Revista Universul Juridic ● nr. 7, iulie 2019, pp. 74-108

O PERSPECTIVĂ ŞI ANALIZĂ CRITICĂ A GDPR. PROTECȚIA INTIMITĂȚII, DREPT SAU ILUZIE. APEL LA CONŞTIENTIZAREA RISCURILOR MEDIULUI DIGITAL ASUPRA DREPTULUI LA INTIMITATE ŞI VIAȚA PRIVATĂ

Avocat Oxana D. CHIRONDA
Senior Partner SCA Dumitrache-Chironda, Ivu şi Asociații
ECPC-B - Certified Data Protection Officer by European Centre of Privacy and Cybersecurity Maastricht University
Certificată CIPP/E (Certified Information Privacy Professional – Europe GDPR)
Membru al IAPP – International Association of Privacy Professionals

Abstract

*This thesis aims to challenge the **hypnotize** that while indeed innovating, **GDPR does not put in control the people over their data**. It was not designed in this propose. All the made statements will be developed, supported, and explained and as much possible try to address in the body of the essay. Such as: Is the privacy yet a fundamental classic freedom right as used to refer in EU Charter of Fundamental Rights or Convention 108? Are yet the people real owner and masters of their data? Are data merchandisable commodities and GDPR regulating its marketing? And researching in response to series of such chain questions, that keep arising along the research journey I can stop fell the main Lucius Cassius' painfully restless Cui prodest?*

Keywords: *personal data, GDPR, privacy, Case Schrems, ECHR Case-law, CJUE Case-law, legitimacy crises and democratic deficit of EU institutions, private and family life*

I. Premisele GDPR. Lumea noastră digitală

În discursul privind starea Uniunii Europene din 14 septembrie 2016, preşedintele Jean Claude Juncker a subliniat: „*A fi european înseamnă a avea dreptul ca datele tale cu caracter personal să fie protejate de legi puternice, europene. Pentru că europenilor nu le plac dronele care zboară pe deasupra lor şi le înregistrează fiecare mişcare, nici companiile care contabilizează fiecare click pe mouse. De aceea, Parlamentul, Consiliul şi Comisia au convenit în mai anul acesta un regulament comun privind protecția datelor cu caracter personal. Acest regulament este o lege europeană fermă aplicabilă companiilor, indiferent de locul în care îşi au sediul şi ori de câte ori prelucrează datele dumneavoastră*

cu caracter personal. Pentru că, în Europa, păstrarea confidențialității datelor personale contează. Această chestiune ține de demnitatea umană".

Regulamentul UE nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor, denumit în continuare GDPR) vine deloc întâmplător după dezvăluirile lui Edward Snowdon (2013), *Cauza Maximillian Schrems c. Data Protection Commissioner* EU:C:2015, C-362/14, scandalul *Cambridge Analitica*, publicațiile Wikileaks şi arestarea lui Julian Assange, jurnalistului şi activistului pentru drepturile omului, invalidarea de către CJUE a Directivei 2006/24/CE[1] în cauza cunoscută sub denumirea *Digital Rights Ireland*[2] etc. când s-a întețit presiunea dintre activismul democratic şi sistemele guvernamentale. Sistemul guvernamental a replicat printr-un set de instrumente legislative şi măsuri de control.

Decizia pronunțată în *Cauza Schrems*, (pe care o vom analiza mai detaliat în Capitolul al VI-lea al prezentului articol), reprezintă o piatră de temelie care a scandalizat şi revoluționat abordarea şi implementarea principiilor de bază, a standardelor de evaluare a aplicării efective a politicilor şi măsurilor de protecție a datelor şi respectare a dreptului fundamental la viață privată atât în UE cât şi în SUA. A fost factorul declanşator al revoluției în materia protecției datelor în UE şi catalizatorul legislației în acest domeniu pe continental nord-american şi nu numai.

Volumul de date create şi colectate peste tot în lume a crescut exponențial în ultimii ani. Prin studiul realizat de către IBM se arată că aproximativ 90% din volumul actual al datelor au fost create şi colectate în doar ultimii 2 ani (2016-2018), reprezentând aproximativ 2.5 quintilioane de bytes produse în fiecare zi, în aproape fiecare industrie şi sector de activitate economică. International Data Corporation se aşteaptă că până în 2020, în lume vor fi create şi replicate cca 163 zetabytes sau 163 trilioane gigabytes în fiecare an.

II. Motivarea demersului şi considerentele

Curiozitatea intelectuală şi provocarea profesională mă determină să mă aplec cu pasiune asupra modului în care instituțiile europene şi cele mondiale abordează

[1] Directiva 2006/24/CE privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice şi de modificare a Directivei 2002/58/CE.

[2] Cauzele reunite C-293/12 and C-594/12 Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others EU:C:2014:238. 21.

