât reducerile constatate nu reprezintă prejudiciul suferit de persoana prejudiciată. Diminuările cuantificabile ale acestor indicatori economici vor reprezenta repere de care instanţa va ţine seama la stabilirea daunelor cuvenite.

14. La stabilirea prejudiciului instanţa va ţine seama şi de o serie de elemente care nu sunt cuantificabile economic:

- situaţia de fapt a societăţii prejudiciate considerate *în contextul* naturii informaţiei postate;

- poziţia în mediul de afaceri a societăţii prejudiciate şi modul în care poziţia respectivă ar fi putut sau nu ar fi putut fi afectată de declaraţia controversată;

- numărul de consultări (accesări) ale site-ului, însă aceasta nu face să se cunoască numărul de persoane care au accesat informaţia, întrucât din momentul în care o informaţie este postată pe internet, particularii se transformă imediat, voluntar sau involuntar, în distribuitori de informaţii prin reţele de socializare, prin comunicare electronică, prin linkuri, prin bloguri sau prin orice alte mijloace oferite de internet. Chiar şi o singură accesare a informaţiei conduce la concluzia că se produce o „distribuţie".

- limba paginii de internet, respectiv a postării, contribuie la delimitarea influenţei informaţiilor denigratoare publicate într-o anumită zonă. Cu toate acestea, odată cu dezvoltarea traducerii automate şi cu publicarea informaţiilor în limbile de circulaţie internaţională, acest criteriu nu mai este atât de semnificativ cu privire la posibila accesare a informaţiei si, implicit, a stabilirii prejudiciului cauzat societăţii defăimate.

- publicitatea conţinută pe pagina de internet, în cazul în care există, poate da o serie de indicii cu privire la care raza teritorială în care informaţia are vocaţia de a fi consultată şi implicit de a cauza prejudicii societăţii defăimate.

- conduita administratorului paginii de internet (acolo unde este cazul) cu privire la îndeplinirea obligaţiile pozitive de a cenzura sau a împiedica publicarea mesajelor cu un conţinut defăimător.

15. Situaţia prejudiciului nepatrimonial. În principiu, încălcarea drepturilor personalităţii, care sunt drepturi nepatrimoniale, poate genera prejudicii patrimoniale şi prejudicii nepatrimoniale. Acoperirea acestora din urmă se realizează prin acordarea de daune morale.

Problema acordării daunelor morale persoanelor juridice a fost dintotdeauna controversată, în principiu susţinându-se că persoanele juridice nu au o asemenea vocaţie. Totuşi, pe tărâmul art. 54 alin. 1 din Decretul nr. 31/1954 privind persoanele fizice şi juridice[22], o parte a doctrinei admitea că

[22] Art. 54 din Decretul nr. 51/1934 privind persoanele fizice și persoanele juridice, publicat în Buletinul Oficial nr. 8 din 30 ianuarie 1954 (abrogat) prevedea că*: „(1) Persoana care a suferit o atingere în dreptul său la nume ori la pseudonim, la denumire, la onoare, la reputație, în dreptul personal nepatrimonial de autor al unei opere științifice, artistice ori literare, de inventator sau în orice alt drept personal nepatrimonial, va putea cere instanței judecătorești încetarea săvârșirii faptei care aduce atingerea drepturilor mai sus arătate. (2) Totodată, cel care a suferit o asemenea atingere va putea cere ca instanța judecătorească să oblige pe autorul faptei săvârșite fără drept, să publice, pe socoteala acestuia, în condițiile stabilite de instanța, hotărârea pronunțată ori să îndeplinească alte fapte destinate să restabilească dreptul atins"*.

sunt supuse reparaţiei şi prejudiciile cauzate ca urmare a încălcării drepturilor sale cu conţinut neeconomic.

În jurisprudenţa penală mai veche s-a afirmat deseori că persoanele juridice nu pot primi daune morale, întrucât nu există un prejudiciu psihic în aceste situaţii, afirmându-se că „este nelegală soluţia de obligare a inculpatului la plata daunelor morale către persoane juridice, acestea acordându-se numai persoanelor fizice care au suferit un prejudiciu moral de pe urma comiterii unei suferinţe.”[23]

Mai târziu, pe cale jurisprudenţială, s-a arătat că „nu se poate generaliza în sensul că prejudiciul moral nu poate fi încercat decât de o persoană fizică, chiar dacă în marea majoritate a cazurilor doar aceste subiecte de drept sunt predispuse la suferirea unui astfel de prejudiciu. Existenţa daunelor morale a fost recunoscută pentru a stabili o modalitate de reparare a suferinţelor fizice încercate sau a atingerilor aduse onoarei, demnităţii, reputaţiei, prestigiului unei persoane. Dacă aceste atribute sunt în general proprii persoanelor fizice, unele dintre ele por fi atribuite şi persoanelor juridice”[24]. În această cauză, partea prejudiciată era o universitate care afirma că i-a fost încălcată reputaţia. Instanţa a reţinut că reputaţia şi prestigiul sunt valori morale inerente unei instituţii de învăţământ superior şi care, împreună cu calitatea actului de învăţământ pe care îl oferă, îi generează acesteia o anumită poziţie în ierarhia universitară, obligând la plata de daune morale.

Ulterior, în anul 2012, instanţa supremă a obligat o persoană juridică la plata daunelor morale pentru prejudicii cauzate altei persoane juridice pentru fapte de contrafacere şi concurenţă neloială. Prin hotărârea amintită pentru prima oară, o societate comercială a fost condamnată penal pentru săvârşirea a două infracţiuni de contrafacere de marcă şi pentru o infracţiune de concurenţă neloială, iar pe latura civilă a cauzei obligă inculpaţii în solidar la plata de daune materiale şi 20.000 lei daune morale.

[23] A se vedea Curtea de Apel Bucureşti, Secţia a I-a penală, Decizia nr. 162/03.02.2004.

[24] A se vedea Curtea de Apel Timişoara, Secţia civilă, Decizia nr. 348 din 5 aprilie 2011, nepublicată, citată în A.-R. Ilie, *Pot fi acordate daune morale unei persoane juridice în cadrul acţiunii civile exercitate în procesul penal*?, [Online] la https://www.juridice.ro/256275/pot-fi-acordate-daune-morale-unei-persoane-juridice-in-cadrul-actiunii-civile-exercitate-in-procesul-penal.html, accesat la 25.10.2017.

Cu privire la daunele morale, instanţa a motivat că acordarea unei sume de 20.000 lei „este de natură a acoperi prejudiciul moral suferit prin contrafacerea mărfii şi concurenţă neloială efectuate de inculpaţi".

O observaţie se impune: în ceea ce priveşte infracţiunea de concurenţă neloială, posibilitatea acordării de daune morale este prevăzută expres de art. 9 din Legea nr. 11/1991 privind combaterea concurenţei neloiale, însă instanţa nu a reţinut acest articol ca temei de drept pentru acordarea daunelor morale. Potrivit textului de lege amintit, dacă „infracţiunea cauzează daune morale, cel prejudiciat este în drept să se adreseze instanţei competente cu acţiune în răspundere civilă corespunzătoare". Textul nu distinge după cum cel prejudiciat este o persoană fizică ori juridică. Însă, cu privire la infracţiunea de contrafacere, nu există un text similar, ceea ce ar sugera că daunele morale pot fi acordate independent de existenţa vreunei menţiuni exprese în legea specială[25] .

Însă în anul 2016, instanţa supremă printr-o altă hotărâre a stabilit că doar în cazul în care prin legi speciale se recunoaşte expres dreptul la daune morale, acestea pot fi acordate în temeiul textului din legea specială şi nu apreciind întrunirea condiţiilor generale ale răspunderii civile consacrate în Codul civil. În decizia invocată, Înalta Curte de Casaţie şi Justiţie arată că rolul daunelor morale este acela de a conduce la o reparare a suferinţelor fizice încercate sau a atingerilor aduse onoarei, demnităţii, reputaţiei, prestigiului unei persoane. În continuare, instanţa supremă afirmă că: „deşi aceste atribute sunt în general proprii persoanelor fizice, unele dintre ele pot fi atribuite şi persoanelor juridice, însă, în aceste cazuri, legiuitorul a recunoscut în mod expres posibilitatea acordării daunelor morale persoanei juridice (de exemplu, pentru fapte de concurenţă neloială sau pentru nesocotirea dreptului la denumire, sediu, emblemă, marcă de fabrică)". Prin urmare, Înalta Curte a reţinut că „posibilitatea acordării daunelor morale nu poate fi extinsă artificial pentru a putea analiza îndeplinirea cumulativă a cerinţelor impuse de Codul civil, întrucât persoana juridică nu poate pretinde un prejudiciu psihic sau vreo suferinţă fizică provocată".[26]

---

[25] https://www.juridice.ro/256275/pot-fi-acordate-daune-morale-unei-persoane-juridice-in-cadrul-actiunii-civile-exercitate-in-procesul-penal.html. A se vedea, A.-R. Ilie, *Notă* la sentinţa 41 din 10 martie 2011 a Tribunalului Buzău, în Curierul Judiciar nr. 2/2013.

[26] I.C.C.J, sect. a II-a civ., Decizia nr. 373 din 24 februarie 2016, [Online] la https://www.juridice.ro/446645/iccj-admisibilitatea-acordarii-de-daune-morale-unei-persoane-juridice.html, accesat la 14.10.2017.

Şi totuşi, sistemul noului Cod civil recunoaşte drepturile nepatrimoniale ale persoanei juridice şi consacră expres posibilitatea reparării prejudiciilor materiale sau morale cauzate prin încălcarea lor. Astfel, art. 253 C.civ.[27] – *„Mijloace de apărare”* – prevede expres că: *„De asemenea, persoana prejudiciată poate cere despăgubiri sau, după caz, o reparaţie patrimonială pentru prejudiciul, chiar nepatrimonial, ce i-a fost cauzat, dacă vătămarea este imputabilă autorului faptei prejudiciabile”*.

Daunele morale se justifică doar dacă s-a făcut dovada faptului că publicarea informaţiilor respective a avut o influenţă directă asupra activităţii comerciale desfăşurate de societatea prejudiciată în mediul de afaceri, respectiv că ar fi condus la micşorarea şanselor sale în competiţia comercială, evaluarea trebuind să fie făcută în funcţie de circumstanţele concrete ale cauzei, sens în care s-a pronunţat şi CEDO în mod constant.

16. Dacă se admite posibilitatea acordării de daune morale persoanelor juridice se pune problema cuantificării sumelor cuvenite persoanelor prejudiciate.

Prejudiciile morale constituie consecinţe dăunătoare care nu pot fi evaluate în bani, deci cu un conţinut neeconomic şi care rezultă din încălcările drepturilor personale nepatrimoniale.

În materia daunelor morale, dată fiind natura prejudiciului care le generează, practica judiciară şi literatura de specialitate au subliniat că nu există criterii precise pentru cuantificarea lor, respectiv că problema stabilirii despăgubirilor morale nu trebuie privită ca o cuantificare economică a unor

[27] Art. 253 C.civ. cu denumirea marginală *„Mijloace de apărare”* are următorul conținut: *„(1) Persoana fizică ale cărei drepturi nepatrimoniale au fost încălcate ori ameninţate poate cere oricând instanţei: a) interzicerea săvârşirii faptei ilicite, dacă aceasta este iminentă; b) încetarea încălcării şi interzicerea pentru viitor, dacă aceasta durează încă; c) constatarea caracterului ilicit al faptei săvârşite, dacă tulburarea pe care a produs-o subzistă. (2) Prin excepţie de la prevederile alin. (1), în cazul încălcării drepturilor nepatrimoniale prin exercitarea dreptului la libera exprimare, instanţa poate dispune numai măsurile prevăzute la alin. (1) lit. b) şi c). (3) Totodată, cel care a suferit o încălcare a unor asemenea drepturi poate cere instanţei să îl oblige pe autorul faptei să îndeplinească orice măsuri socotite necesare de către instanţă spre a ajunge la restabilirea dreptului atins, cum sunt: a) obligarea autorului, pe cheltuiala sa, la publicarea hotărârii de condamnare; b) orice alte măsuri necesare pentru încetarea faptei ilicite sau pentru repararea prejudiciului cauzat. (4) De asemenea, persoana prejudiciată poate cere despăgubiri sau, după caz, o reparaţie patrimonială pentru prejudiciul, chiar nepatrimonial, ce i-a fost cauzat, dacă vătămarea este imputabilă autorului faptei prejudiciabile. În aceste cazuri, dreptul la acţiune este supus prescripţiei extinctive”*.

drepturi şi valori nepatrimoniale (cum ar fi demnitatea, onoarea), ci ca o evaluare complexă a aspectelor în care vătămările produse se exteriorizează, supusă puterii de apreciere a instanţelor de judecată. Despăgubirile solicitate ca răspuns la informaţiile prejudiciabile publicate pe internet corespund, în realitate, pierderilor comerciale pentru entităţile juridice.[28]

Stabilirea daunelor morale nu este supusă unor criterii legale de determinare, la evaluarea acestora, urmând a fi avute în vedere consecinţele negative suferite, importanţa valorilor lezate, intensitatea cu care au fost percepute consecinţele vătămării etc.

Principiul ce se degajă din jurisprudenţa CEDO în materia daunelor morale, pe care instanţele naţionale sunt obligate să îl aplice, este acela al statuării în echitate asupra despăgubirii acordate victimei, în raport de circumstanţele particulare ale fiecărui caz în parte şi nu în funcţie de criterii de evaluare prestabilite. De asemenea, conform aceleiaşi jurisprudenţe, despăgubirile acordate trebuie să păstreze un raport rezonabil de proporţionalitate cu paguba suferită[29]. Totodată, trebuie să existe un echilibru între prejudiciul moral suferit şi despăgubirile acordate, care, pe de o parte, să permită celui prejudiciat anumite avantaje care să atenueze suferinţele morale, dar pe de altă parte să nu permită să se ajungă în situaţia îmbogăţirii fără just temei.

17. Concluzii. În bine sau în rău, internetul a schimbat complet regulile jocului: a democratizat publicarea. În era paginilor de internet private, a postărilor personale, a blogurilor şi a reţelelor sociale, se pot distribui cu foarte mare uşurinţă informaţii privind oricare altă persoană, fie că este vorba despre persoane fizice sau juridice sau autorităţi publice.

Caracterul global şi permanent al informaţiilor contribuie la agravarea prejudiciului ce poate fi suferit de către titularul dreptului fundamental şi la dificultăţi enorme în evaluarea acestuia. Imposibilitatea cunoaşterii numărului de accesări ale informaţiei şi lipsa controlului privind

[28] „Datorită împrejurării că un astfel de prejudiciu nu poate fi evaluat direct în bani şi că legiuitorul nu a fixat nişte limite sau criterii orientative, în practică judecătorul nu poate recurge la probe, astfel încât va trebui să acorde societăţii o anumită sumă globală, care să compenseze prejudiciul moral suferit" – G. Boroi, L. Stănciulescu, *Drept civil. Curs selectiv pentru licenţă. Teste grilă*, ediţia a 3-a, revăzută şi actualizată, Editura Hamangiu, Bucureşti, 2006, pag. 257.

[29] Cu privire la aceste aspecte a se vedea, Î.C.C.J., sect I-a civ., Decizia nr. 36/2017 [Online] la *https://www.universuljuridic.ro/accident-rutier-conditiile-de-acordare-a-daunelor-materiale-si-morale-ncpc-legea-136-1995/*, accesat la 17.10.2017.

difuzarea informaţiei fac aproape imposibilă sarcina instanţei de a cuantifica prejudiciul suferit de către persoana juridică.

Este unul dintre motivele pentru care apreciem că anumite categorii juridice, printre care se numără şi cele care au constituit obiectul prezentului studiu, reclamă cel puţin o nuanţare atunci când sunt avute în vedere în raport cu relaţiile care se desfăşoară prin internet.

ANALELE ȘTIINȚIFICE ALE UNIVERSITĂȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

PROVOCĂRI JURIDICE ALE COMERȚULUI ONLINE CU MEDICAMENTE

LEGAL CHALLENGES OF E-COMMERCE WITH PHARMACEUTICALS

ȘTEFAN RĂZVAN TATARU[1]

Rezumat: Comerțul online cu medicamente reprezintă un fenomen de actualitate și importanță crescută având în vedere posibilele consecințe ale acestor operațiuni desfășurate de cele mai multe ori la limita legalului sau în afara lui. Având în vedere faptul că industria farmaceutică este una dintre cele mai profitabile, Internetul este mediul propice în care se pot dezvolta afaceri ilegale de distribuție a medicamentelor la nivel internațional. Prezentul studiu își propune să evidențieze stadiul reglementării comerțului online cu medicamente, avantajele și dezavantajele utilizării e-farmaciilor, precum și implicațiile utilizării medicamentelor contrafăcute sau falsificate. Studiul cuprinde analiza vidului legislativ privind funcționarea e-farmaciilor în România, reglementările prezente la nivel european și modalitățile de combatere a e-farmaciilor pirat de către autorități.
Cuvinte cheie: farmacie online, drept farmaceutic, comerț electronic cu medicamente, medicamente contrafăcute.

Abstract: Online drug trading is a phenomenon of topicality and increased importance given the possible consequences of these operations that are carried out, most times, at the legal limit or beyond. Considering that the pharmaceutical industry is one of the most profitable, the Internet is the auspicious environment in which illicit drug distribution operations can develop internationally. The present study aims to emphasize the stage of regulation on the online drug trade, the advantages and disadvantages of using e-pharmacies, and the implications of the use of counterfeit or falsified medicines. The study contains an analysis of the legislative gap regarding the functioning of e-pharmacies in Romania, the regulations available in the European Union and the methods used by the authorities to combat ilegal e-pharmacies.

[1] Doctorand, Universitatea "Alexandru Ioan Cuza" din Iași, Facultatea de Drept, email: razvantataru@gmail.com.

Keywords: online pharmacy, pharmaceutical law, e-commerce with medicines, counterfeit medicines.

I. Aspecte introductive privind comerțul online cu medicamente

Comercializarea online a medicamentelor[2] reprezintă o etapă inevitabilă în contextul expansiunii comerțului electronic, generând provocări unice din punct de vedere al responsabilităților legale, practicilor de bună de distribuție, conținutului informației, precumși al calității produselor. Provocările nu influențează numai vânzătorul care pune produse farmaceutice pe piața online sau consumatorul final, pacientul, ci și autoritățile de reglementare și control, medici prescriptori, farmaciști etc.[3]

Una dintre preocupările majore ale organizațiilor ce activează în domeniul sanitar este fenomenul bine cunoscut al medicamentelor falsificate[4]și / sau contrafăcute[5], comercializate prin intermediul website-

[2] Medicamentul reprezintă *"orice substanță sau combinație de substanțe prezentată ca având proprietăți pentru tratarea sau prevenirea bolilor la om; sau orice substanță sau combinație de substanțe care poate fi folosită sau administrată la om, fie pentru restabilirea, corectarea sau modificarea funcțiilor fiziologice prin exercitarea unei acțiuni farmacologice, imunologice sau metabolice, fie pentru stabilirea unui diagnostic medical"* - conform art. 695 din Legea nr. 95 din 14 aprilie 2006 privind reforma în domeniul sănătății, publicată în M. Of. nr. 372, 28.04.2006. Pe parcursul prezentului studiu vom folosi următoarele noțiuni cu același înțeles: "produs farmaceutic", "produs medicamentos" și "medicament".

[3] A.K.Chaturvedi, U.K.Singh, A.Kumar, *Online Pharmacy: An e-Strategy for medication* în *International Journal of Pharmaceutical Frontier Research*, http://www.ijpfr.com, 2011, p. 147, material disponibil [Online] la: https://www.researchgate.net/publication/237201481, accesat 10.10.2017; M.Hatzikou, T.Liappis, *E-commerce on Pharmaceuticals: a positive trend or a technological deamon?*, în Value in Health Journal, volume 7, issue 3, 2004, doi 10.1016_s1098-3015(10)62539-9.

[4] Medicamentul falsificat reprezintă "*orice medicament pentru care se prezintă în mod fals: (a) identitatea, inclusiv ambalajul și etichetarea, denumirea sau compoziția în ceea ce privește oricare dintre ingredientele sale, inclusiv excipienți și puterea ingredientelor respective; (b) sursa, inclusiv producătorul, țara de fabricație, țara de origine, deținătorul autorizației de introducere pe piață; sau (c) istoricul, inclusiv înregistrările și documentele referitoare la canalele de distribuție utilizate. Această definiție nu include deficiențele calitative neintenționate și nu aduce atingere încălcărilor drepturilor de proprietate intelectuală.*" – conform art. 1 alin. 33 din Directiva 2001/83/CE a Parlamentului European și a Consiliului din 6 noiembrie 2001 de instituire a unui cod comunitar cu privire la medicamentele de uz uman, publicată în JO L 311, 28.11.2001.

[5]Medicamentul contrafăcut reprezintă medicamentul care, în mod intenționat și fraudulos, a fost fabricat cu încălcarea drepturilor de proprietate intelectuală, de un alt producător decât cel autorizat, realizându-se o copie sau o imitație a unui produs original, cu scopul de a fi

urilor pirat. Prin urmare, monitorizarea, controlul și asigurarea calității acestor produse a devenit o sarcină importantă și dificilă pentru autorități.[6]

Tehnologizarea accelerată a determinat evoluții de amploare în mediul business, majoritatea companiilor fiind nevoite să își dezvolte activitatea comercială și în mediul online. Industria farmaceutică și domeniul medical nu au făcut excepție de la acest trend, ajungându-se imediat la comercializarea online a medicamentelor și la practicarea telemedicinei[7].

Farmaciile online, numite și e-farmacii sau cyber-farmacii, comercializează medicamente și dispozitive medicale asemeni unei farmacii tradiționale, însă pot oferi și alte servicii conexe precum consultațiile online[8].

E-farmaciile pot fi clasificate în funcție de mai multe criterii. În funcție de tipul produselor comercializate, se face distincție între farmaciile online care oferă exclusiv medicamente ce nu necesită prescripție medicală (*Over-the-counter drugs*, denumite abreviat *OTC*-uri) și cele care oferă toată gama de medicamente, incluzând aici și medicamentele eliberate cu prescripție medicală (*Recipe*, denumite abreviat *Rx*-uri).

Farmaciile online, în funcție de locul desfășurării activității principale, pot fi clasificate în e-farmacii independente, care își desfășoară

---

introdus pe piață și vândut drept un medicament original. Deși similare, termenul de "falsificare" va fi preferat pentru a evidenția riscurile de atingere a sănătății publice, pe când termenul de "contrafacere" va fi utilizat pentru a sublinia atingerile aduse drepturilor de proprietate intelectuală.

