

Datele cu caracter personal: *res digitalis* în sfera actelor încheiate *inter vivos* și a actelor *mortis causa*

Personal Data: *res digitalis*, Object of Acts Concluded *inter vivos* and of Acts Concluded *mortis causa*

Crina-Maria STANCIU¹, Codrin-Alexandru ȘTEFĂNIU²

Rezumat: Această prezentare își propune să exploreze echilibrul complex dintre valorificarea potențialului AI pentru progresul societății și abordarea implicațiilor etice ale utilizării datelor. În zilele noastre, datele sunt adunate și se stochează informații despre utilizatori, procedeu care trebuie să respecte un set de legi foarte specifice. Acest lucru dă putere cercetătorilor din domeniul AI să-și antreneze modelele fără a le alimenta cu date decriptate de utilizator. Dar cine decide cum să folosească datele? În prezent, majoritatea companiilor care colectează informații de la clienții lor trebuie să urmeze un set de directive ale Comisiei UE. Prin urmare, evoluția inteligenței artificiale nu ar însemna invadarea intimității personale. În această lucrare sperăm să creștem necesitatea tratării datelor ca obiect legal cărui i se vor aplica reguli reinterpretate, conform fluxului de dezvoltare a AI. Ne vom concentra mai mult asupra conținutului datelor și asupra momentului în care datele ar putea fi stocate și transferate ca urmare a creșterii valorii lor (valoare economică). Datele sunt un activ care poate fi tranzacționat. De asemenea, datele pot ajuta la crearea unei personalități a utilizatorilor (de aceea valoarea datelor poate crește). O altă întrebare la care vom încerca să răspundem se referă la conceptul de „moștenire digitală” și datele post-mortem. După ce o persoană moare, ce se va întâmpla cu forma sa digitală, cum ar fi banii digitali (bitcoin sau active câștigate într-un joc), cu contul de Facebook, contul Google etc.? Datele personale ale omului vor crea oameni artificiali care vor supraviețui morții naturale?

Cuvinte cheie: IA, *machine learning*, acte *inter vivos*, acte *mortis causa*, proprietate.

Abstract: This presentation aims to explore the intricate balance between harnessing the potential of AI for societal advancement and addressing the ethical implications of data utilization. Nowadays data centers where user information is stocked must follow a very specific set of laws. This empowers researchers in the field of AI to train their models without feeding them with decrypted user data. But who decides how to use the data? Currently most companies that gather information from their customers must follow a set

¹ Drd., Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iași, e-mail: crina.stanciu@uaic.ro.

² Inginer software, e-mail: codrinstefaniu36@gmail.com.

of directives from the EU Commission. Therefore, the evolution of the artificial intelligence would not mean the invasion of personal privacy. In this paper we hope to increase the necessity of treating data as legal object to which will apply reinterpreted rules, according to the flow of AI development. We will focus more on the content of data and to the moment when the data might be stored and transferred because of its increasing value (economic value). Data is an asset who can be traded. Also, data can help to create a personality of the users (this is why the value of data can increase). Another question we will try to answer concerns the concept of „digital estate” and postmortem data. After a person dies what will happen with its digital form like digital money (bitcoin or assets won in a game), with the Facebook account, Google account etc.? Data from people will make artificial people who will survive the natural death?

Keywords: AI, *machine learning*, acts *inter vivos*, acts *mortis causa*, property.

1. Introducere

În vederea încadrării datelor cu caracter personal în sfera bunurilor asupra cărora persoana dobândește dreptul de proprietate, vom desluși, înainte de toate sensul acestora, folosind art. 4 al General Data Protection Regulation (Regulamentul UE 2016/679 GDPR):

„«date cu caracter personal» 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.”³.

Datele cu caracter personal decurg din principalele caracteristici ale persoanei. Prin difuzarea acestora pe calea internetului s-a ajuns la crearea unor noi tipuri de comerț. De această dată comerțul implică transferul de date personale, fapt care se traduce prin transferul de informații cu privire la persoane, transfer care operează, de cele mai multe ori, dintr-un capăt al lumii în celălalt.

O problemă aparține survine la momentul în care se analizează și se transferă colecțiile de date denumite și „big data”. Astfel, într-o primă fază datele sunt adunate de către o organizație fie pe cale directă (fiind obținute direct de la persoanele vizate prin variate chestionare adresate în mediul on-line), fie pe cale indirectă (prin intermediul brokerilor de date personale) sau prin combinarea unor date deja dobândite. O a doua fază are în vedere analizarea datelor în vederea obținerii de cunoștințe, de informații (analiză realizată prin tehnici *machine learning*). În final, cunoștințele se vor aplica și va fi creat un algoritm care poate arăta probabilitatea unei persoane, de exemplu, de a cumpăra un anumit produs într-un anumit interval de timp. În cazul în care datele și algoritmul astfel creat ar

³ Regulamentul UE 2016/679, JOUE L119, 4.05.2016.

fi vândute unei terțe persoane se adresează întrebarea cum anume sunt protejate acele date împotriva abuzurilor variatelor organizații⁴.

De un real interes este Carta Drepturilor Fundamentale a Uniunii Europene în cadrul căreia dreptul la protecția datelor este reprezentat de articolul 8⁵. Acesta stabilește dreptul fiecărei persoane la protejarea datelor cu caracter personal. De asemenea procesarea acestor date trebuie realizată numai pentru scopuri bine delimitate, având drept fundament consimțământul persoanei vizate sau un alt temei legal. În plus, fiecare persoană are posibilitatea de a accesa propriile date colectate, precum și dreptul de a le modifica sau de a le corecta. Subliniem faptul că acest drept fundamental nu are în vedere doar datele personale care sunt în legătură cu sfera privată a persoanelor, ci stabilește o metodă de protecție a acestora oricând are loc procesarea datelor cu caracter personal⁶.

În vederea realizării unei analize pertinente vom avea în vedere modul în care se coroborează și se auto influențează art. 7 și art. 8 ale Cartei Drepturilor Fundamentale a Uniunii Europene. Articolul 7 are în vedere dreptul persoanei de a-i fi respectate viața privată și viața de familie, casa și căile de comunicare⁷.