*intimitatea p*ersoanei şi cum înțeleg acestea să instituționalizeze controlul datelor personale. La programul centrului de cercetare privind protecția datelor cu caracter personal, desfăşurat în martie 2019 de către *European Center of Privacy and Cybersecurity* al Universității de la Maastricht, Profesorul P. Breitbarth[3] en passant a atins subiectul delicat al *dreptului persoanei de a se opune comercializării* datelor sale personale ('do-not-sell' right) reglementat expres de către legiuitorul american (californian) prin *California Consumer Privacy Act*[4] (CCPA).

Aşa cum ştim, regulamentul GDPR nu reglementează şi nu recunoaşte expres acest drept persoanei, legiuitorul european omițând să reglementeze acest drept. Având o sensibilitate specială cu privire la acest subiect, am profitat de ocazie să întreb cum în Europa *democratică* se dă eficacitate acestui drept (de a ne opune vânzării), în mod efectiv şi real. Sau şi mai simplu: care prevedere din GDPR ar putea fi invocată de către o persoană în Europa, pentru a se opune a priori vânzării şi comercializării datelor sale?

Simplă sau nu întrebarea ea exprimă esențialul: are sau nu o persoana în Europa control asupra datelor sale sub umbrela GDPR? Putem sau nu proactiv să ne opunem vânzării datelor noastre personale? Poate o persoană să oblige operatorul[5] să o informeze sau să-i ceară acordul înainte de a **vinde** datele sale? Şi aici ne referim, nu la o informare generică privind un eventual *transfer* al datelor către terți (alături de celelalte informații care se vor furniza potrivit dispozițiilor art.13 GDPR). Ci o informare explicită şi expresă, operatorul să fie obligat să ceară *a priori* acordul **de a vinde** (de a obține venit din tranzacționarea datelor), indicând explicit cui doreşte să le vândă, valoarea tranzacției, durata pentru care se vinde, scopul în care vor fi utilizate de către cumpărător, riscurile sau avantajele pentru persoana vizată. De relevanță pentru prezenta analiză nu este totuşi întrebarea, ci răspunsul.

Spre uimirea mea, fără ezitare, aproape imediat am primit răspunsul că GDPR nu urmăreşte să dea control persoanei asupra datelor sale, că nu este reglementată o astfel de instituție precum controlul persoanei asupra datelor sale.

Un astfel de răspuns chiar dacă intuit într-un mod foarte timid, acum venea dintr-un mediu academic credibil. Şi a pus la îndoială însăşi *raison d'etre* al acestui

---

[3] Prezentarea şi cursul ținut de către Profesorului Paul Breitbarth privind prezentarea sistemelor şi mecanismelor de gestionarea securității datelor (Executive Week – Martie 2019).

[4] The California Consumer Privacy Act (CCPA) este o act legislative (bill) care reglementează protecția datelor şi a intimității (privacy) consumatorilor (spre deosebire de termenul folosit în Europa - a *persoanelor*) rezidenți în California, SUA. Actul a fost adoptat şi a trecut de Consiliul Statului California şi semnat de către Dl. Jerry Brown, Guvernatorul statului California, în data de 28 iunie 2018. CCPA urmează să intre în vigoare în data de 1 Ianuarie 2020.

[5] „Operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern" – art. 4 pct.7 GDPR.

regulament? Oare nu am fost învățați că Regulamentul privind protecția datelor GDPR este o reglementare destinată protejării intereselor cetățenilor? Oare nu asta urmăresc eu însămi prin aprofundarea acestor studii, să ajut cetățenii să navigheze în acest cadru instituțional european?

Nefiind tocmai o persoana naivă, eu cu sinceritate cred şi militez pentru adevăr şi bine. Acesta este şi motivul pentru care am îmbrățişat meseria de avocat, să ajut semenii, în nevoie. Regulamentul GDPR îmi apărea ca o cauză justă, care merită lupta, un succes pentru drepturile omului şi un instrument eficient în protejarea persoanei. Să ne amintim de campaniile de informare lansate şi susținute de media *(„Data back to people!")*, reiterate inclusiv în mesajul video publicat de către EDPB pe pagina sa https://edpb.europa.eu/about-edpb/about-edpb_en (secunda 00:50). Instituțiile europene şi naționale din Europa prin care se indica explicit că GDPR este o reglementare detaliată a dreptului la intimitate şi protecția datelor recunoscut prin art.8 al Convenției 108 (28 ianuarie 1981)? Calea către GDPR părea să fie rezultatul unei lupte pentru drepturile persoanei, pentru libertatea şi intimitatea fiecăruia din noi?

Aproape imediat, mi-a răsărit în minte articolul Profesorului Woodrow Hartzog publicat în European Data Protection Law Review (EDPL) nr.4/2018 *„The Case Against Idealising Control"*[6]. Inițial, la prima lectură, am considerat că Prof. Hartzog exprimă o opinie personală uşor subiectivă. Însă, în contextul răspunsul primit la ECPC în martie 2019, articolul Prof. Hartzoog şi considerentele dezvoltate de Prof. Christopher Kuner[7], toate trei opinii exprimate în medii academice de încredere, au zdruncinat crezul meu şi m-au determinat să aprofundez şi să cercetez cu atenție subiectul care mă frământa de o vreme: este regulamentul GDPR şi măsurile instituțiilor europene orientate să ofere **persoanei** controlul real asupra datelor sale?

