

VIITORUL IDENTITĂȚII ÎN SOCIETATEA INFORMAȚIONALĂ

THE FUTURE OF IDENTITY IN THE INFORMATION SOCIETY

George NICULESCU

Professor PhD - "CONSTANTIN BRÂNCUȘI" UNIVERSITY OF TÂRGU JIU
e-mail: gniculesco@yahoo.com

Abstract: *The digitization of ever-increasing information has led to an Information Society, where more and more information is available almost anywhere, anytime.*

In the information society, identity becomes a major issue.

The development of the information society is closely linked to the evolution of the ICT industry and to the diffusion of ICT in everyone's lives. Identifying customers and knowing their identity attributes is increasingly becoming a major asset for organizations.

Knowledge about customer identity will play a major role in future value creation processes. Identity management is becoming increasingly important.

With the growing importance of identities and identity management in the information society, identity criminality is also growing. Combating crimes such as identity theft and identity fraud is a major challenge for policy-makers.

Ciber-identity is characterized by fluidity and uncertainty.

Checkpoints, control, accountability and sanctioning in virtual space are reduced or even lacking.

Substitution of identity and multiple identities turns virtual space into an unsafe and unpredictable environment.

Keywords: *identity, identity management, virtual world, digitization.*

INTRODUCERE

Conceptul de *identitate* este tot mai vehiculat în limbajul modern. Adesea întâlnim lucrări, articole ori diverse studii focusate pe acest subiect.

Științele politice și sociologia tratează identitatea socială ca pe o caracterizare personală a individului care aparține unor grupuri particulare, cu referire la naționalitate, clasă socială,

subcultură, apartenență etnică, etc., totul analizat prin prisma modificărilor istorice și a circumstanțelor culturale. Filosofia definește identitatea ca fiind acel concept ce o entitate, făcând-o recunoscutibilă, cu referire la o serie de caracteristici care o fac diferită de alte entități distincte.

Științele logicii definesc identitatea ca pe o relație între o entitate și ea însăși.

Este nevoie de o abordare multidisciplinară pentru a explica conceptul identității în spațiul digital. Ne concentrăm asupra următoarelor aspecte: conceptualizarea spațiului digital ca o lume digitală constituită de digital și de discursul digi-participanților; ciber-limbaj; practici online de numire și nume utilizate pe internet; construirea ciber-identității/identităților în diferite spații digitale. Ne îndreptăm atenția asupra modului în care utilizatorii exprimă/construiesc ciber-identități prin conținutul exprimat (identitate narativă) și prin comportamentul lingvistic.

Menținerea în afara conectării la rețeaua de informații mondială nu mai este posibilă. Învățământul în general, și cel superior în special, datorită ritmului deosebit de dezvoltare are nevoie de sisteme deschise. Pentru realizarea acestor sisteme deschise este nevoie de utilizarea în comun a resurselor existente și de asigurarea compatibilității dintre diferite sisteme informatice.

Pentru a avea acces la informațiile din mediul virtual (mai ușor de utilizat și din ce în ce mai variate și complexe) este nevoie de a face parte din comunitatea virtuală care le administrează. Resursele tehnologice devin, în condițiile societății informatizate, un act de identitate pentru orice organizație, comunitate sau țară¹. În spațiul digital, utilizatorii își exprimă identitatea sau își asumă o altă identitate.

Inițiativa *i2010 a* reprezintă un pachet de politici proactive menite a stimula potențialul unei economii electronice de a furniza creștere economică, locuri de muncă și servicii publice electronice, fiind considerată o adevărată 'locomotivă' a procesului de realizare a Strategiei de la Lisabona. Inițiativa *i2010 a* cuprinde trei direcții majore de acțiune: crearea instrumentelor normative (legislație) necesare societății electronice, stimularea puternică a cercetării și dezvoltării în domeniu și crearea unei societăți informaționale (*eEurope*) accesibile tuturor, în special prin furnizarea de servicii publice electronice, cu accent pe administrația electronică, sănătatea electronică, învățământul electronic și afacerile electronice.