Carta a fost prezentată prima dată de Parlamentul European, de Consiliu și de Comisie la data de 7 decembrie în anul 2000 la Nisa, producând efecte de la data de 1 decembrie 2009.

În articolele vizate observăm faptul că sintagma „viață privată” nu are un singur sens, ci o multitudine. Aceasta nu poate face obiectul unei reglementări singulare deoarece articolul astfel creat ar conduce la limitarea sferei de aplicare a ceea ce este „privat”. Autori precum Samuel Warren și Louis Brandeis au văzut în viața privată „dreptul de a fi lăsat în pace”⁸. Cu alte cuvinte, viața privată a persoanei va fi analizată de o manieră *in extenso* în sfera juridică pentru a-i putea oferi aria de aplicare cea mai largă.

Conferința de Nord a Juriștilor din anul 1967, a întărit convingerea că o componentă a protecției datelor cu caracter personal este acest drept al persoanei de a fi lăsată în pace, cu o minimă ingerință din exterior. Cu alte cuvinte, dreptul

⁴ M. Backhoum, B. C. Gallego, M. O. Mackenrodt, *et. alii*, *Personal Data in Competition, Consumer Protection and Intellectual Property Law. Toward a Holistic Approach?*, în *MPI Studies on intellectual Property and Competition Law* 28, Springer, Berlin, 2018, pp. 15-18, <https://doi.org/10.1007/978-3-662-57646-5>.

⁵ Carta drepturilor fundamentale a Uniunii Europene, JOUE C303, 14.12.2007. [Online] la <https://fra.europa.eu/ro/eu-charter/article/8-protectia-datelor-cu-caracter-personal>, accesat la 02.2.2024.

⁶ T. Naef, *Data Protection without Data Protectionism. The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law*, in *loc. cit.*, Marc Bungenberg, Christoph Herrmann, Markus Krajewski, *et. alii.*, *EYIEL Monographs-Studies in European and International Economic Law*, Vol. 28, Springer, 2021, p. 30, <https://doi.org/10.1007/978-3-662-57646-5>.

⁷ Carta drepturilor fundamentale a Uniunii Europene, JOUE C303, 14.12.2007.

⁸ S. D. Warren, L. D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, Vol. IV, decembrie 1890, [Online] la https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html, accesat 12.04.2024.

la protecția datelor cu caracter personal ajunge să includă și protecția împotriva atingerilor aduse familiei, vieții de acasă, aspectelor vieții cu privire la nume, identitate⁹.

Evoluția tehnologică atacă această sferă a vieții private, fapt care poate fi observat mai ales în activitatea de supraveghere continuă realizată de colecționarii de date: colectează mari cantități de date ale persoanelor din e-mailurile private, locația telefonului, istoricul web, toate acestea fără consimțământul persoanei și fără un fundament legal.

Îmbinarea celor două articole amintite a condus către limitarea accesului statului în viața privată a persoanei, fără o justificare temeinică. Protecția datelor și regulile care o implică nu exclud procesarea datelor cu caracter personal, creând un temelie juridic, limitând modurile în care datele cu caracter personal vor putea fi procesate. Un bun exemplu este articolul 9 GDPR care împiedică procesarea anumitor categorii specifice de date cu caracter personal în ceea ce privește originea etnică, rasa, opinia politică, religioasă, credințele filozofice, apartenența la o asociație de comerț, procesarea datelor genetice, în vederea identificării persoanei fizice, a datelor cu caracter medical sau acelea care au în vedere orientarea sexuală a persoanei, în aliniatul al doilea al articolului fiind prevăzute excepții.

Articolul 8 al Cartei Drepturilor Fundamentale a Uniunii Europene va fi coroborat cu art. 4 GDPR în vederea aflării conținutului acestui drept fundamental, al protecției datelor cu caracter personal. Deducem, astfel, faptul că datele precum adresa IP, date de identificare ale persoanelor fizice vor fi incluse în noțiunea de „date”. Mai mult decât atât, se afirmă faptul că informația referitoare la persoană este mult mai voluminoasă, mai complexă decât informațiile care au în vedere strict acea persoană. Toate aceste informații vor fi protejate împotriva procesării datelor, procesarea însemnând colectarea, înregistrarea, depozitarea, combinarea, transferul datelor dintr-un stat în altul.

Aliniatul al doilea al articolului 8 din Cartă, este de asemenea edificator în ceea ce privește conținutul protecției datelor, structurată fiind pe trei trepte de analiză: procesarea datelor trebuie să se facă de o manieră corectă, de bună-credință; procesarea datelor trebuie să aibă în vedere un scop bine determinat; procesarea datelor trebuie realizată cu consimțământul persoanei vizate sau să aibă un alt fundament legal¹⁰.

Pentru ca procesarea datelor să poată fi realizată de o manieră corectă, de bună-credință, persoana vizată trebuie să cunoască existența datelor și a procesării. Cu alte cuvinte, procesarea datelor personale fără un fundament legal bine determinat va avea un caracter ilicit.

De asemenea, scopul procesării datelor cu caracter personal are în vedere așteptarea rezonabilă a subiectului vizat, precum și limitele existente și alipite

⁹ T. Naef, *op. cit.*, pp. 32-33.

¹⁰ T. Naef, *op. cit.*, p. 39.

procesului. Scopul este întotdeauna stabilit înainte de procesarea datelor cu caracter personal pentru o mai mare siguranță a raportului juridic astfel creat.

Fundamentul legal al procesării datelor cu caracter personal trebuie să poată fi identificat întotdeauna, iar consimțământul persoanei vizate la procesarea datelor va trebui acordat de o manieră liberă, serioasă, fără eroare, așa cum este solicitat și de art. 4 al GDPR.

Articolul 8 din Cartă acordă persoanei vizate alte două prerogative, respectiv dreptul de a avea acces la datele colectate și dreptul de a corecta datele procesate. În acest fel, subiectul de drept va putea observa modul în care îi sunt procesate datele, operațiunile stabilite, putând verifica corectitudinea datelor personale și dacă îi sunt respectate drepturile prevăzute de legislația în vigoare. Prin urmare, subiectul de drept dobândește un oarecare control asupra procedului de procesare a propriilor date cu caracter personal.