[6] B. Baert, B. De Spiegeleer, *Quality analytics of internet pharmaceuticals* în Analytical and Bioanalytical Chemistry, Volumul 398, numărul 1, Editura Springer-Verlag, Septembrie 2010, doi: 10.1007/s00216-010-3912-4.

[7] Telemedicina, conform definiției oferite de Comisia Europeană, reprezintă furnizarea de servicii de asistență medicală, bazată pe utilizarea TIC, în situații în care cadrul medical și pacientul (sau două cadre medicale) se află în locații diferite. Pentru detalii privind conceptul de telemedicina a se vedea: *Comunicare a Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor privind telemedicina și beneficiile sale pentru pacienți, pentru sistemele de sănătate și pentru societate*, Bruxelles, 4 noiembrie 2008, material disponibil [Online] la: http://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52008DC0689&from=EN, accesat 10.10.2017 și V.Raposo, *Telemedicine: The legal framework (or the lack of it) in Europe* în GMS Health Technology Assessment, 16 august 2016,[Online] la: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4987488/, accesat 10.10.2017.

[8] A se vedea R. Binns, B. Driscoll, *The Internet, pharmaceuticals and the law* în Drug Discovery Today, Volumul 6, numărul 9, mai 2001, p. 452-453, doi: 10.1016/S1359-6446(01)01781-0.

activitatea exclusiv online, neavând o adresă fizică la care pacientul poate merge pentru a achiziționa produsele dorite și e-farmacii ce acționează ca o interfață online a unei farmacii tradiționale care urmărește extinderea sau dezvoltarea afacerii pe Internet.

În funcție de modalitatea de funcționare, există e-farmacii autorizate sau legitime și e-farmacii pirat sau ilegale. În funcție de serviciile conexe oferite, există e-farmacii care oferă spre comercializare produse farmaceutice și e-farmacii care oferă inclusiv consultații medicale în vederea emiterii unei rețete și/sau eliberarea unui produs medicamentos în conformitate cu nevoile clientului-pacient.

E-farmaciile prezintă un caracter internațional prin însăși natura lor, conceptul de "online" implicând incontestabil o dimensiune "internațională", acestea desfășurându-și activitatea în *world-wide-web*.[9] Website-urile pot fi vizitate din orice stat și prin urmare pot face obiectul jurisdicției oricărui stat, în limitele principiului teritorialității legilor.

II. Stadiul reglementării comerțului online cu medicamente

Apariția, dezvoltarea și utilizarea la scară largă a e-farmaciilor a constituit un subiect amplu de discuții în mediul online, în cadrul organizațiilor profesionale din domeniul sanitar, al organizațiilor de pacienți, precum și al autorităților de reglementare în domeniu. La nivel instituțional, dezbaterile au condus la propuneri de reglementare și campanii de monitorizare și control al comerțului cu produse farmaceutice pe Internet.[10]

În anul 1998, Organizația Mondială a Sănătății a cerut statelor membre să revizuiască legislația existentă, pentru a se asigura că reglementările aplicabile sunt suficient de cuprinzătoare pentru a acoperi problemele legate de publicitatea, promovarea și vânzarea de produse farmaceutice folosind Internetul și de a dezvolta și pune în aplicare strategii de monitorizare, supraveghere și aplicare.[11]

---

[9] A se vedea și C.T. Ungureanu, *Contractul electronic* în Revista Dreptul, nr. 9/2015, pp. 158-160.

[10] A se vedea și C. Randjak, *Comercializarea online a medicamentelor*, octombrie 2014, [Online] la: http://pharma-business.ro/comercializarea-online-a-medicamentelor, accesat 10.10.2017.

[11] Pentru detalii a se vedea World Health Organization website, *Essential Drugs Monitor No. 025-026*, 1998, [Online] la: http://apps.who.int/medicinedocs/en/d/Jwhozip10e/5.14.html, accesat 10.10.2017.

În România, dezbaterile pe tema comerțului cu produse farmaceutice pe Internet au fost inițiate la începutul anilor 2000, dar nu s-au concretizat într-un act normativ. În septembrie 2015 a fost inițiată o propunere legislativă pentru modificarea și completarea Legii farmaciei nr. 266/2008[12], cu dispoziții privind comerțul online cu medicamente, obținând avizul Consiliului Legislativ și ulterior fiind adoptată de Senat. În prezent, propunerea legislativă a fost trimisă la Camera Deputaților pentru dezbatere[13].

Legea farmaciei prevede expres și limitativ situațiile în care se poate realiza comerțul cu medicamente, precum și condițiile de înființare și funcționare a farmaciilor. *Per a contrario*, până la momentul apariției unor reglementări exprese privind comerțul online cu medicamente în România, vânzarea unor asemenea produse prin mijloace informaționale este ilegală. Or, în România există numeroase e-farmacii active, ce comercializează produse farmaceutice, obținând cifre de afaceri semnificative. Din analiza termenilor și condițiilor e-farmaciilor românești putem observa că majoritatea se prevalează de dispozițiile Legii nr. 365/2002 privind comerțul electronic[14], fără respectarea interdicțiilor prevăzute în Legea farmaciei.

La nivelul Uniunii Europene, comercializarea produselor farmaceutice pe Internet a fost reglementată prin Directiva 2011/62/UE[15], oferind statelor membre posibilitatea de a permite sau de a interzice aceste operațiuni. Comercializarea prin mijloace informaționale a medicamentelor de tip OTC este permisă în majoritatea statelor membre ale Uniunii

[12] Legea farmaciei nr. 266 din 7 noiembrie 2008, republicată în M.Of. nr. 85, 2.02.2015.

[13] Pentru detalii privind Propunerea legislativă nr. L461/2015 și stadiul acesteia, a se vedea: https://www.senat.ro/legis/lista.aspx?nr_cls=L461&an_cls=2015, accesat 10.10.2017.

[14] Legea nr. 365 din 7 iunie 2002 privind comerțul electronic, publicată în M.Of. nr. 483, 5.07.2002 și ulterior republicată în M.Of. nr. 959, 29.11.2006, actualizată.

[15] Directiva 2011/62/UE a Parlamentului European și a Consiliului din 8 iunie 2011 de modificare a Directivei 2001/83/CE de instituire a unui cod comunitar cu privire la medicamentele de uz uman în ceea ce privește prevenirea pătrunderii medicamentelor falsificate în lanțul legal de aprovizionare, publicată în JOL 174, 1.07.2011, transpusă în legislația națională prin O.U.G. nr. 91/2012 din 12 decembrie 2012, publicată în M.Of. nr. 886, 27.12.2012. Notă: "*Titlul VIIA - Vânzarea la distanță către populație*" din Directivă nu a fost transpus în O.U.G. 91/2012.

Europene. În privința medicamentelor de tip Rx, situația se inversează, foarte puține state[16] permițând comercializarea lor online.[17]

Problematica comerțului electronic cu medicamente a fost examinată de Curtea de Justiție a Uniunii Europene în Hotărârea din 11 decembrie 2003 dată în cauza C-322/01, Deutscher Apothekerverberand eV v. 0800 Doc Morris și J. Waterval NV[18]. Societatea Doc Morris oferea spre vânzare produse farmaceutice pentru consumatorii germani, unele medicamente fiind autorizate în Germania, însă majoritatea în alte state membre ale Uniunii. Curtea a reținut că interdicția generală de vânzare a medicamentelor prin intermediul unui site web este nelegitimă, fiind considerată o măsură cu efect echivalent, în sensul art. 28 din Tratatul privind funcționarea Uniunii Europene (TFUE)[19]. Această interdicție este considerată dăunătoare activității comerciale desfășurate de farmaciile străine, pentru care Internetul poate fi un instrument important în accesul la o piață națională, și nu afectează farmaciile naționale în raport cu cele ale altor state membre. Articolul 30 din TFUE poate fi invocat pentru a justifica interzicerea comerțului online cu medicamente ce pot fi vândute exclusiv prin intermediul farmaciilor, din motive de sănătate publică, însă numai cu referire la medicamentele eliberate pe bază de prescripție medicală, nu și pentru medicamentele tip OTC. Prin urmare, o interdicție generală privind vânzarea de medicamente la distanță prin intermediul Internetului, cuprinsă în legislația națională, nu este compatibilă cu dreptul comunitar. Mai mult

[16] Danemarca, Republica Cehă, Germania, Olanda, Slovacia, Suedia și Regatul Unit al Marii Britanii și Irlandei de Nord, conform datelor indicate în P.Kanavos, W.Schurer, S.Vogler, *The pharmaceutical distribution chain in the European Union: structure and impact on pharmaceutical prices*, European Commission, Brussels, Belgium, 2011, p. 27, [Online] la: http://eprints.lse.ac.uk/51051/, accesat 10.10.2017.

[17] Riscurile utilizării unor produse contrafăcute sau falsificate, ce pot periclita sănătatea sau viața, subzistă inclusiv în cazul medicamentelor de tip OTC sau al suplimentelor alimentare. Pentru mai multe informații a se vedea:N.Yoshida, M.Numano, Y.Nagasaka, K.Ueda, H.Tsuboi, T.Tanimoto, K.Kimura, *Study on health hazards through medicines purchased on the Internet: a cross-sectional investigation of the quality of anti-obesity medicines containing crude drugs as active ingredients* în BMC Complementary and Alternative Medicine Journal, 2015, doi: 10.1186/s12906-015-0955-2.

[18] Pentru detalii a se vedea Hotărârea CJUE în cauza Deutscher Apothekerverband eV v. 0800 DocMorris NV and Jacques Waterval, C-322/01, ECLI:EU:C:2003:664, [Online] la: http://curia.europa.eu/juris/liste.jsf?language=ro&jur=C,T,F&num=c-322/01.

[19] Tratatul privind funcționarea Uniunii Europene (versiunea consolidată), publicat în JO C326, 26.10.2012.

decât atât, nu există nicio interdicție privind publicitatea care ar putea avea ca efect împiedicarea vânzării legale de medicamente de tip OTC pe Internet.[20]

III. Avantajele și dezavantajele utilizării e-farmaciilor

Farmaciile online oferă o serie de beneficii printre care amintim: identificarea ușoară a produselor medicamentoase și prețurile avantajoase, disponibilitate non-stop pentru lansarea comenzii, livrarea rapidă a produselor și confidențialitatea procedurii. Pacienții cu mobilitate limitată sau cei care nu au o farmacie în vecinătatea domiciliului pot beneficia de serviciile farmaciilor online prin eliminarea deplasărilor la o farmacie tradițională.

În plus, farmaciile online pot oferi confidențialitate, aspect care lipsește adesea într-o farmacie tradițională, unde discuțiile dintre clienți și vânzătorul-farmacist sunt publice. Așa cum am afirmat anterior, unele e-farmacii oferă și consultanță prin intermediul unui medic sau farmacist licențiat, disponibil 24 de ore pe zi, pentru a răspunde la întrebări, prin telefon, e-mail sau mesagerie instant, eficientizând comunicarea cu clienții.

E-farmaciile pot oferi diverse beneficii clienților, avantaje ce nu pot fi disponibile în cadrul farmaciilor tradiționale, precum transmiterea de alerte prin e-mail atunci când pacientul are nevoie de o nouă prescripție sau medicamente[21].

În același timp, farmaciile online prezintă un interes crescut pentru țările cu piețe de desfacere mici sau în care medicamentele pentru boli rare nu se găsesc.

Consumatorii se îndreaptă spre farmaciile online bazându-se pe faptul că astfel de achiziții sunt mai economice, atât din punct de vedere al prețurilor practicate, cât și al timpului, nefiind necesară prezentarea unei rețete sau așteptatul la coadă. Nu în ultimul rând, achiziționarea online a produselor farmaceutice se presupune a fi confidențială, evitându-se astfel situațiile inconfortabile determinate de dezvăluirea unor informații personale

[20] Pentru similitudine a se vedea și Q.Lombardo, *Vendita online di medicinali, la direttiva UE*, 4 martie 2012, articol [Online] pe website-ul IusFarma.it – Osservatoriu di Diritto Farmaceutico, la adresa: http://www.iusfarma.it/vendita-online-di-medicinali-la-direttiva-ue-it, accesat 10.10.2017.

[21] A.K.Chaturvedi, U.K.Singh, A.Kumar, *op.cit.*, p. 148.

și sensibile privind starea de sănătate către un farmacist în prezența potențială a unor alte persoane aflate în farmacia tradițională.[22]

Industria farmaceutică a profitat de această oportunitate pentru a moderniza modalitățile de comercializare a medicamentelor și, de ce nu, ridicarea anumitor bariere precum obligativitatea prezentării unei prescripții medicale.[23]

Înființarea unei e-farmacii pirat necesită un capital inițial redus, însă produce profituri exorbitante.[24] Apariția farmaciilor online a determinat acțiuni de reglementare și monitorizare la nivel național,internațional și la nivelul organizațiilor profesionale. Autoritățile întâmpină dificultăți în ceea ce privește stoparea comerțului online cu medicamente contrafăcute sau falsificate datorită lipsei reglementărilor privind activitățile desfășurate pe Internet.[25] E-farmaciile prezintă un potențial pericol pentru sănătatea publică și necesită reglementări internaționale.[26]

Un alt potențial dezavantaj poate fi reprezentat de dificultatea sau chiar imposibilitatea consumatorilor de a deconta, prin casele de asigurări de sănătate, costul medicamentelor achiziționate online.

Printre dezavantajele utilizării farmaciilor online se numără și auto-diagnosticarea și auto-medicația, ambele fenomene fiind facilitate de informațiile disponibile pe Internet și posibilitatea clienților de a cumpara medicamente prescrise fără a fi consultat, la modul real, de un farmacist sau un medic. Astfel de fenomene apar din cauza dificultăților de a beneficia de o consultație promptă din partea unui medic și, nu în ultimul rând, de reticența individului de a discuta problema de sănătate cu orice persoană de specialitate.[27] Aceste aspecte prezintă o relevanță deosebită în contextul în

---

[22] A se vedea și K.S. Lee, S.M. Yee, S.T.R. Zaidi, R.P. Patel, Q. Yang, Y.M. Al-Worafi, L.C. Ming, *Combating Sale of Counterfeit and Falsified Medicines Online: A Losing Battle* în *Frontiers in Pharmacology Journal – Pharmaceutical Medicine and Outcomes Research*, May 2017, Volume 8, doi: 10.3389/fphar.2017.00268, p. 1.

[23] A.K. Chaturvedi, U.K.Singh, A. Kumar, *op.cit.*, pp. 146-147.

[24] European Alliance for Access to Safe Medicines, *Counterfeiting the Counterfeiter*, Essex, 2012, [Online] la: http://www.eaasm.eu/, accesat 10.10.2017.

[25] K.S.Lee, S.M. Yee, S.T.R. Zaidi, R.P. Patel, Q. Yang, Y.M. Al-Worafi, L.C. Ming, *op.cit.*, p. 1.

[26] A.K. Chaturvedi, U.K.Singh, A.Kumar, *op.cit.*, pp. 146-147.

[27] B.S.Bloom, R.C.Iannacone, *Internet availability of prescription pharmaceuticals to the public* în Annals of Internal Medicine, Decembrie 1999, doi: 10.7326/0003-4819-131-11-

care există e-farmacii ce eliberează medicamente de tip Rx, fără o prescripție medicală valabilă. Într-o asemenea circumstanță, în care un consumator beneficiază de o consultație online prin telemedicină sau achiziționează online medicamente Rx, procesul prin care se urmărește ameliorarea stării de sănătate a individului devine automat susceptibil unor erori, cu potențiale repercusiuni pentru acesta din urmă.[28]

IV. Problematica comercializării medicamentelor în mediul online

Farmaciile online ce pot fi accesate de orice consumator interesat reprezintă o mică parte din comerțul desfășurat pe Internet cu produse farmaceutice. Aceste farmacii se găsesc pe Internetul cunoscut, accesibil direct oricărui utilizator. Însă Internetul este mult mai vast decât "suprafața cunoscută" sau indexată, cuprinzând și zone necunoscute precum rețeaua web adâncă (*deep web* – ce nu este indexată) și rețeaua web neagră (*dark web*). Rețeaua *dark web* poate fi accesată numai de persoane ce dețin uneltele și cunoștințele necesare. Internetul ascuns este locul unde se desfășoară piața neagră de armament, acte de identitate, droguri și produse farmaceutice.[29]

Comerțul online ilegal cu produse farmaceutice "respectă" principii ale industriei farmaceutice, urmărind o oarecare trasabilitate[30] a medicamentelor. Astfel, lanțul ilicit pornește de la promovarea medicamentelor, prin mesaje de tip Spam[31], ce conduc potențialul cumpărător către e-farmaciile pirat și se încheie prin achiziția

199912070-00005, [Online] la: http://europepmc.org/abstract/med/10610627, accesat 10.10.2017.

[28] A.K.Chaturvedi, U.K.Singh, A.Kumar, *op.cit.*, p. 149.

[29] Pentru detalii privind *deep-web*, *dark-web* și comercializarea produselor farmaceutice pe aceste rețele a se vedea: Interpol, *Pharmaceutical Crime on the Darknet – A study of illicit online marketplaces*, Lyon, 24 februarie 2015, material disponibil [Online] la: http://www.gwern.net/docs/sr/2015-interpol-pharmaceuticals.pdf sau http://www.interpol.int, accesat 10.10.2017.

[30] Trasabilitatea, principiu ce guvernează industria farmaceutică, reprezintă capacitatea de reconstituire a drumului parcurs de produsul farmaceutic de la primul proces de fabricație a materiilor prime farmaceutice și până la beneficiarul final al medicamentului, pacientul, pe baza înregistrărilor.

[31] Spam-ul reprezintă e-mail-ul nesolicitat, trimis unui număr mare de destinatari, având conținut publicitar.

medicamentelor contrafăcute, eliberate fără prescripție medicală sau neautorizate de o autoritate statală competentă.

Internetul facilitează deplasarea individului, în mod virtual, în străinătate. Astfel, acesta fiind, din punct de vedere juridic, în măsură să achiziționeze medicamente într-un anumit stat, el poate realiza aceleași operațiuni în mediul online. În situația dată, achiziția încheiată între e-farmacia și consumatorul situați în două state diferite este considerată legală numai dacă comercializarea medicamentelor pe Internet este permisă în țara vânzătorului.[32]

Chiar și în situația favorabilă în care o farmacie online deține toate autorizațiile de funcționare și eliberează medicamente conform legislației aplicabile în vigoare, identitatea cumpărătorului este necunoscută sau neverificabilă, generând riscul ca produsele comandate să fie eliberate minorilor.

Biroul Federal de Investigații aparținând Departamentului de Justiție al Statelor Unite avertizează că "*sectorul sănătății e vulnerabil la criminalitate informatică*".[33] Datele privind sănătatea unui individ sunt mai valoroase pentru hackeri pe piața neagră decât detaliile unui card bancar, pentru că acestea conțin de regulă informații ce permit accesarea conturilor bancare sau obținerea unor rețete medicale de o valoare însemnată.

O altă problemă generată de vânzarea online a medicamentelor este cea privind importul acestora, în urma achiziției dintr-o e-farmacie străină. Asemenea achiziții, realizate având ca prim motiv costul redus al medicamentelor, ridică semne de întrebare în ceea ce privește respectarea prețurilor stabilite de autoritățile naționale pentru medicamente de tip Rx[34], a

[32] Platforma E-learning a *Proiectului Oper@tion Hippocr@tes – Fight against online fake medicine*, [Online] la: http://www.hippocrates-project.eu/ro, accesat 10.10.2017.

[33] J. Finkle, *Exclusive: FBI warns healthcare sector vulnerable to cyber attacks* în Reuters Technology News, 23 aprilie 2014, [Online] la: https://www.reuters.com/article/us-cybersecurity-healthcare-fbi-exclusiv/exclusive-fbi-warns-healthcare-sector-vulnerable-to-cyber-attacks-idUSBREA3M1Q920140423, accesat 10.10.2017.

[34] De exemplu, în România prețurile medicamentelor tip Rx sunt supuse aprobării Ministerului Sănătății, în timp ce prețurile medicamentele de tip OTC se stabilesc și se modifică în mod liber. Pentru detalii a se vedea: Normele privind modul de calcul și procedura de aprobare a prețurilor maximale ale medicamentelor de uz uman din 28.03.2017, publicate în M.Of. nr. 215, 29.03.2017.

drepturilor de proprietate intelectuală, precumși a reglementărilor privind importul paralel[35] sau politicile de marketing ale produselor farmaceutice.

Importul de medicamente, prin intermediul Internetului, este permisîn cazul în care achiziția se face de către persoane fizice, în cantități corespunzătoare uzului personal, și fără a crea suspiciunea valorificării ulterioare a produselor farmaceutice importate, prin distribuirea către public.[36]

Dacă analizăm confidențialitatea, avantaj menționat în favoarea utilizării e-farmaciilor, vom observa potențiale riscuri asupra protecției datelor furnizate online. Deși nu există nicio garanție a confidențialității într-o farmacie tradițională, informațiile transmise și stocate de farmaciile online sunt vulnerabile atacurilor informatice.[37]

Mai mult decât atât, unele e-farmacii și farmacii tradiționale furnizează, contracost, informații despre clienți unor terțe părți care desfășoară campanii de marketing pentru producătorii de medicamente, acțiuni discutabile din punct de vedere etic și legal. Această divulgare necorespunzătoare sau accidentală a informațiilor medicale poate conduce la un spectru larg de consecințe, precum discriminarea în societate sau la locul de muncă, creșterea primelor de asigurare de sănătate sau de viață ori chiar refuzul asigurării.[38]

V. Modalități de stopare a comerțului online ilicit cu produse farmaceutice

[35] Importul paralel reprezintă "*operația prin care un medicament pentru care a fost eliberată o autorizație de punere pe piață de către Agenția Națională a Medicamentului (ANM) este introdus în România prin alte canale de distribuție decât cele agreate de deținătorul autorizației de punere pe piață a medicamentului respectiv; se acceptă diferențe minore între medicamentul importat paralel și cel care a fost autorizat de punere pe piață în România, cu condiția să nu existe nicio diferență în efectul terapeutic, în comparație cu medicamentul originar care este distribuit direct*."- conform art. 1 lit. a) din Procedura de eliberare a autorizațiilor de import paralel pentru medicamente de uz uman din 2 decembrie 2008, publicată în M.Of. nr. 867, 22.12.2008.

[36] Platforma E-learning a *Proiectului Oper@tion Hippocr@tes – Fight against online fake medicine*, [Online] la: *http://www.hippocrates-project.eu/ro*, accesat 10.10.2017.