¹ Kai. Rannenberg et al. Editors, *The Future of Identity in the Information Society*, Springer-Verlag Berlin Heidelberg, 2009, p. 22

Importanța guvernării electronice și a desfășurării serviciilor electronice în toată Uniunea Europeană este subliniată și de programul *eTEN* (eTransEuropean Network).

În mediul electronic se formează adevărate comunități virtuale bazate pe o formă sau alta de rețea socială². Întâlnim identități în spații digitale pe rețelele online de socializare ((*Facebook, Couchsurfing, BeWelcome, MySpace, LinkedIn*), e-mail și servicii chat (G-mail și Yahoo), bloguri și platforme de jocuri (*Catan, Conquiztador.ro/com*).

Lumile virtuale și studiul acestora dezvoltă noi discipline ce vor dobândi tot mai multă rigoare științifică, adunând elemente din sociologie, psihologie, economie și suprapunându-le peste științele exacte cum ar fi matematica și fizica.

O mare parte a acestor informații este controlată în exterior: de către guverne sau instituții, cum ar fi birourile fiscale, organizațiile de asistență medicală, companiile (de exemplu compania care angajează persoana sau banca ei); de către entitățile comerciale (cum ar fi firmele de marketing) sau prin "opinia publică" (ziarele sau rețelele informale). Găsirea unor modalități mai bune de a restricționa o entitate externă de a stoca, manipula și exploata informații personale poate ajuta la rezolvarea acestei probleme.

Unele mecanisme (juridice, tehnice etc.) pot fi folosite pentru a aplica bunele practici atunci când o entitate (guvernamentală, comercială etc.) gestionează informații personale, cum ar fi definirea informațiilor pe care o anumită categorie de entități are dreptul să le stocheze, precum și modul în care aceste informații pot fi exploatare. De exemplu, companiilor li se poate interzice stocarea informațiilor medicale, poliției i se poate interzice accesul la informații medicale, iar comerțul cu anumite liste de clienți poate să nu fie permis. Pentru acest scop ar putea fi utilizate mecanisme diverse (juridice, tehnice, educaționale etc.) sau o combinație de mecanisme. În domeniul dreptului, este important de remarcat faptul că SUA și Europa au adoptat abordări diferite în această privință, SUA renunțând la reglementarea unor astfel de probleme în mare măsură la întreprinderile private (elaborarea de coduri de conduită, bune practici etc.), în timp ce Europa a încercat să legifereze această problemă.

Modelul identități adevărate, identității atribuite și identității abstractizate

² Ibidem, pp. 35-39

În acest model, Andre Durand³ distinge trei categorii (sau niveluri) de identități:

- Nivelul 1: Identitatea personală (identitatea interioară și atemporală). Aceasta este adevărata identitate personală care este deținută și controlată în întregime de către persoană.

- Nivelul 2: identitatea corporativă (identitatea atribuită). Această identitate se referă la un anumit context (de exemplu, o relație de afaceri) și reprezintă o caracteristică temporară atribuită sau eliberată persoanei, cum ar fi: un anumit post, un număr de telefon etc.

- Nivelul 3: identitatea de marketing (identitatea abstractizată sau agregată). Acest identitatea este mai difuză și corespunde unui anumit rezultat al profilării. Un exemplu ar putea fi: "clientul care aparține unei categorii sociale" de nivel superior, de vârstă mijlocie, având o mașină mai veche de cinci ani, care trăiește într-unul din orașele mari din vestul țării și care este contactat de un agent de vânzări.

Conceptul de identitate introduce mai multe caracteristici pentru identitate: temporalitatea, condiționalitatea și concretețea sa. Astfel, identitatea personală reprezintă o proprietate inerentă a persoanei și este atât atemporală, cât și necondiționată. Identitatea corporativă este, dimpotrivă, condiționată și temporară și există într-un anumit context.

Această identitate ulterioară poate fi de asemenea considerată atașată unei persoane, mai degrabă decât a fi parte a persoanei.

Aceste proprietăți ale temporalității și condiționalității sunt importante în contextul gestionării identității, deoarece permite o distincție între cele două fațete care pot fi gestionate diferit.