Alte două articole din GDPR sunt strâns legate de aceste componente ale art. 8 din Cartă, respectiv art. 15 GDPR (care stabilește că subiectul de drept va primi un document cu informațiile referitoare la procesarea datelor, scopul procesării, precum și cu țările, subiectele de drept/operatorii care vor primi rezultatul acelei procesări) și art. 16 GDPR (care stabilește necesitatea rectificării oricărui date incorecte, de îndată, fără întârziere)¹¹.

În România, implementarea Directivei Uniunii Europene 95/46/EC cu privire la protecția datelor cu caracter personal a avut loc înainte ca țara să adere la Uniune, prin adoptarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date¹². Cu

¹¹ *Idem*, p. 41.

¹² În art. 3 al Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date se specifică:

„În înțelesul prezentei legi, următorii termeni se definesc după cum urmează:

a) date cu caracter personal – orice informații referitoare la o persoană fizică identificată sau identificabilă; o persoană identificabilă este acea persoană care poate fi identificată, direct sau indirect, în mod particular prin referire la un număr de identificare ori la unul sau la mai mulți factori specifici identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;

b) prelucrarea datelor cu caracter personal – orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvaluirea către terți prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

c) stocarea – păstrarea pe orice fel de suport a datelor cu caracter personal culese;

d) sistem de evidență a datelor cu caracter personal – orice structură organizată de date cu caracter personal, accesibilă potrivit unor criterii determinate, indiferent dacă aceasta structură este organizată în mod centralizat ori descentralizat sau este repartizată după criterii funcționale ori geografice;

e) operator – orice persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autoritățile publice, instituțiile și structurile teritoriale ale acestora, care stabilește

toate acestea, în anul 2004 s-a considerat că exista o lipsă în modul în care era supravegheată respectarea legii și modul în care era pusă în aplicare. De aceea, România a reacționat și a întărit modul de implementare a noii legi. În acest fel, legea a fost mai bine structurată și organizată, punctând faptul că subiectele de drept aveau dreptul a fi informate, dreptul la acces, dreptul ca datele personale să fie schimbate sau modificate, dreptul la ștergerea datelor, dreptul de a face plângeri la autoritatea privind protecția datelor sau de a se adresa instanțelor de judecată. Modificările GDPR nu au mai fost incluse în legislația din România, precum dreptul la portabilitate a datelor, dreptul la a fi uitat¹³, dreptul la a fi notificat în caz de

scopul și mijloacele de prelucrare a datelor cu caracter personal; dacă scopul și mijloacele de prelucrare a datelor cu caracter personal sunt determinate printr-un act normativ sau în baza unui act normativ, operator este persoana fizică sau juridică, de drept public ori de drept privat, care este desemnată ca operator prin acel act normativ sau în baza celui act normativ;”.

¹³ Art. 17 GDPR „(1) Persoana vizată are dreptul de a obține din partea operatorului 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:

(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, 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 prelucrare; (c) 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);

(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 menționate la articolul 8 alineatul (1).

(2) În cazul în care operatorul a făcut publice datele cu caracter personal și este obligat, în temeiul alineatului (1), să le șteargă, operatorul, ținând seama de tehnologia disponibilă și de costul implementării, ia măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal că persoana vizată a solicitat ștergerea de către acești operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.

(3) (a) Alineatele (1) și (2a) nu se aplică în măsura în care prelucrarea este necesară:

(a) pentru exercitarea dreptului la liberă exprimare și la informare;

(b) 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 investit operatorul;

(c) 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);

încălcarea a modului de procesare a datelor cu caracter personal¹⁴.

De un real interes este articolul 28 al legii care îi obligă pe profesioniști să redacteze coduri de conduită care să primească aprobarea Autorității pentru protecția datelor.

2. Datele cu caracter personal – *res digitalis*, obiect derivat al dreptului de proprietate? Datele cu caracter personal incluse la nivelul actelor încheiate *inter vivos*

Comportamentul persoanei în ceea ce privește bunurile pe care le deține este unul specific proprietarului, de stăpân, putând folosi, dispune și poseda bunul, iar acest comportament se extinde nu doar asupra a ceea ce este corporal, ci și a ceea ce este intangibil, necorporal. Cu alte cuvinte, lexemele „a avea” se extind și asupra ideilor persoanei, dar și a datelor cu caracter personal din sfera digitală.

Dreptul de proprietate este unul perpetuu, exclusiv, absolut, fiind, prin urmare, opozabil *erga omnes*, iar tipologia sa precum și conținutul îi sunt atribuite de către lege. Obiectul trebuie să fie bine determinat și adus la cunoștința publicului¹⁵. Pe cale de consecință, unul dintre doctrinarii elvețieni, Eckert, a considerat că datele cu caracter personal sunt bunuri necorporale care ar trebui incluse în categoria bunurilor digitale, *res digitalis*, deoarece îndeplinesc cerința de control al proprietarului întocmai ca bunurile corporale¹⁶. Avem, astfel, în vedere și Codul Civil al Elveției¹⁷ care statuează că forțele naturii supuse controlului uman pot face obiectul dreptului de proprietate, iar condiția corporalității bunurilor ar trebui să primească o interpretare *lato sensu*. Cu toate acestea, au fost aduse două critici acestei opinii fundamentate pe articolului Codului elvețian¹⁸.

(d) 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

(e) pentru constatarea, exercitarea sau apărarea unui drept în instanță.”

¹⁴ B. Custers, Alan M. Sears, F. Dechesne *et. alii*, *EU Personal Data Protection in Policy and Practice*, in S. van der Holf *et alii*, *Information Technology and Law Series* vol. 29, Ed. T.M.C. ASSER PRESS, Haga, 2019, pp. 153-173, <https://doi.org/10.1007/978-94-6265-282-8>.

¹⁵ G. Boroi, C.A. Anghelescu, B. Nazat, *Curs de drept civil. Drepturile reale principale*, Ed. Hamangiu, București, 2013, pp. 16-17.