[37] A.K. Chaturvedi, U.K. Singh, A. Kumar, *op.cit.*, p. 150. Pentru similitudine a se vedea și: C.Randjak, *Comercializarea online a medicamentelor*,octombrie 2014,material disponibil online la adresa: http://pharma-business.ro/comercializarea-online-a-medicamentelor, accesat 10.10.2017.

[38] A.K.Chaturvedi, U.K.Singh, A.Kumar, *op.cit.*, p. 150.

Comerțul desfășurat de e-farmaciile pirat poate fi oprit sau, cel puțin, redus doar cu ajutorul unei creșteri a gradului de conștientizare în rândul populației, prin campanii de educare și informare a publicului cu privire la riscurile la care sunt supuși achiziționând medicamente contrafăcute sau falsificate.[39] Eficiența anchetelor instituțiilor abilitate trebuie susținută de o legislație clară și cât mai puțin interpretabilă, care să vizeze atât comerțul ilegal, online sau offline, cu medicamente.[40]

Măsuri precum îmbunătățirea reglementărilor privind e-farmaciile, monitorizarea și controlul acestor operațiuni comerciale,câtși o bună informare a pacienților/consumatorilor poate contracara comerțul ilegal cu produse farmaceutice.[41]

V.1. Logo-ul comun european pentru farmaciile online

Dacă realizăm o analiză a două cyber-farmacii diferite, una legal autorizată și una pirat, nu vom identifica elemente distinctive, de aici și riscul crescut de a achiziționa un produs farmaceutic falsificat sau contrafăcut.[42] Pentru a reduce riscul de confuzie a consumatorului, Comisia Europeană a introdus Directiva nr. 2011/62/UE de modificare a Directivei 2001/83/CE[43] de instituire a unui cod comunitar cu privire la medicamentele de uz uman în ceea ce privește prevenirea pătrunderii medicamentelor falsificate în lanțul legal de aprovizionare. Noutatea introdusă de directivă constă în obligativitatea e-farmaciilor de a incorpora pe propriile website-uri

[39] Media Kompas, *Comerțul online cu medicamente din surse necontrolate - Raport de monitorizare retroactivă*, București, 2017, p. 52,

[Online] la: https://www.mediakompass.ro/wp-content/uploads/2017/06/Raport_MK.pdf, accesat 10.10.2017.

[40] Pentru similitudine a se vedea și U.S. Food & Drug Administration Website, *The Possible Dangers of Buying Medicines over the Internet*,

[Online] la:https://www.fda.gov/ForConsumers/ConsumerUpdates/ucm048396.htm, accesat 10.10.2017.

[41] Media Kompas, *op.cit.*, p. 53.

[42] A se vedea și U.S. Food & Drug Administration Website, *The Possible Dangers of Buying Medicines over the Internet*, [Online] la:

https://www.fda.gov/ForConsumers/Consumer Updates/ucm048396.htm, accesat 10.10.2017.

[43] Directiva 2001/83/CE a Parlamentului European și a Consiliului din 6noiembrie 2001 de instituire a unui cod comunitar cu privire la medicamentele de uz uman, publicată în JO L 311, 28.11.2001, transpusă în legislația națională prin Legea nr. 95 din 14 aprilie 2006 privind reforma în domeniul sănătății,publicată în M.Of. nr. 372, 28.04.2006.

logo-ul comun european[44]. Logo-ul va permite clienților să identifice comercianții online autorizați și să îi diferențieze de cei neautorizați. Farmaciile online autorizate trebuie să furnizeze un hyperlink pe pagina lor de Internet către site-ul web al autorității naționale de reglementare farmaceutică, pentru a se asigura că potențialii clienți pot verifica încrucișat autenticitatea autorizației comerciantului[45].

V.2. Codul unic pentru medicamente - Serializarea produselor farmaceutice

O altă măsură de combatere a produselor farmaceutice contrafăcute constă în introducerea unui cod unic pe ambalajul medicamentelor. Odată cu implementarea acestei măsuri, se diminuează riscul ca medicamentele contrafăcute să ajungă pe piață și, totodată, trasabilitatea produselor farmaceutice va fi mai ușor de monitorizat și controlat.

Regulamentul delegat (UE) 2016/161[46] al Comisiei, de completare a Directivei 2001/83/CE privind medicamentele falsificate,"*prevede măsuri de prevenire a pătrunderii medicamentelor falsificate în lanțul legal de aprovizionare solicitând introducerea de elemente de siguranță care constau într-un identificator unic și un dispozitiv de protecție împotriva modificărilor ilicite pe ambalajul anumitor medicamente de uz uman pentru a permite identificarea și autentificarea acestora."* Regulamentul devine aplicabil de la 9 februarie 2019, dată până la care titularii autorizațiilor de punere pe

[44] Pentru detalii privind logo-ul comun destinat identificării e-farmaciilor a se vedea Regulamentul de punere în aplicare (UE) nr. 699/2014 al Comisiei din 24 iunie 2014 privind designul pentru logo-ul comun destinat identificării persoanelor care oferă medicamente spre vânzare la distanță către populație și cerințele tehnice, electronice și criptografice pentru verificarea autenticității acestuia, publicat în JO L 184, 25.06.2014.

[45] Pentru similitudine a se vedea și A.Boiciuc, *Vânzarea medicamentelor pe internet, ilegală în România, nu și în UE. Cum afli dacă o farmacie online din Europa este autorizată?*, iunie 2015, [Online] pe website-ul AvocatNet.ro la: https://www.avocatnet.ro/articol_41015/Vanzarea-medicamentelor-pe-internet-ilegala-in-Romania-nu-si-in-UE-Cum-afli-daca-o-farmacie-online-din-Europa-este-autorizata.html, accesat 10.10.2017

[46] Regulamentul delegat (UE) 2016/161 al Comisiei din 2 octombrie 2015 de completare a Directivei 2001/83/CE a Parlamentului European și a Consiliului prin stabilirea de norme detaliate pentru elementele de siguranță care apar pe ambalajul medicamentelor de uz uman, publicat în JO L 32, 9.02.2016, [Online] la: http://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32016R0161, accesat 10.10.2017.

piață sunt obligați să se conformeze noilor condiții de comercializare a medicamentelor[47].

V.3. Combaterea comerțului online ilicit cu medicamente de către autorități

Datorită rețelelor extinse de intermediari și furnizori din întreaga lume, autoritățile se confruntă cu dificultăți în monitorizarea și controlul vânzărilor de medicamente contrafăcute prin intermediul farmaciilor online ilegale. Astfel de operațiuni ilegale funcționează prin utilizarea registratorilor de domenii online, a sistemelor de plăți electronice și a serviciilor de curierat internațional și local. Măsurile luate de autoritățile naționale în vederea combaterii acestui fenomen nu au reușit să anihileze e-farmaciile pirat, ci doar să le întrerupă temporar funcționarea, ele redevenind complet operaționale după câteva zile.[48]

Având în vedere necesitatea unei operațiuni integrate pentru diminuarea drastică a comerțului ilicit cu produse farmaceutice, INTERPOL împreună cu alte agenții au lansat PANGEA. Operațiunea Pangea este o săptămână internațională de acțiune care abordează vânzarea online a medicamentelor contrafăcute și subliniază pericolele achiziționării unor asemenea produse. Coordonată de INTERPOL, operațiunea anuală reunește autoritățile vamale, autoritățile de reglementare în domeniul sănătății, poliția națională și sectorul privat din țări din întreaga lume. Dacă la momentul lansării operațiunii în anul 2008 au luat parte 10 țări, în prezent Pangea X (2017) a reunit peste 100 de state participante, printre care și România[49].

Activitățile vizează cele trei componente principale utilizate de site-urile web ilegale pentru a-și desfășura activitatea - furnizorul de servicii Internet, sistemele de plată și serviciul de livrare. În urma desfășurării

[47] Pentru similitudine și detalii privind serializarea medicamentelor a se vedea: N.Fotin, A.Crupariu, *Implementarea Directivei 2011/62/UE a medicamentelor falsificate – un proces în desfășurare în România*, în Revista Politici de Sănătate, iulie 2017, [Online] la: http://www.politicidesanatate.ro/implementarea-directivei-201162ue-medicamentelor-falsificate-un-proces-desfasurare-romania/, accesat 10.10.2017

[48] K.S. Lee, S.M. Yee, S.T.R. Zaidi, R.P. Patel, Q. Yang, Y.M. Al-Worafi, L.C. Ming, *op.cit.*, p. 2.

[49] Pentru detalii privind Operațiunea Pangea a se consulta website-ul agenției INTERPOL, secțiunea Pharmaceutical Crime, subsecțiunea Operations, [Online] la:https://www.interpol.int/Crime-areas/Pharmaceutical-crime/Operations/Operation-Pangea, accesat 10.10.2017.

operațiunii Pangea X (2017) au fost confiscate medicamente falsificate și contrafăcute în valoare de peste 51 milioane de dolari, au fost arestate aproximativ 400 de persoane și au fost închise 3.584 website-uri pirat.[50]

Concluzii

Achiziționarea de produse farmaceutice prin intermediul Internetului este un fenomen de actualitate, dinamic și în expansiune. Existența e-farmaciilor pirat ce distribuie o gamă largă de medicamente falsificate sau contrafăcute este o problemă, adesea subevaluată, care poate contribui la creșterea morbidității, mortalității, rezistenței la antibiotice și pierderea încrederii în sistemele de sănătate.

Legislația din domeniul supus prezentului studiu nu ar trebui să se limiteze la interzicerea farmaciilor online ilegale, ci ar trebui să permită dezvoltarea comerțului electronic și a industriei farmaceutice, prin consolidarea conceptului de "*farmacie online*" și reglementarea clară, la nivel internațional, a operațiunilor desfășurate de o asemenea entitate.

Comercializarea online a medicamentelor prezintă avantaje, dezavantaje dar și pericole. Or, în situația dată, sănătatea publică este cea asupra căreia planează pericolul iar singura modalitate de diminuare și prevenire constă într-o amplă și complexă reglementare a comerțului cu produse farmaceutice prin mijloace informaționale. O asemenea reglementare trebuie realizată la nivel național, regional și internațional, asigurând siguranța beneficiarului final al medicamentelor, bolnavul. Nu în ultimul rând, un asemenea demers legislativ ar trebui să creeze premisele înființării unui organism internațional cu rol de monitorizare și control a acestor activități.

Internetul poate extinde accesul pacienților la servicii de sănătate, însă cu costuri tot mai mari în ceea ce privește garanția calității și siguranței medicamentelor achiziționate online. Calitatea unei consultații medicale online este discutabilă și există posibilitatea unor abuzuri grave. Clienții pot furniza cu ușurință informații incorecte sau false pentru a obține medicamente. În plus, e-farmaciile se pot afla într-un conflict de interese deoarece acestea profită din vânzarea medicamentelor ce rezultă în urma

[50] INTERPOL Website - News, *Millions of medicines seized in largest INTERPOL operation against illicit online pharmacies*, [Online] la: https://www.interpol.int/News-and-media/News/2017/N2017-119, accesat 10.10.2017.

prescripțiilor date prin telemedicină, dacă consultația online este oferită ca serviciu conex activității de comerț online cu produse farmaceutice.

Cu toate că Hipocrate nu a anticipat apariția comerțului online cu medicamente și nici provocările generate de acesta, jurământul[51] formulat în urmă cu peste 2300 de ani poate reglementa aspecte actuale privind eliberarea necontrolată de produse farmaceutice către consumatori, calitatea și siguranța medicamentelor,precumși confidențialitatea datelor medicale.

[51] Jurământul lui Hipocrate: *"Jur pe Apollo medicul, pe Esculap, pe Higea și Panacea și pe toți zeii și zeițele, pe care îi iau ca martori, că voi îndeplini acest jurământ și poruncile lui, pe cât mă ajută forțele și rațiunea (...) Atât cât mă ajută forțele și rațiunea, prescripțiunile mele să fie făcute numai spre folosul și buna stare a bolnavilor, să-i feresc de orice daună sau violență. Nu voi prescrie niciodată o substanță cu efecte mortale, chiar dacă mi se cere, și nici nu voi da vreun sfat în această privință. (...)Sacră și curată îmi voi păstra arta și îmi voi conduce viața. În orice casă voi intra, o voi face numai spre folosul și bunăstarea bolnavilor (...) Orice voi vedea sau voi auzi în timpul unui tratament voi păstra în secret, pentru că aici tăcerea este o datorie (...)."*

ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

CONTRACTUL CLOUD COMPUTING

CLOUD COMPUTING CONTRACT

IONELA-DIANA PĂTRAȘC-BĂLAN[1]

Rezumat: Importanța domeniului cloud este reflectată de politicile și direcțiile de acțiune adoptate la nivelul UE ca element al punerii în aplicare a Strategiei pentru Piața Digitală Unică și a pachetului privind digitalizarea industriei europene. Analiza contractelor cloud computing ce reglementează în prezent relațiile în mediul cloud subliniază necesitatea standardizării clauzelor contractuale pornindu-se de la realitatea existentă conform căreia avantajele certe ale cloud computingului sunt contrabalansate de riscurile asociate acestuia. Respectarea drepturilor fundamentale, confidențialitatea, protecția datelor, drepturile de proprietate intelectuală și informațiile sensibile reprezintă provocări ce vor trebui să își găsească reflectarea în demersurile comunitare cu scopul de a crea o infrastructură digitală sigură și fiabilă și care să asigure un nivel de securitate informatică ridicat.
Cuvinte cheie: Contractul cloud computing, clauze contractuale, standardizare, protecția datelor, drepturile de proprietate intelectuală, Piața Digitală Unică

Abstract: The importance of the cloud is reflected by the policies and the directions of action adopted at EU level as part of the implementation of the Strategy for the Digital Single Market and the package on the digitisation of european industry. The cloud computing analysis currently governing cloud computing emphasizes the need for standardisation the contractual clauses starting from the existing reality that the clear advantages of cloud computing are counterbalanced by the risks associated with it. Respect for fundamental rights, confidentiality, data protection, intellectual property rights and sensitive information are challenges that will need to be reflected in Community approaches in order to create a secure and reliable digital infrastructure and to ensure a high security level.
Key-words: Cloud computing contract, contract terms, data protection, intellectual property rights, Digital Single Market

[1] Doctorand, Universitatea Alexandru Ioan Cuza din Iași, Facultatea de Drept, email:dianapat27@yahoo.com

Introducere

În Comunicarea Comisiei către Parlamentul European intitulată *Valorificarea cloud computingului în Europa*[2] s-a arătat că dezvoltarea acestor servicii poate însemna o creștere cu 45 miliarde euro a cheltuielilor directe în favoarea cloud computingului în UE în 2020 și pot produce un efect cumulativ global de 957 de miliarde euro asupra PIB și 3,8 milioane de locuri de muncă pînă în 2020.

Avantajele certe ale cloud computingului sunt contrabalansate de riscurile asociate acestuia. Sunt vizate în primul rând lipsa controlului asupra datelor și informațiile insuficiente cu privire la operațiunea de prelucrare în sine.

Limitele contractului cloud computing reprezentate de împrejurarea că de cele mai multe ori contractul este un contract standard, de tipul take-it or leave-it, fără posibilitatea negocierii clauzelor sale, pot constitui o barieră importantă în dezvoltarea acestui tip de serviciu.

Deși negocierea contractului cloud computing nu este uzuală, intervenind în special în cazul clienților precum întreprinderile mari cu putere economică considerabilă, instituții financiare sau agenții guvernamentale, aceasta poate viza chestiuni precum nivelul serviciilor, protecția și securitatea datelor, modificarea contractului, excluderea/limitarea răspunderii furnizorului.

1.Noțiune și caracteristici

1.1. Definiție

Noțiunea cloud computing nu cunoaște o singură definiție. Încercări de a contura sfera caracteristicilor acestui concept se regăsesc într-o serie de documente internaționale precum și în doctrina de specialitate.

Cea mai citată dintre acestea este cea oferită de către Institutul de Standarde și Tehnologie (NIST)[3] din SUA ce prezintă cloud computing ca fiind “un model care permite la cerere, accesul comod prin internet la un ansamblu de resurse informatice (de exemplu rețele, servere, echipamente de

[2] *Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul economic și social și Comitetul Regiunilor Valorificarea cloud computingului în Europa,* [Online] la http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:ro:PDF., accesat 2.05.2017.

[3] *The NIST Definition of Cloud Computing*, [Online] la http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf., accesat 2.05.2017.

stocare, aplicaţii şi servicii) ce pot fi puse la dispoziţia utilizatorului în mod rapid şi livrate cu efort sau cu interacţiune minime din partea furnizorului de servicii."

Conform unei definiții simplificate cuprinse în documentul *Valorificarea cloud computingului în Europa,* termenul „cloud computing" se referă la stocarea, procesarea și utilizarea de date pe computere aflate la distanță și accesate prin intermediul internetului. Acest lucru înseamnă că utilizatorii pot dispune la cerere de o putere de calcul aproape nelimitată, că nu trebuie să facă investiții de capital majore pentru a-și satisface exigențele și că își pot accesa datele din orice loc, cu ajutorul unei conexiuni la internet.

Totodată, se poate reține că, în fapt, cloud computing constă într-un set de tehnologii și modele de servicii care se axează pe utilizarea și furnizarea de aplicații informatice, capacitate de prelucrare, stocare și spațiu pentru memorie, toate bazate pe internet.[4]

În literatura de specialitate[5] s-a subliniat faptul că, în ceea ce privește contractul de cloud computing acesta este o formă a contractului de externalizare (outsourcing) a stocării datelor întreprinderii. În aceeași definiție[6] s-a arătat că acest concept înseamnă distributed computing prin intermediul unui network, internetul și că acesta constă în abilitatea de a face să funcționeze un program sau o aplicație în același timp în mai multe computere conectate între ele.

Deși outsourcing-ul IT a devenit foarte obișnuit, cloud computing reprezintă o schimbare esențială în modul în care organizațiile și persoanele fizice își împart responsabilitatea asupra infrastructurii și serviciilor informatice.[7]

1.2. Caracteristici și avantaje

Conform documentului intitulat *Valorificarea cloud computingului în Europa,* cloud computingul prezintă o serie de trăsături definitorii:

[4] *Avizul nr.05/2012 privind clod computing* adoptat de Grupul de lucru pentru protecția datelor instituit în temeiul art.29 din Directiva 95/46/CE, [Online] la http://ec.europa.eu/justice/data-protection/index_ro.htm., accesat 2.05.2017.

[5] C.T.Ungureanu, *Dreptul comerțului internațional, Contracte de comerț internațional,* Editura Hamangiu, București, 2014, p. 86.

[6] C.T.Ungureanu , *op. cit.*,p. 34.

[7] S. Bradshaw, Ch. Millard, I. Walden, *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computings Services* în Queen Mary University of London, School of Law, Legal Studies Research Paper No.63/2010, p. 15, [Online] la http://ssrn.com/abstract=1662374, accesat 3.05.2017.

hardware-ul (computere, dispozitive de stocare) este deținut de furnizorul de servicii de cloud computing, nu de utilizatorul care interacționează cu acesta prin internet, utilizarea hardware-ului este optimizată dinamic printr-o rețea de computere, furnizorii de servicii de cloud deplasează adesea sarcinile de lucru ale propriilor utilizatori pentru a optimiza utilizarea hardware-ului disponibil, hardware-ul la distanță stochează și procesează datele și le pune la dispoziție prin intermediul aplicațiilor, organizațiile și persoanele fizice își pot accesa conținutul și își pot utiliza software-ul atunci când și unde au nevoie (pe computere desktop, laptopuri, tablete și smartphone-uri).

În principiu, utilizatorii plătesc în funcție de utilizare, evitând costurile inițiale și fixe ridicate pe care le presupun configurarea și exploatarea unor echipamente informatice sofisticate. În același timp, utilizatorii pot modifica foarte ușor volumul de hardware utilizat prin adăugarea de noi capacități de stocare online, cu câteva clicuri de mouse. Consumatorii pot utiliza serviciile de cloud pentru a stoca informații (fotografii sau e-mailuri) și pot utiliza programe software (de exemplu, rețele sociale, conținut video și muzică în streaming și jocuri).

Organizațiile, inclusiv administrațiile publice, pot utiliza serviciile de cloud pentru a înlocui progresiv centrele de date operate intern și departamentele IT. Întreprinderile pot folosi servicii de cloud pentru a testa și a extinde rapid oferta adresată clienților lor, deoarece pot face acest lucru fără a investi în infrastructuri fizice sau a construi astfel de infrastructuri.

1.3. Riscurile în ceea ce privește protecția datelor asociate cloud computing au fost subliniate în cuprinsul Avizul nr.05/2012 privind cloud computing adoptat de Grupul de lucru pentru protecția datelor instituit în temeiul art.29 din Directiva 95/46/CE a Parlamentului European și a Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date[8].

Majoritatea acestor riscuri a fost încadrată în două mari categorii: lipsa controlului asupra datelor și informații insuficiente cu privire la operațiunea de prelucrare în sine (absența transparenței).

Lipsa controlului

[8] *Avizul nr.05/2012 privind cloud computing* ,[Online] la http://ec.europa.eu/justice/data-protection/index_ro.htm., accesat 3.05.2017.

Prin încredințarea datelor cu caracter personal sistemelor gestionate de un furnizor de servicii de cloud computing, este posibil ca clienții acestuia să nu mai poată deține controlul exclusiv asupra datelor și să nu mai poată implementa măsurile tehnice și organizaționale necesare asigurării disponibilității, integrității, confidențialității, transparenței, izolării, posibilității de intervenție și portabilității datelor.

Lipsa controlului se poate manifesta prin: lipsa disponibilității cauzată de lipsa interoperabilității, lipsa integrității cauzată de partajarea resurselor, lipsa confidențialității privind cererile de aplicare a legii adresate direct unui furnizor de servicii de cloud computing, lipsa posibilității de intervenție cauzată de complexitatea și dinamica lanțului de externalizare, lipsa posibilității de intervenție, lipsa izolării.

Lipsa informațiilor privind prelucrarea (transparență)

Informațiile insuficiente cu privire la operațiunile de prelucrare ale unui furnizor de cloud computing prezintă un risc atât pentru operatori, cât și pentru persoanele vizate deoarece este posibil ca aceștia să nu fie conștienți de potențialele amenințări și riscuri și, prin urmare, să nu poată adopta măsurile pe care le consideră adecvate. O serie de potențiale amenințări ar putea rezulta din faptul că operatorul nu știe că lanțul de prelucrare are loc prin implicarea mai multor persoane împuternicite și subcontractanți.

