CZU: 366.5:004
DOI: https://doi.org/10.5281/zenodo.19950298

IMPACTUL ALGORITMILOR DE PERSONALIZARE ASUPRA CONSIMȚĂMÂNTULUI LIBER AL CONSUMATORULUI ÎN MEDIUL ONLINE

Oxana EȘANU,
doctorandă, asistent universitar, Catedra Drept Privat,
Academia „Ștefan cel Mare" a MAI; avocat în C.A. „Eșanu Oxana",
e_oxana@yahoo.com,
https://orcid.org/0000-0002-4304-2919

Rezumat. ***Prezentul articol analizează modul în care algoritmii de personalizare utilizați de platformele digitale afectează consimțământul liber al consumatorului în mediul online. Prin intermediul tehnicilor de micro-targetare (identificare), filtre informaționale și arhitecturi persuasive ale interfeței (dark patterns), companiile tehnologice structurează mediul decizional al utilizatorilor în moduri care subminează autonomia de voință și liberul arbitru, ridicate la rang de principii fundamentale ale dreptului civil și ale dreptului consumatorului. Articolul explorează cadrul juridic european și internațional aplicabil, cu accent pe Regulamentul General privind Protecția Datelor (RGPD), Directiva privind drepturile consumatorilor, Digital Services Act (DSA) și Digital Markets Act (DMA), propunând totodată o analiză critică a lacunelor legislative și a provocărilor de ordin practic în asigurarea unui consimțământ veritabil și informat în economia digitală.***

Cuvinte-cheie: algoritmi de personalizare, consimțământ liber, consumator online, dark patterns, RGPD, autonomie de voință, economie digitală, DSA, protecția datelor personale, dreptul consumatorului.

Abstract. ***This article examines how personalization algorithms used by digital platforms affect the free consent of consumers in the online environment. Through micro-targeting techniques, information filters, and persuasive interface architectures (dark patterns), technology companies structure users' decision-making environments in ways that undermine autonomy of will and free agency, which are fundamental principles of civil law and consumer law. The article explores the applicable European and international legal framework, focusing on the General Data Protection Regulation (GDPR), the Consumer Rights Directive, the Digital Services Act (DSA), and the Digital Markets Act (DMA), while also proposing a critical analysis of legislative gaps and practical challenges in ensuring genuine and informed consent in the digital economy***

Keywords: personalization algorithms, free consent, online consumer, dark patterns, GDPR, autonomy of will, digital economy, DSA, personal data protection, consumer law.

Introducere

Revoluţia digitală a transformat radical modul în care consumatorii interacţionează cu piaţa. Dacă odinioară decizia de cumpărare se forma în spaţiul fizic al magazinului, supusă influenţelor sociale directe şi transparente, astăzi aceasta este modelată, în mod preponderent, de algoritmi invizibili care operează în spatele ecranelor dispozitivelor noastre. Personalizarea algoritmică – procesul prin care sistemele informatice analizează datele comportamentale ale utilizatorilor pentru a le oferi conţinut, publicitate şi opţiuni adaptate profilului lor – a devenit coloana vertebrală a economiei digitale contemporane.

Paradoxul central al acestei realităţi constă în aceea că personalizarea, prezentată public ca un beneficiu pentru consumator, poate deveni, în esenţă, un instrument de manipulare subtilă a voinţei sale. Consimţământul, ca element fundamental al oricărui raport juridic civil sau comercial, presupune în mod tradiţional că este liber, neviciat, informat şi exprimat de o persoană cu discernământ. Algoritmii de personalizare pun sub semnul întrebării fiecare dintre aceste condiţii, creând medii decizionale artificiale în care autonomia de voinţă a consumatorului devine, cel puţin parţial, iluzorie.

Dreptul european al consumatorului şi cadrul normativ privind protecţia datelor personale au înregistrat progrese semnificative în ultimul deceniu, însă viteza cu care tehnologia evoluează depăşeşte în continuare capacitatea de reacţie a legiuitorului. Regulamentul General privind Protecţia Datelor (RGPD) [1], intrat în vigoare în mai 2018, a stabilit pentru prima dată la nivel european un standard înalt pentru consimţământul privind prelucrarea datelor, dar aplicarea sa în contextul algoritmilor de personalizare ridică probleme juridice complexe şi adesea nerezolvate.

Prezentul studiu îşi propune să analizeze, dintr-o perspectivă preponderent juridică, dar cu deschideri necesare spre psihologie cognitivă şi economie comportamentală, felul în care algoritmii de personalizare afectează consimţământul liber al consumatorului în spaţiul online. Demersul academic urmăreşte identificarea mecanismelor concrete de influenţare a voinţei, examinarea cadrului juridic aplicabil şi formularea unor propuneri de *lege ferenda* menite să consolideze protecţia reală a consumatorului digital.

Algoritmi de personalizare – noţiune, tipologie şi mecanisme de funcţionare

Definiţie şi caracteristici generale

Termenul „algoritm de personalizare” desemnează, în sens larg, orice sistem automatizat de prelucrare a datelor care utilizează informaţii despre comportamentul, preferinţele, caracteristicile demografice sau istoricul unui

utilizator pentru a-i oferi conținut, produse, servicii sau mesaje publicitare adaptate profilului său individual. Aceste sisteme nu sunt simple filtre tehnice – ele reprezintă, în realitate, instrumente de inginerie comportamentală la scară industrială.

Din perspectivă tehnică, algoritmii de personalizare funcționează prin colectarea masivă de date (big data), procesarea acestora prin tehnici de machine learning și inteligență artificială, și generarea de predicții privind comportamentul viitor al utilizatorului. Astfel, platforma anticipează nu doar ce dorește utilizatorul în prezent, ci și ce ar putea dori în viitor, construind un profil predictiv care depășește cu mult simpla preferință declarată.