Este **persoana** centrul gravitațional al acestui regulament? Şi dacă nu, cui foloseşte GDPR?

De ce instituțiile europene au reglementat acest domeniu prin GDPR? *Cui prodest*?

La o analiză mai atentă, răspunsul care s-a impus: Adevărat este. GDPR nici pe departe nu este despre a da vreun control persoanei asupra datelor sale[8].

---

[6] https://edpl.lexxion.eu/article/EDPL/2018/4/5.

[7] În lucrarea „Reality and Illusion in EU Data Transfer Regulation Post Schrems" https://germanlawjournal.com/volume-18-no-04/.

[8] You probably recall the picture form Mrs. Leena Kuusniemi presentation „One Regulation to rule them all, One stop-shop to find them, One DPA to bring them all and in the darkness fine them" stating DATA-POWER TO THE PEOPLE.

https://www.theguardian.com/commentisfree/2017/oct/03/data-tech-giants-trail-digital-age.

https://www.rug.nl/rechten/news/in-de-media/archief/2018/jonida-milaj-weishaar-will-we-get-back-control-of-our-data.

Desigur, **GDPR reglementează controlul.** Dar nu un control exercitabil de persoană. *Per a contrario,* în fapt, **persoana este marfa**[9].

III. Cui prodest ?

Trebuie să admitem că pentru a putea trata în prezenta lucrare regimul juridic al protecției datelor aşa cum a fost acesta elaborat şi legiferat de către Comisia Europeană şi cum a trecut prin 2 lecturi în Parlamentul European, nu putem să omitem poate cel mai important capitol în care să analizăm şi răspundem cu onestitate dacă prin acest Regulament GDPR legiuitorul European a dat controlul persoanei asupra datelor sale, să încercăm să identificăm şi să răspundem argumentat şi obiectiv cine este de fapt beneficiarul real al GDPR, C*ui prodest*? Care este cadrul instituțional european în care acest regulament a fost conceput şi dezbătut, pentru a ajunge al noi, în forma pe care o cunoaştem astăzi?

IV. Datele sunt bunuri. Oamenii sunt marfă

Retrăgându-ne şi privind cu atenție în urmă procesele şi modificările care au avut loc în ultimele 2-3 decade, oamenii, *demosul,* s-a dovedit a fi o marfă, care furnizează (sau de la care se poate extrage) nu doar muncă, dar şi identitatea, intelectul însuşi. Poate suna provocator. Dar vă invit prin aceasta lucrare să dați o şansa analizei acestei teze. Cum se ştie, **datele au valoare pecuniară**. Având valoare financiară, ele se comercializată pe piață. Fac obiectul intermedierilor şi a unui comerț intens. Analytics, big data, market profiling, inteligența artificială (AI), blockchain, IoT (internet-of-things) etc. – sunt doar câteva domenii notorii şi prezente pe piața digitală.

Toate domeniile economiei şi finanțelor în activitatea curentă, gestionează baze masive de date (banking, asigurări, servicii medicale private, contabilitate etc.) şi îşi construiesc strategiile pe baza unor intense şi din ce în ce mai sofisticate operațiuni de profilare şi prelucrare a datelor personale.

Datelor personale le este recunoscută valoarea comercială în mod explicit inclusiv prin dispozițiile Articolul 3, primul paragraf din Directiva privind Contractele de furnizare de conținut digital şi de servicii digitale 26 martie 2019, recunoscându-se datelor personale valoare de plată, prin care se achită un serviciu: *„Prezenta directivă se aplică şi atunci când comerciantul furnizează sau se angajează să furnizeze consumatorului conținut digital sau un serviciu digital, iar consumatorul furnizează sau se angajează să furnizeze comerciantului* ***date cu caracter personal...".***

https://www.cbsnews.com/news/gdpr-the-law-that-lets-europe-take-back-their-data-from-big-tech-companies-60-minutes/.

[9] Ne duce cu gândul la sclavie, nu-i aşa?

Monetizarea inclusiv pe cale legislativă a valorii datelor personale este o realitate juridică. Această formă consolidată a textului legislativ European a trecut în lectura Parlamentului European şi a fost agreată de către Consiliul European[10], în pofida opoziției Autorității de Supraveghere Europeană a Datelor (EDPS) care a exprimat critici şi rezerve prin Opinia nr.4/2017 din 14.03.2017[11].

EDPS solicita reformularea acestui paragraf sau cel puțin eliminarea cuvântului „contra-prestație" care în versiunea anterioară (din 9 decembrie 2015[12]) era inclus în text în mod explicit. Parlamentul a eliminat sintagma *„în contraprestație"*, dar din analiza semantică a textul acestui aliniat exact acest lucru se desprinde, chiar dacă sintagma este reformulată voalat.