Prelucrate datelor cu caracter personal în diferite locații geografice din cadrul Spațiul Economic European are un impact direct asupra legislației aplicabile în cazul unor litigii privind protecția datelor care ar putea apărea între utilizator și furnizor.

Când datele cu caracter personal sunt transferate către țări terțe din afara SEE, țările terțe ar putea să nu ofere un nivel adecvat de protecție a datelor, iar transferurile ar putea să nu fie protejate prin măsuri adecvate (clauze contractuale standard sau reguli corporatiste obligatorii) fiind, astfel, ilegale.

1.4. Modele de implementare[9]

[9] *Avizul nr.05/2012 privind cloud computing* ,[Online] la http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_ro.pdf, p. 29, accesat 3.05.2017.

Există patru tipuri de modele de implementare, fiecare dintre acestea cu propriile caracteristici, utilizatorul fiind chemat să aleagă pe cel care corespunde cel mai bine nevoilor sale.

Mediu de cloud computing privat descrie o infrastructură de tehnologia informației dedicată unei organizații individuale. Acesta este localizat la sediul organizațiilor sau gestionarea acestuia este externalizată către o parte terță (de obicei, prin intermediul găzduirii serverului) care se află sub autoritatea strictă a operatorului. Un mediu de cloud computing privat poate fi comparat cu un centru de date convențional – diferența constând în faptul că măsurile tehnologice sunt implementate pentru a optimiza utilizarea resurselor disponibile și pentru a consolida resursele respective prin intermediul investițiilor mici realizate treptat, în timp.

Mediu de cloud computing public este o infrastructură deținută de un furnizor specializat în furnizarea de servicii care pune la dispoziție și partajează sistemele sale pentru/în rândul unor utilizatori, întreprinderi și/sau organisme administrative publice. Serviciile pot fi accesate prin intermediul internetului, fapt care implică transferarea operațiunilor de prelucrare a datelor către sistemele furnizorului de servicii. Prin urmare, furnizorul de servicii își asumă un rol cheie în ceea ce privește protecția efectivă a datelor încredințate sistemelor sale. Împreună cu datele, un utilizator este obligat să transfere o mare parte din controlul său asupra datelor respective.

Pe lângă mediile de cloud computing „publice” și „private”, există *mediile de cloud computing „intermediare” sau „hibride”* în care serviciile furnizate de infrastructurile private coexistă cu serviciile achiziționate din mediile publice.

Mediile de cloud computing comunitare sunt mediile în care infrastructura de tehnologia informației este partajată de mai multe organizații în beneficiul unei comunități specifice de utilizatori.

1.5. Modele de furnizare a serviciilor[10]

În funcție de cerințele utilizatorilor, există mai multe soluții de cloud computing disponibile pe piață. Acestea pot fi grupate în trei categorii mari

[10] *Avizul nr.05/2012 privind cloud computing* ,[Online] la http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_ro.pdf, p. 30, accesat 3.05.2017.

sau „modele de servicii”, care se aplică, de obicei, atât soluțiilor de cloud computing private, cât și celor publice:

- IaaS (Cloud Infrastructure as a Service): Un furnizor închiriază o infrastructură tehnologică (servere virtuale la distanță) pe care utilizatorul final se poate baza în conformitate cu mecanisme și măsuri astfel încât să facă simplă, eficientă precum și avantajoasă opțiunea de a înlocui sistemele corporatiste de tehnologia informației de la sediul întreprinderii și/sau să utilizeze infrastructura închiriată împreună cu sistemele corporatiste. Furnizorii sunt, de obicei, actori specializați care operează pe piață și se pot baza pe o infrastructură fizică complexă care cuprinde deseori mai multe zone geografice.

Exemple de IaaS: Amazon Web Service (AWS), Google Compute Engine (GCE), Rackspace Open Cloud, IBM SmartCloud Enterprise, HP Enterprise Converged Infrastructure.

În România, Institutul Național de Cercetare și Dezvoltare în Informatică București pune la dispoziție prin proiectul ICIPRO o platformă tip cloud pentru instituțiile publice din România.

- SaaS (Cloud Software as a Service): Un furnizor oferă, prin intermediul internetului, diferite servicii de aplicații pe care le pune la dispoziția utilizatorilor finali. Serviciile sunt deseori destinate să înlocuiască aplicațiile convenționale instalate de utilizatori în sistemele lor locale. Utilizatorii sunt în cele din urmă obligați să-și externalizeze datele către furnizorul individual. Acest lucru este valabil în cazul aplicațiilor de birou tipice bazate pe internet precum fișiere, instrumente de editare a textelor, registre și agende computerizate, calendare partajate etc.; cu toate acestea, serviciile în cauză includ, de asemenea, aplicații e-mail bazate pe medii de cloud computing.

Exemple de SaaS: Microsoft Office 365, Google Gmail, Google Docs, Zoho Office, Salesforce, Citrix GoToMeeting, Cisco WebEx.

- PaaS (Cloud Platform as a Service): Un furnizor oferă soluții pentru dezvoltarea și găzduirea avansată de aplicații. Serviciile se adresează, de regulă, actorilor care operează pe piață care le utilizează pentru a dezvolta și găzdui soluții bazate pe aplicații proprietare pentru a îndeplini cerințe stabilite la nivel intern și/sau pentru a furniza servicii către terți.

Serviciile furnizate de către un furnizor PaaS fac inutil recursul unui utilizator la componente hardware sau soluții informatice specifice și/sau adiționale la nivel intern.

Exemple de PaaS: Engine Yard, Google App Engine, Heroku, AppFog, Windowss Azure Cloud Services, Amazo Web Services AWS, Caspio.

2. Încheierea contractului

2.1. Părțile contractului

Contractul cloud computing este prin natura lui un contract internațional ce atrage aplicarea regulilor de drept internațional privat cu privire la legea aplicabilă contractului și cu privire la autoritatea competentă să soluționeze litigiile care se nasc în legătură cu acesta[11].

Părțile contractului cloud computing sunt furnizorul serviciului cloud și clientul serviciului care poate fi un consumator sau un profesionist și care utilizează serviciul furnizat. În unele contracte pot apărea intermediarii, subcontractanți ai serviciilor.

2.1.1. Clientul serviciului cloud computing

Clientul serviciilor de cloud computing determină scopul final al prelucrării și decide cu privire la externalizarea operațiunii de prelucrare și la delegarea parțială sau totală a activităților de prelucrare către o organizație externă.

Clientul serviciilor de cloud computing poate însărcina furnizorul să aleagă metodele și măsurile tehnice și organizaționale care urmează a fi utilizate în vederea atingerii scopurilor formulate de către operator.

2.1.2. Furnizorul de servicii cloud computing

Furnizorul de servicii cloud computing reprezintă entitatea care pune la dispoziție servicii de cloud computing sub cele trei forme cunoscute.

Atunci când furnizorul de servicii oferă mijloacele și platforma, acționând în numele clientului serviciilor, acesta este considerat persoană împuternicită de către operator.

2.1.3. Subcontractanții

Serviciile cloud computing pot presupune implicarea unui număr de părți contractate care acționează ca persoane împuternicite de către operator. Este o practică obișnuită ca persoanele împuternicite de operator să

[11] C.T. Ungureanu, *Contractul cloud computing în comerțul internațional*, în Revista Moldovenească de Drept Internațional și Relații Internaționale, vol.37, nr.3/2015, [Online] la http://www.usem.md/uploads/files/Activitate_%C8%98tiin%C8%9Bific%C4%83_USEM/rmdiri/RMDIRI,_2015,_Nr_3.pdf, pp. 25-36, accesat 3.05.2017.

contracteze subcontractanți adiționali care obțin ulterior acces la datele cu caracter personal.

2.2. Obiectul contractului

În cazul acestui tip de contract, obiectul este determinat având în vedere modelul de serviciu oferit clientului de cloud computing[12].

Obiectul contractului de furnizare de servicii de aplicații (SaaS) va fi diferit de obiectului contractului privitor la închirierea unei infrastructuri tehnologice (IaaS) sau a celui care oferă soluții pentru găzduirea avansată de aplicații (PaaS).

Descrierea și domeniul de aplicare al obiectului contractului sunt factori determinanți în definirea ulterioară a obligațiilor ce le incumbă părților, dar și pentru soluționarea eventualelor litigii ce s-ar putea naște în legătură cu contractul.

2.3. Categorii de contracte

Contractele cloud computing se clasifică în două categorii: contracte în care furnizorul oferă servicii de cloud gratuite și contracte în care serviciile oferite sunt contra cost.[13]

În literatura de specialitate[14] s-a subliniat faptul că această distincție nu este una clară. Există unele servicii "gratuite" care pot impune costuri nemonetare clientului, cum ar fi publicitatea contextuală sau impunerea termenilor de licență care permit furnizorului să utilizeze din nou datele clientului conform propriilor scopuri.

În aceeași măsură, există unele serviciile care pot oferi o perioadă de testare gratuită care dau detalii ulterioare de plată și care apoi se transformă într-un contract plătit.

Contractele cloud gratuite sunt întotdeauna contracte standard adresându-se consumatorilor și clienților cu o putere economică mică.

În situația în care clienții serviciilor cloud computing sunt companii mari termenii contractului pot fi negociați.

---

[12] C.A. Rohrmann, J. Falci, S.R. Cunha, *Some legal aspects of cloud computing contracts* în Journal of International Commercial Law and Technology Vol. 10, No.1 (2015), p. 41, [Online] la www.jiclt.com/index.php/jiclt/article/download/230/227, accesat 3.05.2017.

[13] C.T. Ungureanu, *op. cit.*, p. 88.

[14] S. Bradshaw, Ch. Millard, I. Walden, *op. cit.*, p. 15.

2.4. Standardizarea contractului cloud computing

Clauze contractuale și condiții sigure și echitabile în contractul cloud computing reprezintă acțiunea-cheie nr.2 a acțiunilor specifice a Comisiei Europene privind Valorificarea cloud computingului în Europa[15].

Necesitatea standardizării clauzelor contractuale în cloud computing a pornit de la realitatea existentă conform căreia flexibilitatea mai mare a cloud computingului în comparație cu externalizarea tradițională este contrabalansată de siguranța redusă a clientului, cauzată de contractele insuficient de specifice și de echilibrate cu furnizorii de cloud.

S-a constatat că din cauza complexității și a incertitudinii cadrului juridic aferent, furnizorii de servicii de cloud utilizează deseori contracte complexe sau acorduri privind nivelul serviciilor care au clauze extinse de declinare a răspunderii. Utilizarea contractelor standard de tipul „dacă îți convine bine, dacă nu, nu” (take-it-or-leave-it) îi permite furnizorului să facă economii, însă adesea utilizatorul, și în special utilizatorul final, găsește condițiile inacceptabile. Astfel de contracte pot impune de asemenea alegerea legislației aplicabile sau pot interzice recuperarea datelor. Chiar și întreprinderile mai mari nu au decât puțină putere de negociere și, deseori, contractele nu prevăd răspunderea pentru integritatea sau confidențialitatea datelor, ori pentru continuitatea serviciului.

Contractul cloud computing ar trebui să acopere aspecte precum conservarea datelor după încetarea contractului, divulgarea și integritatea datelor, amplasarea și transferul datelor, răspunderea directă și indirectă, dreptul de proprietate asupra datelor, modificarea serviciului de către furnizorii de cloud și subcontractarea.

La 18 iunie 2013, Comisia a înființat un grup de experți care să definească condiții de siguranță corecte și să identifice cele mai bune practici pentru contractele de tip cloud computing pentru consumatori și firme mici.

În cadrul celor șapte reuniuni de lucru ale Grupului de experți au fost elaborate Documente de lucru reprezentând analize și propuneri în materia vizată referitoare la informații precontractuale, comutarea-portabilitatea datelor la comutare, răspunderea pentru nerespectarea obligațiilor privind

[15] Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul economic și social și Comitetul Regiunilor *Valorificarea cloud computingului în Europa*, [Online] la http://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX%3A52012DC0529, accesat 4.05.2017.

protecția datelor, datele privind locația și de securitate, clauze abuzive în contractele cloud computing, disponibilitatea serviciului, subcontractarea, audit și raportare, transferurile de date, switching-transferul și ștergerea datelor după închiderea relației[16].

Comisia a lansat un studiu comparativ privind contractele de tip "cloud computing" pentru a completa activitatea grupului de experți[17].

Necesitatea accelerării activității de standardizare a contractelor cloud computing a fost subliniată recent și în cuprinsul Propunerii de Rezoluție a Parlamentului European referitoare la inițiativa europeană în domeniul cloud computingului din 16.02.2017[18] pornindu-se de la premisa că ameliorarea standardelor și a interoperabilității va permite comunicarea între diferitele sisteme de cloud computing și evitarea dependenței de un singur furnizor pentru produsele și serviciile cloud.

3.Clauze contractuale

Clauzele contractului standard cloud computing sunt concepute de regulă de către furnizorul de servicii fără a da posibilitatea clientului de negociere. Încheierea contractului are loc prin metoda click - wrap.[19]

Perfectarea contractului standard se realizează prin simpla apăsare a butonului de acceptare.

Contractul poate prezenta forma unui singur document sau a mai multor documente separate denumite *Terms and Conditions*.

Pe baza analizei a unui număr de 31 de servicii cloud oferite prin intermediul unor contracte standard au fost identificate mai multe categorii de servicii puse la dispoziția clientului de cloud [20]:

- *Plătit/gratuit*

---

[16] *Expert Group on Cloud Computing Contracts*, [Online] la http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm, accesat 7.05.2017.

[17] *Comparative study on cloud computing contracts*, [Online] la https://publications.europa.eu/en/publication-detail/-/publication/40148ba1-1784-4d1a-bb64-334ac3df22c7,accesat 7.05.2017.

[18] *Propunere de Rezoluție a Parlamentului European referitoare la inițiativa europeană în domeniul cloud computingului*, [Online] la http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0006+0+DOC+XML+V0//RO, accesat 6.05.2017.

[19] C.T. Ungureanu, *op. cit.*, p. 88.

[20] S. Bradshaw, Ch. Millard, I. Walden, *op. cit.*, p. 8.

Serviciile plătite sunt serviciile pentru care clientul de cloud plătește o taxă de abonament sau utilizare; există furnizori Cloud care oferă ambele versiuni, gratuită și plătită ale produselor care pot diferi în mică măsură.

- *Natura serviciilor*

După natura serviciilor oferite, contractele cloud computing vizează SaaS, PaaS sau IaaS. Din analiza asupra serviciilor chestionate a rezultat că majoritatea dintre acestea sunt din categoria SaaS sau IaaS, o mică parte a acestora vizând servicii PaaS (Google Apps fiind cel mai utilizat exemplu).

- *Tipul de client:*

Clienții contractului cloud pot fi: consumatorii, întreprinderile mici/ mijlocii (IMM) și organizațiile mari/ instituții din sectorul public/administrația publică.

Unele servicii cloud (Apple MobileMe) sunt comercializate în primul rând pentru consumatori mici, însă acest lucru nu exclude utilizarea acestora pentru afaceri.

Aceeași situație este valabilă și pentru serviciile cloud care există în primul rând pentru găzduirea de conținut generat de utilizatori, precum Facebook, care pot fi, de asemenea, folosite de organizații în scopuri de publicitate.

La celălalt capăt al pieței, servicii precum cele oferite de Salesforce se adresează în mare măsură organizațiilor mari, corporatiste sau publice.

Documentele diferite care conțin termenii ce reglementează relația dintre client și furnizorul de servicii fac referire la următoarele[21]:

- *Termeni și condiții (Terms of Service - ToS)*

În cuprinsului documentului se detaliază relația generală dintre client și furnizor. Conține de obicei termeni comerciali, mențiunea dacă serviciul oferit este plătit și include clauze precum alegerea legii și renunțarea la drepturi.

- *Acord privind nivelul de servicii (Service Level Agreement - SLA)*

Specifică nivelul serviciului pe care furnizorul își propune să îl livreze, punerea în executare a penalităților prevăzute pentru serviciile care nu au fost furnizate conform contractului, un anumit nivel de asistență acordat clientului, tipul de software sau hardware care va fi furnizat.

Acordul privind nivelul de servicii este asociat doar cu serviciile plătite.

[21] S. Bradshaw, Ch. Millard, I. Walden, *op. cit.*, p. 15.

- *Politica de utilizare acceptată (Acceptable Use Policy - AUP)*

Acest document detaliază utilizări ale serviciului oferit clientului cloud, stabilind o utilizare acceptabilă a acestora bazată pe aprecierea furnizorului.

- *Politica de confidențialitate (Privacy Policy)*

În acest tip de document se încorporează termenii care se referă în mod specific la protecția datelor.

Deși unii furnizori prezintă toate cele patru documente, se întâlnesc situații în care politica de utilizare acceptată (AUP) este încorporată în termenii și condițiile contractului (ToS), în timp ce multe servicii nu oferă un acord privind nivelul de servicii (SLA).

În situația în care documentele referitoare la diferitele categorii de clauze sunt prezentate separat, trimiterea la celelalte documente este făcută prin referință.

3.1. Clauze standard în contractul cloud computing

O analiză comparativă a contractelor standard cloud computing[22], a reliefat o serie clauze comune referitoare la:

3.1.1. Legea aplicabilă

Majoritatea contractelor includ clauze referitoare la alegerea unei anumite jurisdicții, de regulă cea în care furnizorul își are sediul principal de activitate.

În cazul furnizorilor cu operațiuni internaționale, contractul poate specifica că se aplică legea în funcție de locația clientului.

În cazul furnizorului de cloud Salesforce, au fost create zone geografice de aplicabilitate a legii stabilite inițial după localizarea clientului: pentru clienții SUA, Mexic, America centrală și de sud și Caraibe legea aplicabilă este legea federală din California. Pentru clienții din Europa, Orientul Mijlociu sau Africa, legea aplicabilă este legea engleză[23].

3.1.2 Competența privind soluționarea litigiilor

Clauza referitoare la alegerea instanței pentru soluționarea litigiilor dintre furnizor și clientul este asemănătoare celei privind alegerea legii.

În general, furnizorii de servicii aleg o jurisdicție compatibilă cu sistemul juridic specificat.

---

[22] S. Bradshaw, Ch. Millard, I. Walden, *op. cit*., p. 15.

[23] C.T. Ungureanu, *op. cit*., p. 90.

S-a constatat că în multe cazuri, mai ales acolo unde este aplicabilă legea unui anumit stat american furnizorul include o clauză care să precizeze că litigiul va fi soluționat de instanțele unui anumit oraș din acel stat (Symantec cere ca cererile să fie introduse în instanțele din Santa Clara).

Pe lângă alegerea unei jurisdicției, un număr de furnizori încearcă să impună termene de prescripție relativ scurte referitoare la acțiunile derivate din executarea contractelor: IBM și Rackspace solicită ca pretențiile să fie introduse în termen de 2 ani, Apple, un termen de un an și ADrive, un termen de 6 luni[24].

3.1.3. Arbitrajul

Un contract de servicii cloud computing poate oferi opțiunea de arbitraj comercial ca o alternativă de soluționare a litigiilor.

Potrivit reglementărilor în materia protecției consumatorilor, clauza compromisorie de arbitraj poate fi considerată abuzivă în ceea ce îi privește pe consumatori în lumina Directivei 93/13/CEE a Consiliului privind clauzele abuzive în contractele încheiate cu consumatorii.

Studiul privind comparația și analiza clauzelor contractului cloud computing realizat asupra a 31 astfel de contracte[25] a arătat împrejurarea că 7 din cele 31 de contracte includ o formă de clauză care încearcă să impună arbitraj: trei furnizori (ADrive, Nirvanix și Zoho) au impus această formă de soluționare a litigiilor cu clienții în toate cazurile, în timp ce 3Tera procedează astfel pentru creanțe evaluate peste 500 de dolari.

IBM, Iron Mountain și Microsoft (pentru LiveMesh) au prevăzut arbitrajul în relațiile contractuale cu clienților aparținând anumitor țări: IBM, pentru Smart BusinessCloud, mandatează arbitrajul pentru litigiile care apar în Republica Populară Chineză, Statele din Asia de Sud-Est și statele din Europa de Est sau din fosta Uniune Sovietică. O posibilă justificare ar putea reflecta lipsa familiarizării sau lipsa de încredere în eficiența sistemelor judiciare din aceste țări.

3.1.4. Utilizare acceptabilă (AUC)

Prin clauza cu privire la modul de utilizare a serviciilor de cloud, furnizorii impun reguli asupra modului în care clienții le pot folosi serviciul. Aceste clauze reflectă dorința prestatorilor de serviciu cloud de a se proteja de răspunderea care decurge din comportamentul ilegal al clienților lor.

[24] S. Bradshaw, Ch. Millard, I. Walden, *op. cit*., p. 18.

[25] S. Bradshaw, Ch. Millard, I. Walden, *op. cit*., p. 19.

Astfel de regulile sunt adesea prezentate într-un AUP separat.

Marea majoritate a termenilor de utilizare acceptabilă interzic un set consistent de activități. Furnizorii consideră că reprezintă utilizări ilegale ale serviciului lor: E-mail comercial nesolicitată ("spam"), frauda, jocurile de noroc, hacking în alte sisteme, găzduirea de conținuturi obscene, defăimătoare sau de promovare a discriminării sau incitare la ură.

Unii furnizori au excluderi care reflectă piața țintă: IronMountain, care oferă un serviciu adaptat în mod special la backup-ul de date de afaceri, interzice utilizarea cloud-ului pentru alte scopuri.

3.1.5. Modificarea unilaterală a contractului

Posibilitatea modificării unilaterale a contractului cloud computing este, de regulă inserată în contract, variind procedura de efectuare a acestei modificări.

Unii furnizori încorporează un termen care stipulează că pot modifica contractul prin postarea unei versiuni actualizate pe site-ul lor web și că utilizarea continuă a serviciului de către client este considerată consimțământ pentru astfel de modificări.

În cazul în care serviciile sunt furnizate în cadrul unui contract plătit, modificarea este însoțită de o clauză de încetare a contractului în ipoteza în care un client nu dorește să accepte noile condiții.

Apple își rezervă dreptul de a-și modifica contractul sub condiția informării clienților prin intermediul e-mail, în timp ce Google Apps Premier, Iron Mountain și Salesforce CRM o vor face în scris numai cu acordul ambelor părți.

3.1.6. Integritatea datelor (Data Integrity)

O preocupare constantă a clienților cloud computing este reprezentată de protejarea datelor introduse de furnizorii cloud împotriva pierderii integrității acestor date sau a încălcării securității datelor prin dezvăluiri neautorizate.