Caracteristicile esențiale ale algoritmilor de personalizare, relevante din perspectivă juridică, sunt: (i) caracterul opac al funcționării lor – utilizatorul nu știe care date sunt colectate, cum sunt procesate și ce concluzii sunt extrase; (ii) caracterul dinamic și adaptiv – algoritmul se actualizează continuu pe baza noilor date generate; (iii) caracterul persuasiv – scopul nu este neutru, algoritmul optimizează spre un obiectiv comercial, de regulă maximizarea angajamentului sau a vânzărilor; (iv) scalarea – același algoritm operează simultan asupra milioanelor de utilizatori, cu efecte sociale agregate semnificative.

Tipuri de algoritmi de personalizare cu relevanță juridică

Literatura de specialitate distinge mai multe categorii de algoritmi de personalizare, fiecare cu implicații juridice distincte, care necesită abordări normative diferențiate.

a) Algoritmii de recomandare (recommendation engines) – prezenți pe platforme precum Netflix, Amazon, Spotify sau YouTube – sugerează utilizatorilor conținut sau produse pe baza istoricului lor de navigare, cumpărare sau vizionare. Deși aparent neutri, acești algoritmi pot crea „bule informaționale" (filter bubbles[2]) care limitează accesul utilizatorului la informație diversă și îi consolidează prejudecățile cognitive existente, cu consecințe relevante atât în dreptul consumatorului, cât și în dreptul mass-media și al comunicărilor.

b) Algoritmii de afișare a publicității direcționate (targeted advertising algorithms) – operaționalizați de platforme precum Google Ads sau Meta Ads – utilizează profilurile comportamentale ale utilizatorilor pentru a le difuza mesaje publicitare personalizate. Aceștia reprezintă nucleul economic al majorității platformelor digitale gratuite și ridică cele mai acute probleme din perspectiva consimțământului informat, întrucât funcționează pe baza unor date colectate adeseori fără cunoștința reală a utilizatorului.

c) Algoritmii de prețuri dinamice (dynamic pricing algorithms) – utilizați de companii aeriene, platforme de transport sau comercianți online –

ajustează prețurile în timp real în funcție de profilul utilizatorului, momentul accesării și comportamentul său anterior. Practicile de discriminare prin preț, deși nu sunt ilegale per se în toate jurisdicțiile, pot constitui practici comerciale neloiale atunci când se bazează pe date personale prelucrate fără un consimțământ valid, aducând atingere principiului egalității de tratament.

d) Algoritmii de scor de creditare și de evaluare a riscului – utilizați de instituții financiare, companii de asigurări sau platforme fintech – produc decizii automatizate cu impact major asupra drepturilor și intereselor consumatorilor, intrând astfel în sfera directă de aplicare a art. 22 din RGPD privind dreptul de a nu fi supus unor decizii exclusiv automatizate, cu toate garanțiile procedurale aferente [2].

Economia atenției și arhitectura persuasivă a platformelor

Înțelegerea deplină a modului în care algoritmii de personalizare afectează consimțământul consumatorului necesită o scurtă incursiune în conceptul de „economie a atenției" (attention economy), formulat de Herbert Simon [3] și dezvoltat ulterior de autori precum Tim Wu [4] sau Shoshana Zuboff [5]. Conform acestei paradigme, atenția umană constituie resursa economică principală în mediul digital, iar platformele concurează agresiv pentru captarea și menținerea acesteia, algoritmii de personalizare reprezentând instrumentul principal în atingerea acestui obiectiv.

Algoritmii de personalizare nu se limitează la adaptarea conținutului la preferințele existente ale utilizatorului, ci modelează activ acele preferințe, exploatând mecanisme psihologice recunoscute în literatura de specialitate: (i) efectul de confirmare (confirmation bias), prin afișarea preferențială a conținutului care confirmă credințele existente ale utilizatorului; (ii) variabilitatea recompensei (variable reward scheduling), principiu preluat din psihologia comportamentală skineriană, care face ca utilizatorul să revină compulsiv pe platformă în așteptarea conținutului „surpriză"; (iii) dovada socială (social proof), prin evidențierea reacțiilor altor utilizatori pentru a influența comportamentul individual; (iv) urgența artificială (artificial scarcity/urgency), utilizată extensiv în comerțul electronic pentru a accelera deciziile de cumpărare.

Aceste tehnici, atunci când sunt implementate prin intermediul interfețelor digitale, compun ceea ce literatura de specialitate denumește „arhitecturi de alegere" (choice architectures) manipulative sau, în terminologia juridică emergentă, dark patterns – despre care vom discuta în secțiunea dedicată. Consecința juridică imediată este că mediul decizional în care operează consumatorul online nu este neutru, ci este construit și optimizat de platformă în scopuri proprii, punând sub semnul întrebării caracterul liber al oricărui consimțământ exprimat în acest context.

Consimţământul liber al consumatorului – fundamente juridice şi conceptuale

Consimţământul în dreptul civil clasic

Consimţământul reprezintă, în dreptul civil, manifestarea de voinţă a unei persoane prin care aceasta acceptă sau refuză încheierea unui act juridic. Doctrina clasică, pornind de la principiile dreptului roman, a identificat condiţiile esenţiale ale unui consimţământ valabil: acesta trebuie să fie serios – exprimat cu intenţia de a produce efecte juridice –, liber – neviciat prin eroare, dol sau violenţă – şi în cunoştinţă de cauză, ceea ce presupune că persoana dispune de informaţiile relevante pentru a lua o decizie raţională.

Viciile de consimţământ – eroarea, dolul şi violenţa – sunt reglementate în toate codurile civile de tradiţie romanistă, inclusiv în Codul Civil al Republicii Moldova [7] şi în Codul Civil Român [6]. Dolul, definit ca inducerea în eroare a celeilalte părţi prin mijloace viclene sau prin omisiunea intenţionată a unor informaţii esenţiale, prezintă cea mai mare relevanţă în contextul algoritmilor de personalizare, întrucât mecanismele dark patterns pot fi calificate, în anumite circumstanţe, drept mijloace dolosive în sens juridic, subminând liberul arbitru al consumatorului.

