ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVI/SUPLIMENT, ŞTIINŢE JURIDICE, 2020

# Reflecţii juridice cu privire la activităţile de „urmărire” şi „publicitate personalizată” pe reţelele sociale

# Legal reflections on tracking and targeted advertising on social networks

**Lăcrămioara Popa, Lorena-Elena Stănescu**[1]

**Rezumat:** Activităţile de monitorizare a utilizatorilor şi publicitate personalizată în cadrul reţelelor sociale au reprezentat subiectul criticilor din raţiuni psiho-sociale, dar observăm că, după intrarea în vigoare a Regulamentului general privind protecţia datelor, instanţele europene n-au ezitat să sancţioneze aceste practici. În prezentul articol supunem unei analize comparative politicile de confidenţialitate ale principale reţele sociale prin examinarea condiţiilor de colectarea a informaţiilor despre utilizatori, dar nu numai, şi de folosire a acestor pentru scopurile de publicitate. Gândindu-ne la cazul Cambridge Analytica, dincolo de interesele politice aflate la mijloc, înţelegem din analiza faptelor petrecute că supravegherea pasivă a utilizatorilor ce folosesc diverse platforme de socializare a trecut la o formă de control activ a vieţilor acestora şi a structurilor sociale construite organic de către oameni. Prelucrarea automată a profilurilor de utilizatori şi recomandarea selectivă doar a unor tipuri de mesaje, respectiv, persoane, pune în pericol însăşi libertatea de a alege.

**Cuvinte-cheie**: reţele sociale; urmărire; publicitate personalizată; profilare; protecţia datelor.

**Abstract**: Users tracking activities and targeted advertising on social networks have been the subject of criticism for psycho-social reasons, but we note that after the entry into force of the General Regulation on the protection of data, European courts have not hesitated to sanction these practices. In this article, we conduct a comparative analysis of the privacy policies of the main social networks by examining the conditions for collecting information about their users, but not only users, and using them for advertising purposes. Considering the case of Cambridge Analytica, beyond the political interests at stake, we understand from the analysis of the past facts that the passive surveillance of users using various social platforms has moved to a form of active control of their lives and the social structures built organically by the people. The automated processing of the users profiles and the targeted recommendation of only certain types of messages, respectively, people, puts in danger the freedom to choose itself.

**Keywords**: social networks; tracking; targeted advertising; profiling; data protection.

[1] Adresa de e-mail: lacramioara.maftei@gmail.com.

## 1. Distopia digitală

De principiu, accesarea serviciilor reţelelor sociale este gratuită. Gratuitatea aduce, însă, la pachet un set de condiţii contractuale prin care utilizatorul acceptă implicit sau explicit, în funcţie de situaţie, monitorizarea comportamentului său pentru scopul unor servicii de publicitate ce finanţează activitatea platformei digitale. Astfel, se naşte „Dilema socială”[2] ce ne arată că „utilizatorul nu este mereu conştient (n.n. că este monitorizat) şi este posibil să nu reiasă imediat din natura serviciului prestat, ceea ce face aproape imposibil ca persoana vizată să facă în practică o alegere în cunoştinţă de cauză în ceea ce priveşte utilizarea datelor sale.”[3]. Această lipsă de vizibilitate a utilizatorului cu privire la datele sale „poate conduce la situaţii în care utilizatorii pierd orice control asupra difuzării datelor lor, în funcţie de modul – transparent sau opac – în care se efectuează colectarea şi prelucrarea acestor date”[4].

Analizând fluxul datelor – provenite direct sau indirect de la utilizatori – se conturează tot mai clar ideea că modelul de afaceri al reţelelor de socializare se bazează pe agregarea şi dezvoltarea unor baze de date în vederea extragerii informaţiilor ce pot oferi valoare pentru alte companii cum sunt agenţiile de publicitate sau firmele ce se promovează în mediul online. Prin urmare, reţelele sociale generează valoare pentru companii.

Într-un efort de a majora profiturile şi eficacitatea anunţurilor publicate, companiile dezvoltă constant practici publicitare inovatoare, folosind cele mai avansate tehnologii digitale disponibile. Dintre metodele utilizate pentru creşterea impactului asupra destinatarilor, companiile utilizează metode de publicitate personalizată[5] ce măresc probabilitatea ca mesajele lor de promovare să ajungă la publicul potrivit.

---

[2] Un documentar despre cum sunt construite reţelele sociale şi potenţialele consecinţe asupra dezvoltării societăţii. Mai multe informaţii la adresa: https://financialintelligence.ro/cnbc-documentarul-de-pe-netflix-dilema-sociala-ii-determina-pe-utilizatorii-de-social-media-sa-regandeasca-facebook-instagram-si-altele/, accesată la 14.11.2020.