În lucrarea sa „*The use of big data as a risk for individual self-determination and the implementation of competition law in the digital market - A comparative approach between the European Union and the United States of America*" publicată în revista italiană de specialitate Eurojus[13], Fiorela Deal Monte arată „Se crede cu fermitate în rândul cadrelor universitare că datele cu caracter personal sunt materia primă pe baza căreia funcționează în prezent cea mai mare parte a economiei globale, dar este, de asemenea, un fel de monedă care poate fi oferită în schimbul altor servicii sau bunuri aparent libere[14]".

Studiul desfăşurat de către Financial Times pe Sole24Ore în data de 14 iunie 2013, în articolul *Big Data*: *tre profili a confronto sul valore dei dati personali*[15], demonstrează că în general persoanele nu sunt deloc conştiente de valoarea datelor lor şi le dau o însemnătate redusă, subevaluându-le. În timp ce valoarea datelor personale ale acestora sunt comercializate şi tranzacționate la valori din ce în ce mai ridicate de către cei care le colectează şi combină în scop comercial şi nu doar.

---

[10] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2019-0232+0+DOC+XML+V0//RO.

[11] 4 https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf.

[12] *„Prezenta directivă se aplică şi atunci când comerciantul furnizează sau se angajează să furnizeze consumatorului conținut digital sau un serviciu digital, iar consumatorul în* ***contra-prestație*** *îi furnizează sau se angajează să furnizeze comerciantului* ***date cu caracter personal****...".* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015PC0634&from=EN.

[13] http://rivista.eurojus.it/wp-content/uploads/pdf/I.2-FIORELLA-DAL-MONTE-The-use-of-big-data-as-a-risk-for-individual-self-determination-and-the-implementation-of-competition-law-in-the-digital-market..-.pdf.

[14] „It is strongly believed among academics that personal data is the raw material upon which most part of global economy currently works, but it also is a sort of currency that can be given in exchange for other services or goods that are apparently free", făcându-se referire în special la F. PANAGOPOULOU-KOUTNATZI, *Facebook as a challenge to privac*y, in M. BOTTIS (ed.), *Privacy and Surveillance, Current aspects and future perspectives,* Atena, 2013, p. 217; A. ACQUISTI.

[15] (http://www.ilsole24ore.com/art/tecnologie/2013-06-14/data-profiliconfronto-o12622.shtml?uuid=AbTdmq4H.

Această anomale se datorează inclusiv modului subversiv de colectare a datelor, oferindu-se aparent servicii digitale "gratuite", iar colectarea, efectuându-se de cele mai multe ori în moduri aproape imperceptibile de către persoane. Colectarea datelor nu este doar una activă (persoana comunică în mod conştient datele sale), ci „colectări" masive de date au loc instantaneu şi automat prin însăşi accesarea unor servicii online, vizitarea unor site-uri sau accesarea unor link-uri sau prin utilizarea unui dispozitiv (telefon, tabletă, laptop, ceas, aparat fitness etc.), trimițându-se automat informații ale persoanei privind traficul de date, istoricul accesării (data logs), localizarea teritorială, evidențele pulsului, tensiunea (prin utilizarea aparatului de fitness, ceas etc.) – aşa cum s-a reținut de către WP29 prin *Ghidul privind portarea datelor WP 242*[16].

Pericolul a fost sesizat şi de către oficialitățile UE. Autoritatea Europeană privind Protecția Datelor (AEPD sau eng-EDPS[17]) confirma în *Avizul privind eficacitatea aplicării legii în economia societății digitale din 2016*[18] că „Serviciile de acest tip prestate pe internet au ajuns să depindă de urmărirea – adesea disimulată – a persoanelor, care nu sunt în general conştiente de natura şi amploarea acestei urmăriri[19]".

Tot în septembrie 2016, AEPD arată că „Am adresat instituțiilor UE câteva recomandări provizorii, care au fost îmbunătățite în urma unui atelier de lucru găzduit de AEPD în iunie 2014, printre care: 1. să înțeleagă mai bine **„valoarea"** datelor cu caracter personal pe pieţele digitale şi să revizuiască metodologiile de analiză a pieței, în special a serviciilor prestate pe internet şi promovate ca „gratuite", cu o analiză retrospectivă sau ex-post a impactului deciziilor de aplicare a legii[20]".

Autoritățile UE recunosc inclusiv prin corespondența oficială că datele cu caracter personal sunt **marfă** de vânzare şi schimb. Datele personale fac obiectul

---

[16] https://www.dataprotection.ro/servlet/ViewDocument?id=1383.