Autonomia de voinţă – principiul libertăţii contractuale combinat cu regula „pacta sunt servanda" – constituie, în dreptul privat modern, prezumţia de bază a oricărei interacţiuni juridice. Această autonomie devine însă o ficţiune în condiţiile în care mediul decizional al consumatorului este construit şi optimizat de algoritmi cu scopuri comerciale, iar consumatorul nu poate percepe şi nici înţelege mecanismele care îi modelează preferinţele şi comportamentul.

Consimţământul în dreptul european al consumatorului

Dreptul european al consumatorului a construit, în decursul ultimilor patruzeci de ani, un edificiu normativ care recunoaşte dezechilibrul structural dintre consumator şi comerciant şi încearcă să îl corecteze prin mecanisme de protecţie specifice. Directiva 93/13/CEE privind clauzele abuzive [8], Directiva 2011/83/UE privind drepturile consumatorilor [9] şi Directiva 2005/29/CE privind practicile comerciale neloiale [10] formează nucleul acestui corpus normativ, aplicabil şi în contextul comercializării de produse şi servicii prin intermediul platformelor digitale.

Principiul transparenţei informaţionale constituie pilonul central al protecţiei consumatorului digital. Comerciantul are obligaţia de a furniza consumatorului, anterior încheierii contractului, informaţii clare, complete şi comprehensibile privind natura produsului sau serviciului, preţul total, condiţiile de reziliere, dreptul de retragere şi identitatea comerciantului. Aceste obligaţii, concepute iniţial pentru mediul comercial tradiţional, de-

vin insuficiente în contextul algoritmizat, în care condițiile contractuale sunt prezentate prin interfețe optimizate să descurajeze lectura și înțelegerea lor.

Jurisprudența Curții de Justiție a Uniunii Europene a evoluat treptat spre o interpretare funcțională a consimțământului consumatorului, recunoscând că simplul acces la informație nu echivalează cu informarea reală. În cauza Planet49 [11], Curtea a statuat că bifarea prealabilă a căsuțelor de consimțământ nu constituie un consimțământ valabil în sensul Directivei ePrivacy și al RGPD, trasând astfel o linie clară între consimțământul formal și cel real, cu caracter de precedent interpretativ în materia platformelor digitale.

Consimțământul în regimul RGPD – standard ridicat și limitele sale practice

RGPD a reprezentat un salt calitativ major în materia consimțământului privind prelucrarea datelor cu caracter personal. Art. 4 alin. (11) definește consimțământul ca „orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, că datele cu caracter personal care o privesc să fie prelucrate". Considerentul 42 precizează că consimțământul nu ar trebui să fie valabil în cazul în care persoana vizată nu are posibilitatea reală de a alege sau este constrânsă, în orice mod, să și-l acorde.

Cerința că consimțământul să fie „liber" (freely given) ridică probleme acute în contextul platformelor digitale. Art. 7 alin. (4) din RGPD și Considerentul 43 stabilesc că atunci când executarea unui contract sau furnizarea unui serviciu este condiționată de acordarea consimțământului pentru prelucrarea datelor care nu este necesară pentru executarea contractului, consimțământul nu este liber. Totuși, modelul de business al majorității platformelor digitale gratuite se bazează tocmai pe această condiționare implicită: accesul la serviciu este schimbat pe consimțământul la profilarea comportamentală și la publicitatea targetată (îndreptată spre un grup-țintă).

Comitetul European pentru Protecția Datelor (CEPD) a emis Orientările 05/2020 privind consimțământul [12], care clarifică în detaliu condițiile unui consimțământ valid în temeiul RGPD, subliniind că dezechilibrul de putere dintre platformele digitale și utilizatorii individuali creează o prezumție de constrângere care poate invalida consimțământul. Cu toate acestea, implementarea practică a acestor orientări rămâne deficitară, întrucât mecanismele de control și sancțiune variază semnificativ de la un stat membru la altul, generând o aplicare inegală a standardului european

Dark patterns – manipularea consimțământului prin design digita

Definiție și taxonomie

Conceptul de „dark patterns" a fost introdus în literatura academică de Harry Brignull [13] în 2010, pentru a descrie tehnicile de design al inter-

feţei utilizator care manipulează utilizatorul să ia decizii nedorite sau neavantajoase pentru el, în beneficiul platformei. Deşi termenul are origine în designul UX (User Experience), acesta a dobândit rapid relevanţă juridică, reprezentând una dintre cele mai semnificative provocări pentru consimţământul liber al consumatorului online.

Comitetul European pentru Protecţia Datelor a publicat în 2022 Orientările 03/2022 privind modelele de interfaţă înşelătoare [14], identificând şase categorii principale: (i) overloading – supraîncărcarea utilizatorului cu informaţii, solicitări sau opţiuni pentru a-l determina să accepte mai mult decât intenţionează; (ii) skipping – proiectarea interfeţei în aşa fel încât utilizatorul să omită informaţii sau setări de protecţie importante; (iii) stirring – apelul la emoţii sau exploatarea prejudecăţilor cognitive pentru a influenţa decizia utilizatorului; (iv) obstructing – crearea de obstacole în calea utilizatorilor care doresc să-şi protejeze viaţa privată sau să-şi retragă consimţământul; (v) fickle – proiectarea inconsistentă a interfeţei care induce confuzie; (vi) left in the dark – utilizatorul nu primeşte informaţii suficiente pentru a înţelege consecinţele acţiunilor sale.

Această taxonomie are o importanţă juridică deosebită, întrucât permite operaţionalizarea conceptelor juridice tradiţionale – dolul, practicile înşelătoare, clauzele abuzive – în contextul specific al interfeţei digitale. Dark patterns nu sunt simple inconveniențe tehnice: ele reprezintă, în esența lor juridică, tehnici de viciere a consimțământului consumatorului, cu consecințe asupra valabilității actelor juridice încheiate în astfel de condiții.