¹⁶ Eckert, M., *Digitale Daten als Wirtschaftsgut: digitale Daten als Sache*, 112 *Schweizerische Juristen-Zeitung* 245, 2016, *apud*, M. Backhoum, B. C. Gallego, M. O. Mackenrodt, *et alii*, *op. cit.*, p. 260.

¹⁷ Codul civil Elvețian în vigoare din data de 1.01.1912 art. 641: „Proprietarul are dreptul de a dispune de bunul său, așa cum va dori, însă în limitele stabilite de lege. El sau ea are dreptul de a obține bunul de la oricine îl deține fără drept și de a-l proteja împotriva oricărei activități nedorite.”

¹⁸ M. Backhoum, B. C. Gallego, M. O. Mackenrodt *et alii*, *op. cit.*, pp. 258-261.

<https://doi.org/10.1007/978-3-662-57646-5>.

Pe de o parte, obiectul dreptului de proprietate trebuie să fie bine particularizat, determinat, iar datele cu caracter personal nu îndeplinesc această cerință. Mai mult decât atât, s-a subliniat faptul că nu se poate cunoaște cu exactitate dacă datele avute în vedere sunt cele furnizate direct de persoană sau acelea transmise către toate celelalte subiecte de drept care au primit acces la date (cu alte cuvinte, nu se cunoaște dacă avem în vedere o copie a datelor cu caracter personal sau datele își regăsesc originea în sursa principală).

Publicitatea datelor cu caracter personal reprezintă o altă critică adusă includerii acestora în sfera dreptului de proprietate. De esența datelor cu caracter personal este confidențialitatea. Acestea sunt motivele pentru care considerăm că ar trebui creată o nouă categorie de drepturi de proprietate cu privire la mediul virtual, categorie care să fie inclusă în aria stabilită de legiuitori. Cu toate acestea, o bună soluție la acest moment este includerea bunurilor digitale și a drepturilor aferente în categoriile deja cunoscute pentru a le oferi efectele necesare: avem în vedere suportul care depozitează datele, dreptul fiind legat de acest suport fizic.

La momentul în care datele sunt tratate ca obiect al unui contract, acestea vor fi analizate, mai degrabă, prin prisma conținutului acestora. Nu există la acest moment o singură definiție care să înglobeze toate sensurile aferente datelor ca obiect al contractului. Pentru o mai mare stabilitate se consideră necesar a fi cercetat conținutul datelor pentru a putea stabili cu exactitate conținutul viitorului act juridic care se va încheia. Datele sunt informații codificate *machine-readable*. La nivelul actelor încheiate între vii datele sunt incluse în sfera obiectului actului sau sunt considerate bunuri cu valoare economică¹⁹.

Informația percepută ca un bun se remarcă prin intermediul conținutului, codului sursă și dispozitivului pe care este aceasta stocată. Astfel, informația ca bun are o anumită semnificație, fiind redată prin simboluri (biții redați prin 0 și 1) și este stocată sub o formă tangibilă, fizică (se are în vedere dispozitivul sau aplicația care stochează informațiile necesare). La momentul în care se realizează transferul datelor pe calea unui contract, de la o parte la cealaltă, vom observa modul în care sunt concepute clauzele, acestea trebuind să cuprindă semnele necesare care să descrie datele sau conținutul acestora va trebui descris de o manieră clară. Astfel, clauzele cu privire la datele personale și la transferul acestora vor trebui să stabilească cu claritate conținutul acestora și, eventual, să indice dispozitivul pe care sunt stocate sau codul de acces la aplicația de stocare a datelor necesare. De un real interes ne apar aceste trei niveluri de analiză a datelor, după cum s-a putut observa, respectiv pe cale semantică, sintactică și fizică.

Contractul va avea, astfel, un conținut digital definit prin intermediul art. 2 paragraf 11 al Directivei 2011/83/EU: „„conținut digital” înseamnă date produse și livrate în formă digitală”²⁰. Pentru a putea fi considerate bunuri, datele trebuie

¹⁹ H. Zech, *Data as Tradeable Commodity*, in loc. cit., A. de Franceschi, *European Contract Law and The Digital Single Market. The Implications of the Digital Revolution*, Ed. Intersentia, Cambridge, 2016, p. 53.

²⁰ Directiva 2011/83/EU. [Online] la <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32011L0083>, accesat 4.10.2024.

să aibă o anumită utilitate²¹. În plus, modul în care vor putea fi utilizate datele va aduce cu sine posibilitatea de a include datele în sfera proprietății. În ceea ce privește posesia datelor, ca bunuri necorporale, se vor avea în vedere modurile în care s-ar putea crea o anumită exclusivitate în ceea ce privește utilizarea lor. Astfel, această exclusivitate va putea fi acordată prin intermediul dreptului de autor sau al brevetului de invenție. Cu alte cuvinte, soluția pentru a trata datele ca pe un obiect al actelor încheiate între vii se poate găsi în sfera proprietății intelectuale: brevetul limitează utilizarea informației, dar nu și accesul la aceasta, iar dreptul de autor reduce accesul la datele create în temeiul algoritmilor și calculelor²². Același drept de proprietate va acorda deținătorului posibilitatea de a distruge datele respective sau de a le transfera.

Actele juridice încheiate *inter vivos* pot avea în vedere modalitatea în care este oferit accesul la informațiile din datele create. Aceste contracte vor răspunde mai multor întrebări dintre care cele mai relevante apar ca fiind „Cine are acces la datele care fac obiectul contractului?”, „Care sunt datele la care va avea acces partea contractuală vizată?”, „Care este perioada de timp pentru care se acordă accesul la datele descrise prin contract?”. Accesul la date va oferi părții contractante beneficiare posibilitatea de a copia datele, de a le cerceta conținutul sau de a le include pe un suport separat și a le transmite către terțe persoane bine determinate. De un real interes ne apar ca fiind contractele mai bine caracterizate, respectiv acelea care oferă accesul la date exclusiv anumitor persoane, cu condiția ca datele să nu fie distribuite, să fie păstrate secrete. În acest context ne întrebăm ce formă juridică sau ce concept ar putea fi alăturat datelor pentru ca acestea să poată fi „traduse” din punct de vedere juridic. Problema vizată este, în principal, rezolvată prin intermediul clauzei de confidențialitate deoarece datele vor putea fi percepute ca un secret de comerț, ocrotit de către diferitele companii. Cu toate acestea, o atare clauză nu oferă o exclusivitate în folosirea datelor și nu stabilește o protecție împotriva oricărui tip de utilizare a datelor de către terțele persoane²³.