În acelaşi sens este importantă poziția Autorității Europene Protecție Datelor în *Opinia nr.3/2018 publicată în JOUE C233/9*: pag.1 „Datele cu caracter personal sunt necesare pentru a segmenta, ținti şi personaliza mesajele transmise persoanelor fizice, însă majoritatea agenților de publicitate nu sunt conştienți de maniera în care sunt luate aceste decizii, iar **majoritatea persoanelor fizice nu conştientizează modul în care sunt folosite**." https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_summary_ro.pdf.

[17] European Data Protection Supervisor https://edps.europa.eu.

[18] https://edps.europa.eu/sites/edp/files/publication/17-01-13_big_data_ex_summ_ro.pdf.

[19] Tot în septembrie 2016 AEPD arată că "Am adresat instituțiilor UE câteva recomandări provizorii, care au fost îmbunătățite în urma unui atelier de lucru găzduit de AEPD în iunie 2014, printre care:

1. să înțeleagă mai bine „**valoarea" datelor** cu caracter personal pe pieţele digitale şi să revizuiască metodologiile de analiză a pieței, în special a serviciilor prestate pe internet şi promovate ca „gratuite", cu o analiză retrospectivă sau ex-post a impactului deciziilor de aplicare a legii;" https://edps.europa.eu/sites/edp/files/publication/17-01-13_big_data_ex_summ_ro.pdf.

[20] https://edps.europa.eu/sites/edp/files/publication/17-01-13_big_data_ex_summ_ro.pdf accesat la 01.07.2019.

unui volum uriaş de tranzacţii, fără informarea şi avizarea persoanei însăşi. Acumularea masivă a acestor *mărfuri* şi în special controlul sursei de generare a mărfii (datele persoanele), duce la acumularea de putere şi influenţă.

Curios faptul că pentru a colecta această marfă (datele), nu este nevoie nici să o plantezi, nici să o îngrijeşti sau hrăneşti, nici nu trebuie să aştepţi ajungerea la maturitate a produsului pentru a îi colecta beneficiile sau a îl comercializa[21].

Marfa reprezentând datele, pur şi simplu, stau în drum, plutesc în aer, sunt peste tot (oriunde există elementul uman). Şi sunt colectate şi folosite în diverse scopuri de către operatori privaţi şi publici, instituţii. Astfel că, chiar dacă GDPR evită şi nu o spune explicit, datele sunt în realitate o marfă valoroasă.

Şi cum bine ştim, unde este un bun, trebuie să fie şi un stăpân al bunului. Nu există proprietate, fără să existe şi un proprietar. Un stăpân, proprietar la bunului este cel care îl deţine sau dispune de el, indiferent de sursa originară de dobândire, fie prin dobândire naturală, fie chiar prin furt sau jaf… sau **prin lege**. Să admitem cu sinceritate, jaful este considerat sursa primară a proprietăţii.

Datele nu sunt o excepţie, în acest sens. Datele au avut o traiectorie specifică. Datele au stăpân. Datele au proprietar. Ar fi naiv să credem că persoanele însuşi ar fi proprietarii propriilor date. Categoric, nu. Cum am arătat mai sus, **persoana este însăşi marfa** (nu proprietarul ei).

Persoana consimte sau tolerează, inconştient, cedarea datelor sale şi a intimităţii sale, fiind totalmente dezinformată cu privire la modul în care sunt folosite datele sale şi neavând înţelegerea adecvată a mecanismelor digitale a căror subiect devine.

Marea majoritate a populaţiei (dacă nu cumva am putea spune toată populaţia urbană şi majoritatea populaţiei rurale) utilizează acum dispozitive capabile să îşi înregistreze locaţia. Pe lângă dispozitivele care pot fi purtate cu tehnologie de geolocaţie, un sondaj Deloitte din 2017 a constatat că 85% din populaţie deţine sau are acces la un smartphone, iar compania a estimat că în 2018 acest număr ar fi ajuns la 92%.

Această tendinţă a fost însoţită de upgrade-uri la infrastructura de geolocalizare globală, în special sistemul Galileo al Agenţiei Europene de Satelit, care atinsese în 2018 deja o acurateţe la aproximativ 1 metru şi va spori acurateţea şi fiabilitatea serviciilor de localizare în Europa, deoarece în sistem în anii următori se adaugă sateliţi. Tehnologia bazată pe satelit este o piaţă în plină creştere: organizaţia „IoT UK" arată că piaţa globală prin satelit a M2M *(Machine-to-Machine)* şi IoT *(internet-of-things)* ajunge la 5,8 milioane de terminale funcţionale M2M / IoT prin satelit până în 2023[22].

---

[21] Paradoxal, dar aceasta marfă (datele) cu cât este mai *tânără* (datele minorilor), cu atât este mai uşor de colectat şi manipulat etc. (copii şi tinerii sunt mai puţin reticenţi să îşi ofere datele şi sunt mult mai influenţabili, astfel încât cunoscându-le prin profilare comportamentul mult mai uşor li se pot inocula tendinţe, preferinţe, alegeri, determina comportamentul şi deciziile etc.