Mecanisme concrete de viciere a consimţământului

Analiza practicilor concrete ale platformelor digitale permite identificarea unor mecanisme specifice de viciere a consimţământului, fiecare cu o calificare juridică distinctă şi cu consecinţe diferite asupra valabilităţii actului juridic sau a răspunderii operatorului.

a) Confirmshaming – utilizarea unor texte cu încărcătură emoţională negativă pentru opţiunea de refuz (de exemplu: „Nu, prefer să rămân neinformat" sau „Nu doresc oferte avantajoase"), în scopul inducerii unui sentiment de vinovăţie sau inadecvare care îl determină pe utilizator să accepte. Această practică poate fi calificată drept practică comercială agresivă în sensul art. 8-9 din Directiva 2005/29/CE, întrucât exercită o presiune psihologică nejustificată asupra consumatorului, afectând în mod semnificativ libertatea sa de alegere.

b) Roach motel – crearea unui sistem în care intrarea (acceptul consimţământului, înscrierea la un serviciu) este facilă, iar ieşirea (retragerea consimţământului, dezabonarea) este deliberat dificilă sau obscură. Această practică violează direct cerinţa art. 7 alin. (3) din RGPD, potrivit căreia re-

tragerea consimțământului trebuie să fie la fel de ușoară ca acordarea lui, și poate constitui totodată o clauză abuzivă în sensul Directivei 93/13/CEE, prin crearea unui dezechilibru semnificativ în detrimentul consumatorului.

c) Misdirection – atragerea atenției utilizatorului spre elemente vizuale care distrag de la opțiunile de protecție a datelor sau de la informațiile relevante pentru consimțământ. Prin tehnici de design (culori, dimensiuni, animații, contrast), platforma ierarhizează vizual informația în favoarea opțiunilor care îi servesc interesele comerciale. Această practică poate constitui o omisiune înșelătoare în sensul art. 7 din Directiva 2005/29/CE, prin prezentarea informației într-un mod care afectează capacitatea consumatorului de a lua o decizie informată.

d) Privacy zuckering – termenul desemnează practica de a înșela utilizatorul să partajeze mai multe informații personale decât intenționează, prin interfețe proiectate să maximizeze divulgarea. Aceasta ridică probleme atât în temeiul RGPD – principiul minimizării datelor, art. 5 alin. (1) lit. c) –, cât și în dreptul comun al contractelor, prin lipsa de claritate a obiectului consimțământului acordat.

e) Trick questions – formularea întrebărilor privind consimțământul în limbaj negativ dublu sau în termeni tehnici excesiv de complecși, astfel încât să inducă în eroare utilizatorul privind consecințele alegerii sale. Această practică poate constitui un viciu de eroare sau dol în sensul dreptului civil, afectând fundamental valabilitatea consimțământului exprimat.

Dark patterns și răspunderea juridică – stadiul actual

Calificarea dark patterns ca practici ilicite și stabilirea răspunderii juridice a platformelor care le utilizează ridică provocări semnificative în dreptul pozitiv actual. Directiva 2005/29/CE oferă o bază normativă pentru calificarea dark patterns ca practici comerciale neloiale, înșelătoare sau agresive, dar aplicarea sa în contextul digital s-a dovedit deficitară, în principal din cauza dificultăților de probă și a resurselor limitate ale autorităților naționale de supraveghere.

Digital Services Act (DSA) [15], intrat în vigoare în 2022 și aplicabil în totalitate din august 2023, a adus o inovație normativă semnificativă: art. 25 interzice explicit platformelor online utilizarea de interfețe sau tehnici care induc în eroare utilizatorul, îi afectează capacitatea de alegere sau îi viciază consimțământul. Platformele de dimensiuni mari (Very Large Online Platforms – VLOPs) au obligații suplimentare, inclusiv auditări independente anuale și accesul cercetătorilor la date, sub sancțiunea unor amenzi de până la 6% din cifra de afaceri globală anuală.

Micro-„targetarea" și manipularea comportamentală – dimensiunea juridică

Micro-„targetarea" – concept și implicații juridice

Micro-targetarea (micro-targeting) reprezintă practica de difuzare a unor mesaje personalizate – comerciale, politice sau de altă natură – către segmente extrem de precise de utilizatori, definite pe baza unor profiluri comportamentale detaliate. Tehnica, dezvoltată inițial în marketing politic, a fost generalizată în toate domeniile comunicării comerciale și non-comerciale online, devenind astăzi un instrument standard al economiei digitale.

Din perspectivă juridică, micro-„targetarea" ridică probleme de ordin constituțional – dreptul la viață privată, libertatea de opinie, egalitatea de tratament –, civil – consimțământul, dolul, abuzul de drept – și administrativ – protecția datelor, practicile comerciale neloiale. Specificul micro-targetării constă în aceea că exploatează nu numai comportamentul trecut al utilizatorului, ci și vulnerabilitățile sale psihologice actuale, momentele de fragilitate emoțională sau circumstanțele personale nefavorabile, amplificând astfel riscul de viciere a consimțământului.

Scandalul Cambridge Analytica [16], care a demonstrat utilizarea datelor personale a milioane de utilizatori Facebook pentru micro-targetare politică, a reprezentat un punct de inflexiune în conștientizarea publică și politică a acestor riscuri. Anchetele desfășurate ulterior de autoritățile de protecție a datelor din Irlanda, Marea Britanie și Statele Unite au confirmat că practicile de micro-targetare pot depăși limitele consimțământului acordat de utilizatori și pot constitui prelucrări de date ilegale, cu consecințe sancționatorii semnificative pentru operatori.

Exploatarea vulnerabilităților cognitive și psihologice

Economia comportamentală, fondată de Kahneman și Tversky [17] și dezvoltată ulterior de Thaler și Sunstein[18] prin conceptul de „nudge", a demonstrat că deciziile umane nu sunt rezultatul unui proces de maximizare rațională a utilității, ci sunt puternic influențate de factori cognitivi, emoționali și contextuali. Algoritmii de personalizare exploatează sistematic aceste descoperiri ale psihologiei cognitive pentru a-și atinge obiectivele comerciale.

Principalele vulnerabilități cognitive exploatate de algoritmii de personalizare includ: (i) efectul de ancorare (anchoring effect) – prezentarea unui preț de referință ridicat înainte de cel real, pentru a-l face pe acesta să pară mai avantajos; (ii) efectul de disponibilitate (availability heuristic) – afișarea preferențială a recensiunilor pozitive care confirmă valoarea produsului; (iii) aversiunea față de pierdere (loss aversion) – accentuarea riscului de a „pierde" o ofertă limitată în timp, pentru a crea urgență artificială; (iv) efectul de dotare (endowment effect) – oferirea de probe gratuite urmată de facturare automată, mizând pe inerția utilizatorului.