Datele cu caracter personal pot face obiectul unui contract și să fie incluse în sfera know-how-ului care poate fi corotit de o manieră parțială prin intermediul clauzei de confidențialitate, dar și cu ajutorul dreptului de proprietate deoarece datele pot avea un conținut economic care să determine stabilirea unor prejudicii mai mari în caz de încălcare a regulilor stabilite prin contract. Cu alte cuvinte, unei clauze de confidențialitate îi va fi alipită o clauză penală bine determinată în raport cu impactul pe care l-ar avea divulgarea datelor. Nu uităm de mijloacele de ocrotire a datelor prin intermediul regulilor contractuale care stabilesc necesitate îndeplinirii obligațiilor de către părți și a respectării drepturilor aferente. Ceea ce dorim să arătăm este faptul că datele trebuie privite ca pe oricare alte bunuri deoarece, odată incluse în sfera contractuală, li se vor alipi anumite drepturi și li se vor aplica principiile efectelor specifice actului juridic. Pentru a le putea ocroti va fi putea fi utilizat inclusiv remediul executării în natură a obligațiilor deoarece

²¹ H. Zech, *op. cit.*, p. 56.

²² *Ibidem*, p. 57.

²³ H. Zech, *op. cit.*, p. 63.

acestea de pe urmă vor fi legate de utilizarea, de transferarea, de transformarea datelor.

Autorul Herbert Zech afirmă faptul că regulamentul aplicabil protecției datelor cu caracter personal ar putea fi transformat într-un act pentru protejarea dreptului de proprietate cu privire la aceste date²⁴. Pe cale de consecință, aplicarea acestuia ar putea fi extinsă către sfera economică și către o uniformizare a regimului juridic al datelor în cadrul unui contract de sine stătător. Aplicarea regulilor contractuale cu privire la datele cu caracter personal va trebui să aibă în vedere și o oarecare limitare redată prin necesitatea de a ocroti persoana despre ale cărei date este vorba.

După cum se poate observa, datele cu caracter personal din cadrul actelor încheiate între vii vor putea fi ocrotite pe mai multe căi, prin alocarea unor reguli variate: regulile aplicabile dreptului de proprietate, regulile aplicabile contractului și regulile aplicabile în domeniul proprietății intelectuale.

În ceea ce privește modul în care vor putea fi transferate datele cu caracter personal vom avea în vedere Directiva 2011/83/EU privind drepturile consumatorilor care stabilește: „Conținut digital înseamnă acele date care sunt produse și livrate în formă digitală, cum sunt programele de calculator, aplicațiile, jocurile, muzica, înregistrările video sau textele, indiferent dacă sunt accesate prin descărcare sau prin flux continuu, de pe un suport material sau prin orice alte mijloace. Contractele de livrare a conținutului digital ar trebui incluse în sfera de aplicare a prezentei directive. Dacă un conținut digital este livrat pe un suport material, cum sunt CD-urile sau DVD-urile, acesta ar trebui considerat drept un bun, în sensul prezentei directive.”²⁵. Cu alte cuvinte, vor putea fi transferate atât datele care se află pe un suport tehnic, cât și acelea incluse în aplicații sau pe suporturi intangibile, stabilite prin intermediul Internetului. Se vorbește, astfel, despre conceptul de „Internet of Things” care presupune schimbul datelor cu ajutorul suportului conectat la Internet. Spre exemplu un senzor care să aibă în vedere datele referitoare la comportamentul persoanei cu privire la alimentele din frigider sau aplicațiile care culeg datele referitoare la alegerile vestimentare ale persoanei.

Datele cu caracter personal pot avea și rolul unei contraprestații la nivelul contractelor. Astfel, se poate solicita de aplicație o anumită cantitate de date personale din partea subiectului de drept pentru ca acesta să-i poată utiliza funcțiunile²⁶. Principalul mod de ocrotire împotriva pierderii datelor este acela al stabilirii clare a conținutului datelor și oferirea consimțământului cu privire la transfer.

²⁴ *Ibidem*, p. 66.

²⁵ Directiva 2011/83/EU. [Online] la <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32011L0083>, accesat 4.10.2024.

²⁶ C. Twigg-Flesner, *Disruptive Technology – Disrupted Law? How The Digital Revolution affects (Contract) Law in loc. cit.*, A. de Franceschi, *European Contract Law and The Digital Single Market. The Implications of the Digital Revolution*, Ed. Intersentia, Cambridge, 2016, p. 40.

Referitor la contractele de vânzare a datelor cu caracter personal vom menționa faptul că acestea sunt valabile (nu sunt interzise prin GDPR) atâta vreme cât sunt respectate anumite standarde precum: stabilirea exactă a datelor care vor fi transmise; scopul transmiterii și fundamentul legal; modul în care au fost obținute datele cu caracter personal; perioada de timp în care va avea loc procesarea datelor și modul în care vor putea să fie exercitate drepturile astfel dobândite²⁷.

Alte tipuri de contracte care pot conține date cu caracter personal sunt acelea de tipul click-wrap. Astfel, datele cu caracter personal se vor regăsi la nivelul unor contracte de adeziune, partea care nu propune încheierea actului trebuind să apese butonul de acceptare a termenilor din căsuța apărută pe site-ul web accesat. În acest fel este obținut consimțământul celeilalte părți pentru transferul datelor²⁸.

Aspectele analizate nu au făcut decât să sublinieze diferitele forme juridice pe care datele cu caracter personal le pot lua la nivelul actelor încheiate între vii, precum și modul în care le putem ocroti: prin intermediul dreptului de proprietate, regulilor contractuale (principiul forței obligatorii a contractului jucând un rol esențial) sau proprietății intelectuale.