[3] Orientările 2/2019 privind prelucrarea datelor cu caracter personal în temeiul articolului 6 alineatul (1) litera (b) din RGPD în contextul furnizării de servicii online persoanelor vizate, adoptate la data de 8 octombrie 2019, de către Autoritatea Europeană pentru Protecţia Datelor, disponibile la adresa: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_ro.pdf, accesată la 14.11.2020, denumite în continuare „*Orientările 2/2019*”.

[4] Grupul de lucru „Articolul 29” pentru protecţia datelor, Avizul 8/2014 privind evoluţiile recente din sfera internetului obiectelor adoptat la 16 septembrie 2014, p.8, denumit în continuare „*Avizul 8/2014*”.

[5] Publicitatea contextuală, publicitatea bazată pe geo-localizare, publicitatea comportamentală.

„*Behavioural targeting*” (publicitatea comportamentală) este un tip de publicitate „bazată pe observarea comportamentului indivizilor în timp, vizând studierea caracteristicilor acestui comportament luând în considerare acţiunile acestora (vizitarea repetată a unor site-uri, interacţiunile, cuvintele cheie, producţia de conţinuturi online etc.), pentru realizarea unui profil specific şi furnizarea, în acest fel, a unor materiale publicitare adaptate intereselor persoanelor vizate, astfel cum pot fi deduse din acest comportament”[6].

Furnizorii de reţele de socializare intră în posesia datelor: (i) prin colectarea directă de la persoane fizice (de exemplu: postări, mesaje, reacţii), (ii) prin colectarea indirectă de la utilizatori prin observarea activităţii online a acestora, folosind tehnologii de urmărire (de exemplu, cookie-uri, pixeli de urmărire) şi (iii) prin obţinerea de la terţi (platforme de campanii online, servicii de marketing de date şi aplicaţii folosite de utilizatori).

Într-un astfel de scenariu, personalizarea poate avea consecinţe grave, deoarece ar putea implica faptul că, comportamentul (ne)utilizatorilor este manipulat, libertatea de autodeterminare şi autonomia personală sunt limitate, iar libertatea societăţii este erodată. Conceptul de „personalizare” ca atare nu este unul nou, deoarece includerea şi excluderea fac parte din viaţa noastră de zi cu zi, precum şi adaptarea la situaţii şi, în acest caz, tehnologii noi. Cu toate acestea, controlul facilitat de serviciile de personalizare poate avea consecinţe (grave) asupra libertăţii informaţiei, precum şi asupra interesului public al diversităţii culturale şi politice.

Dintre cele mai cunoscute situaţii în care reţelele sociale au participat, chiar şi neintenţionat, la campaniile de dezinformare, în Raportul Comisiei LIBE[7] sunt menţionate propagandă politică digitală cu ocazia alegerilor din SUA din 2016[8], Cambridge Analytica[9], Referendumul Brexit (2016)[10], campania

[6] Grupul de lucru „Articolul 29” pentru protecţia datelor, Avizul 2/2010 privind publicitatea comportamentală online, din 22 iunie 2010, , p.5.

[7] Comisia pentru libertăți civile, justiție și afaceri interne din cadrul Parlamentului European, *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, disponibil la adresa: https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2019)608864, accesată la 12.11.2020, pp. 41-50.

[8] *Russia 'meddled in all big social media' around US election*, 17.12.2018, disponibil la adresa: https://www.bbc.com/news/technology-46590890, accesată la 05.10.2020; S.C. Woolley, P.N. Howard, *Computational propaganda. Political parties, politicians, and political manipulation on social media,* Oxford University Press, New York, 2019, pp.21-40. *„ EU strategic communication to counteract anti-EU propaganda by third parties* ”din data de 23.11.2016, disponibilă la adresa: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016IP0441&from=DE, accesată în 05.10.2020.

[9] Rezoluţia Parlamentului European din 25 octombrie 2018 referitoare la folosirea datelor utilizatorilor Facebook de către Cambridge Analytica şi impactul asupra protecţiei datelor, disponibilă la adresa: https://www.europarl.europa.eu/doceo/

împotriva Rohingya din Myanmar[11], precum şi alegerile electorale din Franţa (2017)[12], campania anti-migranţi şi anti-Soroş[13], alegerile generale din Italia din 2018, alegerile prezidenţiale din Brazilia din 2018[14].

Studiile de caz ne arată că metodele de urmărire şi de profilare a oamenilor şi campaniile de manipulare încalcă, direct sau indirect, drepturilor şi libertăţile omului. Analiza juridică a situaţiilor de fapt expuse relevă două categorii principale de probleme : (1) impactul asupra protecţiei datelor, confidenţialităţii, demnităţii umane şi autonomiei şi (2) încălcarea libertăţii de exprimare şi a dreptului de a căuta şi primi informaţii.