Din punct de vedere juridic, exploatarea sistematică a acestor vulne-

rabilități cognitive prin algoritmi de personalizare poate constitui o practică comercială agresivă în sensul Directivei 2005/29/CE, dacă afectează în mod semnificativ libertatea de alegere a consumatorului mediu. Conceptul de „consumator mediu" utilizat ca standard de referinţă în dreptul european al consumatorului devine însă problematic atunci când comportamentul consumatorului este sistematic modelat de algoritmi, întrucât standardul normativ este construit pe premisa unui consumator care acţionează în condiţii decizionale neutre.

Profilarea și decizia automatizată – regimul art. 22 RGPD

Art. 22 din RGPD consacră dreptul persoanei vizate de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv profilarea, care produce efecte juridice sau care o afectează în mod semnificativ într-un mod similar. Această dispoziţie are o relevanţă deosebită pentru algoritmii de personalizare care generează decizii automate privind accesul la produse, preţuri, servicii financiare sau oportunităţi de angajare.

Condiţiile în care decizia automatizată este permisă prin excepţie (art. 22 alin. (2) RGPD) includ: (a) necesitatea pentru executarea sau încheierea unui contract; (b) autorizarea printr-un act legislativ al Uniunii sau al statului membru; (c) consimţământul explicit al persoanei vizate. În toate aceste cazuri, operatorul trebuie să implementeze „măsuri adecvate" pentru protejarea drepturilor persoanei vizate, inclusiv dreptul de a obţine intervenţie umană, de a-şi exprima punctul de vedere şi de a contesta decizia.

Interpretarea CJUE şi a CEPD sugerează că termenul „afectează în mod semnificativ" trebuie interpretat extensiv, incluzând nu numai deciziile cu efecte juridice formale, ci şi pe cele care influenţează substanţial comportamentul sau oportunităţile persoanei vizate. Prin această interpretare, o parte semnificativă a deciziilor generate de algoritmii de personalizare ar putea cădea sub incidenţa art. 22 RGPD, cu consecinţa necesităţii unui consimţământ explicit şi a garantării dreptului la intervenţie umană [18].

Cadrul juridic european și internațional – analiză comparativă

Pilonii legislativi europeni

Uniunea Europeană a adoptat în ultimii ani un pachet legislativ fără precedent în materia reglementării algoritmilor şi a platformelor digitale, care transformă fundamental raportul de putere dintre platforme și utilizatori. Principalele instrumente juridice cu relevanţă directă pentru subiectul prezentei analize sunt:

Regulamentul General privind Protecţia Datelor (RGPD) reprezintă, cum am arătat, standardul de referinţă pentru consimţământul privind prelucrarea datelor. Sancţiunile prevăzute – până la 4% din cifra de afaceri globală anuală sau 20 milioane EUR, oricare este mai mare – au demonstrat un

efect disuasiv semnificativ, amenzile impuse platformelor majore atingând sute de milioane de euro, cu efecte de conformare la nivelul întregii industrii.

Digital Services Act (DSA) introduce obligații specifice pentru platformele online privind transparența algoritmilor de recomandare (art. 27), interzicerea publicității targetate bazate pe date sensibile sau direcționate către minori (art. 26) și interzicerea dark patterns (art. 25). Platformele de dimensiuni mari au obligații suplimentare, inclusiv auditări independente anuale și accesul cercetătorilor la datele privind funcționarea algoritmilor de recomandare.

Digital Markets Act (DMA) – Regulamentul (UE) 2022/1925 [19] – vizează platformele cu putere de gatekeeper pe piețele digitale, impunând obligații specifice privind interoperabilitatea, portabilitatea datelor și interzicerea combinării datelor utilizatorilor din diferite surse fără consimțământ explicit. DMA creează astfel o presiune structurală pentru reducerea dependenței utilizatorilor de o singură platformă și pentru creșterea concurenței, factori care contribuie indirect la consolidarea libertății de alegere a consumatorului.

AI Act [20] – adoptat în 2024 – introduce o abordare bazată pe risc pentru reglementarea sistemelor de inteligență artificială, clasificând anumite aplicații ca având „risc inacceptabil" – interzise, cum ar fi sistemele de manipulare subliminală sau de scoring social – sau „risc ridicat" – supuse unor cerințe stricte de transparență și audit. Sistemele care utilizează tehnici subliminale pentru a influența comportamentul consumatorului în detrimentul acestuia vor fi interzise, reprezentând un pas major în protecția autonomiei de voință în mediul digital

Abordarea SUA – autoreglementare și litigii private

Statele Unite nu dispun de un cadru legislativ federal unitar în materia protecției datelor personale sau a reglementării algoritmilor de personalizare, adoptând în schimb o abordare sectorială și bazată preponderent pe autoreglementare și litigii private. California Consumer Privacy Act (CCPA), adoptat în 2018 și modificat prin California Privacy Rights Act (CPRA) în 2020, reprezintă cel mai avansat instrument legislativ la nivel de stat, recunoscând consumatorilor dreptul de opt-out din vânzarea datelor personale și din profilare pentru publicitate, servind ca model pentru legislații similare din alte state.

Federal Trade Commission (FTC) a jucat un rol central în reglementarea practicilor de personalizare prin acțiuni de enforcement bazate pe Secțiunea 5 a FTC Act, care interzice practicile înșelătoare sau neloiale în comerț. Constatările FTC în cazuri majore (Facebook/Meta, Google, Amazon) au demonstrat că practicile de colectare excesivă de date și de profilare fără

un consimțământ real pot constitui practici înșelătoare. Totuși, sancțiunile financiare impuse de FTC, deși record ca valoare absolută, reprezintă adesea o fracțiune neglijabilă din veniturile platformelor, limitând semnificativ efectul disuasiv.