Majoritatea furnizorilor includ în mod expres o prevedere în conformitate cu care clientul este pe deplin responsabil pentru păstrarea confidențialității și integrității datelor, corelativ cu exonerarea acestora de răspundere.

Un număr de furnizori recomandă clienților criptarea datelor stocate în cloud-ul furnizorului (GoGrid, Microsoft) sau efectuarea de copii (backup).

3.1.7. Protecția datelor (Data Preservation)

După încheierea relațiilor contractuale, pentru clienți apare problema referitoare la existența posibilității de a avea acces la date pentru a fi utilizate în altă parte și a asigurării din partea furnizorului că datele vor fi efectiv șterse după această etapă.

În ceea ce privește chestiunea legată de modul în care furnizorii de servicii cloud declară că vor gestiona informațiile despre clienți după încetarea contractului, s-a constatat că există furnizori care afirmă că vor păstra datele despre clienți după încheierea contractului de servicii[26].

Amazon, ElasticHost și ZecterToate stipulează 30 de zile (sau o lună) ca perioadă de grație în care un fost client își mai poate accesa datele. Această perioadă de grație poate să nu fie aplicabilă în cazul în care contractul a fost reziliat pentru încălcarea relevantă a AUP.

Există furnizori care oferă o perioadă mai scurtă de grație: Nirvanix 15 zile pentru Decho 3.

Și accesul în timpul perioadei de grație poate fi supus unor taxe și altor condiții (de exemplu, AmazonAWS T & C).

O altă categorie de furnizori afirmă că datele despre clienți vor fi șterse imediat, chiar și în situația unui serviciu cu plată (de exemplu Apple pentru produsul său MobileMe).

O a treia categorie de furnizori stipulează în contract prevederea conform căreia nu își asumă obligația păstrării datelor după încheierea relației, dar nici nu se angajează să șteargă aceste date: Flexiant prevede că accesul la datele clienților va fi la discreția sa, Google, pentru GoogleDocs, afirmă că datele despre clienți pot fi șterse în orice moment. Microsoft neagă orice obligație de păstrare a datelor despre clienți după încetarea contractului (Net și Live Mesh) sau eliminarea datelor de către clienți la terminare (baza de date SQL Azure).

În cazul altor furnizori (Facebook), s-a constatat facilitatea de "a memora" conturile utilizatorilor care au murit, păstrând totuși conținutul acestora și permițând afișarea limitată a comentariilor.

O altă abordare o reprezintă poziția luată de IBM în ceea ce privește Smart Business Cloud, unde se declară în mod expres că furnizorul nu are nicio obligație de confidențialitate în ceea ce privește datele despre clienți și nu își asumă responsabilitatea pentru păstrarea acestora.

[26] S. Bradshaw, Ch. Millard, I. Walden, *op. cit.*, p. 23.

3.1.8. Divulgarea datelor (Data Disclosure)

În ceea ce privește circumstanțele în care furnizorii vor dezvălui informațiile despre clienți (inclusiv datele despre clienți stocate pe Cloud-ul furnizorului), acestea vizează în principal obligația rezultând dintr-o hotărâre judecătorească.

Unii furnizori instituie garanții procedurale. Salesforce prevede că clientul va primi o notificare prealabilă a unei divulgări solicitate, cu excepția cazului în care o astfel de notificare este interzisă.

Există furnizori care au fixat un prag inferior celui reprezentat de o hotărâre a instanței pentru a accepta cererile de divulgare a datelor, precum solicitările venite de la agențiile de aplicare a legii recunoscute sau în cazul în care există o nevoie clară și imediată de a divulga informații în interes public sau pentru de a proteja viața.

Facebook, de exemplu, va dezvălui autorităților informații despre contactul cu clienții în astfel de situații: "De asemenea, putem să divulgăm informații atunci când fiind de bună-credință, credem că acest lucru este necesar pentru a preveni frauda sau altă activitate ilegală, orice vătămare corporală iminentă."

3.1.9. Locația / transferul datelor (Data Location)

Una dintre cele mai frecvent ridicate preocupări legale cu privire la cloud computing este aceea privind împrejurarea că datele unui client pot fi stocate sau prelucrate în totalitate într-o locație necunoscută. Unii furnizori majori de cloud (Amazon) au oferit "zone regionale" în care clientul ar putea fi asigurat că îi vor fi păstrate datele. Pentru situația în care clientul cloud computing nu intră în sfera de protecție a legislației comunitare și naționale (de exemplu întreprinderile), se poate uza de doctrina "doctrine of unconscionability" sau "red hands rules" în conformitate cu care cu cât o clauză este mai nerezonabilă cu atât mai mult trebuie adusă la cunoștința clientului care aderă la un contract standard [27].

Pe lângă întrebarea unde sunt stocate datele despre clienți, o preocupare suplimentară este reprezentată de securitatea acestor date în tranzit, întrucât caracterul internațional al serviciilor Cloud presupune că datele despre clienți vor fi, de obicei, transferate între client și furnizor prin intermediul Internetului.

[27] C.T. Ungureanu, *op. cit.*, p. 93.

Cu excepția cazului în care furnizorul cloud a construit sau a închiriat propria rețea securizată și transferurile între centrele de date ale aceluiași prestator folosesc conexiunile la Internet.

Mai mulți furnizori (37Signals, UKFast) avertizează clientul că datele pot fi transferate necriptate prin rețelele nesigure.

În schimb, Dropbox precizează în mod specific, mai degrabă pe site-ul său decât în cuprinsul contractului că toate transferurile de date sunt criptate și identifică Amazon S3 ca serviciu de stocare a furnizorului[28]

3.1.10. Monitorizarea clientului de către furnizorul cloud

Deși clienții serviciilor cloud computing nu doresc monitorizarea activității lor în cadrul serviciului oferit de către furnizor, s-a constatat că o astfel de inițiativă există, chiar dacă unii dintre prestatorii serviciilor nu declară adoptarea unei politici în acest sens.

Analiza susținută a datelor a dezvăluit că o cantitate considerabilă de informații despre utilizarea serviciilor criptate este deținută de către furnizori și că acestea nu se refereau doar la date privind la frecvența și volumul de mișcare a datelor[29].

Din perspectiva politicii de monitorizare, există furnizorii care nu declară o existența unei astfel de practici (3Tera, Google, Nirvanix și Salesforce).

Există și categoria furnizorilor care afirmă că monitorizează utilizarea serviciului de către clienți, dar numai în ceea ce privește natura serviciului (consumul de lățime de bandă) în scopul asigurării unei bune calități a prestării de servicii (Microsoft pentru baza de date SQL Azure).

O a treia categorie de furnizori a arătat că pot monitoriza datele pe care clientul le încarcă în Cloud, în mod obișnuit în scopul aplicării AUP (Rackspace, GoGrid). În acest context nu s-a precizat dacă o astfel de monitorizare este proactivă sau ca răspuns la suspiciuni specifice referitoarea la activitatea desfășurată.

Unii furnizori (The Planet) au prevăzut în contract clauza conform căreia pot fi obligați din punct de vedere legal să monitorizeze activitățile clienților fără notificare.

3.1.11. Drepturi asupra serviciului / conținutului

[28] S. Bradshaw, Ch. Millard, I. Walden, *op. cit.* , p. 29.

[29] S. Bradshaw, Ch. Millard, I. Walden, *op. cit.*, p. 30.

Marea majoritate a contractelor standard cloud computing nu se referă în mod specific la termeni care descriu dacă contractul pentru cloud servicii dă naștere la drepturi de proprietate asupra conținutului sau a datelor încărcate în cloud. În cele câteva cazuri identificate (Decho, Flexiant, Joyent) acest termen se referă numai la dreptul de proprietate intelectuală a furnizorului, fără nicio mențiune în ceea ce privește clientul.

În cazul mai multor contracte a fost identificată o clauză conform căreia clientul acordă furnizorului permisiunea de a republica unele sau toate datele clientului în scopul furnizării serviciului. Acest lucru este valabil în special pentru consumatori serviciilor care încurajează găzduirea și stocarea conținutului clientului (Apple și Google)[30].

3.1.12. Garanția serviciilor oferite clienților

Există o diferență de abordare între modul în care furnizorii de cloud care supun contractul legii și jurisdicției statelor americane și cele care pretind că sunt înțelegerea părților este guvernată de legile unei țări europene[31].

În ceea ce privește prima categorie s-a observat o renunțare la orice garanție oferită clienților în ceea ce privește performanța serviciului oferit. Un exemplu în acest sens îl reprezintă GoGrid în ceea ce privește serviciul Cloud, care arată că nu garantează că serviciul va fi neîntrerupt, fără erori sau viruși sau alte componente dăunătoare, serviciul nu este furnizat cu garanții în ceea ce privește securitatea, fiabilitatea, protecția împotriva atacurilor, integritatea datelor.

Furnizori supuși legislației europene nu exclud acceptarea garanțiilor implicit legale (UKFast).

3.1.13. Răspunderea directă

Prin "răspundere directă" se înțelege răspunderea ce incumbă furnizorilor de servicii pentru daunele suferite de client în legătură cu pierderea sau compromiterea datelor găzduite de serviciul Cloud.

Furnizorii de servicii cloud din SUA încearcă să nege cât mai mult răspunderea pentru daune directe prin clauze cât mai generale (GoGrid), această excludere funcționând chiar și acolo unde clientul a contractat în mod special servicii de tipul celor pentru care garanția nu este exclusă.

[30] S. Bradshaw, Ch. Millard, I. Walden, *op. cit*., p. 31.

[31] *Ibidem.*

Furnizorii cu sediul în Europa tind să fie mai puțin vizibili în ceea ce privește excluderea răspunderii, din cauza faptului că majoritatea legislațiilor interzic acest lucru. În aceste cazuri, excluderile intervin în caz de forța majoră (Flexiant sau ElasticHosts), pană de curent, supratensiune, atacuri teroriste, boală sau pandemie, act, eșec sau omisiune a oricărei autorități guvernamentale[32].

3.1.14. Limitarea răspunderii

În ciuda negării garanțiilor și excluderilor de răspundere prevăzute în mod obișnuit, furnizorii încearcă să se impună termeni care să limiteze daunele de care furnizorul ar putea fi responsabil.

Majoritatea furnizorilor chestionați (19 din cele 31 contracte)[33] stabilesc drept despăgubiri o sumă maximă care este mai mare decât suma plătită reprezentând taxele de serviciu ale clientului pe o perioadă determinată, adesea cu o limită superioară.

GoGrid și Salesforce își limitează răspunderea la suma totală plătită de client pe durata contractului în ultimele 12 luni, Rackspace până la de 12 ori taxa lunară, UKFast și ElasticEste prevăd limitarea răspunderii la taxa datorată pe o lună.

Decho, care oferă atât servicii gratuite cât și plătite, își limitează răspunderea pentru cele din urmă la suma totală plătită de client și notează că în ceea ce privește serviciile gratuite acest lucru echivalează cu o negare totală a răspunderii.

ADrive, care oferă consumatorilor servicii de depozitare, are o răspundere limitată la de 100 USD, la fel ca și Dropbox și Facebook., iar IBM o limită de răspundere pentru clienții europeni de 500 000 de euro.

3.1.15. Compensația

Alături de negarea sau limitarea răspunderii proprii în contractele cloud computing, majoritatea furnizorilor includ clauze de despăgubire în conformitate cu care clientul trebuie să plătească compensații financiare furnizorului în cazul existenței oricărei reclamații împotriva prestatorului care decurge din utilizarea de către client a serviciului.

Din perspectiva consumatorilor sau a IMM-urilor, astfel de termeni sunt impuși nu numai de către furnizorii care percep taxe pentru serviciile Cloud, ci și de către furnizorii de servicii gratuite (Dropbox și Facebook) .

[32] S.Bradshaw, Ch. Millard, I. Walden, *op. cit*., p. 34.

[33] S.Bradshaw, Ch.Millard, I.Walden, *op. cit*., p. 34

O serie de furnizori se angajează să despăgubească clientul în anumite condiții. 3Tera, Akamai, Google (pentru Google Apps Premier) și Salesforce (pentru Salesforce CRM) - despăgubesc clienții împotriva plângerilor aduse lor pentru încălcarea dreptului de proprietate care decurge din utilizarea serviciului furnizorului[34].

Clauza de compensație a Google Apps Premier cere ca clientul să permită furnizorului să monitorizeze cursul litigiilor.

3.2. Clauze negociate în contractul cloud computing

Deși contractul cloud computing este, de regulă, unul standardizat, clienți precum întreprinderi mari, instituții financiare, agenții guvernamentale pot încerca negocierea unor clauze.

Furnizorii mari refuză, în general, orice schimbare a termenilor lor standard, arătând că serviciile lor sunt pe principiul" take it or leave it"[35], unii utilizatori acceptând această incapacitatea generală de a negocia termenii standard și fiind de acord cu termenii impuși.

Negocierea poate viza clauze referitoare la nivelul serviciilor oferite, protecția și securitatea datelor, modificarea clauzelor contractuale, drepturi de proprietate intelectuală, excluderea sau limitarea răspunderii furnizorului[36].

Concluzii

Flexibilitatea mai mare a cloud computingului în raport cu externalizarea tradițională este minimizată de siguranța redusă a clientului cauzată de contracte insuficient de specifice și de echilibrate cu furnizorii.

Importanța domeniului cloud este reflectată de politicile și direcțiile de acțiune adoptate la nivelul UE în materie ca element al punerii în aplicare a Strategiei pentru piața unică digitală și a pachetului privind digitalizarea industriei europene, susținând astfel creșterea economiei digitale europene, contribuind la competitivitatea întreprinderilor și serviciilor europene și consolidând poziționarea pe piața mondială.

---

[34] *Idem*, p. 35.

[35] W.K. Hon, Ch. Millard, I. Walden, *Negociating cloud contracts:looking at clouds from both sides now*, în Journals.law.stanford.edu, [Online] la https://journals.law.stanford.edu/sites/default/files/stanford-technology-law-review/online/cloudcontracts.pdf, p. 89, accesat 18.05.2017.

[36] C.T. Ungureanu, *op. cit.*, p. 94.

Activitatea de standardizare în cloud computing ca factor de ameliorare a standardelor și a interoperabilității ce va permite comunicarea între diferitele sisteme de cloud computing și evitarea dependenței de un singur furnizor pentru produsele și serviciile cloud reprezintă una dintre prioritățile Comisiei Europene.

Respectarea drepturilor fundamentale, confidențialitatea, protecția datelor, drepturile de proprietate intelectuală și informațiile sensibile reprezintă provocări ce vor trebui să își găsească reflectarea în demersurile comunitare vizînd impunerea unor clauze contractuale standard cu scopul de a crea o infrastructură digitală sigură și fiabilă și care să asigure un nivel de securitate informatică ridicat.

ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

REGLEMENTAREA BITCOIN. ASPECTE JURIDICE PRIVIND UTILIZAREA DE BITCOIN

REGULATING BITCOIN. LEGAL ASPECTS REGARDING THE USE OF BITCOIN

DESPINA-MARTHA ILUCĂ[1]

Rezumat: Instrument prin natura sa dematerializat, independent de orice suveranitate statală, circulând exclusiv prin intermediul Internetului, bitcoin este o creaţie a mediului privat, folosirea sa fiind o realitate indiscutabilă, cu numeroase implicaţii juridice. Pornind de la definirea noţiunii de bitcoin şi de la principalele sale trăsături, prezentul studiu își propune să determine dacă s-a conferit caracter legal acestui instrument și dacă este recunoscut în diferite legislaţii, dacă tranzacţionarea de bitcoin înseamnă încheierea unui contract și dacă acesta îndeplinește condiţiile de validitate ale actului juridic, dacă veniturile obţinute din tranzacţionarea de bitcoin se înscriu în sfera licită sau ilicită și dacă este posibilă fiscalizarea acestor venituri, precum și dacă există jurisprudenţă în materie și care ar fi optica instanţelor în această chestiune.
Cuvinte cheie: bitcoin, reglementarea bitcoin, tranzacţii cu bitcoin, fiscalizarea bitcoin

Abstract: An instrument dematerialized by nature, independent of any state sovereignty, available exclusively via Internet, bitcoin is a creation of the private environment, its use being an indisputable reality, with numerous legal implications. Starting from the definition of bitcoin and its main characteristics, this study intends to address whether bitcoin use is legal or not and if it is recognized by the law of different states, whether bitcoin transactions mean concluding a contract and if such a contract meets the conditions of validity, whether the income from bitcoin transactions is licit or illicit and if it can be subjected to taxation, as well as the existence of jurisprudence in this matter and the courts' view of the problem.
Keywords: bitcoin, regulating bitcoin, bitcoin transactions, taxation of bitcoin

[1] Doctorand, Universitatea „Alexandru Ioan Cuza" din Iași, Facultatea de Drept, email: despina.iluca@gmail.com.

1. Aspecte preliminare

Un prim pas în prezentul studiu îl reprezintă însăşi clarificarea valenţelor titlului lucrării de faţă şi, pe cale de consecinţă, stabilirea obiectivelor demersului nostru. Aşadar, „reglementarea bitcoin" este mai degrabă un oximoron decât un epitet şi un deziderat al anumitor state mai degrabă decât o realitate. Într-o formă foarte simplificată de exprimare – pe care o vom dezvolta în cele ce urmează – bitcoin „nu vrea" să fie reglementat: este plămădit din linii de cod şi trăieşte în propriul său norişor (*i.e.* în *cloud*), independent de orice părinte instituţional, revoltat şi rezistent în faţa suveranităţilor statale.

În esenţă, discuţiile despre reglementarea bitcoin sunt determinate de obişnuinţa noastră de a ne raporta la norme de drept şi la interpretarea lor prin toate metodele cunoscute pentru a găsi soluţia chiar în conţinutul prevederii legale. Or, astfel cum urmează să vedem în cele expuse mai jos, misiunea juristului pus în faţa unei tranzacţii cu bitcoin este cu atât mai grea cu cât problema se desfăşoară într-un cadru nereglementat, marcat de incertitudine în privinţa naturii juridice a bitcoin-ului în sine, a actelor juridice încheiate folosind bitcoin, precum şi al caracterului lor licit sau ilicit.

Pe cale de consecinţă, vom structura logic prezentul studiu pornind de la funcţionarea bitcoin din punct de vedere tehnic (informatic) şi economic, cu identificarea principalelor avantaje şi dezavantaje, urmând să dezbatem posibila natură juridică a bitcoin – de bun sau de monedă – şi, implicit, calificarea actelor încheiate folosind bitcoin, cu antamarea principalelor opinii doctrinare exprimate până la acest moment şi expunerea opticii instanţelor care s-au pronunţat în materie. Fiind un domeniu nereglementat, prin lucrarea de faţă nu ne propunem să dăm răspunsuri tranşante, exhaustive şi la adăpost de orice critici, ci mai degrabă să provocăm discuţii doctrinare subsecvente.

2. Scurte consideraţii privind apariţia şi funcţionarea bitcoin

Deşi vom evita la acest moment să calificăm bitcoin ca bun sau monedă, trebuie precizat că ideea unei cripto-monede predatează anii 2000, însă criza economică mondială începută la finele anului 2007 (supranumită şi „marea recesiune") a determinat scăderea dramatică a nivelului de

încredere generală în instituţiile financiare şi bancare tradiţionale[2]. Având în vedere faptul că băncile au fost printre principalii învinuiţi (*n.b.*, şi printre marii perdanţi) pentru aceste schimbări care au afectat considerabil masele, dorinţa de a elimina aceste entităţi din circuitul monetar a devenit din ce în ce mai pregnantă.

În lumina acestor evenimente, în anul 2009, programatorul „Satoshi Nakamoto" (numele său real fiind necunoscut) semnează lucrarea „*Bitcoin: A Peer-to-Peer Electronic Cash System"*, stabilind ca scop al reţelei facilitarea transferurilor valorice online între entităţi pseudonime, printr-un mediu descentralizat şi lipsit de interferenţe guvernamentale. Avantajul declarat al sistemului este abilitatea de a tranzacţiona direct, bilateral, fără alţi terţi implicaţi, securitatea transferului fiind bazată pe dovezi criptografice şi nu pe încrederea acordată de părţi intermediarului[3]. Astfel, bitcoin transformă neîncrederea în instituţiile financiare într-o veritabilă filosofie de funcţionare[4].

Bitcoin nu este nimic altceva decât un fişier de calculator, însă îşi atinge scopul declarat prin crearea unei reţele de calculatoare care verifică tranzacţiile pe măsură ce acestea se desfăşoară, instituind aşadar propriul său mecanism de autoreglare, asigurat prin combinarea a două procese: înscrierea în registrul public comun numit *block-chain* şi operaţiunea de *mining*[5].

Fiecare utilizator de bitcoin deţine o cheie publică (sau număr de cont), care este vizibilă celorlalţi utilizatori, precum şi o cheie secretă privată, folosită pentru semnarea tranzacţiilor, în scopul de a asigura atât confidenţialitatea, cât şi validitatea transferurilor. Semnătura oferă confirmarea matematică a provenienţei tranzacţiei şi împiedică modificarea acesteia.

---

[2] G. V. Ficcaglia, *Heads Or Tails: How Europe Will Become The Global Hub For Bitcoin Business If The United States Does Not Reexamine Its Current Regulation Of Virtual Currency*, în Suffolk Transnational Law Review, 40 Suffolk Transnat'l L. Rev. 103, 2017, p. 104.

[3] M. Prentis, *Digital Metal: Regulating Bitcoin As A Commodity*, în Case Western Reserve Law Review, 66 Case W. Res. 609, 2015, p. 612.

[4] D. Sonderegger, *A Regulatory and Economic Perplexity: Bitcoin Needs Just a Bit of Regulation*, în Washington University Journal of Law and Policy, 47 Wash. U.J.L. & Pol'y 175, 2015, p. 177.

[5] În ceea ce ne priveşte, vom folosi în întreg conţinutul studiului terminologia în limba engleză, traducerea noţiunilor tehnice fiind improprie de această dată.

Fiecare tranzacţie este verificată, confirmată şi înregistrată în ordine cronologică în *block-chain*, care constituie coloana vertebrală a sistemului de verificare. La confirmarea tranzacţiei, aceasta se include în *block-chain*[6] şi este înregistrată în fiecare nod sau, cu alte cuvinte, în fiecare calculator din reţeaua Bitcoin[7]. Întrucât fiecare *block* trebuie să facă trimitere la *block*-ul anterior pentru a fi valid, aplicându-se o marcă temporală, tentativele de fraudă la bitcoin echivalează cu încercarea (*n.a.* sortită eşecului) de a rescrie întreg istoricul respectivului bitcoin din *block-chain*[8].