Dreptul la viaţă privată garantează libertatea de autodeterminare a indivizilor, dreptul lor de a fi diferiţi, de a avea propria identitate şi autonomia de a se angaja în relaţii, libertatea de alegere, autonomia lor în ceea ce priveşte

document/TA-8-2018-0433_RO.html, accesată la 06.10.2020. K. Ward, *Social networks, the 2016 US presidential election, and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioral microtargeting*, Journal of Media Ethics, 33:3, 2018, DOI: 10.1080/23736992.2018.1477047, p. 133.

[10] L. Dearden, "*Pro-Brexit Twitter Account with 100,000 Followers Could Be Part of Russian 'Disinformation Campaign.*'", *The Independent*, August, 2017, articol disponibil la adresa: http://www.independent.co.uk/news/uk/home-news/david-jones-pro-brexit-ukip-twitter-account-russia-fake-bot-troll-trump-disinformation-followers-a7920181.html), accesată la 12.11.2020. P. Howard, B. Kollanyi,*#StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum*, COMPROP Research note 2016.1: Oxford University, disponibil la adresa: https://arxiv.org/ftp/arxiv/papers/1606/1606.06356.pdf, accesată în 12.11.2020. Comisia pentru libertăţi civile, justiţie şi afaceri interne din cadrul Parlamentului European, *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, pp. 41-42, disponibil la adresa: https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2019)608864, accesată în 12.11.2020.

[11] P. Mozur, A *Genocide Incited on Facebook, With Posts From Myanmar's Military*, The New York Times, 18.10.2018, sec. Technology, disponibil la adresa: https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html, accesat la 12.11.2020. BBC News,*Facebook admits it was used to 'incite offline violence' in Myanmar*, 6.11.2018, disponibil la adresa: https://www.bbc.com/news/world-asia-46105934, accesată la 12.11.2020.

[12] Este suspectat Guvernul rus că ar fi urmărit reducerea şanselor de câştig a candidatului „*En Marche*", Emmanuel Macron, şi promovarea candidatei Frontului Naţional, Marine Le Pen, prin acţiuni ca „spargerea" adreselor de e-mail şi „scurgerea" de informaţii confidenţiale, spionarea pe Facebook, răspândirea propagandei pe RT şi Sputnik.

[13] Conform studiilor, Guvernul maghiar a urmărit consolidarea loialităţii faţă de partidul de guvernământ Fidesz şi politica sa externă.

[14] A fost folosită aplicaţia WhatsApp pentru transmiterea alegătorilor de multe mesaje de dezinformare.

– de exemplu – sexualitatea, sănătatea[15], construirea personalităţii, aspectele sociale şi comportamentale şi aşa mai departe[16].

## 2. Cu privire la încălcările drepturilor şi libertăţilor fundamentale pe platformele de socializare

Oamenii au devenit detectabili şi corelabili mult dincolo de controlul lor, şi urmele pe care le produc încep aibă propria identitate, devenind resursele unei reţele de profilare ce generează informaţii direct sau indirect despre acestea. O astfel de schimbare necesită o monitorizare atentă din perspectiva statului constituţional democratic, deoarece presupune, probabil, o serie de ameninţări şi riscuri, cum ar fi influenţarea comportamentului individual (acţionezi diferit dacă ştii că urmele pe care le laşi vor fi analizate), pierderea controlului, personalizarea şi normalizarea conduitei, eroziunea consecventă a libertăţii atât negative, cât şi pozitive, şi, nu în ultimul rând, luarea deciziilor nemotivate şi unilaterale despre indivizi[17].

Nu putem beneficia de un spaţiu virtual sigur, cu o securitate cibernetică eficace, solidă, decât dacă aceasta se bazează pe drepturile şi libertăţile fundamentale, valori consacrate prin Declaraţia universală a drepturilor omului, Carta drepturilor fundamentale a Uniunii Europene şi Convenţia europeană pentru apărarea drepturilor omului şi a libertăţilor fundamentale.

### *2.1. Cu privire la activităţile de „tracking”, „profiling” şi „microtargeting” a utilizatorilor pe platformele digitale prin intermediul tehnologiilor online*

Tehnologiile online de urmărire („*tracking*”) şi de publicitate utilizează informaţiile primite de pe browserul şi dispozitivile utilizatorului. Principala tehnologie de urmărire utilizată pentru monitorizarea utilizatorilor pe internet se bazează pe „module cookie de urmărire”, ce pot oferi date despre activitatea online a utilizatorilor pentru o perioadă îndelungată de timp şi pentru domenii diferite. Din categoria tehnologiile de urmărire mai pot fi menţionate utilizarea adreselor IP, a amprentelor digitale, identificatori de dispozitiv – cum ar fi Identificatorii Apple iOS pentru agenţii de publicitate („IDFA”) şi ID-ul de publicitate Google Android, semnăturilor browserelor.