3. Datele cu caracter personal și protecția acestora după decesul persoanei

Întrebările pe care și le adresează subiecte de drept cel mai adesea sunt: „ce se va întâmpla cu datele și acei „coins” obținuți în jocul video?”; „cine va putea să citească mesajele de pe platforma Facebook când persoana va deceda?”; „ce se va întâmpla cu contul YouTube, cu moneda digitală Bitcoin obținută?”.

A fost creată o diferențiere a datelor cu caracter personal în funcție de originea și localizarea acestora. Mult mai ușor se stabilește situația datelor incluse pe un *memory stick*, acel obiect fiind inclus în moștenire și, prin urmare acordat, eredelui căruia i se cuvine. În cazul în care s-ar dori separarea datelor de carcasa care le include, împărțirea acestora între moștenitori ar fi una dificilă. Pentru datele transmise în mediul on-line, moștenirea digitală va căpăta o altă formă în funcție de modul în care se vor aplica sau nu regulile din materia dreptului de proprietate intelectuală. Astfel, în ceea ce privește avatarul creat de *de cujus*, videoclipurile, colajele de fotografii create și care respectă cerința originalității, vor putea face obiectul dreptului de autor, stabilindu-se, în acest fel, soarta acestora.

În ceea ce privește celelalte conturi create de *de cujus* se vor aplica regulile din materia obligațiilor civile și a contractelor. Totuși, unele companii, din dorința de a asigura o modalitate transparentă și sigură pentru transmiterea datelor

²⁷ B. Fiten, *What should one keep in mind whwn selling, purchasing or licensing personal data?*. [Online] la <https://www.timelex.eu/en/blog/what-keep-in-mind-selling-purchasing-licensing-personal-data>, accesat la 4.10.2024.

²⁸ R. Momberg, *Standard Terms and Transparency in Online Contracts*, in loc. cit., A. de Franceschi, *European Contract Law and The Digital Single Market. The Implications of the Digital Revolution*, Ed. Intersentia, Cambridge, 2016, p. 192.

utilizatorilor după decesul acestora, au încercat stabilirea unor mecanisme proprii. Un bun exemplu este crearea contului inactiv de către Google, cont prin intermediul căruia se va stabili cine va putea primi acces la contul principal dacă clientul principal decedează, precum și informațiile care vor putea fi accesate ulterior. Facebook stabilește, de asemenea, instituția moștenitorului de contact care funcționează ca un *trust*, prin acordarea accesului la contul celui decedat unei persoane de încredere (persoana nu va putea să citească mesajele sau să schimbe postările)²⁹. Astfel, persoana de încredere va administra datele primite în folosul unui beneficiar determinat de constitutorul transmitător.

4. Datele cu caracter personal și procesarea acestora. Modul în care sunt create și procesate datele care vor fi incluse în cadrul actelor juridice

Dacă în contextul actelor încheiate între vii, precum și în acela al moștenirii digitale, datele cu caracter personal sunt văzute din perspectiva dreptului de proprietate, transmiterea lor implicând reguli juridice și contractuale bine stabilite, într-un cadru tehnologic, acestea capătă o cu totul altă valoare. În era digitală actuală datele nu reprezintă doar o resursă personală, ci și un element esențial în dezvoltarea unor tehnologii avansate precum inteligența artificială

În era digitală actuală, caracterizată de progrese rapide în inteligența artificială (AI), preprocesarea eficientă și etică a datelor este esențială pentru dezvoltarea modelelor de învățare automată (ML). Modelele AI precum GPT-4 se bazează pe seturi de date pentru a putea reproduce într-un mod cât mai nuanțat limbajul natural, uman. Preprocesarea datelor implică un set complex de pași tehnici pentru a transforma datele brute (sub formă de text, imagini sau videoclipuri) în date utilizabile pentru instruirea modelului.

Utilizarea datelor în instruirea modelelor lingvistice (ML) este unul dintre aspectele principale ale inteligenței artificiale (AI) și ale procesării limbajului natural (PLN). Modele lingvistice precum GPT-4 sau Gemini sunt instruite pe seturi vaste de date care includ texte din diverse surse, inclusiv cărți, articole, site-uri web și rețele sociale. Această instruire, bazată pe datele de intrare primite, le permite modelelor de inteligență artificială să genereze texte, imagini sau videoclipuri să îndeplinească o gamă largă de sarcini lingvistice sau matematice. Totuși, procesul de colectare și de pregătire a datelor reprezintă o provocare întrucât atât calitatea datelor, cât și veridicitatea acestora, nu poate fi garantată.

Calitatea și diversitatea datelor utilizate pentru instruirea modelelor lingvistice sunt esențiale pentru performanța acestora. Astfel, dacă un model AI este instruit cu un set amplu de date, respectivul model va putea să învețe nuanțele limbajului, să înțeleagă contextul și să genereze texte coerente și relevante pentru utilizatori. Datele de instruire pentru modelele lingvistice includ, de obicei, o gamă largă de genuri, stiluri și subiecte pentru a se asigura că modelul poate gestiona diverse construcții și contexte lingvistice. Această diversitate ajută modelul să se

²⁹ M. Backhoum, B. C. Gallego, M. O. Mackenrodt *et alii*, *op. cit.*, pp. 262-266.

adapteze mai rapid la datele noi și care nu au mai fost procesate anterior, făcându-l mai complex și mai robust.

Datele de intrare folosite pentru instruirea modelelor lingvistice de AI provin din diverse surse, precum: extrase de pe pagini web: colecții de date textuale de pe site-uri web, bloguri și forumuri care oferă o gamă largă de utilizare a limbajului contemporan și colocvial, literatură și publicații: cărți, articole științifice și alte materiale publicate care oferă texte bine structurate și de înaltă calitate, contribuie la înțelegerea de către model a limbajului formal și tehnic; rețele sociale: postări și interacțiuni de pe platforme precum Twitter, Facebook și Reddit oferă perspective asupra limbajului informal și asupra subiectelor de actualitate; date tranzacționale: înregistrări de servicii pentru clienți, dialoguri și alte forme de comunicare tranzacțională, pot ajuta modelul de inteligență artificială să reproducă secvențe de dialog din situații practice.