Verificarea tranzacţiilor se realizează prin *mining*, operaţiune care implică rezolvarea unor probleme matematice complexe prin care se descoperă şi se adaugă *block*-uri în *block-chain*. Confirmarea transferurilor se realizează de ceilalţi utilizatori ai reţelei, numiţi *miners*, prin punerea la dispoziţia sistemului a propriilor lor capacităţi computaţionale[9]. Întrucât aceste capacităţi sunt costisitoare şi mult superioare celor obişnuite, primul *miner* care validează o tranzacţie este recompensat automat în cadrul acestui mecanism cu o anumită sumă de bitcoin[10], aceasta fiind de altfel metoda prin care noi unităţi de bitcoin sunt create.

În acest sens, discuţia ne conduce în mod evident la una dintre cele mai importante implicaţii de ordin economic ale bitcoin, aceea că numărul de bitcoin care se vor putea genera vreodată este limitată algoritmic[11] la 21 milioane. În concret, la geneză, recompensa pentru descoperirea unui nou *block* – şi, implicit, emisiunea de noi unităţi – era 50 bitcoin. O dată la fiecare 210.000 *blocks* descoperite, recompensa se înjumătăţeşte, în prezent aflându-ne în etapa de generare a 25 bitcoin/*block*. După 34 de astfel de înjumătăţiri, valoarea rezultată nu va mai putea fi înjumătăţită din nou, întrucât cele 8 zecimale în care se poate fracţiona bitcoin nu vor mai fi suficiente pentru exprimarea noului rezultat, atingându-se aşadar limita

[6] Cum funcţionează Bitcoin?, Bitcoin, [Online] la https://bitcoin.org/ro/cum-functioneaza, accesat la 07.11.2017.

[7] Folosirea noţiunii de „Bitcoin" (redactat cu majusculă) echivalează cu referinţa la sistemul informatic şi nu la elementul tranzacţionat.

[8] D. Tapscott, A. Tapscott, *Revoluţia blockchain: despre felul în care tehnologia aflată la baza bitcoinului transformă banii, afacerile şi lumea*, Editura ACT şi Politon, Bucureşti, 2017, p. 35.

[9] G. V. Ficcaglia, *op.cit.*, p. 107.

[10] D. Sonderegger, *op.cit.*, p. 182.

[11] Pentru detaliere, a se vedea [Online] https://en.bitcoin.it/wiki/Controlled_supply#Projected_Bitcoins_Long_Term, accesat la 07.11.2017.

matematic posibilă a generării de bitcoin. Având în vedere ritmul actual de validare a *block*-urilor, se estimează că ultimul bitcoin va fi „minat" în jurul anului 2140.

3. Avantajele bitcoin

3.1. Controlul inflaţiei

Datorită caracterului său de resursă limitată, bitcoin este adesea asemănat cu aurul, însă apreciem că existenţa unui grafic de generare a bitcoin şi plafonarea numărului de unităţi care pot fi emise la 21 milioane contribuie în mod substanţial la controlarea fenomenului inflaţionist[12]. Admitem că este neobişnuit să analizăm indicatorul inflaţiei pentru o monedă virtuală, dar arătăm că în ciuda a ceea ce am fi tentaţi să credem, rata inflaţiei bitcoin se situează în prezent în jurul a 4,35%, un procent de confort pentru o monedă lipsită de valoare intrinsecă şi de protecţie statală, comparativ cu inflaţia dolarului american şi a leului românesc de aproximativ 2%.

Aplicaţia acestui avantaj economic a fost exploatată în anul 2012 în cursul crizei monetare din Iran, în care rialul iranian (moneda naţională) se confrunta cu hiperinflaţia, iar dolarul american se regăsea în sume mici în Iran datorită sancţiunilor impuse de Statele Unite şi de aliaţii săi. În faţa riscului de a deţine o monedă naţională afectată de un fenomen sever de inflaţie, o serie de cetăţeni iranieni au optat pentru convertirea sumelor deţinute din rial iranian în bitcoin, apreciind că le oferă mai multă stabilitate din punct de vedere al valorii, precum şi mobilitate din punct de vedere al efectuării tranzacţiilor online[13]. O abordare similară s-a constatat şi în privinţa pesoului argentinian, marcat de aceeaşi problemă a inflaţiei[14].

3.2. Independenţa financiară

Argumentul adus anterior se leagă în mod indisolubil de avantajul independenţei financiare a bitcoin, care subsumează două aspecte:

---

[12] N. D. Swartz, *Bursting the Bitcoin Bubble: The Case To Regulate Digital Currency as a Security or Commodity*, în Tulane Journal of Technology and Intellectual Property, 17 Tul. J. Tech & Intell. Prop. 319, 2014, p. 320.

[13] M. Kien-Meng Ly, *Coining Bitcoin's "Legal Bits": Examining The Regulatory Framework For Bitcoin And Virtual Currencies*, în Harvard Journal of Law & Technology, 27 Harv. J. Law & Tec 587, 2014, p. 594.

[14] N. D. Swartz, *op.cit.*, p. 322.

independenţa faţă de o instituţie guvernamentală şi independenţa faţă de alţi terţi intermediari.

În ceea ce priveşte independenţa faţă de instituţiile statale, aceasta este determinată de lipsa susţinerii bitcoin de către un guvern sau o bancă centrală, avantaj care se traduce prin faptul că bitcoin nu este afectat, în principiu, de reglementări (*n.a.* vom expune în cele de mai jos şi câteva modele de reglementări) sau de instabilitatea unei monede naţionale[15], devenind uneori chiar o alternativă viabilă la acestea, astfel cum am văzut în exemplele de mai sus.

3.3. Reducerea costurilor

Întrucât sunt evitate barierele statale şi costurile de schimb valutar, bitcoin permite tranzacţii de valori mici, care încurajează comerţul electronic[16] şi comerţul internaţional. Costurile de procesare pentru plăţile cu bitcoin sunt foarte mici în comparaţie cu valoarea comisioanelor bancare[17], ceea ce înseamnă că poate fi folosit oriunde în lume, chiar şi în pieţele emergente, prin conectarea persoanelor lipsite de un cont bancar la economia mondială.

3.4. Securitatea şi validitatea tranzacţiilor

Bitcoin soluţionează şi problema falsificării care, în domeniul monedelor digitale, reprezintă problema dublei-cheltuiri[18], adică a folosirii aceleiaşi unităţi valorice de două (sau mai multe) ori. Prin mecanismul verificării, confirmării şi înscrierii tranzacţiilor în *block-chain*, această problemă este în mod definitiv exclusă, ceea ce conferă caracterul sigur al transferurilor, chiar şi în lipsa unui terţ care să se asigure de acest lucru.

3.5. Confidenţialitatea

Sistemul *peer-to-peer* asigură utilizatorilor un înalt grad de confidenţialitate, care îi poate plasa chiar sub umbrela anonimatului, deoarece nu se solicită niciun fel de date cu caracter personal, ci doar un

[15] *Ibidem.*

[16] Pentru detalieri în privinţa comerţului electronic, a se vedea C.T. Ungureanu, *Dreptul comerţului internaţional. Contracte de comerţ internaţional*, Editura Hamangiu, Bucureşti, 2014, pp. 42-48.

[17] N. D. Swartz, *op.cit.*, p. 321.

[18] D. Sonderegger, *op.cit.*, p. 183.

număr de cont[19] reprezentat de adresa bitcoin. Un utilizator poate avea oricâte adrese bitcoin doreşte, astfel că folosirea de adrese diferite pentru fiecare tranzacţie face imposibilă asocierea lor[20], determinarea unui circuit monetar şi identificarea utilizatorului faptic.

4. Provocări în utilizarea bitcoin

4.1. Facilitarea comportamentelor ilicite

Speculând avantajul anonimatului, multiple tranzacţii se înscriu în sfera ilicitului penal, ceea ce motivează şi reticenţa statelor de a recunoaşte bitcoin cu titlu oficial. Unul dintre cele mai cunoscute exemple de activitate infracţională a fost cea desfăşurată pe site-ul Silk Road (şi versiunile sale ulterioare), în prezent considerat a fi închis, o piaţă online unde se tranzacţionau substanţe ilicite şi armament. *Dark web* – reţeaua de website-uri ilicite folosite pentru pornografie infantilă, trafic de persoane, trafic de stupefiante, spălare de bani – este suprasaturată în folosirea de bitcoin, profitându-se de anonimat[21].

4.2. Riscul de evaziune fiscală

Tot în sfera ilicitului, însă de această dată de sorginte fiscală, se înscrie şi riscul de evaziune fiscală[22] în tranzacţionarea de bitcoin, manifestată prin două forme[23]: (i) câştigul obţinut din diferenţa pozitivă dintre preţul de vânzare a bitcoin şi preţul cu care utilizatorul îl cumpărase în prealabil (speculându-se fluctuaţiile valorice) şi (ii) acceptarea de plăţi în bitcoin de către comercianţi pentru bunuri şi servicii. Corelând şi cu anonimatul tranzacţiilor, apreciem că probabilitatea neexecutări (cel puţin a) obligaţiilor declarative este una generalmente crescută.

4.3. Lipsa protecţiei asigurate prin mijloace de drept civil

Făcând abstracţie de deficienţele de natură penală, sub aspectul dreptului civil – mai exact, al obligaţiilor – ne apare ca importantă provocarea dată de imposibilitatea invocării excepţiei de neexecutare sau a

[19] M. Kien-Meng Ly, *op.cit.*, p. 593.
[20] N. D. Swartz, *op.cit.*, p. 322.
[21] *Ibidem.*
[22] Pentru detalieri privind evaziunea fiscală, a se vedea I.M. Costea, *Combaterea evaziunii fiscale şi frauda comunitară,* Editura C.H. Beck, Bucureşti, 2010, pp. 2-123.
[23] M. Kien-Meng Ly, *op.cit.*, p. 595.

garanţiilor pentru evicţiune ori pentru vicii ascunse. Dacă este să admitem că tranzacţionarea cu bitcoin[24] înseamnă încheierea de acte juridice (a căror validitate poate fi totuşi contestată sub aspectul obiectului şi cauzei), problemele privind neexecutarea, executarea necorespunzătoare a obligaţiilor, apariţia viciilor nu vor putea fi soluţionate prin mijloacele convenţionale de drept comun, datorită aceluiaşi caracter anonim discutat anterior, precum şi a specificului tehnic dat de posibilitatea survenirii unor erori de hard disk, erori umane sau a *malware*-ului.

4.4. Volatilitatea

Una dintre cele mai mari critici aduse la adresa bitcoin este însă volatilitatea, cauzată de fluctuaţiile valorice ale unei unităţi; în 2013, volatilitatea bitcoin era de 133%, comparativ cu volatilitatea monedei tradiţionale de 8-12% şi cea a acţiunilor tranzacţionate pe o piaţă internaţională de 20-30%[25]. Analizând fie şi doar anul 2017, valoarea bitcoin a crescut de la aproximativ 1.000 USD (la care ajunsese după 5 ani de existenţă) la peste 7.000 USD, în timp ce creşterea de la 6.000 USD la 7.000 USD a necesitat doar 13 zile. Este evident că au existat şi perioade corespunzătoare de declin, apărute în special ca răspuns la tentativele de reglementare provenite din partea anumitor state sau ca răspuns la optica anumitor instituţii, fie ele cu putere jurisdicţională sau nu.

Volatilitatea bitcoin este cauzată şi de imposibilitatea de a fi echivalat cu o anumită unitate dintr-un bun cu existenţă fizică, ceea ce determină şi dificultatea de a fixa preţul bunurilor şi serviciilor în bitcoin[26]. În literatura de specialitate[27] s-a avansat şi ideea că bitcoin nu este inerent volatil, ci că această volatilitate este mai degrabă o expresie a noutăţii tehnologiei şi că aceasta va scădea invers proporţional cu gradul de folosire şi de popularitate a bitcoin.

[24] Ne referim în special la folosirea bitcoin pentru cumpărarea de bunuri şi servicii şi nu la tranzacţiile a căror unic scop este achiziţionarea de bitcoin (schimbul „valutar" de la o monedă fiduciară la bitcoin).

[25] D. Yermack, *Is Bitcoin a Real Currency? An Economic Appraisal*, în National Bureau of Economic Research, Nat'l Bureau of Econ. Research, Working Paper no. 19747, 2013, p. 41.

[26] D. Sonderegger, *op.cit.*, p. 186.

[27] J. Brito, H. Shadab, A. Castillo, *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets & Gambling*, în The Columbia Science and Technology Law Review, 16 Colum. Sci. & Tech. L. Rev. 144, 2014, p. 156.

4.5. Riscul de furt

O ultimă dificultate la care ne vom referi privind folosirea bitcoin este expunerea la acte de furt, spre exemplu, prin sustragerea cheii private a unui utilizator şi semnarea cu aceasta a unor tranzacţii neautorizate de utilizatorul real. Două dintre cazurile cunoscute au avut loc în februarie 2014 când unităţi de bitcoin în valoare de 2,7 milioane USD au fost furate de pe site-ul Silk Road 2 şi când cel mai mare exchange de bitcoin, Mt. Gox, a intrat în faliment după ce a anunţat că au dispărut un număr de 850.000 bitcoin din portofoliile clienţilor săi[28].

5. Probleme de calificare juridică

Aspectele prezentate până la acest punct al studiului nostru reprezintă, de fapt, principalele trăsături ale bitcoin, din care – în mod teoretic – ar trebui să se poată desprinde şi natura juridică a acestuia. După cum vom vedea însă, această sarcină nu este una uşoară, în plan internaţional exprimându-se multiple ipoteze de calificare juridică şi de reglementare pe care le vom aminti punctual, oprindu-ne în mod special la optica Curţii de Justiţie a Uniunii Europene, pe care o apreciem ca lămurind o serie de aspecte controversate, prin interpretarea bitcoin ca fiind o monedă virtuală şi excluderea încadrării acesteia în categoria bunurilor corporale.

Deşi în literatura de specialitate au fost avansate diferite opinii privind natura juridică a bitcoin, în cvasi-totalitatea lor acestea se încadrează în una din două categorii: calificarea bitcoin ca monedă (bani), respectiv calificarea bitcoin ca bun (altul decât monedă)[29], ambele având efecte diferite în ceea ce priveşte calificarea actelor juridice încheiate cu ocazia folosirii de bitcoin.

---

[28] N. D. Swartz, *op.cit.*, p. 324.

[29] În ceea ce priveşte raportul dintre monedă, unitatea monetară şi formele monetare (bani, unitatea bănească şi formele băneşti), a se vedea opinia – la care ne raliem – expusă de R. I. Motica, L. Bercea, *Banii în Codul civil român*, în volumul Sesiunii ştiinţifice „Codul civil român, între tradiţie şi reformă, la 140 de ani de aplicare", organizată deFacultatea de Drept din cadrul Universităţii din Craiova, noiembrie 2005, pp. 28-36, *„Dacă funcţional Codul civil nu ignoră complet banii, calităţile lor de bun în sine au fost mai degrabă indiferente legiuitorului. Doctrina a manifestat, însă, un anume interes în ceea ce priveşte calificarea juridică a monedei ca bun (…). Moneda este reputată a fi un bun de gen, consumptibil şi fungibil, aceste calităţi fiind exprimate în mod constant în doctrină. Dincolo de faptul că unele dintre criteriile de clasificare a bunurilor sunt în sine criticabile, nici una dintre aceste caracterizări nu poate fi absolutizată în cazul banilor; dimpotrivă, dificultăţi serioase se evidenţiază când moneda este supusă categorizărilor ordinare din dreptul civil. Varietatea formelor monetare ale prezentului este cea care repune în discuţie calificările doctrinei (…)"*.

În prima ipoteză, dacă admitem că bitcoin este o monedă, atunci apreciem că la dobândirea bitcoin prin achiziţionarea acesteia contra unei monede fiduciare are loc de fapt un schimb valutar, iar cu ocazia folosirii pentru plata contravalorii unor bunuri sau servicii, actele juridice încheiate au valoarea unor contracte de vânzare-cumpărare.

În a doua ipoteză, dacă admitem că bitcoin este un bun, opinăm că operaţiunile vor fi calificate în sens invers, respectiv achiziţionarea bitcoin înseamnă cumpărarea unui bun folosind o monedă fiduciară, deci încheierea unui contract de vânzare-cumpărare, în timp ce plata contravalorii unui bun cu bitcoin ar echivala cu un contract de schimb, iar plata contravalorii unui serviciu cu bitcoin ne-ar putea situa chiar pe teritoriului unui contract de antrepriză de servicii al cărui preţ este o prestaţie nepecuniară.

5.1. Dualismul de interpretare în Statele Unite ale Americii

În ciuda faptului că pare greu de conceput, cele două mari ipoteze de calificare a bitcoin coexistă în Statele Unite ale Americii. În interpretarea dată de Internal Revenue Service (autoritatea fiscală americană, echivalentul A.N.A.F.) în 2014, bitcoin este considerat un bun în scopul aplicării impozitului pe veniturile obţinute din tranzacţii cu bitcoin. Astfel, orice operaţiune cu bitcoin reprezintă un fapt generator al impunerii care, conform legislaţiei fiscale din SUA, se impozitează ca un câştig de capital, cu posibilitatea aplicării unei cote reduse de impunere dacă dreptul de proprietate asupra bunului este păstrat de acelaşi contribuabil cel puţin un an. În acest context, autoritatea fiscală a descurajat circulaţia bitcoin ca metodă de plată[30]şi a încurajat păstrarea acestora în patrimoniul propriu al contribuabililor care, bucurându-se de creşterea valorii bitcoin din ultimii ani, ajung să îl folosească drept investiţie.

Pe de cealaltă parte, optica unei instanţe federale (District Court for the Eastern District of Texas), în cauza S.E.C. (Securities and Exchange Comission) v. Shavers, defineşte bitcoin ca fiind o monedă, motivându-şi decizia în cheie teleologică, având în vedere posibilitatea de a achiziţiona bunuri şi servicii cu bitcoin şi aptitudinea de a fi schimbată cu o monedă fiduciară[31].

[30] G. V. Ficcaglia, *op.cit.*, p. 121.
[31] D. Sonderegger, *op.cit.*, p. 191-192.

5.2. Incertitudini europene

În timp ce Statele Unite au acceptat cu o oarecare reticenţă folosirea bitcoin, reacţiile altor state au fost variate: unele au dorit interzicerea tranzacţiilor cu bitcoin şi au prevăzut în reglementările interne sancţiuni în acest sens[32], altele au manifestat cel puţin un grad de toleranţă – dacă nu chiar acceptare – a acestei realităţi. State precum Belgia, Elveţia şi Danemarca[33] au abordat o atitudine pasivă declarată, apreciind că la acest moment bitcoin nu necesită o reglementare.

Politicile economice ale Marii Britanii converg spre ţinta acestui stat de a deveni un nod pentru tehnologiile financiare, astfel că în martie 2015, Trezoreria (Majestăţii Sale) a finalizat un program prin care a fixat obiectivul de a aplica în materie de bitcoin reglementările destinate prevenirii şi combaterii spălării de bani. Mai mult decât atât, a fost elaborată o schemă de impozitare care încurajează folosirea bitcoin prin scutirea de TVA a schimburilor valutare dintre bitcoin şi moneda fiduciară şi aplicarea tratamentului fiscal al câştigurilor de capital doar tranzacţiilor în bitcoin făcute cu titlu de investiţie[34].

5.3. Posibile răspunsuri: Uniform Commercial Code

Uniform Commercial Code („UCC”), adoptat în Statele Unite ale Americii, ar putea constitui o sursă de reglementare suficientă pentru tranzacţiile cu bitcoin, întrucât, la o primă vedere, tinde să confere caracter legitim acestor operaţiuni şi nu să le interzică, făcând astfel aplicarea principiului efectului util. În lumina UCC, calificarea bitcoin ca bun sau ca monedă nu afectează validitatea actelor juridice încheiate; astfel, dacă bitcoin este considerată o monedă, aceasta ar avea regimul unei valute străine, tranzacţiile în monedă străină fiind recunoscute prin UCC; pe de cealaltă parte, aprecierea bitcoin ca bun plasează actele juridice încheiate în scopul obţinerii de bunuri sau servicii în categoria celor de schimb (*barter*

[32] În acest sens, a se vedea decizia Chinei din decembrie 2013 de a interzice instituţiilor financiare acceptarea tranzacţiilor referitoare la bitcoin şi de a interzice comercianţilor să îşi exprime preţurile în bitcoin, precum şi propunerea Ministerului de Finanţe din Rusia de a interzice tranzacţiile cu bitcoin începând cu 2015 şi de a aplica sancţiuni sub forma amenzilor.

[33] E. E. Lambert, *The Internal Revenue Service and Bitcoin: A Taxing Relationship*, în Virginia Tax Review, 35 Va. Tax Rev. 88, 2015, p. 103.

[34] G. V. Ficcaglia, *op.cit.*, p. 130.

transactions). Aşadar, în ambele ipoteze de interpretare, UCC oferă cheia de validare sub aspect juridic a tranzacţiilor cu bitcoin[35].

5.4. Deznodământul european: răspunsul Curţii de Justiţie a Uniunii Europene

La nivelul Uniunii Europene, răspunsurile vin din partea Curţii de Justiţie, care s-a pronunţat în materie de bitcoin în cauza C-264/14 (Hedqvist)[36] prin hotărârea pe care o expunem în extras în cele de mai jos. Cauza are la bază un litigiu din Suedia, între Skatteverket (administrația fiscală suedeză), pe de o parte, şi domnul Hedqvist, pe de altă parte, în legătură cu un aviz prealabil dat de Skatterättsnämnden (Comisia de Drept Fiscal suedeză) cu privire la supunerea la taxa pe valoarea adăugată a operațiunilor de schimb de monede tradiționale cu monedă virtuală bitcoin sau invers, pe care domnul Hedqvist intenționează să le efectueze prin intermediul unei societăți.

Referindu-se la un raport din anul 2012 al Băncii Centrale Europene privind monedele virtuale, instanța de trimitere arată că o monedă virtuală poate fi definită ca un tip de monedă digitală nereglementată, emisă şi controlată de dezvoltatori şi acceptată de membrii unei comunități virtuale specifice. Moneda virtuală bitcoin face parte dintre monede virtuale aşa-numite „cu flux bidirecțional", pe care utilizatorii le pot cumpăra şi vinde în funcție de cursul de schimb. Astfel de monede virtuale sunt similare celorlalte monede convertibile în ceea ce priveşte utilizarea lor în lumea reală. Ele permit cumpărarea de bunuri şi de servicii, atât reale, cât şi virtuale. Monedele virtuale se disting de moneda electronică, astfel cum este definită în Directiva 2009/110/CE a Parlamentului European şi a Consiliului din 16 septembrie 2009 privind accesul la activitate, desfăşurarea şi supravegherea prudențială a activității instituțiilor emitente de monedă electronică, de modificare a Directivelor 2005/60/CE şi 2006/48/CE şi de abrogare a Directivei 2000/46/CE (JO L 267, p. 7), în măsura în care, spre deosebire de această monedă, în cazul monedelor virtuale, fondurile nu sunt

[35] M. Kien-Meng Ly, *op.cit.*, p. 600.