Proliferarea litigiilor private de tip class action în instanțele americane a compensat parțial limitele acțiunilor administrative. Cauze precum In re Facebook, Inc. Consumer Privacy User Profile Litigation sau Calhoun v. Google LLC au generat despăgubiri substanțiale și au contribuit la conturarea standardelor privind consimțământul informat în mediul digital. Totuși, complexitatea tehnică a algoritmilor de personalizare creează dificultăți probatorii semnificative pentru reclamanți, limitând accesul efectiv la justiție al consumatorilor individuali.

Cadrul normativ în Republica Moldova

Republica Moldova, în calitate de stat asociat al Uniunii Europene prin Acordul de Asociere semnat în 2014 și candidat la aderarea la UE din iunie 2022, a adoptat un parcurs de aliniere a legislației naționale la acquis-ul comunitar în materia protecției datelor și a drepturilor consumatorilor, cu progrese semnificative în ultimii ani.

Legea nr. 133/2011 privind protecția datelor cu caracter personal, supusă unui proces de revizuire pentru alinierea la standardele RGPD, reprezintă cadrul normativ de bază în materie. Centrul Național pentru Protecția Datelor cu Caracter Personal (CNPDCP) a emis recomandări și decizii în materie de consimțământ, deși resursele limitate ale instituției afectează capacitatea de supraveghere efectivă a practicilor platformelor digitale active pe teritoriul Republicii Moldova.

Legea nr. 105/2003 privind protecția consumatorilor stabilește cadrul general al drepturilor consumatorilor, inclusiv dreptul la informare corectă și completă. Transpunerea directivelor europene în materia practicilor comerciale neloiale și a drepturilor consumatorilor a furnizat instrumente juridice suplimentare, dar aplicarea lor în contextul platformelor digitale și al algoritmilor de personalizare rămâne insuficient dezvoltată atât în practica judiciară, cât și la nivelul organelor de supraveghere, reflectând o lacună instituțională care necesită adresare urgentă.

Lacune legislative și provocări practice

Insuficiența conceptului de „consumator mediu" în era algoritmică

Standardul „consumatorului mediu" – persoana rezonabil informată, atentă și circumspectă – care stă la baza mare parte a legislației europene în materia practicilor comerciale, a fost conceput pentru un mediu comercial pre-digital, în care consumatorul dispunea de timp și de informație suficientă pentru a lua decizii raționale. În mediul digital contemporan, dominat de

algoritmi de personalizare, acest standard devine problematic din mai multe perspective.

În primul rând, algoritmii de personalizare sunt proiectați tocmai pentru a exploata devierile sistematice de la raționalitate ale consumatorului mediu – devieri identificate și documentate de economia comportamentală. Astfel, standardul „consumatorului mediu" legitimează, paradoxal, practici care exploatează iraționalitatea cognitivă umană ca pe o resursă. În al doilea rând, personalizarea algoritmică implică faptul că nu există un „mediu digital mediu" – fiecare utilizator trăiește o experiență online unică, construită special pentru el, ceea ce face imposibilă evaluarea practicii comerciale dintr-o perspectivă unitară și obiectivă.

O soluție parțială la această problemă o reprezintă adoptarea unui standard situațional sau funcțional, care să ia în considerare vulnerabilitatea specifică a utilizatorului în contextul concret al interacțiunii cu algoritmul. Art. 5 alin. (3) din Directiva 2005/29/CE conține deja un astfel de element, prevăzând protecție sporită pentru consumatorii vulnerabili, dar aplicarea sa în contextul digital necesită o interpretare evolutivă din partea instanțelor și a autorităților de supraveghere.

Problema opacității algoritmice și a „explainabilității"

Una dintre cele mai semnificative lacune ale cadrului juridic actual privind consimțământul în contextul algoritmilor de personalizare rezidă în opacitatea fundamentală a acestor sisteme. Algoritmii de machine learning de ultimă generație, în special rețelele neurale profunde (deep neural networks), sunt sisteme a căror funcționare internă nu poate fi înțeleasă sau explicată nici de către creatorii lor – fenomen cunoscut drept „problema cutiei negre" (black box problem) –, creând o tensiune fundamentală cu cerințele de transparență ale dreptului pozitiv.

Această opacitate creează o tensiune fundamentală cu cerința RGPD privind transparența prelucrării datelor și cu dreptul persoanei vizate de a obține explicații privind deciziile automate (art. 13-15 și art. 22 alin. (3) din RGPD). Chiar dacă operatorul furnizează informații despre logica deciziei automate, aceste informații sunt adesea insuficient de detaliate pentru a permite consumatorului să înțeleagă cu adevărat mecanismele care îi influențează comportamentul și deciziile.

Cerința de „explainabilitate" a algoritmilor de inteligență artificială, consacrată parțial de AI Act și discutată extensiv în literatura de specialitate, reprezintă un răspuns tehnico-juridic la această provocare. Cu toate acestea, există limite tehnice reale ale „explainabilității" sistemelor complexe de AI, iar soluțiile propuse (LIME, SHAP, explicații contrafactuale) rămân insuficient de intuitive pentru utilizatorul obișnuit, ridicând problema dacă „explai-

nabilitate" a tehnică echivalează cu informarea reală necesară unui consimțământ valabil în sens juridic.

Consimțământul dinamic și gestionarea preferințelor

Caracterul dinamic și continuu al prelucrării algoritmice contrastează cu natura punctuală și statică a consimțământului, astfel cum este conceput în modelele juridice tradiționale. Utilizatorul care acceptă termenii și condițiile unei platforme la momentul înregistrării nu poate anticipa cum vor evolua practicile de personalizare ale platformei în cursul anilor următori, nici cum vor fi utilizate datele acumulate pentru a-i construi un profil din ce în ce mai precis și mai predictiv.