Prima este foarte importantă pentru persoana respectivă și ar trebui, prin urmare, să fie controlată cât mai mult posibil de acea persoană (sau de entități terțe de încredere) și puternic protejată. Într-adevăr, amenințările cu privire la această identitate "omniprezentă" (intervine în multe aspecte ale vieții unei persoane) vor avea unele consecințe mai grave pentru persoana respectivă, deoarece ea ar putea avea un impact potențial asupra multor părți din viața ei și pentru o lungă perioadă de timp. De exemplu, cel care fură identitatea personală (făcută în scopul efectuării de acțiuni ilegale) are un impact asupra reputației victimei, care poate avea

³ A, Durand, (2002), *Three Tiers of Identity*, Digital Identity World, March 16, 2002, apud *The Future of Identity in the Information Society*, Editors Kai Rannenberg Denis Royer André Deuker, Springer-Verlag Berlin Heidelberg 2009

consecințe asupra muncii ei (interzicerea accesului la anumite locuri de muncă), a vieții ei sociale (izolarea persoanei în societate) sau viața personală a acestuia (distrugerea încrederii în familie sau în cercul prietenilor).

A doua identitate este mai mult legată de rolul persoanei într-o anumită situație și poate fi supusă mai mult controlului de către o terță parte. În plus, aspectul critic al protejării individului cu gestionarea acestei identități poate fi orientat spre transparență și responsabilitate, mai degrabă decât spre confidențialitate. Acest lucru ar putea fi relevant pentru atenuarea responsabilității individului, de exemplu în cazul acțiunilor efectuate ca reprezentant al unei organizații și pentru izolarea reprezentării acestei identități într-un anumit domeniu.

Digitalizarea informațiilor în continuă creștere a dus la o Societate Informațională, în care tot mai multe informații sunt disponibile aproape oriunde și oricând.

Internetul a deschis noi spații pentru viața (virtuală și suplimentară), așa-numitele identități virtuale, create din motive de siguranță, profit, confort sau chiar distracție (de exemplu, pentru comunitățile de agrement). Ceea ce a fost o identitate "naturală" este acum la fel de virtuală ca un cont de utilizator la un portal web, o adresă de e-mail sau un număr de telefon mobil. Aceste identități virtuale și multiple, precum și paradigmele din spatele lor se hrănesc în lumea "fizică", oferind un amestec de identități și procese pluraliste fizice și virtuale. Identitatea într-o lume în schimbare⁴.

În societatea informațională identitatea devine o problemă de discuții și uneori conflicte majore. Una dintre întrebările de bază este dacă entitățile au o singură identitate sau mai multe identități (parțiale).

Identitatea unică (continuă) a fost văzută de mult timp ca un semn al integrității caracterului și al sănătății personalității: în contrast, o criză de identitate este diagnosticată, atunci când un individ își pierde simțul identității personale și continuitatea istorică. Multe repere ale dezvoltării sociale au apărut odată cu schimbările majore ale economiei. Dezvoltarea societății informaționale este strâns legată de evoluția industriei TIC și de difuzarea TIC în viața

⁴ David-Olivier Jaquet-Chiffelle, *Virtual Persons and Identities*, apud Kai. Rannenberg et al. Editors, *The Future of Identity in the Information Society*, Springer-Verlag Berlin Heidelberg, 2009, pp 76-79

fiecăruia. Identificarea clienților și cunoașterea atributelor lor de identitate devine din ce în ce mai mult un avantaj major pentru întreprinderi. În funcție de zona de afaceri și modelul de afaceri, rolul identității poate fi diferit în procesul de creare a valorii. În mod tradițional, identificarea și identitatea joacă un rol major în procesul de plată, de exemplu, pentru a evalua bonitatea clienților. Cunoștințele despre identitatea clienților au fost întotdeauna o parte centrală a programelor de relații cu clienții. În zilele noastre, în plus față de aplicațiile clasice, attributele de identitate sunt din ce în ce mai utilizate pentru a vinde sau crea mai bine produse în lumea online:

- comercianții online cu amănuntul folosesc preferințele clienților pentru a recomanda bunuri și servicii.
- Publicitatea individualizată în rețelele și comunitățile sociale se bazează pe attributele de identitate stocate în profilurile utilizatorilor.
- Tarifarea automată a bunurilor și serviciilor în funcție de identitatea clienților.