[36] Hotărârea din 22 octombrie 2015 pronunțată de CJUE, Camera a cincea în Cauza C-264/14 Skatteverket împotriva David Hedqvist, disponibilă [Online] la http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5c24c612cd6fb4fc8983ad6dea40e4a04.e34KaxiLc3eQc40LaxqMbN4PaNeSe0?text=&docid=170305&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=299689, accesat la 07.11.2017.

exprimate într-o unitate de cont tradițională, de exemplu în euro, ci într-o unitate de cont virtuală, precum bitcoin.

Instanța de trimitere arată că operațiunile pe care domnul Hedqvist le are în vedere ar avea loc sub formă electronică, prin intermediul site-ului Internet al societății sale. Diferența dintre prețul de cumpărare şi prețul de vânzare al bitcoin ar constitui profitul societății domnului Hedqvist, care nu ar factura alte cheltuieli.

Având îndoieli cu privire la problema dacă una dintre scutirile prevăzute la articolul 135 alineatul (1) din Directiva TVA[37], pentru serviciile financiare, mai precis cele prevăzute la punctele (d)-(f) se aplică unor astfel de operațiuni, Högsta förvaltningsdomstolen (Curtea Administrativă Supremă) a hotărât să suspende judecarea cauzei şi să adreseze Curții următoarele două întrebări preliminare: prima este dacă în lumina prevederilor Directivei TVA, operaţiunile de schimb de monedă virtuală cu monedă tradiţională şi invers efectuat pe baza unei contraprestații cuprinse de furnizor în calculul cursului de schimb, constituie prestări de servicii efectuate cu titlu oneros; dacă da, a doua întrebare este dacă aceste operaţiuni sunt scutite de TVA.

În privința primei întrebări, Curtea notează că trebuie constatat, în primul rând, că moneda virtuală cu flux bidirecțional bitcoin, care va fi schimbată în monedă tradițională în cadrul operațiunilor de schimb, nu poate fi calificată ca „bun corporal” în sensul articolului 14 din Directiva TVA, dat fiind că această monedă virtuală nu are alte finalități decât aceea de mijloc de plată.

Mai mult decât atât, în cauza principală, reiese din elementele dosarului prezentat Curții că între domnul Hedqvist şi cocontractanții săi ar exista un raport juridic sinalagmatic în cadrul căruia părțile la operațiune s-ar angaja reciproc să cedeze sume într-o anumită monedă şi să primească contravaloarea acestora într-o monedă virtuală cu flux bidirecțional sau invers. Se precizează de asemenea că această societate ar fi remunerată pentru prestarea sa de servicii printr-o contraprestație care corespunde marjei pe care ar integra-o în calcularea cursurilor de schimb la care ar fi dispusă să vândă şi să cumpere monezile în cauză.

[37] Directiva 2006/112/CE a Consiliului din 28 noiembrie 2006 privind sistemul comun al taxei pe valoarea adăugată, disponibilă [Online] la http://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32006L0112&from=RO, accesat la 07.11.2017.

Având în vedere că Directiva TVA clasifică operaţiunile ce intră sub incidenţa sa „prin diferenţă” – în sensul că ceea ce nu este livrare de bunuri este prestare de servicii – Curtea răspunde la prima întrebare că articolul 2 alineatul (1) litera (c) din Directiva TVA trebuie interpretat în sensul că reprezintă prestări de servicii efectuate cu titlu oneros, în sensul acestei dispoziții, operațiuni precum cele în discuție în litigiul principal.

Cu privire la a doua întrebare, cu titlu introductiv, Curtea aminteşte că, potrivit jurisprudenței sale, scutirile prevăzute la articolul 135 alineatul (1) din Directiva TVA constituie noțiuni autonome de drept al Uniunii care au ca obiect evitarea unor divergențe în aplicarea sistemului TVA de la un stat membru la altul.

Curtea înlătură multiple alte calificări ale naturii juridice a bitcoin, reţinând că întrucât moneda virtuală bitcoin este un mijloc de plată contractual, aceasta nu poate, pe de o parte, să fie considerată un cont curent şi nici un cont de depozit, o plată sau un virament. Pe de altă parte, spre deosebire de creanțe, de cecuri sau de alte instrumente negociabile prevăzute la articolul 135 alineatul (1) litera (d) din Directiva TVA, ea constituie un mijloc de plată direct între operatorii care o acceptă.

Pentru a răspunde la a doua întrebare, se constată problema diferitelor versiuni existente ale dispoziţiei legale în limbile Uniunii. Diferitele versiuni lingvistice ale articolului 135 alineatul (1) litera (e) din Directiva TVA nu permit să se stabilească fără ambiguitate dacă această dispoziție se aplică numai operațiunilor privind monedele tradiționale sau dacă, dimpotrivă, aceasta are în vedere şi operațiunile care implică o altă monedă. În prezența unor divergențe lingvistice, întinderea expresiei respective nu poate fi apreciată pe baza unei interpretări exclusiv textuale. Această expresie trebuie interpretată în lumina contextului în care se înscrie, a finalităților şi a economiei Directivei TVA.

Având în vedere considerațiile precedente, Curtea răspunde la a doua întrebare astfel: articolul 135 alineatul (1) litera (e) din Directiva TVA trebuie interpretat în sensul că prestări de servicii, precum cele în discuție în litigiul principal, care constau în schimbul de monede tradiționale cu unități ale monedei virtuale bitcoin şi invers, efectuate contra plății unei sume care corespunde marjei constituite de diferența dintre, pe de o parte, prețul la care operatorul în cauză cumpără monedele şi, pe de altă parte, prețul la care le vinde clienților săi, constituie operațiuni scutite de TVA, în sensul acestei dispoziții.

Scurte concluzii

În final, în privinţa bitcoin, lupta se poartă între două concepţii juridice: *„dacă nu este reglementat, nu este legal”* şi *„dacă nu este interzis, este permis”*. Deşi pronunţată de ceva timp, hotărârea CJUE se pare că a adus doar în parte lumină în ceea ce priveşte problemele abordate în studiul de faţă. Fără doar şi poate, bitcoin este prezent şi în peisajul românesc: o serie de comercianţi acceptă plata cu bitcoin, deşi recunosc că încă se confruntă cu semne de întrebare în privinţa înregistrării contabile şi a obligaţiilor fiscale subsecvente; organele de conducere ale diferitelor corpuri profesionale emit dispoziţii privind actele juridice încheiate folosind bitcoin; organele de cercetare penală urmăresc în activitatea lor inclusiv contrapartidele în bitcoin şi identifică grupuri infracţionale organizate.

Instituţiile guvernamentale nu vor putea ignora existenţa şi folosirea bitcoin şi vor fi puse în cele din urmă în mod imperativ în faţa unor decizii dificile: de a reglementa sau nu moneda virtuală şi de a identifica echilibrul necesar pentru a nu crea imixtiuni inutile într-o problemă ce se doreşte a fi autoreglată, autonomă, autosuficientă, eminamente de drept privat. În eventualitatea unor decizii de reglementare, acestea ar trebui să aibă în vedere şi un model combinat (*combined regulatory model*[38]), adaptat obiectivelor şi politicilor guvernamentale ale fiecărui stat, apt să dezvolte avantajele actuale ale bitcoin şi să diminueze pe cât de mult posibil riscurile sale inerente.

[38] D. Sonderegger, *op.cit.*, pp. 211-215.

ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI
TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II

REGLEMENTAREA DREPTULUI DE A FI UITAT

THE ENACTMENT OF THE RIGHT TO BE FORGOTTEN

ANDREEA ȘERBAN[1]

Rezumat: Reiterarea și dezvoltarea dreptului la ștergerea datelor, cunoscut ca dreptul de a fi uitat în Regulamentul privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, nu este doar rezultatul unor controverse jurisprudențiale și doctrinare, ci și a traseului legiuitorului european în vederea stabilirii unui echilibru între interesul legitim al utilizatorilor de Internet, operatorilor de date și respectarea drepturilor persoanei vizate ale cărei informații personale sunt prelucrate. Pentru analizarea și înțelegerea acestui drept este necesară observarea cursului ascendent al tehnologiei, a jurisprudenței în domeniul protecției datelor și linia firavă între noțiunea de viață privată, activitate nesupravegheată și necontrolată în mediul online și o societate care se dezvoltă pe Internet.
Cuvinte-cheie: date cu caracter personal, dreptul de a fi uitat, dreptul la ștergerea datelor, regulamentul general privind protecția datelor personale

Abstract: The reiteration and the development of the right to erasure of personal data, known as the right to be forgotten, in the Regulation on the protection of natural persons with regard to the processing of personal data, is not only the result of jurisprudential and doctrinaire controversies, but also of the path of the European legislator for creating a balance between the legitimate interest of Internet users, data controllers and respecting the rights of the data subject whose personal information is being processed. In order to analyse and understand this right, it is necessary to observe the advancement of technology, the data protection jurisprudence and the thin line between the concept of private life, unsupervised and uncontrolled online activity and a society that develops on the Internet.
Key-words: personal data, the right to be forgotten, the right to erasure, general data protection regulation

1. Considerații generale privind datele cu caracter personal

[1] Doctorand, Universitatea „Alexandru Ioan Cuza" din Iași, Facultatea de Drept, email: andreeaserban20@yahoo.com

Contemporaneitatea surprinde un rapid progres tehnologic căruia i se construiește treptat un cadru legislativ național și supranațional. Sunt vizate, în primul rând, valorile și principiile fundamentale, drepturile și libertățile cetățenilor. Provocarea constă în modul și mijloacele prin care se răspunde acestui progres în vederea protejării aspectelor sociale, economice, religioase și culturale care ne definesc. Trecerea de la modalitățile tradiționale de supraveghere a cetățenilor la cele avansate – prin intermediul Internetului, aduce în discuție o nouă caracteristică a epocii contemporane și anume, datele cu caracter personal ale individului și modul în care acestea sunt utilizate.

Revoluția digitală are în vedere apariția conceptului de date – diverse, nestructurate și cu schimbare rapidă. Acestea au o deosebită importanță pentru o multitudine de domenii privind, printre altele, aplicarea legii, securitatea națională, tehnologia, referitoare la cercetare și altele. Astfel, în fiecare sector, analizarea datelor este o practică tot mai des utilizată pentru a răspunde unor nevoi private sau publice, după caz. Presiunea schimbării și a progresului tehnologic este deplin simțită în Uniunea Europeană, Directiva 95/46/CE[2] (în continuare Directiva) nemaifiind aplicabilă efectiv asupra tuturor ipotezelor și domeniilor în care datele cu caracter personal sunt prelucrate și utilizate. Comisia Europeană a recunoscut că, deși protecția drepturilor și libertăților fundamentale ale persoanelor, în special al dreptului fundamental la protecția datelor, este de continuă actualitate și pertinență, cadrul legislativ trebuie să răspundă noilor situații[3].În acest sens, a fost adoptat Regulamentul nr. 679[4](în continuare Regulamentul) în anul 2016, urmând să fie aplicat începând cu anul 2018, care răspunde multor întrebări ridicate în practică, privește noi aspecte ale protecției datelor și dezvoltă alte anumite chestiuni inițiate prin Directivă.

[2]Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, publicată în J. O. L 281 din 23.11.1995.

[3]A se vedea Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social și Comitetul Regiunilor, *O abordare globală a protecției datelor cu caracter personal în Uniunea Europeană*, COM (2010) 609 final din 4 noiembrie 2010.

[4]Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), publicat în J.O., L 119 din 4 mai 2016.

Pentru o prezentare eficientă a dreptului de a fi uitat în prezentul studiu, este necesară definirea unor termeni precum *date cu caracter personal*, *persoana vizată* și*prelucrarea datelor*.

Astfel, *datele cu caracter personal*, în sensul Regulamentului, se referă la informații care privesc „o persoană fizică identificată sau identificabilă (*persoana vizată*); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare […]". Cu titlu de exemplu, sunt date personale toate acele informații cu elemente care definesc identitatea fizică, genetică, psihică, culturală sau socială, conform art. 4 pct. 1 din Regulament. Din jurisprudența Curții de Justiție a Uniunii Europene (în continuare, CJUE) reiese că, în general, noțiunea de date personale se referă la un domeniu vast de informații, exprimându-se în acest sens opinia că, în situația în care prelucrarea[5] are în vedere o persoană identificată ori identificabilă, chiar și numărul de la pantof este o informație cu caracter personal[6].În jurisprudența Curții au fost considerate ca fiind date personalenumele unei persoane, numărul de telefon, condițiile de muncă sau activitățile de interes personal[7], informații referitoare la starea de sănătate a unei persoane[8], evidența timpului de lucru al unei persoane, a întreruperilor sau a pauzelor corespunzătoare[9], veniturile din muncă și din capital și informații referitoare la patrimoniul persoanelor fizice[10], precum și referințele la data nașterii,

[5]Prin prelucrare se înțelege „orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea", conform art. 4 pct. 2 din Regulamentul general privind protecția datelor.

[6]G. Zanfir, *Protecția datelor personale. Drepturile persoanei vizate*, Editura C.H.Beck, București 2015, p. 23.

[7]CJUE, Hotărârea din 6 noiembrie 2003, C-101/01, *Bodil Lindqvist*, pct. 24, [Online] lawww.curia.europa.eu, accesat 26.09.2017.

[8]*Ibidem.*

[9]CJUE, Hotărârea din 30 mai 2013, C-342/12 *Worten*, pct. și 22, [Online] lawww.curia.europa.eu,accesat 26.09.2017.

[10]CJUE, Hotărârea din 16 decembrie 2008, C-73/07 *Satakunnan Markkinaporssi și Satamedia*, pct. 37, disponibil pe www.curia.europa.eu,accesat 26.09.2017.

sexul, etnia, religia, limba unei persoane fizice identificate prin nume[11] și altele.

Noțiunea de *date cu caracter personal* este atât de generoasă încât trebuie evitată o abordare statică și inflexibilă, având în vedere, totuși, că informațiile și circuitul acestora se transformă constant. În acest sens, întrucât există o strânsă legătură între date personale și dreptul la viață privată, Regulamentul instituie sau readuce în discuție o serie de drepturi de care persoana fizică dispune în vederea protejării în ceea ce privește prelucrarea acestor date precum dreptul la informare și acces la date cu caracter personal, dreptul la ștergerea datelor, dreptul la restricționarea prelucrării, dreptul la portabilitatea datelor, precum și dreptul la opoziție. De asemenea, trebuie subliniat caracterul personal al prevederilor Regulamentului în sensul că acestea se referă *in concreto* la prelucrarea datelor cu caracter personal a persoanelor vizate și nu la prelucrarea datelor *in extenso*.

Prin *prelucrarea datelor* se înțelege, în sensul Regulamentului, acea operațiune efectuată asupra datelor cu caracter personal. Aceasta poate viza „colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea". În hotărârile CJUE[12] s-a arătat că inclusiv referirea pe anumite pagini de Internet la diverse persoane și publicarea unor informații precum numărul de telefon sau date privind starea lor de sănătate ori pasiunile lor este o prelucrare a datelor cu caracter personal în sensul Directivei, aceeași interpretare putând fi aplicată și conceptului de prelucrare din Regulament.

O caracteristică a activității din societatea informațională actuală este manifestarea unor situații nefaste privind confidențialitatea și viața privată a utilizatorului sau a persoanei ale cărei informații personale sunt vizate în momentul când este deja prea târziu. De exemplu, sunt des întâlnite în practică situațiile în care angajatorii realizează o verificare a activității din mediul online[13] a candidaților în vederea stabilirii caracterului acestuia

[11]CJUE, Hotărârea din 17 iulie 2014 în cauzele C-141/12 și C-372/12 *Minister voor Immigratie*, pct. 38, [Online] lawww.curia.europa.eu,consultat la data de 26 septembrie 2017.

[12]CJUE, Hotărârea din 6 noiembrie 2003, C-101/01, *Bodil Lindqvist*, pct. 27.

[13]Diverse platforme on-line de socializare și motoare de căutare. Cu titlu de exemplu: Facebook, LinkedIn, Google, Yahoo.

raportat la criteriile de angajare pentru locul de muncă respectiv. Nu este posibilă anticiparea tuturor efectelor utilizării datelor cu caracter personal. Și chiar dacă unele ar putea fi prevăzute, acestea sunt abstracte, îndepărtate și incerte. Caracterul abstract este dat de faptul că opiniile și prejudecățile privind viața privată se referă de multe ori la societate și viața socială a unei comunități, caracterul îndepărtat este determinat de faptul că multe dintre efecte apar după o serie de reacții, iar incertitudinea este determinată de imprevizibilitatea și totodată și de posibilitatea ca efectele să nu apară vreodată.[14] Așadar, persoana vizată își asumă faptul că prelucrarea informațiilor sale ar putea să îi dăuneze, însă nu își va schimba comportamentul în scopul prevenirii utilizării acestor date colectate în defavoarea sa, observând că tendința este aceea de a face publice diverse aspecte privind viața noastră privată fără a asigura și un mecanism de protejare a acestora.

Ca un prim pas spre echilibrarea raportului dintre persoana vizată și operatorul de date cu caracter personal, doctrina americană a recunoscut „dreptul de a fi lăsat în pace" în contextul în care s-a evidențiat un progres rapid în diverse aspecte ale vieții, protecția unei persoane și asigurarea securității individului devenind așadar priorități pentru legiuitor. Se asigură fiecărui individ dreptul de a-și determina limitele în care gândurile și orice alte aspecte legate de viața sa pot fi comunicate și celorlalți. Dacă persoana alege să se exprime public, ea își păstrează dreptul de a redetermina limitele publicității pe care dorește să le acorde informațiilor despre sine. Existența acestui drept este independentă de forma ori metoda de publicare a datelor.[15]

Însă restricționarea accesului la date nu reprezintă o măsură suficientă de a asigura protejarea persoanei fizice privind prelucrarea informațiilor sale. Prin restricționare, conform prevederilor Regulamentului, se înțelege „marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora" și posibilitatea persoanei vizate de a dispune de acest drept la restricționare[16].Astfel, pentru a asigura individului

[14]M. L. Ambrose, J. Ausloos, *The Right to Be Forgotten Across the Pond*,în Journal of Information Policy, vol. 3, 2013, p. 4, [Online] la http://www.jstor.org/stable/10.5325/jinfopoli.3.2013.0001, accesat 2.10.2017.

[15]S.D. Warren, L.D. Brandeis, *The Right to Privacy*, în Harvard Law Review, vol. 4, nr. 5, 1890, p. 198-200, [Online] la http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf, accesat 30.09.2017..

[16]A se vedea articolul 18 din Regulamentul general pentru protecția datelor.

o protecție completă în procesul de prelucrare a datelor și pentru a răspunde noilor situații ridicate în practică, a fost enunțată și reglementată posibilitatea de a șterge informațiile, aspect pe care acest studiu urmărește să îl dezvolte în continuare.

Dreptul la ștergerea datelor sau dreptul de a fi uitat, deși nu este o noutate legislativă[17], nu a reprezentat până recent o relevanță semnificativă în contextul protecției datelor, astfel încât nu a fost abordat atât de detaliat până la momentul elaborării Regulamentului. Însă, având în vedere că acest drept a căpătat tot mai multă importanță pentru individ și autorități, prin prezentul studiu se urmărește analizarea dreptului de a fi uitat în epoca digitală, problematica din jurul acestuia și impactul viitor asupra domeniilor în care se răsfrânge.

Un astfel de drept, de a fi uitat, poate oferi persoanelor vizate oportunitatea efectivă de a-și evalua sau reevalua utilizarea informațiilor personale, poate întări controlul individului asupra identității sale și reprezintă o formă de verificare a operatorilor de date și a modului în care aceștia prelucrează informațiile. Aceștia devin mai responsabili în ceea ce privește politicile referitoare la datele personale, persoana vizată având dreptul de a cere ștergerea retroactivă a informațiilor despre sine.[18]

2. Premisele reformei domeniului protecției datelor. Jurisprudența Curții de Justiție a Uniunii Europene asupra reglementării dreptului de a fi uitat și efectele vizibile ale acesteia

Directiva nr. 95/46/CE a avut rolul de a asigura în toate Statele Membre echilibrarea nivelului de protecție a drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, precum și cel de a garanta libera circulație a acestor date în același timp cu protejarea drepturilor și intereselor persoanelor vizate.[19]

[17]Prin art. 12 pct. b) și c) al Directivei 95/46/CE, persoanei vizate îi este garantată dreptul de a obține de la operator ștergerea „datelor a căror prelucrare nu respectă dispozițiile prezentei directive […], precum și „notificarea terților cărora le-au fost comunicate datele cu privire la […] ștergere […] efectuată în conformitate cu litera (b)".

[18]J. Ausloos, *The Right to be Forgotten – Worth remembering?*, în Computer Law and Security, nr. 28/2012, p. 145, [Online] lawww.sciencedirect.com,accesat 5.10.2017.

[19]CJUE, Hotărârea din 6 noiembrie 2003, C- 101/01, *Bodil Lindqvist*, pct. 95 și 96, [Online] la www.curia.europa.eu, accesat 26.09.2017.

Plecând de la premisa că există informații privind o persoană vizată pe care aceasta nu dorește sau nu mai dorește să le publice și să le aducă la cunoștința altor utilizatori pe Internet, s-a pus problema instrumentelor juridice de care persoana dispune pentru a-și proteja datele din mediul online. În acest sens, practicaCJUE a redeterminat modul în care informațiile de pe Internet trebuie tratate, jurisprudența acesteia reprezentând primul pas spre actualizarea legislației privind datele cu caracter personal și prelucrarea acestora.

În anul 2014, în hotărârea CJUE[20]s-a arătat că Directiva nu mai răspunde cerințelor contemporaneității în ceea ce privește abordarea mijloacelor de protecție a datelor personale, iar o reformă în acest sens a devenit necesară.