Această problemă necesită reconsiderarea conceptului de consimțământ dinamic (dynamic consent) – un model în care utilizatorul poate gestiona continuu preferințele privind prelucrarea datelor sale și poate retrage sau modifica consimțământul acordat anterior pentru categorii specifice de prelucrări. Soluții tehnice emergente, precum Privacy Enhancing Technologies (PETs), sistemele de gestionare a consimțământului (Consent Management Platforms – CMPs) certificate și standardele tehnice privind gestionarea preferințelor, reprezintă pași în direcția corectă, dar eficiența lor rămâne limitată fără o obligativitate juridică clară și sancțiuni disuasive pentru nerespectare.

Dificultăți de „enforcement" și fragmentarea jurisdicțională

Aplicarea efectivă a cadrului juridic privind consimțământul liber al consumatorului online se confruntă cu obstacole structurale majore. Natura transfrontalieră a majorității platformelor digitale creează dificultăți de jurisdicție și de executare a sancțiunilor. Principiul „ghișeului unic" (one-stop-shop) prevăzut de RGPD a generat o concentrare excesivă a dosarelor la autoritatea de supraveghere din Irlanda, unde sunt stabilite sediile europene ale majorității platformelor majore, cu acuzații de enforcement insuficient de riguros.

Asimetria de resurse dintre autoritățile naționale de supraveghere și corporațiile tehnologice multinaționale creează un dezechilibru structural care limitează capacitatea de investigare și sancționare. Platformele dispun de echipe extinse de juriști specializați și de capacitatea de a contesta deciziile administrative prin ani de litigii, în timp ce autoritățile operează cu bugete limitate și personal insuficient specializat în aspectele tehnice ale algoritmilor de personalizare.

Dificultățile probatorii în demonstrarea relației cauzale dintre funcționarea unui algoritm de personalizare și vicierea consimțământului unui consumator specific reprezintă un obstacol semnificativ atât în procedurile administrative, cât și în litigiile civile individuale. Accesul la datele interne ale platformelor privind funcționarea algoritmilor este esențial pentru demonstrarea practicilor ilegale, dar obținerea lui în cadrul procedurilor judiciare

se dovedește extrem de dificilă, creând o asimetrie informațională profundă care dezavantajează structural consumatorul și autoritățile de supraveghere.

Propuneri de lege ferenda și recomandări de politică legislativă

Reformarea standardului de consimțământ în contextul algoritmizat

Prima propunere vizează reformarea conceptuală a consimțământului în dreptul european al consumatorului și al protecției datelor, pentru a-l adapta realităților mediului digital algoritmizat. Aceasta ar putea include: (i) introducerea unui standard de „consimțământ cu adevărat informat" (genuinely informed consent) care să impună testarea empirică a înțelegerii reale de către utilizator a consecințelor alegerii sale, nu numai furnizarea formală de informații; (ii) prezumția de viciare a consimțământului în cazul utilizării dovedite a dark patterns, cu inversarea sarcinii probei în sarcina platformei; (iii) reglementarea expresă a obligației de „design neutru" (neutral design) pentru interfețele care colectează consimțământul, cu standarde tehnice minime impuse de autoritățile de supraveghere.

Obligativitatea interoperabilității și a portabilității consimțământului

A doua propunere vizează introducerea obligativității interoperabilității sistemelor de gestionare a consimțământului și a portabilității preferințelor utilizatorului între platforme. Similar portabilității datelor prevăzute de art. 20 din RGPD, aceasta ar permite utilizatorilor să-și configureze preferințele privind personalizarea o singură dată și să le aplice pe toate platformele, eliminând necesitatea acordării repetate a consimțământului în condiții de interfață manipulate. Această abordare ar reduce semnificativ oboseala consimțământului (consent fatigue) – fenomenul prin care utilizatorul ajunge să accepte orice, din epuizare – și ar crește calitatea alegerilor efectuate.

Dreptul la un algoritm neutru de recomandare

A treia propunere, mai ambițioasă, constă în recunoașterea expresă a dreptului consumatorului de a accesa serviciile platformei prin intermediul unui algoritm neutru de recomandare – adică un sistem care nu optimizează spre obiective comerciale ale platformei, ci spre preferințele declarate explicit de utilizator. Această idee, prezentă în germene în art. 27 alin. (3) din DSA (dreptul de opt-out din recomandările bazate pe profilare), ar trebui extinsă și transformată dintr-un drept de opt-out (refuz) într-un drept de opt-in (alegere pozitivă), cu posibilitatea selecției criteriilor de recomandare de către utilizator.

Consolidarea sistemului de sancțiuni și de reparare a prejudiciului

A patra propunere vizează consolidarea sistemului de sancțiuni și de reparare a prejudiciului cauzat consumatorilor prin practici algoritmice ilegale. Aceasta ar include: (i) introducerea unei prezumții de prejudiciu în

cazul constatării utilizării dark patterns sau a profilării fără consimţământ valid, cu consecinţa facilitării acţiunilor colective ale consumatorilor; (ii) crearea unui fond de compensare pentru victimele practicilor algoritmice ilegale, finanţat din amenzile impuse platformelor; (iii) obligativitatea auditurilor independente anuale ale algoritmilor de personalizare, cu publicarea rezultatelor în format accesibil publicului, pentru a asigura transparenţa şi responsabilizarea operatorilor.

Educaţia digitală ca remediu structural

Dincolo de intervenţiile legislative, educaţia digitală a consumatorilor reprezintă un remediu structural indispensabil. Cunoaşterea mecanismelor prin care algoritmii de personalizare influenţează comportamentul decizional este o condiţie prealabilă a exercitării efective a drepturilor garantate de cadrul normativ. Propunem includerea educaţiei privind economia atenţiei şi mecanismele algoritmice în curricula educaţională de la nivel preuniversitar, precum şi campanii de informare publică coordonate de autorităţile de protecţie a consumatorilor şi de protecţie a datelor, pentru a crea un consumator digital informat şi critic.

Concluzii

Analiza desfăşurată în prezentul articol a demonstrat că algoritmii de personalizare reprezintă o provocare fundamentală pentru consimţământul liber al consumatorului în mediul online, cu implicaţii care depăşesc sfera strict tehnică şi angajează principii juridice de profunzime: autonomia de voinţă, „nedolul", transparenţa informaţională şi echilibrul raporturilor contractuale. Această provocare nu este conjuncturală – ea este structurală, înrădăcinată în modelul de business al economiei digitale, şi nu poate fi abordată prin instrumente normative concepute pentru o altă epocă.