Fiecare sursă contribuie la înțelegerea de către model a limbajului, a culturii și a interacțiunii umane, permițându-i să genereze răspunsuri coerente și relevante pentru contextul în care a fost folosit acesta.

Preprocesarea datelor este, de asemenea, un pas esențial în antrenarea modelelor lingvistice. Acest proces asigură formatarea adecvată a datelor pentru a putea fi utilizate de către algoritmi de învățare automată, maximizând astfel eficiența și performanța modelelor. Preprocesarea implică mai multe etape critice, fiecare având rolul său specific în pregătirea datelor pentru modelare.

În primul rând, curățarea datelor implică eliminarea „zgomotului”. Acesta este reprezentat de informațiile irelevante care pot afecta negativ performanța modelului. Astfel, există mai mulți pași pentru a elimina „zgomotul” din datele folosite: eliminarea etichetelor HTML și a tag-urilor: datele extrase de pe web conțin adesea markup HTML, care trebuie eliminat pentru a evita confuziile în modelul lingvistic; îndepărtarea caracterelor speciale: caracteristicile precum simbolurile și caracterele speciale care nu adaugă valoare semantică textului sunt eliminate; gestionarea spațiilor excesive: spațiile multiple sunt reduse la un singur spațiu pentru a standardiza textul; filtrarea liniilor goale: eliminarea liniilor goale și a altor forme de zgomot care pot distorsiona reprezentarea datelor.

În al doilea rând, se poate folosi procesul de „normalizare”. Acesta presupune transformarea textului într-un format consistent, facilitând astfel procesarea ulterioară. Acest proces include: conversia la litere mici („lowercasing”): toate caracterele sunt convertite la litere mici pentru a reduce variația cauzată de utilizarea inconsistentă a literelor mari și mici; standardizarea ortografică: ortografia variabilă a cuvintelor este standardizată pentru a evita confuziile (de exemplu, pentru modelele instruite în limba engleză, „color” vs. „colour”).

În al treilea rând, pentru a putea pregăti datele ce urmează să servească drept „training data” pentru modelul de AI se folosește procedura de „tokenization” ce reprezintă procesul de descompunere a textului în unități mai mici numite token-uri. Token-urile pot fi cuvinte, sub-cuvinte sau caractere, în funcție de metoda de tokenizare utilizată:

a. tokenizare pe cuvinte: textul este împărțit în cuvinte individuale. Această metodă este simplă, dar poate duce la probleme cu cuvintele necunoscute (out-of-vocabulary, OOV).

b. tokenizare pe subcuvinte: tehnici precum Byte-Pair Encoding (BPE) și Sentence Piece sunt utilizate pentru a împărți cuvintele în subunități mai mici. Aceasta ajută la gestionarea cuvintelor necunoscute și reduce dimensiunea vocabularului, îmbunătățind astfel eficiența modelului.

Metoda Byte-Pair Encoding (BPE): BPE pornește cu un vocabular inițial de caractere și iterează prin combinarea celor mai frecvente perechi de caractere într-o nouă unitate, până când se atinge dimensiunea dorită a vocabularului.

Metoda Sentence Piece: o metodă de tokenizare care nu presupune separatoare explicite între cuvinte, facilitând astfel procesarea textelor în diverse limbi.

De asemenea, o altă metodă de pregătire a datelor de intrare constă în filtrarea și selecția caracteristicilor.

- filtrarea „n-gramelor”: în funcție de necesitățile modelului de inteligență artificială antrenată, se pot genera și filtra „n-grame” (secvențe de „n” cuvinte) pentru a capta contextul local.

- selecția caracteristicilor: tehnici statistice pot fi utilizate pentru a selecta caracteristicile relevante ce trebuie antrenate, îmbunătățind, astfel, eficiența modelului.

A cincea abordare folosită în domeniul inteligenței artificiale pentru pregătirea datelor de intrare este reducerea dimensiunilor. Aceasta se poate face fie prin TF-IDF, fie prin metoda „embedding”.

TF-IDF (Term Frequency-Inverse Document Frequency): această tehnică transformă textul în reprezentări vectoriale ponderate, reflectând importanța unui cuvânt în documentul ce servește ca parte a datelor de intrare.

Embedding-uri: utilizarea embedding-urilor de cuvinte (de exemplu, Word2Vec, GloVe) pentru a transforma cuvintele în vectori denși care capturează relațiile semantice dintre cuvinte.

O ultimă metodă este regularizarea prin „oversampling” și „undersampling”. Pentru a aborda posibilul dezechilibru dintre diferite categorii de date din setul de date de intrare, se pot aplica tehnici de oversampling și undersampling.

Prin aplicarea acestor tehnici de preprocesare se asigură că datele sunt optimizate pentru antrenarea modelelor lingvistice, îmbunătățind, astfel, acuratețea și eficiența acestora.

Adăugarea de zgomot în datele folosite pentru instruirea unui model AI poate ajuta la îmbunătățirea complexității modelului. Tehnici precum augmentarea datelor, instruirea adversarială și introducerea intenționată a zgomotului pot produce variații controlate în datele de intrare, ajutând modelele să învețe să ignore variațiile minore și să se concentreze pe aspectele cele mai relevante.

Pentru modelele lingvistice, augmentarea datelor ar putea implica tehnici precum înlocuirea unor cuvinte cu sinonimele lor, traducerea inversă sau

adăugarea de mici erori tipografice. Aceste metode pot simula dialogul cu un utilizator uman și pot îmbunătăți capacitatea modelului de a înțelege și de a genera text în condiții diverse.

Din perspectiva instruirii adversiale, aceasta implică adăugarea intenționată de exemple neobișnuite în setul de date de instruire. Pentru modelele lingvistice, aceasta ar putea însemna construirea de propoziții care sunt corecte din punct de vedere gramatical, dar greșite din punct de vedere semantic, ajutând modelul să învețe să se concentreze pe conținutul semnificativ.