---

[15] *A se vedea,* Ş.R. Tataru, *Protecţia datelor cu caracter personal în activitatea farmaciilor online*, Analele ştiinţifice ale Universitaţii „Alexandru Ioan Cuza” din Iaşi Tomul LXIV, Ştiinţe Juridice, 2018, Supliment.

[16] P. de Hert, S. Gutwirth, *„Privacy, data protection and law enforcement. Opacity of the individual and transparency of power”* în E. Claes, A. Duff, S. Gutwirth (eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2006, p. 70.

[17] M. Hildebrandt, S. Gutwirth (auth.), M. Hildebrandt, S. Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Netherlands, 2008, p. 291.

*2.2. Exemple de activităţi de „tracking" şi „profiling" desfăşurate pe platformele digitale*

Facebook are o politică de utilizare a datelor formulată simplu, completă şi bine organizată. Ceea ce este îngrijorător constă în faptul că Facebook nu doar colectează date de la utilizatori pe baza propriilor informaţii oferite de aceştia, ci poate colecta informaţii despre un utilizator de la prietenii acelui utilizator. Un prieten care-şi încarcă contactele de pe telefon sau joacă un test („*quizz*") online ar putea, în mod involuntar, să furnizeze informaţii despre un alţi prieteni de-ai săi – utilizatori sau nu ai Facebook-ului – , dar fără acordul acestora din urmă.

Această practică a fost sesizată de Oficiul pentru protecţia consumatorilor din Germania, care a contestat ca „neloială prezentarea menţiunilor afişate la apăsarea butonului „Joacă acum" din centralizatorul de aplicaţii, în special pentru motivul încălcării cerinţelor legale privind obţinerea unui consimţământ al utilizatorului valid în temeiul legislaţiei în materie de protecţie a datelor. În plus, acesta consideră menţiunea finală de la jocul „Scrabble" o condiţie comercială generală care dezavantajează în mod nejustificat utilizatorul"[18]. În acelaşi sens, alte astfel de aplicaţii despre care s-a descoperit că „scurg" informaţii sunt FarmVille şi Family Tree[19].

Atragem atenţia asupra faptului că nu doar utilizatorii platformei de socializare oferă informaţii despre ei înşişi sau alte persoane[20], dar şi diverse aplicaţii – ce fac parte din categoria de parteneri ai Facebook-ului – transferă, uneori automat şi fără înştiinţarea şi consimţământul utilizatorilor, date către Facebook[21].

În mod implicit, un profil Facebook este setat pentru a permite doar prietenilor auto-selectaţi să poată vizualiza profilul. Cu toate acestea, setările implicite de vizibilitate ale căutării permit tuturor să vadă fotografia de profil a

[18] Cauza C-319/20: *Facebook Ireland Limited vs. Bundesverband der Verbraucherzentralen und Verbraucherverbände*, Rezumatul cererii de decizie preliminară întocmit în temeiul articolului 98 alineatul (1) din Regulamentul de procedură al Curții de Justiție, disponibil la adresa: http://curia.europa.eu/juris/showPdf.jsf?text=&docid=230961&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=11312023, accesată la 12.11.2020.

[19] *„Privacy violations – the dark side of social media...–BullGuard"*, disponibil la adresa: https://www.bullguard.com/bullguard-security-center/internet-security/social-media-dangers/privacy-violations-in-social-media.aspx, accesată la 01.09.2020.

[20] *A se vedea, C-101/01 Lindqvist [2003] ECR I-12971.*

[21] În acest articol de la Privacy International, disponibil la adresa: https://privacyinternational.org/blog/2758/appdata-update, accesată la 12.11.2020, sunt redate exemple de astfel de aplicaţii, precum şi câteva modalităţi de limitare a transferării datelor de la aplicaţiile accesate către Facebook.

unui utilizator[22], lista de prieteni şi paginile fanilor. Mai mult, o listă de căutare publică este creată automat şi trimisă pentru indexarea motorului de căutare. Astfel, utilizatorii îşi dezvăluie automat datele personale atunci când nu modifică setările implicite ale profilului lor.

Mai adăugăm că aplicaţia Facebook instalată pe un telefon Android are acces la camera foto şi înregistrarea audio, ceea ce-i permite ca oricând să poată colecta toate imaginile înregistrate cu camera dispozitivului.

De asemenea, chiar şi atunci când utilizatorul *logat* în aplicaţie ori o persoană nu are un cont de Facebook, însă vizitează un website ce are un buton „Like" activ sau o trimitere la această reţea de socializare, Facebook înregistrează *ID*-ul utilizatorului, website-ul vizitat, data şi ora accesării, precum şi alte informaţii privitoare la activitatea de navigare pe internet.