[22] https://ico.org.uk/media/action-weve-taken/reports/2259365/the-future-of-political-campaigning.pdf.

Aproape toate aplicațiile mobile utilizează tehnologia de localizare, geolocalizându-şi cu precizie utilizatorii. În 2015, institutul de cercetare Pew a constatat că 281.000 de aplicații Android – 26% din toate aplicațiile din magazinul de aplicații din acel moment – au solicitat permisiunea de a accesa locația exactă a utilizatorului. În 2016, o companie de tehnologie care furnizează servicii de localizare pentru aplicații a constatat că dintr-un 1 milion de telefoane care utilizează serviciile lor, 90% au avut servicii de localizare activate la nivelul dispozitivului[23].

Aceste dispozitive sunt capabile să măsoare şi să colecteze o serie de date privind stilul de viață şi sănătate ale unui utilizator, obiceiurile şi calitatea somnului. Aceste date sunt deja utilizate de industrie, unele companii de asigurări utilizează informații de la dispozitivele de urmărire pentru a ajusta primele de asigurare[24]. Potrivit aceluiaşi studiu[25], având în vedere atitudinile actuale ale consumatorilor, este rezonabil de aşteptat o mai mare adoptare a *tehnologiei purtătoare* în următorii ani. Unii analişti cred că *chip*-urile montate sub piele vor deveni, de asemenea, utilizate în mod obişnuit – nu numai pentru a urmări datele de sănătate vitale, ci şi pentru a permite accesul – deschide uşi, a autentifica tranzacțiile şi confirma identitatea, a efectua plăți şi chiar a sesiza câmpuri magnetice[26]. Televizoarele inteligente, inclusiv cele vândute de Sky şi Fire TV, deja acum includ mecanisme similare de activare a vocii[27].

Marii jucători pe piața digitală şi brokerii datelor dezvoltă şi fac investiții uriaşe în servicii de data analitycs, făcând analize, combinând aceste date cu

---

[23] *Idem*, Aceeaşi sursa arată că „odată cu integrarea surselor largi de date generate de Inteligență Artificială (AI), unii agenți de publicitate fac primii paşi către anunțurile automatizate direct personalizate. IBM Watson Advertising a pilotat mai multe campanii publicitare cu Toyota, GSK şi Campbell's Soup, care reunesc datele personale, implicarea utilizatorilor şi generarea conținutului dinamic. Campbell, de exemplu, a folosit această abordare pentru a comunica mesaje publicitare de ofertare a supei atunci când datele meteorologice dintr-o zonă concretă indică că este rece sau plouă şi să sugereze persoanei monitorizate un set de feluri de mâncare şi rețete dat fiind colectarea informațiilor privind utilizarea unui ingredient de către acel utilizator" a se vedea mai multe AdExchanger, 'Campbell's Soup Comes Back For Seconds With Watson Ads' https://adexchanger.com/platforms/campbells-soup-comes-back-secondswatson-ads/ accesat la 01.07.2019.

Acest lucru este valabil în special în cazul dispozitivelor destinate consumatorilor. Aparatul Echo *„home assistant"* al lui Amazon, de exemplu, este vândut cu aparatul foto şi voce setat pentru a fi „mereu pornit" în mod implicit, ascultând permanent pentru un „cuvânt de trezire" („wake word") care, dacă este detectat, îl va solicita să capteze date pe care să le trimită automat către Amazon.

[24] J Blackstock et al (2018), „Internet of Things: realising the potential of a trusted smart world".

[25] Întocmit în iulie 2018 de către Demos şi publicat de către ICO (Information Commissioner's Office, autoritatea de supraveghere a Marii Britanii).

[26] C Wahlquist (2017), „Under the skin: how insertable microchips could unlock the future", disponibil la adresa: https://www.theguardian.com; Hameed et al (2010), „A novel human-machine interface using subdermal magnetic implants", https://ieeexplore.ieee.org/abstract/document/5898141/accesat la data de 01.07.2019.

[27] Wired (2016) „Alexa and Google Home Record What You Say. But What Happens to That", available from www.wired.com.

informațiile achiziționate sau colectate din diverse surse. Astfel încât este dificil pentru persoanele vizate (consumatori de servicii digitale) să înțeleagă modul în care datele lor sunt colectate şi utilizate. Şi, prin urmare, este just să ne îndoim şi să ne îngrijorăm cu privire la existența reală a unui consimțământ efectiv. Ne mai vorbind că de lipsa vădită a unei decizii informate a persoanei atunci când achiziționează un dispozitiv sau utilizează o aplicație, care îşi condiționează funcționarea şi accesul la serviciu propriu-zis de acceptul persoanei să le permită dezvoltatorilor colectarea şi prelucrarea datelor. Amintim aici considerentele reținute pe bună dreptate de către CNIL (Commission Nationale de l'Informatique et des Libertés, autoritatea de supraveghere din Franța) în Decizia din ianuarie 2019 de sancționare a GOOGLE LLC.[28]

Combinarea surselor de date la scară largă generează abuzuri grave privind ingerința în intimitatea şi viața privată a persoanei. Cine şi când decide unde se întâlneşte şi dacă să întâlneşte un compromis între obținerea beneficiilor funcționale ale combinării datelor şi pericolul de a dezvălui informații potențial sensibile cu privire la persoane?