Cunoștințele despre identitatea clienților vor juca un rol major în procesele viitoare de creare a valorii. Manipularea identităților într-un mod adecvat pentru a preveni invazia zonelor private ale clienților va fi o provocare majoră pentru întreprinderi de a menține vie relația cu clienții lor.

Managementul identității devine din ce în ce mai important. Managementul identității nu este o soluție simplă, ci un cadru complex de tehnologii și funcții diferite. Prin urmare, la introducerea acestuia, organizațiile suportă o varietate de costuri pentru implementare și pentru problemele organizaționale, cum ar fi integrarea proceselor și tehnologiilor⁵.

Criminalitatea legată de identitate și criminalistica

Odată cu importanța crescândă a identității și a managementului identității în societatea informațională, criminalitatea legată de identitate este, de asemenea, în creștere. Combaterea unor infracțiuni precum furtul de identitate și fraudarea identității, nu în ultimul rând cu ajutorul medicinei de identitate, reprezintă o provocare majoră pentru factorii de decizie politică.

⁵ Kai. Rannenberget al., op. cit pp. 36-40

Pentru a înțelege natura infracțiunilor legate de identitate, este util să realizăm că există cazuri legale și ilegale în care apare un fel de nepotrivire între identificator și identitate.

Publicarea sub un pseudonim, de exemplu, este o practică larg acceptată, dar diminuarea contului bancar de către o persoană care se substituie identității deținătorului contului fără consimțământul lui nu este legală. În consecință, o taxonomie ar trebui să includă categorii de neconcordanțe între identificator și identitate care acoperă atât identitatea intenționată, cât și cea neintenționată și legală, precum și pe cea ilegală. Neconcordanța dintre identificator și individ poate fi înțeleasă independent de intenția criminală. În multe cazuri, discrepanța se întâmplă de fapt neintenționat sau accidental.

Coliziunea de identitate ⁶

Atunci când coliziunea rămâne nedescoperită și este provocată deliberat, coliziunea de identitate se poate transforma în schimbarea identității. Schimbarea identității este tipul cel mai strâns legat de noțiunile de fraudă de identitate și de "furt de identitate", în care un identificator fals este legat în mod intenționat de o persoană. În concluzie, putem distinge patru tipuri de probleme legate de legătura dintre identificator și individ.

- Coliziunea de identitate: o legătură greșită este făcută accidental între identificator și individ.

- Schimbarea identității: o legătură greșită este făcută intenționat între identificator și individ (identificatorul poate fi un identificator pentru un individ existent sau unul nou creat.)

- Obstrucția identității: un identificator legat de un anumit individ este, intenționat sau în mod accidental, șters de către sine sau altcineva (ștergerea identificatorului) sau nu se realizează legătura dintre individ și identificator printr-un act intenționat sau accidental (obstrucție de identificare).

- Restaurarea identității: un identificator șters este, de obicei intenționat, restabilit de către individ sau de către altcineva sau este restabilită legătura dintre identificator și individ.

⁶Kai. Rannenberg et al.*op. cit.* pp. 317-320

Obstrucția identității

Accentul se pune pe criminalitatea legată de identitate: conceptele și tehnicile implicate, precum și măsurile juridice, organizaționale și tehnice de combatere a infracțiunilor în care identitatea este utilizată ca instrument principal. Identificarea autorilor este una din funcțiile-cheie ale criminalității și, având în vedere importanța din ce în ce mai mare a managementului identității în societatea informațională, criminalistica legată de identitate devine un domeniu foarte important de studiu. O aplicație specială este profilarea criminalistică, în care sunt folosite urme pentru a desena profile care sunt relevante pentru susținere diverse sarcini de securitate, în special în sistemul de justiție penală⁷.