Facebook precizează, însă, că scopul înregistrării (temporare, de altfel) ar fi acela de a identifica şi rezolva problemele de erori şi „*bug*-uri" în sistemul lor de analiză a interacţiunii utilizatorilor acestor website-uri, de a oferi reclame cât mai relevante, personalizate, şi de a-şi îmbunătăţi serviciile oferite[23].

Mai mult, Facebook utilizează cookie-urile pentru a afişa reclame atunci când utilizatorul este activ pe această platformă, dar şi când foloseşte alte platforme.

Facebook urmăreşte în mod obişnuit utilizatori, non-utilizatori[24] şi utilizatori deconectaţi de pe platforma sa prin intermediul *Facebook Business Tools*. Dezvoltatorii de aplicaţii transmit datele persoanelor ce le folosesc către platforma Facebook prin intermediul *Facebook Software Development Kit* (SDK), un set de instrumente de dezvoltare software ce ajută dezvoltatorii să construiască aplicaţii pentru un anumit sistem de operare. Folosind instrumentul *software* gratuit şi *open source* numit „*mitmproxy*", un proxy HTTPS interactiv, aceste aplicaţii transferă automat datele personale către Facebook în momentul în care un utilizator deschide aplicaţia, înainte ca aceste persoane să poată fi de acord sau să-şi dea consimţământul asupra acestor operaţiuni. Activităţile de transfer de date se întâmplă indiferent dacă oamenii au sau nu un cont Facebook sau dacă sunt conectaţi sau nu la Facebook[25].

[22] *A se vedea,* cauza C-18/18, Eva Glawischnig-Piesczek împotriva Facebook Ireland Limited.

[23] Similar, Amazon utilizează *cookie*-uri pentru a urmări activitatea *online* a utilizatorilor și pentru a plasa reclame și produse personalizate, în scopuri de publicitate, pe *website*-urile partenere (*Amazon Associates* sau cele ce utilizează *Amazon Checkout*).

[24] *A se vedea,* Hotărârea din cazul Duguid v. Facebook, Inc, disponibilă *online* la adresa: https://caselaw.findlaw.com/us-9th-circuit/1905349.html, accesată la 12.11.2020.

[25] Articolul „*Investigating Apps interactions with Facebook on Android*", publicat de către Privacy International, disponibil la adresa: https://privacyinternational.org/taxonomy/term/552 , accesată la 01.09.2020.

În cazul platformei Google[26], cunoaştem cu toţii că aceasta este o companie cu interese şi activităţi în aproape orice subiect legat de internet. Deşi politica de confidenţialitate, ce acoperă toate serviciile Google, este uşor de citit şi foarte clară, poate fi dificil de înţeles cum funcţionează în orice, de la Play Store la Google Search, Gmail, Hărţi, Android, Youtube şi multe altele[27]. Dominaţia Google[28] înseamnă că, probabil, ştie mai multe despre utilizator decât orice altă companie şi, probabil, datorită funcţiilor de analiză, chiar decât ştie utilizatorul despre sine însuşi[29].

### *2.3. Cu privire la posibile încălcări ale legislaţiei protecţiei datelor cu caracter personal, a normelor privind protecţia consumatorilor şi a regulilor de concurenţă*

#### 2.3.1. Facebook vs. Bundeskartellamt

La începutul anului 2019, Oficiul privind reglementarea concurenţei din Germania, *Bundeskartellamt,* a contestat comportamentul Facebook, argumentând că platforma online s-a aflat într-un abuz de exploatare a consumatorilor prin procesul său de colectare şi combinare a datelor din toate unităţile sale de funcţionare şi din alte surse terţe, fără să fi obţinut explicit consimţământul utilizatorilor săi în acest scop. În aceste condiţii, încălcarea

[26] Mai multe detalii despre politicile Google la adresa: https://privacy.google.com/businesses/compliance/ , accesată la 12.11.2020.

[27] Un judecător federal în luna martie a acestui an, când a aprobat acrodul de negociere prin care Google Street View trebuie să plătească suma de 13 milioane de dolari ca urmare a folosirii de vehicule cu acces la rețele Wi-Fi necriptate ale locuințelor oamenilor, cu ajutorul cărora a colectat e-mailuri, parole și alte informații private în perioada 2007-2010. Deși inițial Google s-a apărat motivând că a fost o greșeală, ulterior, s-a dovedit că sistemele au fost în mod intenționat proiectate pentru acest scop. – A. Lancaster, articolul *„Judge Approves $13M Google Street View Privacy Settlement With No Payout to Class"* din 19.03.2020, publicat în Law.com/The Recorder, disponibil la adresa: https://www.law.com/therecorder/2020/03/19/judge-approves-13m-google-street-view-privacy-settlement-with-no-payout-to-class/, accesată în 12.11.2020. C. Duffy, articolul „Google agrees to pay $13 million in Street View privacy case", publicat în CNN Business, la data de 25.07.2019, disponibil la adresa: https://edition.cnn.com/2019/07/22/tech/google-street-view-privacy-lawsuit-settlement/index.html, accesată la 12.11.2020.