Procesul colectării acestor date colectate de la persoane, transformă persoana însăşi în marfa şi țintă vulnerabilă, căci persoana a devenit dependentă de dispozitive mobile precum telefonul, calculatorul, conexiunea internet etc. Datele sale personale o transformă în marfă.

Dar cine este proprietarul datelor personale?

V. Cine este proprietarul datelor cu caracter personal ?

Inițial, la origini, noi am fost pur şi simplu furați de datele noastre sau le-am împărtăşit benevol (ex. agenții publice, autorități, facebook, yahoo etc.), fiind să zicem „corupți" (sau nu) să o facem în schimbul unor beneficii („gratuități"). Ulterior, pasul următor, a fost cel în care, cei care au acumulat un volum imens de date, au început să le comercializeze, acumulând capital şi mai important – putere.

Şi nu orice fel de putere ordinară (precum ar puterea fizică de a lovi pe cineva – nu). Cu o putere fantastică, nemaicunoscută până atunci, Puterea Minunatei Lumi Noi (Brave New World[29] power). Datele în „mâini pricepute" pot genera o

[28] https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf.

[29] *Brave New World* tradusă în româneşte ca Minunată Lume Nouă este un roman distopic scris în 1931 de către autorul englez Aldous Huxley şi publicat în1932. Romanul descrie cum un Guvern Mondial controlează şi manipulează ființele umane, care sunt modificate inclusiv genetic, care nu mai intimidate, nu mai sunt stăpânii propriei identități, nici a propriului bagaj genetic, nu mai pot transmite bagajul genetic, Guvernul Unic fiind stăpânul bagajului genetic, oamenii fiind modificați genetic. Romanul anticipează marile dezvoltări ştiințifice şi tehnologice, care permit controlul intelectului, prin manipulare psihologică etc.

reală putere de manipulare[30]. *Big data* şi *Analytics* (industria cercetării analitice a datelor) generează informații privind un individ mult peste cele cunoscute de către familia şi apropiații săi şi cu certitudine cunoaşte preferințele şi profilul psihologic al individului mult mai bine decât însuşi persoană în cauză.

Cu aceste informații, ei nu doar că pot determina preferințele persoanei de achiziționare a unui produs (ex: laptop), dar chiar să determine un comportament şi o decizie la nivel social, să mergi sau să nu mergi la referendum, cum să votezi, să ai sau nu un copil etc. Iar atunci când *analytics* chiar se străduie cu pricepere, în doar câteva luni va putea transforma o persoană ortodoxă apolitică într-un admirator înfocat al lui Putin.

Potrivit AEPD p. 3 a Opiniei nr. 2/2018 „Cercetările sugerează că manipularea fluxului de ştiri sau a rezultatelor căutărilor persoanelor le-ar putea influența conduita electorală"[31]. Cert este, că astăzi, avem entități care au acumulat şi în continuarea cumulează un imens volum de date, la scară mondială. Şi într-un termen relativ scurt au ajuns să fie nu doar foarte bogate, dar şi cu influență largă. Şi aici nu ne gândim doar la speța Cambridge Analitica. De fapt, această speță relevă doar vârful aisbergului. Mult mai multe se află sub ape…

Oficialitățile UE au admis şi recunoscut oficial aceste realități, Autoritatea Europeană a Protecției Datelor exprimându-şi în Opinia nr. 3/2018[32] *privind Manipularea online şi datele personale* emisă: „Digitalizarea societății şi a economiei are un impact mixt asupra angajamentului civic în luarea deciziilor şi asupra barierelor în calea implicării publice în procesele democratice. *Big data* şi sistemele de inteligență artificială (AI) au permis colectarea, combinarea, analizarea şi stocarea pe termen nelimitat a unor volume masive de date. În ultimele două

[30] Poziția instituțiilor UE Februarie 2019: https://edps.europa.eu/data-protection/our-work/publications/events/europe-votes-2019-how-unmask-and-fight-online_en.

[31] Într-unul din experimente, li s-a spus utilizatorilor platformei sociale cum au spus prietenii lor că au votat, ceea ce a determinat la nivel statistic o creştere semnificativă a segmentului de populație (0,14 % din populația cu vârsta legală pentru a putea vota sau circa 340 000 votanți) care a votat la alegerile de la jumătatea mandatului pentru Congres din 2010; Allcott H. şi Gentzkow M., Social Media and Fake News in the 2016 Election (Primăvara 2017), Stanford University, Journal of Economic Perspectives, vol. 31, nr. 2, p. 211-236., p. 219). Într-un alt studiu, cercetătorii au susținut că diferențele din rezultatele căutărilor pe Google au reuşit să influențeze preferințele de vot ale alegătorilor indeciși cu 20 %; Zuiderveen Borgesius, F. & Trilling, D. & Möller, J. & Bodó, B. & de Vreese, C. & Helberger, N. (2016). Should we worry about filter bubbles? (Ar trebui să ne îngrijorăm din cauza bulelor filtrante?) internet Policy Review, 5(1). DOI: 10.14763/2016.1.401, p. 9.