Adăugarea de zgomot direct în datele de intrare (de exemplu, omiterea cuvintelor, schimbarea cuvintelor sau introducerea de cuvinte aleatorii) poate îmbunătăți capacitatea modelului lingvistic de a genera răspunsuri. Principala problemă la această metodă este faptul că trebuie ca nivelul de zgomot să nu depășească un anumit prag astfel încât să se îmbunătățească capacitatea modelului de a distinge sensul datelor primite fără a afecta semnificativ capacitatea acestuia de a învăța din ele.

Din perspectivă juridică, un important aspect este păstrarea confidențialității. Pentru a ne asigura confidențialitatea datelor ne putem folosi de două metode: confidențialitatea diferențială și învățarea federată.

Confidențialitatea diferențială introduce zgomot în date în timpul procesului de instruire pentru a împiedica modelul să memoreze detalii specifice despre orice cumul de date individual. Prin această tehnică este asigurat faptul că modelul instruit nu dezvăluie în mod neintenționat informații private.

Învățarea federată constă în instruirea modelelor de inteligență artificială pe mai multe dispozitive descentralizate sau servere, unde setul de date locale rămâne pe dispozitivele respective, dar odată ce procesul de instruire al modelului ia sfârșit, versiunea stabilă a sa este partajată, fără a mai avea acces la datele de intrare folosite anterior, reducând astfel riscul de expunere a unor date confidențiale.

Concluzii

Intersecția dintre inteligența artificială, datele și etică prezintă o provocare amplă pentru societatea modernă. Recunoscând datele ca obiect juridic cu valoare economică și personală semnificativă, putem naviga în mod responsabil în complexitatea moștenirii digitale, confidențialității și dezvoltării AI. Calea de urmat necesită un efort concertat din partea legislatorilor, inginerilor software și a societății în general pentru a se asigura că viitorul digital este atât inovator, cât și bazat pe aspecte etice.

Încurajarea dezvoltării etice a AI implică încurajarea unei culturi a practicilor etice în cercetarea și implementarea AI. Aceasta include prioritizarea echității, transparenței și consimțământului utilizatorului. Îmbunătățirea securității datelor implică implementarea unor măsuri avansate de protecție împotriva încălcării datelor și a accesului neautorizat la informațiile confidențiale. Încurajând un mediu de transparență, responsabilitate și îmbunătățire continuă, putem valorifica capacitățile inteligenței artificiale pentru a aduce beneficii societății.

Referințe

- Abadi M., Chu A., Goodfellow I., McMahan H. B., Mironov I., Talwar K., Zhang L. (2016). Deep Learning with Differential Privacy.
- Backhoum M., B. C. Gallego, M. O. Mackenrodt *et alii*, *Personal Data in Competition, Consumer Protection and Intellectual Property Law. Toward a Holistic Approach?*, in *MPI Studies on Tellectual Property and Competition Law 28*, Springer, Berlin, 2018, <https://doi.org/10.1007/978-3-662-57646-5>.
- Boroi G., C.A. Anghelescu, B. Nazat, *Curs de drept civil. Drepturile reale principale*, Ed. Hamangiu, București, 2013, pp. 16-17.
- Chawla N. V., Bowyer K. W., Hall L. O., Kegelmeyer W. P. (2002). SMOTE: Synthetic Minority Over-sampling Technique.
- Custers B., Alan M. Sears, F. Dechesne *et alii*, *EU Personal Data Protection in Policy and Practice*, in S. van der Hof, *et. alii.*, *Information Technology and Law Series*, vol. 29, Ed. T.M.C. ASSER PRESS, Haga, 2019, pp. 153-173. <https://doi.org/10.1007/978-94-6265-282-8>.
- Fadaee M., Bisazza A., Monz C. (2017). Data Augmentation for Low-Resource Neural Machine Translation.
- Franceschi A. de, *European Contract Law and The Digital Single Market. The Implications of the Digital Revolution*, Ed. Intersentia, Cambridge, 2016.
- Kudo T., Richardson J. (2018). SentencePiece: A Simple and Language Independent Subword Tokenizer and Detokenizer for Neural Text Processing.
- McMahan B., Moore E., Ramage D., Hampson S., Arcas B. A. (2017). Communication-efficient Learning of Deep Networks from Decentralized Data.
- Mikolov T., Chen K., Corrado G., Dean J. (2013). Efficient Estimation of Word Representations in Vector Space.
- Miyato T., Dai A. M., Goodfellow I. (2017). Adversarial Training Methods for Semi-Supervised Text Classification.
- Momberg R., *Standard Terms and Transparency in Online Contracts*, in *loc. cit.*, A. de Franceschi, *European Contract Law and The Digital Single Market. The Implications of the Digital Revolution*, Ed. Intersentia, Cambridge, 2016.
- Naef T., *Data Protection without Data Protectionism. The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law*, in *loc. cit.*, Marc Bungenberg, Christoph Herrmann, Markus Krajewski, *et. alii.*, *EYIEL Monographs-Studies in European and International Economic Law*, Vol. 28, Springer, 2021, p. 30. <https://doi.org/10.1007/978-3-662-57646-5>.
- Radford A., Wu J., Child R., Luan D., Amodei D., Sutskever I. (2019). Language Models are Unsupervised Multitask Learners.
- Rajaraman A., Ullman J. D. (2011). Mining of Massive Datasets.
- Sennrich, R., Haddow, B., & Birch, A. (2016). Neural Machine Translation of Rare Words with Subword Units.
- Twigg-Flesner C., *Disruptive Technology – Disrupted Law? How The Digital Revolution affects (Contract) Law* in *loc. cit.*, A. de Franceschi, *European Contract Law and The Digital Single Market. The Implications of the Digital Revolution*, Ed. Intersentia, Cambridge, 2016.
- Warren S.D., L. D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, Vol. IV, decembrie 1890, [Online]
- Zech H., *Data as Tradeable Commodity*, in *loc. cit.*, A. de Franceschi, *European Contract Law and The Digital Single Market. The Implications of the Digital Revolution*, Ed. Intersentia, Cambridge, 2016.