[28] *A se vedea,* Cazurile conexe C-236/08, C-237/08 şi C-238/08 Google France/Inc. v. Louis Vuitton Malletier, cazul AT.39740 – Motorul de căutare Google (Shopping), Cazul AT.40099 – Google Android, cazul AdSense.

[29] *„Google Knows You Better Than You Know Yourself"* de J. Carmichael, publicat în data de 19.08.2014, disponibil la adresa: https://www.theatlantic.com/technology/archive/2014/08/google-knows-you-better-than-you-know-yourself/378608/, accesată la 28.08.2020.

normelor de protecţie a datelor s-a ridicat la un comportament abuziv în temeiul art. 19 GWB, fiind sancţionat de către Oficiu ca fapte de încălcare a practicilor comerciale loiale. Facebook nu a oferit consumatorilor o informare autentică pe baza căreia aceştia să-şi dea consimţământul informat.

Probabil, condiţiile generale în care sunt formulate normele de concurenţă germane au oferit Oficiului un nivel de flexibilitate în tratarea acestui caz, care altfel ar putea să nu fie de competenţa Comisiei Europene în aplicarea articolului 102 din TFUE.

Abordarea Oficiului german este inovatoare din mai multe considerente:

– în primul rând, este adoptată o abordare foarte largă în determinarea a ceea ce reprezintă „consimţământul acordat în mod liber” în scopuri de protecţie a datelor şi se argumentează că o încălcare a normelor de protecţie a datelor constituie o încălcare a normelor de concurenţă;

– în al doilea rând, Oficiul a ridicat problema a ceea ce s-ar aştepta un utilizator rezonabil în ceea ce priveşte folosirea datelor sale personale;

– în al treilea rând, logica deciziei Oficiului este determinată de înţelegerea – exprimată expres în legislaţia germană în materie de concurenţă – că, consumatorii se aflau într-o poziţie de „dependenţă” faţă de Facebook în rolul acestuia din urmă de furnizor dominant de servicii de social media.

Totuşi, în fond, Curtea Regională Superioară din Düsseldorf a anulat Decizia Oficiului privind reglementarea concurenţei din Germania din august 2019[30]. În acest sens, a observat că Decizia s-a abătut în mod necorespunzător de la standardele UE de revizuire în ceea ce priveşte acuzaţiile de putere de piaţă.

Hotărârea instanţei regionale a fost parţial modificată de Curtea Federală de Justiţie, care prin Decizia din 23 iunie 2020, a constatat că[31]:

– Facebook foloseşte termeni şi servicii ce permit, de asemenea, prelucrarea şi utilizarea datelor utilizatorilor care sunt colectate online în afara platformei Facebook;

– *Bundeskartellamt* a impus platformei Facebook interdicţia de a prelucra astfel de date fără acordul suplimentar dat de utilizatori ale căror date erau colectate;

– interdicţia decisă de *Bundeskartellamt* poate fi aplicată.

[30] „*Facebook ./. Bundeskartellamt The Decision of the Higher Regional Court of Düsseldorf (Oberlandesgericht Düsseldorf) in interim proceedings, 26 August 2019, Case VI-Kart 1/19 (V)*”, disponibilă la adresa: https://www.d-kart.de/wp-content/uploads/2019/08/OLG-D%C3%BCsseldorf-Facebook-2019-English.pdf,accesată la 12.11.2020.

[31] Comunicat de presă, disponibil la adresa: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2020/23_06_2020_BGH_Facebook.pdf;jsessionid=88166EC965A482B0ED78E68A737FF799.1_cid390?__blob=publicationFile&v=2, accesată la 12.11.2020.

Din analiza Curţii Federale de Justiţie[32] se reţine că termenii şi condiţiile de funcţionare a reţelei Facebook sunt structuraţi într-un mod ce ar putea afecta concurenţa. Accesul pe care-l are Facebook la o bază de date considerabil de mare creşte puterea „efectelor de blocare" („*lock-in effects*".) deja distincte. În plus, această bază de date mai mare îmbunătăţeşte posibilităţile de finanţare a reţelei sociale utilizând profiturile generate din contractele de publicitate ce depind, de asemenea, de sfera şi calitatea datelor disponibile. Având în vedere efectele adverse asupra concurenţei din perspectiva contractelor de publicitate, nu se poate exclude, în cele din urmă, ca şi piaţa publicităţii online să fie afectată. Contrar opiniei instanţei regionale, nu este necesar să se determine că există o piaţă separată pentru publicitatea online pentru reţelele de socializare şi că Facebook are o poziţie dominantă şi pe această piaţă. Consecinţele încălcării normelor de concurenţă nu trebuie să apară pe piaţa dominată de o companie, ci pot să apară şi pe o a treia piaţă nedominată de această companie.