În cauza care a determinat revizuirea mecanismului de protecție a persoanei fizice cu privire la prelucrarea datelor cu caracter personal, *Google Spania c. Agenției Spaniole de Protecție a Datelor (*în continuare AEPD*) și domnul C. Gonzalez*, un cetățean spaniol – domnul G. – a formulat o reclamație întemeiată pe faptul că la introducerea numelui său în motorul de căutare Google, se obțineau ca rezultate ale căutării două adrese web ale publicației *La Vanguardia*. Aceste rezultate se refereau la un anunț în care prefigura numele său cu privire la o licitație imobiliară asociată unei proceduri de recuperare a unor datorii la asigurările sociale. Domnul G. a solicitat ca Google să șteargă sau să modifice paginile existente astfel încât datele sale personale să fie protejate și să nu mai apară în paginile de Internet ale publicației sau ca rezultate ale motorului de căutare, invocând că menționarea acestora este lipsită de relevanță.AEPD a respins parțial reclamația domnului G. întrucât publicarea informațiilor de către *La Vanguardia* era justificată, însă a admis-o în măsura în care privea Google Spania și Google Inc., considerând că în calitate de operatori de date cu caracter personal, aceștia trebuiau să respecte legislația în materia protecției datelor și recunoscându-și capacitatea de a dispune ca motoarele de căutare să retragă informațiile sau să șteargă datele dacă se constată că prelucrarea acestora poate aduce atingere dreptului persoanei la protecția datelor,

[20]CJUE, Hotărârea din 13 mai 2014, C- 131/12, *Google Spain SL, Google Inc. C. Agencia Espanola de Proteccion de Datos (AEPD)*, [Online] la www.curia.europa.eu, accesat 5.10.2017.

incluzând în acest sens și voința persoanei vizate ca informațiile să nu fie aduse la cunoștință terților.[21]

Curtea a statuat în ceea ce privește ștergerea datelor că persoanele fizice au dreptul de a cere ca motoarele de căutare să șteargă adresele de Internet care fac trimitere la pagini cu informații despre ei. Asta se aplică în situațiile în care informațiile referitoare la persoanele vizate sunt imprecise, neadecvate, irelevante sau excesive pentru scopul prelucrării. Curtea a arătat că acest drept de a fi uitat nu este absolut, întrucât mereu va fi conexat cu alte drepturi fundamentale precum cel la liberă exprimare[22]. Este necesară stabilirea aplicabilității dispozițiilor referitoare la ștergerea datelor în funcție de tipul informațiilor respective, relevanța acestora pentru persoana vizată și pentru viața privată a acesteia, interesul public de a avea acces la aceste date și, dacă este cazul, și statutul persoanei care cere ștergerea informațiilor. Asta nu înseamnă că cei mai puțin cunoscuți publicului vor deveni brusc centrul atenției sau invers[23].

Drept urmare a hotărârii CJUE și totodată și a anunțării reglementării viitoare a dreptului la ștergerea datelor, Google a luat o serie de măsuri pentru a se adapta noilor cerințe europene în ceea ce privește protecția datelor cu caracter personal. Așadar, au fost eliminate paginile apărute ca răspuns la căutarea după nume a persoanei vizate din rezultatele apărute în motorul de căutare și au fost retrase adresele din domeniile de căutare Google[24]. La scurt timp după pronunțarea hotărârii în cauza Google Spania, a fost făcut un număr semnificativ de cereri de ștergere a paginilor care conțin date cu caracter personal, înregistrând peste 27.000 de înregistrări pe data de 29 mai 2014.Din acel moment până în prezent, peste 800.000 de adrese au fost șterse din motorul de căutare.[25]

Având în vedere că Regulamentul este aplicabil începând cu mai 2018, instanțele încă se mai confruntă cu situații problematice sub egida

[21]*Ibidem*, pct. 14-17.

[22]*Ibidem*, pct. 85.

[23]Ghidul Comisiei Europene, *Factsheet on the "Right to be Forgotten" ruling (c-131/12)*, p. 4, [Online] http://ec.europa.eu/justice/data-protection, accesat 17.10.2017.

[24]De exemplu: google.fr, google.ro, google.de, google.es și altele.

[25]Pentru statistica exactă realizată de Google, a se vedea *Search removal under European privacy law*, disponibilă la adresa https://transparencyreport.google.com/eu-privacy/overview, consultată la data de 23 octombrie 2017.

Directivei. Astfel, o instanță franceză[26] a adresat recent o întrebare preliminară CJUEprivind aplicarea dreptului de a fi uitat și respectarea acestuia de către motoarele de căutare (în speță Google) care trebuie să șteargă paginile de Internet și din domeniul exterior teritoriului Uniunii Europene, incluzând în această ipoteză posibilitatea delistării paginilor în cauză de pe întregul domeniu google.com, nu doar motoarele de căutare stabilite la nivelul statelor membre ale Uniunii, autoritatea franceză argumentând că politica de delistare a informațiilor incorecte, irelevante sau învechite despre persoanele fizice ar trebui, ca la cererea acestora, să aibă loc la nivel global și nu doar în motoarele regionale de căutare.

Oricare ar fi deznodământul acestei cauze, va fi destul de dificilă aplicarea normelor europene în materia protecției datelor cu caracter personal în afara spațiului Uniunii Europene. Probabil va fi necesară încheierea unor acorduri bi sau multilaterale în ceea ce privește protecția datelor cu caracter personal auxiliar reglementărilor actuale.[27]

3. Dreptul de a fi uitat conform Regulamentului general privind protecția datelor cu caracter personal

A șterge datele înseamnă a elimina informațiile din baza de date sau de pe paginile de Internet[28]. Ștergerea datele cu caracter personal este o formă de prelucrare a datelor cu caracter personal ale persoanelor vizate care și-au dat consimțământul în acest sens.

[26]Decizia CE nr. 3999[22]din 19 iulie 2017, *Google Inc.*, [Online] la www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC, accesat 18.10.2017.

[27]A se vedea drept exemplu Decizia de punere în aplicare (UE) 2016/1250 a Comisiei din 12 iulie 2016 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA [notificată cu numărul C(2016)4176], [Online] la http://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32016D1250&from=EN, care se referă, printre altele, la posibilitatea ca persoanele „să aibă acces la informațiile cu caracter personal pe care o organizație le deține în legătură cu ele și să le poată […] șterge atunci când sunt incorecte sau au fost prelucrate cu încălcarea principiilor […].”

[28]Deseori în practica motoarelor de căutare, prin „ștergere” se înțelege delistarea paginilor care conțin astfel de informații astfel încât accesul la acestea să fie restricționat. Plecând de la acest considerent, dreptul de a fi uitat e de fapt văzut ca „un drept de a fi găsit mai greu pe Internet”.

Conform art. 17 alin. (1) teza I din Regulament, dreptul la ștergerea datelor este dreptul persoanei vizate „de a obține din partea operatorului ștergerea datelor cu caracter personal, fără întârzieri nejustificate [...]". Operatorul de date are obligația corelativă „de a șterge datele cu caracter personal fără întârzieri nejustificate" dacă se aplică unul dintre motivele enunțate: „(a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate; (b) persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea […] și nu mai există niciun alt temei juridic pentru prelucrare; (c) persoana vizată se opune prelucrării […]; (d) datele cu caracter personal au fost prelucrate ilegal; (e) datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se află operatorul; (f) datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale […]."

În viziunea legiuitorului european[29], persoana vizată are dreptul de a i se asigura ștergerea datelor și neprelucrarea acestora, dacă informațiile nu și-au pierdut din relevanță, nu sunt actuale ori consimțământul asupra publicării acestora a fost retras. Cu titlu de exemplu,dreptul de a fi uitat prezintă o importanță crescută în situația în care informațiile publicate se referă la o persoană lipsită de capacitate de exercițiu și în necunoștință de cauză în ceea ce privește efectele publicării unor astfel de date.

Prevederea din Regulament dezvoltă noțiunea dreptului la ștergerea datelor instituit prin Directivă[30], stabilind condițiile care stau la baza dreptului de a fi uitat, inclusiv obligația operatorului de a informa terții în ceea ce privește cererea persoanei vizate privind ștergerea adreselor web către pagini care conțin informații personale sau orice copie ori reproducere a acestora.

Măsura de ștergere a datelor nu se aplică în situația în care prelucrarea este necesară pentru: „(a) […] exercitarea dreptului la liberă exprimare și la informare, (b) [...] respectarea unei obligații legale care

[29]A se vedea p. 65 și 66 din Preambulul Regulamentului general privind protecția datelor.

[30]Memorandum, Propunere de Regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date (Regulament general privind protecția datelor) / COM/2012/011 final – 2012/0011(COD), [Online] la www. eur-lex.europa.eu, accesat 3.10.2017.

prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului ori pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul, (c) din motive de interes public în domeniul sănătății publice […], (d) în scopul de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori pentru scopuri statistice […] sau (e) pentru constatarea, exercitarea ori apărarea unui drept în instanță".

Dreptul de a fi uitat este abordat într-un mod deosebit în ceea ce privește protejarea vieții private. Sfera de aplicare depinde de o definiție clară și consistentă a noțiunii de *date personale*. În cea mai simplă formă a sa, acest drept sugerează proprietatea persoanei vizate asupra datelor sale cu caracter personal și implică un oarecare grad de drept-control al individului asupra informațiilor, întrucât el decide ce se întâmplă cu acestea[31]. Acest drept este un prim pas spre consolidarea controlului persoanei vizate asupra propriilor date, individul nemaiavând doar posibilitatea, ci dreptul de a-și retrage acceptul privind procesarea informațiilor[32].

Diverse raționamente stau la baza dreptului la ștergerea datelor. Unul dintre acestea este ideea de reabilitare[33] – noțiune ce poate fi privită atât din perspectiva individului, cât și ca un interes social[34]. Faptul că persoanele vizate au dreptul la o a doua șansă – ștergerea informațiilor despre ei – după o perioadă de timp, nu este o idee nouă. Dreptul de a fi uitat nu este doar despre eliminarea datelor privind datoriile anterioare sau faptele prevăzute de legea penală. Se consideră că oamenii au un interes legitim și moral de a se distanța de greșelile și erorile comune. Argumentele în acest sens au în vedere faptul că, de cele mai multe ori, Internetul este descris ca având *memorie de fier*, iar ușurința cu care datele digitale pot fi căutate, accesate și utilizate a determinat îngrijorarea în legătură cu necesitatea protejării, mai ales a tinerilor, împotriva indiscrețiilor sau a lipsei de

[31]J. Ausloos, *op. cit.*, p. 144.

[32]A se vedea discursul Comisarului European pentru Justiție, V. Reding, *Your data, your rights: Safeguarding your privacy in a connected world*, Bruxelles, 16 martie 2011, [Online] la http://europa.eu/rapid/press-release_SPEECH-11-183_en.htm, accesat 4.10.2017.

[33]*Melvin v. Reid* (1931) 122 Cal. App. 258, [Online] la www.casetext.com/case/melvin-v-reid, accesat 8.10.2017.

[34]S. C. Bennett, *The Right to be forgotten: Reconciling EU and US perspective*, în Revista de Drept Internațional de la Berkeley, nr. 1, vol. 30 din 2012, p. 170, [Online] la www.scholarship.law.berkeley.edu, accesat 10.10.2017.

discernământ, după caz. Faptul că oamenii se pot schimba este principala idee a reabilitării, sugerând totodată și o interpretare neexhaustivă a dreptului de a fi uitat.[35]

Regulamentul general privind protecția datelor este limitat și lacunar raportat la aspectul teritorialității și aplicabilității acestuia. Ceea ce caracterizează Internetul este tocmai faptul că informația circulă între servere, putând fi accesată din orice loc, în orice moment. Astfel, deși utilizatorului de Internet i s-au șters datele, acestea nemaiputând fi accesate de pe teritoriul Uniunii Europene, nimic nu împiedică ca acestea să fi fost prelucrate, utilizate și readuse în circuit de către operatori de date care utilizează servere din state terțe. Încetarea contractului de *cloud computing* nu oferă siguranța că informațiile au fost șterse și persoana fizică a fost „uitată" de pe Internet și din cloud.[36]

Art. 17 din Regulament nu răspunde unor situații care în practică ar putea provoca controverse. În primul rând, este posibil ca operatorul de date să nu cunoască sau să se afle în neputința de a contacta terții. În al doilea rând, există posibilitatea ca terții să aibă la îndemânăalte instrumente juridice privind legalitatea procesării datelor astfel încât ștergerea informațiilor să nu fie eficace față de ei, chiar dacă este realizată de către operator. În al treilea rând, în cazul în care datele revin în atenția publică, este neclar cine trebuie să răspundă pentru acest lucru: operatorul sau utilizatorul.

Dreptul de a fi uitat reprezintă un instrument juridic pentru a proteja persoana vizată de utilizarea ilicită a datelor sale. O dată ce persoana și-a dat acordul pentru prelucrarea informațiilor de către operator, este destul de dificil de a redobândi controlul asupra acestora. Astfel, acest drept vine să restaureze acest control, oferindu-i persoanei vizate posibilitatea de a decide cine poate procesa și ce date pot fi procesate cu acordul său[37].

---

[35]A. Bunn, *The curious case of the right to be forgotten*, în Computer Law & Security, nr. 31/2015, p. 340, [Online] la http://sciencedirect.com, accesat 12.10.2017.

[36]Pentru detalii privind contractul de *cloud computing*, a se vedea C.T. Ungureanu,*Contractul Cloud Computing în comerțul internațional*, în Revista Moldovenească de Drept Internațional și Relații Internaționale, nr. 3(37), 2015, p. 25-35, [Online] la http://rmdiri.md/wp-content/uploads/2015/01/RMDIRI-Nr.-3-20159.pdf.

[37]C. Bartolini, L. Siry, *The right to be forgotten in the light of the consent of the data subject*, în Computer Law & Security, nr. 32/2016, p. 229-230, [Online] la http://sciencedirect.com, accesat 12.10.2017.

De asemenea, trebuie avut în vedere faptul că informațiile, mai ales în perioada contemporană, reprezintă putere socială și, în multe cazuri, și putere economică. Marile companii încearcă să promoveze ideea că publicarea datelor este o normă socială și că viața privată este un concept depășit. În același timp, aceleași persoane juridice colectează cantități uriașe de informații în vederea realizării profilurilor indivizilor și pentru a extrage informațiile necesare pentru a-și asigura progresul. Astfel, sunt utilizate aceste informații pentru a îmbunătăți produsul sau serviciul oferit unei anumite categorii de consumatori stabilite în urma unei cercetări de piață și prin filtrarea și interpretarea rezultatelor obținute din colectarea informațiilor cu caracter personal. În acest context, este necesară protejarea libertății de exprimare și a datelor personale[38].

Plecând de la premisa că *Internetul este pentru totdeauna*, ne punem totuși întrebarea ce se întâmplă cu datele după ce sunt șterse. Orice informație încărcată pe rețea, indiferent de forma aleasă de utilizator (*e.g.* simple cuvinte sub forma unor mesaje, imagini, informații audio-video ș.a.) circulă, Internetul devenind astfel un instrument viu al cărui conținut este în permanență reînnoit. De asemenea, nu există granițe, limita teritorială reprezentând doar limita accesului la serverele sau cloud-ul care stochează inițial informațiile. Internetul, în denumirea sa generică, este o rețea globală caracterizată prin interconectivitate, astfel încât odată intrate, datele ajung să fie stocate și de alte servere și prelucrate de operatorii de date care au acces la rețea. Cu toate acestea, accesul la datele personale în acest context poate fi limitat[39] doar în anumite situații.

Așadar, în sensul noii reglementări, datele șterse nu mai pot fi accesate, însă Regulamentul nu prevede și nici nu răspunde ipotezelor referitoare la informațiile accesate din spațiul exterior întinderii teritoriale a serverelor și revenirea datelor în spațiul european sub o altă formă, având în vedere neîntrerupta circulație a informațiilor pe Internet. Iar un cadru legal pentru situația în care datele cu caracter personal sunt disponibile pentru prelucrare după ce au fost șterse de pe un anumit server încă nu a fost

[38]A. Mantelero, *The EU proposal for a general data protection regulation and the roots of the right to be forgotten*, în Computer Law & Security, nr. 29/2013, p. 234-235, [Online] la http://sciencedirect.com, accesat 12.10.2017.

[39]De exemplu, anumite site-uri pot fi accesate doar într-un anumit stat sau în anumite state, accesul fiind posibil doar pentru rezidenții respectivi care accesează Internetul în limita spațiului acoperit de serverele statului.

realizat. În acest sens, pot fi anticipate anumite ipoteze problematice: în primul rând, verificarea compatibilității și asemănarea datelor șterse cu informațiile reintroduse în rețea pentru a stabili dacă acestea au făcut obiectul unei cereri de ștergere a datelor în sensul Regulamentului sau dacă sunt informații noi;în al doilea rând, stabilirea persoanei responsabile pentru realizarea acestei operațiuni și dacă aceasta intră în atribuțiile autorității naționale; în al treilea rând, obligativitatea aducerii la cunoștința persoanei vizate despre revenirea datelor în rețea și disponibilitatea acestora către public și dacă este cazul, momentul în care date au fost șterse cu adevărat și nu doar restricționate[40]și nu în ultimul rând, necesitatea formulării unei noi cereri de ștergere a datelor cu caracter personal de către persoana vizată.

4. Alte reprezentări ale dreptului la ștergerea datelor în acte ale Uniunii Europene

Ținând cont că datele cu caracter personal sunt utilizate în diverse domenii de activitate, este de așteptat ca instituțiile Uniunii Europene să aibă în vedere prelucrarea și protejarea acestora și în alte acte normative.

Este de remarcat că în domeniul cooperării polițienești și judiciare în materie penală[41], ștergerea datelor cu caracter personal este abordată diferit. Acestea sunt șterse dacă nu mai sunt necesare scopului pentru care au fost colectate sau dacă prelucrarea lor a fost suplimentară, în mod legal. De asemenea, se stabilește ca modalitate de ștergere distrugerea suportului de date, conform considerentului numărul 14 al Deciziei-Cadru 2008/977.Însă printre prevederile cele mai interesante se numără întocmai obligarea la stabilirea unor „termene corespunzătoare pentru ștergerea datelor cu caracter personal sau pentru o revizuire periodică a necesității de stocare a datelor”, potrivit art. 5 din Decizia-Cadru 2008/977, aspect ce ar trebui avut în vedere și în noua reglementare în domeniul protecției datelor. Același principiu se

[40]De exemplu, conform termenilor și condițiilor Facebook, deși datele sunt șterse de utilizator ori la cererea acestuia, o copie a acestor informații este păstrată în baza de date pentru o perioadă de timp nelimitată, dar rezonabilă, nedisponibilă terților, fără să fie definită noțiunea de *timp rezonabil* ori să se specifice dacă persoanei vizate îi este adus la cunoștință momentul în care copia de rezervă a fost ștearsă.

[41]Decizia-Cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală, publicată în J.O., L 350 din 30 decembrie 2008.

regăsește și în negocierea cu state terțe[42], urmărindu-se, prin aplicarea acordului cu acestea, efectuarea periodică a unei evaluări pentru identificarea datelor care nu mai sunt necesare și ștergerea acestora.

Ștergerea datelor în situația în care prelucrarea lor este ilegală, mai ales dacă este pusă la îndoială calitatea informațiilor sau a mijloacelor de prelucrare, este, de asemenea, avută în vedere și în cazurile în care prelucrarea datelor cu caracter personal este realizată de către instituțiile și organele comunitare[43].

Într-o propunere de directivă[44] s-a urmărit o alternativă temporară a ștergerii informațiilor prin marcarea datelor cu caracter personal în anumite situații: (i) este contestată exactitatea informațiilor, operatorul având la dispoziție o perioadă pentru verificarea datelor; (ii) acestea trebuie păstrate ca dovadă și (iii) persoana vizată alege restricționarea utilizării informațiilor și se opune ștergerii, conform articolului 16.Într-o manieră similară, această alternativă este prezentă în Directiva 2016/680[45].Operatorul de date are obligația de a șterge informațiile, garantând acest drept al persoanei vizate. În loc de ștergere, acesta poate restricționa datele a căror exactitate ce nu poate fi stabilită cu certitudine este contestată de persoana vizată sau dacă informațiile trebuie păstrate ca mijloace de probă.

[42]A se vedea Decizia Consiliului privind încheierea Acordului dintre Uniunea Europeană și Statele Unite ale Americii privind prelucrarea și transferul datelor de mesagerie financiară din Uniunea Europeană către Statele Unite ale Americii în cadrul Programului de urmărire a finanțărilor în scopuri teroriste (2010/412/UE), publicat în J.O., L 195 din 27 iulie 2010.

[43]Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date, publicat în J.O., L 8 din 12 ianuarie 2001.

[44]Propunerea de Directivă a Parlamentului European și a Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, identificării, investigării sau a urmăririi penale a infracțiunilor sau al executării pedepselor și la libera circulație a acestor date/*COM/2012/010 final – 2012/0010 (COD)*/, [Online] la http://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52012PC0010&from=en.

[45]Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau a urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, publicată în J.O., L din 4 mai 2016.

5. Concluzii

Existența și reglementarea dreptului la ștergerea datelor în noile reglementări la nivel european arată o preocupare evidentă a autorităților și instituțiilor europene pentru drepturile persoanei fizice privind prelucrarea datelor sale cu caracter personal, respectarea acestui drept înclinând balanța către cetățean și oferindu-i cu adevărat puterea și instrumentele necesare de a-și proteja informațiile și totodată și libertatea de a dispune de acestea în mediul public oferit de Internet, după cum dorește. Sunt șterse, în principiu, doar datele pe care persoana vizată le consideră a fi neadecvate sau irelevante.

Acest drept ajută la redefinirea unui comportament al persoanei vizate față de propriile sale date, acesta având posibilitatea de a-și evalua și reevalua informațiile cu caracter personal disponibile publicului, fiindu-i astfel amplificat controlul asupra identității sale.

Dreptul de a fi uitat, în forma impusă de Regulamentul general privind protecția datelor, reprezintă un model pentru statele terțe având în vedere că acesta, prin însăși existența sa, reformează întreaga atitudine a utilizatorilor de Internet privind informațiile care îi privesc.

Urmând modelul Google, multe entități cu domenii atât în spațiul european, cât și în afara acestuia, care prelucrează datele cu caracter personal în mediul online vor respecta legislația nouă și vor răspunde în mare măsură cererilor de ștergere a datelor, însă întrebarea este dacă acestea vor fi dispuse să renunțe doar la o parte semnificativă sau la tot conținutul activității lor de prelucrare. Cel mai probabil o decizie a Curții de Justiție a Uniunii Europene în acest sens va influența considerabil abordarea operatorilor și relația utilizator – furnizor de servicii online, precum și numărul acțiunilor în justiție a persoanelor fizice în vederea protejării datelor lor cu caracter personal.