Concluziile principale ale acestei analize pot fi sintetizate după cum urmează. În primul rând, algoritmii de personalizare nu sunt instrumente tehnice neutre – ei sunt construiţi pentru a servi obiectivele comerciale ale platformelor, structurând mediile decizionale ale consumatorilor în moduri care subminează sistematic libertatea de alegere. În al doilea rând, dark patterns reprezintă tehnici juridic calificabile de viciere a consimţământului, aplicabile normelor existente privind dolul, practicile comerciale neloiale şi clauzele abuzive, necesitând totodată o adaptare interpretativă a acestora la specificul digital.

În al treilea rând, cadrul juridic european actual – construit în jurul RGPD, DSA, DMA şi AI Act – oferă instrumente normative semnificative, dar aplicarea lor eficientă este afectată de asimetrii de putere structurale, dificultăţi probatorii şi fragmentare jurisdicţională. În al patrulea rând, concep-

te juridice tradiționale precum „consumatorului mediu" sau consimțământul punctual trebuie adaptate la dinamica algoritmică, printr-o interpretare evolutivă sau prin noi instrumente legislative.

Prezentul studiu adoptă o perspectivă pragmatic-reformistă: cadrul juridic poate și trebuie adaptat pentru a garanta o libertate reală de alegere în mediul digital, dar aceasta necesită voință politică, resurse instituționale adecvate și o colaborare transdisciplinară între juriști, experți în tehnologie, psihologi comportamentali și economiști. Protecția consimțământului liber al consumatorului nu este o chestiune de reglementare formală sau de birocrație normativă – ea reprezintă, în esență, protecția demnității umane și a autonomiei individuale în fața puterii crescânde a corporațiilor algoritmice, o misiune fundamentală a dreptului contemporan.

Surse bibliografice:

1. 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 (RGPD), publicat în Jurnalul Oficial al Uniunii Europene L 119 din 4 mai 2016.

2. Pariser, Eli, The Filter Bubble: What the Internet Is Hiding from You, Penguin Press, New York, 2011.

3. Simon, Herbert A., „Designing Organizations for an Information-Rich World", în Greenberger, Martin (ed.), Computers, Communication, and the Public Interest, Johns Hopkins Press, Baltimore, 1971, pp. 40-41.

4. Wu, Tim, The Attention Merchants: The Epic Scramble to Get Inside Our Heads, Alfred A. Knopf, New York, 2016

5. Zuboff, Shoshana, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, PublicAffairs, New York, 2019.

6. Codul Civil al Republicii Moldova, adoptat prin Legea nr. 1107 din 6 iunie 2002, republicat în Monitorul Oficial al Republicii Moldova nr. 66-75 din 1 martie 2019.

7. Legea nr. 287/2009 privind Codul Civil Român, publicată în Monitorul Oficial al României, Partea I, nr. 511 din 24 iulie 2009.

8. Directiva Consiliului 93/13/CEE din 5 aprilie 1993 privind clauzele abuzive în contractele încheiate cu consumatorii, publicată în Jurnalul Oficial al Comunităților Europene L 95 din 21 aprilie 1993.

9. Directiva 2011/83/UE a Parlamentului European și a Consiliului din 25 octombrie 2011 privind drepturile consumatorilor, publicată în Jur-

nalul Oficial al Uniunii Europene L 304 din 22 noiembrie 2011.

10. Directiva 2005/29/CE a Parlamentului European şi a Consiliului din 11 mai 2005 privind practicile comerciale neloiale ale întreprinderilor faţă de consumatori pe piaţa internă, publicată în Jurnalul Oficial al Uniunii Europene L 149 din 11 iunie 2005.

11. CJUE, hotărârea din 1 octombrie 2019, Bundesverband der Verbraucherzentralen und Verbraucherverbände c. Planet49 GmbH, Cauza C-673/17, ECLI:EU:C:2019:801.

12. Comitetul European pentru Protecţia Datelor, Orientări 05/2020 privind consimţământul în temeiul Regulamentului 2016/679, versiunea 1.1, adoptate la 4 mai 2020.

13. Brignull, Harry, „Dark Patterns: Deception vs. Honesty in UI Design", prezentare la conferința UX Brighton, 2010, disponibilă la https://www.deceptive.design

14. Comitetul European pentru Protecţia Datelor, Orientări 03/2022 privind modelele de interfaţă înşelătoare pe platformele de socializare, adoptate la 14 martie 2022.

15. Regulamentul (UE) 2022/2065 al Parlamentului European şi al Consiliului din 19 octombrie 2022 privind o piaţă unică pentru serviciile digitale (Digital Services Act – DSA), publicat în Jurnalul Oficial al Uniunii Europene L 277 din 27 octombrie 2022.

16. Information Commissioner's Office (UK), „Investigation into the use of data analytics in political campaigns", Raport final, noiembrie 2018. A se vedea şi Cadwalladr, Carole; Graham-Harrison, Emma, „Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", The Guardian, 17 martie 2018.

17. Kahneman, Daniel; Tversky, Amos, „Prospect Theory: An Analysis of Decision under Risk", Econometrica, vol. 47, nr. 2, 1979, pp. 263-291.

18. Thaler, Richard H.; Sunstein, Cass R., Nudge: Improving Decisions about Health, Wealth, and Happiness, Yale University Press, New Haven, 2008.

19. Regulamentul (UE) 2022/1925 al Parlamentului European şi al Consiliului din 14 septembrie 2022 privind pieţele contestabile şi echitabile în sectorul digital (Digital Markets Act – DMA), publicat în Jurnalul Oficial al Uniunii Europene L 265 din 12 octombrie 2022.

20. Regulamentul (UE) 2024/1689 al Parlamentului European şi al Consiliului din 13 iunie 2024 privind stabilirea unor norme armonizate privind inteligenţa artificială (AI Act), publicat în Jurnalul Oficial al Uniunii Europene L, 2024/1689, 12 iulie 2024.