### 2.3.2. Facebook vs. Verbraucherzentrale Bundesverband [33]

Conform Legii germane federale privind protecţia datelor, datele cu caracter personal pot fi colectate şi utilizate numai cu acordul persoanei vizate. Pentru a permite utilizatorilor să ia o decizie conştientă, prestatorii de servicii trebuie să furnizeze informaţii clare şi uşor de înţeles despre natura, domeniul de aplicare şi scopul utilizării datelor intenţionate.

Facebook nu a îndeplinit aceste cerinţe. În aplicaţia Facebook pentru smartphone-uri, de exemplu, a fost pre-activat un serviciu de localizare care dezvăluie locaţia unui utilizator persoanelor cu care conversează. În setările de confidenţialitate, casetele care permiteau motoarelor de căutare să se conecteze la cronologia utilizatorului era presetate ca acceptate. Aceasta însemna că oricine poate găsi rapid şi uşor profiluri personale de pe Facebook.

Judecătorii de la de Curtea Regională din Berlin au decis că toate cele cinci setări implicite de pe Facebook sesizate de *Verbraucherzentrale Bundesverband* (Oficiul pentru protecţia consumatorilor) sunt invalide ca declaraţii de consimţământ. Judecătorii au constatat nu există vreo garanţie că utilizatorii vor şti chiar că acele setări sunt acolo.

Suplimentar, Curtea Regională din Berlin care a reţinut că Facebook a încălcat legislaţia protecţiei consumatorilor prin includerea în Termenii şi condiţiile de funcţionare ale platformei de prevederi contractuale ilegale: clauza „*real-name*", permisiunea implicită ca Facebook să folosească numele şi

[32] *Ibidem.*

[33] Comuniat de presă al Oficiului pentru protecţia consumatorilor din Germania, 14.02.2018, Facebook In Breach Of German Data Protection Law, disponibil la adresa: https://www.vzbv.de/sites/default/files/downloads/2018/02/14/18-02-12_vzbv_pm_facebook-urteil_en.pdf, accesată la 12.11.2020.

imaginea de profil a utilizatorilor „pentru conţinut comercial, sponsorizat sau conex” şi condiţia implicită de transfer al datele utilizatorilor în S.U.A..

În această speţă, recent, instanţa germane a adresat Curţii de Justiţie a Uniunii Europene întrebarea preliminară privind calitatea procesual activă a Autorităţii pentru protecţia consumatorilor (şi alte organizaţii similare) în astfel de litigii[34].

### 3. Perspective de viitor privind publicitatea pe platformele online. Concluzii.

Profilarea cetăţenilor prin trasarea unor inferenţe bogate despre ei va fi una dintre tendinţele-cheie în dezvoltarea şi aplicarea viitoare a noilor tehnologii, însă, trebuie avute în vedere instrucţiunile Autorităţii Europene pentru Protecţia Datelor: „serviciile de socializare ar trebui să asigure setări de confidenţialitate prestabilite, inclusiv setări care limitează accesarea profilului la propriile contacte selectate de utilizator. Setările ar trebui, de asemenea, să necesite consimţământul utilizatorului înainte ca un profil să devină accesibil unor părţi terţe, iar profilurile al căror acces este restricţionat nu ar trebui să poată fi găsite prin utilizarea unor motoare de căutare interne.”[35].

Prin urmare, publicitatea online bazată pe urmărire trebuie descurajată prin aplicarea riguroasă a Directivei existente privind E-Privacy, a GDPR-ului şi prin adoptarea, cel mai curând, a unui regulament robust de E-Privacy, care interzice „*tracking walls*” şi include alte garanţii conform recomandărilor autorităţilor de reglementare din domeniu.

De asemenea, drepturile şi obligaţiile legale ale furnizorilor de platforme digitale ar trebui reglementate în mod clar.

Furnizorii de platforme online nu sunt responsabili pentru conţinutul terţilor, dar ar trebui să răspundă pentru algoritmii lor, pentru respectarea drepturilor omului, inclusiv protecţia datelor şi pentru administrarea platformelor lor (spre exemplu: exploatarea ilegală a datelor personale obţinute pe orice cale de la (ne)utilizatori).

Intermediarii sunt actori importanţi în mediul online, deoarece găzduiesc infrastructura şi software-ul prin care informaţiile sunt procesate şi pe care sunt construite comunităţile online. În timp ce Directiva privind comerţul electronic a recunoscut rolul important, dar dificil al intermediarilor online şi a

[34] Cauza C-319/20 – Facebook Ireland Limited/Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V., disponibilă la adresa: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:62020CN0319, accesată la 12.11.2020.