Crima legată de identitate și implicațiile acesteia pentru criminalistică, precum și profilul criminalistic, se dezvoltă pe tehnologii și proceduri de identificare, care au devenit din ce în ce mai variate și mai complexe odată cu apariția societății informaționale. Deficiențele în procedurile de identificare care permit criminalitatea asociată identității sunt la fel de relevante pentru a fi conștiente de criminalistica în materie de identitate, în cazul în care dovezile despre cine a săvârșit o infracțiune sau delictuală pot depinde în mod crucial de legătura dintre urme de dovezi și un anumit individ. În mod deosebit într-un mediu digital, stabilirea legăturii dintre identificatori și individ este departe de a fi ușoară. Cunoașterea detaliată a tehnologiilor implicate este crucială, dar nu este suficientă. La fel de importante sunt o bună înțelegere a procedurilor de identificare, a contextului organizațional al măsurilor de identificare, precum și a contextului juridic.

Concluzii

Multiplele identități ale persoanei sunt impuse în procesul de digitalizare, în continuă dezvoltare, care creează noi posibilități de acces la diferite domenii ale lumii virtuale.

Identitățile digitale sunt forme incomplete ale identității înțelese în sens clasic, realizându-se doar prin simpla aderare la grupul/comunitatea virtuală.

⁷*Ibidem*, . pp. 134-136

Identitățile digitale sunt ușor dobândite (doar prin înscrierea unor date, de cele mai multe ori false, prin care se face identificarea și diferențierea față de ceilalți membri ai comunității virtuale), dar la fel de facil de renunțat la ele.

Aceste identități nu sunt limitate, ceea ce permite unei persoane să dobândească identități multiple. De fapt, spațiul virtual nu permite să ai aceeași identitate în comunități virtuale diferite.

Ciber-identitatea este caracterizată prin fluiditate, incertitudine și joc constant. Mai mult, susținem că identitatea este un amestec cu două intrări: exprimare (input 1) și construire (input 2). În afara spațiului digital, de obicei, domină primul input, iar al doilea domină de cele mai multe ori în spațiul digital. De aceea, este justificată utilizarea conceptului de identitate fluidă.

Posibilitățile de verificare, control, responsabilizare și sancționare în spațiul virtual sunt reduse sau chiar lipsesc.

Substituirea identității și identitățile multiple transformă spațiul virtual într-un mediu nesigur și imprevizibil.

Există o permanentă dispută între cei predispuși să încalce regulile spațiului virtual și cei responsabilizați să-l reglementeze legal.

Bibliografie

1. Ashley, P., Hada, S., Karjoth, G., Powers, C., Schunter, M. (2003), '*Enterprise Privacy Authorization Language (EPAL)*', IBM Research, url: <http://www.zurich.ibm.com/security/enterprise-privacy/epal/specification>.
2. Bennett, K. and Grothoff, C., *GAP – Practical Anonymous Networkin*, Proceedings of the Privacy Enhancing Technologies Workshop (PET), 2003
3. Casassa Mont, M., Pearson, S., Bramhall, P., *Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services*, Proceedings of the 14th International Workshop on Database and Expert Systems Applications, 2003
4. Durand A., *Three Tiers of Identity*, Digital Identity World, March 16, 2002,
5. Rannenber Kai et al. Editors, *The Future of Identity in the Information Society*, Springer-Verlag Berlin Heidelberg, 2009

6. Pfitzmann, A. and Hansen, M. (2009), *Anonymity, unobservability, and pseudonymity: A proposal for terminology*, in: Federrath, H. (ed.), *Designing Privacy Enhancing Technologies (PET'00)*, LNCS vol. 2009,
7. Pretschner, A., Hilty, M., Basin, D., Schaefer, C., Walter, T. *Mechanisms for Usage Control*, Proceedings of the ACM Symposium on Information, Computer & Communication Security (ASIACCS '08), 2008
8. Sackmann, S., Strüker, J., Accorsi, R., *Personalization in Privacy-Aware Highly Dynamic Systems*, Communications of the ACM, 2006
9. Wohlgemuth, S., *Privatsphäre durch die Delegation von Rechten*, Ph.D. thesis at the University of Freiburg, Germany, 2008.