[35] *Avizul privind promovarea încrederii în societatea informațională…., op. cit.*. Avizul Autorității Europene pentru Protecția Datelor privind promovarea încrederii în societatea informațională prin încurajarea protecției datelor și a confidențialității, punctul 75, Jurnalul Oficial al Uniunii Europene, C 280/1,16.10.2010.

introdus un regim special de protecţie juridică pentru unii dintre aceşti intermediari, poziţia intermediarilor rămâne, totuşi, dificilă. Instanţele judecătoreşti nu ştiu în ce măsură ar trebui să răspundă intermediarii pentru informaţiile prelucrate de terţi; utilizatorii nu ştiu în ce măsură intermediarii pot folosi conţinutul pe care l-au încărcat către intermediar; guvernele vor să reducă bariera pentru a deveni intermediar online, dar în acelaşi timp le impun funcţii de poliţie; unii intermediari (Web 2.0 şi *cloud computing*) ce sunt actori-cheie în prezent, nu sunt acoperiţi conform prevederilor Directivei privind comerţul electronic[36].

Consumatorii joacă un rol important în protejarea confidenţialităţii informaţiilor atunci când navighează pe internet. De exemplu, atât tehnologiile de îmbunătăţire a confidenţialităţii (PET), cât şi Platforma pentru preferinţe de confidenţialitate (P3P) plasează sarcina protejării datelor asupra utilizatorilor. Ne-a surprins plăcut abordarea tot mai fermă a AEPD ce promovează „cazul în care browserele ar fi prevăzute cu setări de confidenţialitate prestabilite. Cu alte cuvinte, dacă ar fi prevăzute cu setarea „neacceptarea modulelor cookie terţe". (...) Utilizatorii care doresc să fie monitorizaţi cu scopul de a primi mesaje publicitare vor fi informaţi corespunzător şi vor trebui să modifice setările browserului. Astfel, aceştia vor avea control sporit asupra datelor lor personale şi confidenţialităţii."[37].

De asemenea, autorităţile de protecţie a datelor ar trebui încurajate şi susţinute în direcţia de exercitare a competenţelor în temeiul articolului 58 din GDPR, inclusiv efectuarea de investigaţii privind practicile de micro-targeting a agenţiilor de publicitate şi companiilor de analiză a datelor pe platformele digitale. Totodată, considerăm benefic un exerciţiu de verificare a platformelor digitale din perspectiva respectării principiilor *privacy by default and by design*, precum şi a normelor referitoare la consimţământul liber, fără ambiguităţi şi informat.

De altfel, în Avizul AEDP privind promovarea încrederii în societatea informaţională prin încurajarea protecţiei datelor şi a confidenţialităţii[38], se menţionează că, pe lângă auto-reglementare, ar trebui implementate standarde minime de protecţie. În categoria acestor standarde minime de protecţie pot fi incluse şi măsurile tehnice şi organizatorice adecvate („atât în momentul proiectării sistemului de prelucrare, cât şi în cel al prelucrării în sine"), pentru a menţine securitatea şi a preveni prelucrarea neautorizată.

[36] DLA Piper, *EU study on the New rules for a new age? Legal analysis of a Single Market for the Information Society*, p. 23, disponibil la adresa: https://ec.europa.eu/digital-single-market/en/news/legal-analysis-single-market-information-society-smart-20070037, accesată la 12.11.2020.

[37] *Avizul privind promovarea încrederii în societatea informațională..., op. cit.*

[38] *Ibidem.*

În Orientările nr. 4/2019, AEPD recomandă ca măsurile şi garanţiile ce apără principiul echităţii şi, de asemenea, drepturile şi libertăţile persoanelor vizate, în special dreptul la informaţie (transparenţă), dreptul la intervenţie (acces, ştergere, portabilitatea datelor, rectificare) şi dreptul de a limita prelucrarea (dreptul de a nu fi supus la luarea deciziilor individuale automatizate şi nediscriminarea persoanelor vizate în astfel de procese) să fie bazate pe câteva elemente-cheie precum: autonomie, interacţiune,aşteptări, nediscriminare, neexploatare, alegerea consumatorului, echilibrul de putere, fără transfer de risc, fără înşelăciune, respectarea drepturilor, a normelor de etică şi a adevărului, intervenţie umană şi algoritmi echitabili.

În concluzie, tehnologia nu este incompatibilă cu modul nostru de viaţă, dar, totuşi, modelul de business ales de furnizorii de platforme digitale amintiți determină sancţionarea derapajelor ce afectează dezvoltarea organică a omului şi a societăţii în ansamblul ei.