Autoritatea de supraveghere Britanică, ICO, a derulat o serie de investigații şi a publicat concluzii rezultate privind influenta şi utilizarea manipulatorie a data analytics in scopuri politice şi de manipulare electorală în următoarele Rapoarte oficiale: *Investigation into data analytics for political purposes, The Future of Political Campaigning , Democracy disrupted? Personal information and political influence, Investigationin to the use of data analytics in political campaigns* pot fi studiate rapoartele aici https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/.

[32] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_summary_ro.pdf.

decenii, a apărut un model dominant de afaceri pentru majoritatea serviciilor bazate pe web, care se bazează pe urmărirea online a persoanelor şi culegerea de date despre caracterul lor, despre sănătate, relații, gânduri şi opinii, în vederea generării veniturilor din publicitatea digitală"[33]

Dar de ce sistemul instituțional european are nevoie de GDPR? Oare sistemul guvernamental nu avea acces liber şi nelimitat la date şi până la GDPR? Oare sistemul instituțional guvernamental nu este el însuşi un *Big Data*[34]? Toate sistemele guvernamentale au acces la toate datele cetățenilor şi cu certitudine monitorizează populația, inclusiv sub pretextul securității de stat, aşa cum am arătat în Capitolul al III-lea al prezentei lucrări, în concluziile aferente analizei Cauzei Schrems. Cu toți suntem conştienți că instituțiile guvernamentale au capacitate tehnologică de monitorizarea masivă a cetățenilor şi asta fireşte nu doar în China (şi poate că nu ne vom fi gândit doar la programul guvernamental SUA de monitorizare masivă PRISM).

Operatorii, aşa cum sunt aceştia definiți cf. art.26 GDPR (dar şi persoanele împuternicite – art. 28 GDPR), sunt stăpânii datelor *(data owners).* Amintim, aşa cum am arătat anterior, persoanele sunt marfă (nu proprietari). Paradoxal sau nu, însuşi legiuitorul european denumeşte persoana, omul a cărui date fac obiectul raportului juridic (operațiunii de colectare sau prelucrare) îi defineşte conform art. 4 pct.1 GDPR, **persoană vizată**. Şi mai plastic este termenul original, din limba engleză – *Subject Data*. Care în traducere directă este subiectul.

Astfel, persoana ale cărei date fac obiectul raportului juridic, despre ale cărei date este vorba în operațiunea de colectare, nu acționează în calitate de titular/proprietar/stăpân al datelor, ci în calitate de persoană vizată de raport, obiect al raportului. Marfă. Persoana despre al cărei teren vorbim este proprietară a terenului, în timp ce persoana despre ale cărei date vorbim – este obiect al

[33] „The digitisation of society and the economy is having a mixed impact on civic engagement in decision-making and on the barriers to public involvement in democratic processes. Big data analytics and artificial intelligence systems have made it possible to gather, combine, analyse and indefinitely store massive volumes of data. Over the past two decades, a dominant business model for most web-based services has emerged which relies on tracking people online and gathering data on their character, health, relationships and thoughts and opinions with a view to generating digital advertising revenue". Aceste piețe digitale au ajuns să fie concentrate în jurul câtorva companii care acționează ca gardieni eficienți ai internetului şi dețin valori de capitalizare bursieră ajustate la inflație mai mari decât orice alte companii din istorie. Opinia nr.3/2018 EPDS privind manipularea digital şi datele personale pag. 1 https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_summary_ro.pdf.

[34] Definiția oficială a UE privind Big Data publicată de către EPDS https://edps.europa.eu/node/3671: **Big data** *means large amounts of different types of data produced at high speed from multiple sources, requiring new and more powerful processors and algorithms to process and to analyse. These practices and technologies could offer major benefits for economic growth and various sectors including energy transportation and health. Not all of this information is personal, but businesses and* ***governments*** *are more and more using big data to understand, predict and shape human behaviour. Big data is therefore a long term strategic concern.*

raportului (de prelucrare sau colectare a datelor sale), nu proprietară a datelor. În timp ce, entitatea care colectează sau prelucrează datele – este proprietara datelor *(Data Owner)*[35].

Prin Comunicarea Comisiei către Parlamentul european, Consiliu, Comitetul economic şi social european şi Comitetul Regiunilor denumită „Construirea unei Economii Europene A Datelor", la pagina 11 a comunicatului Comisia Europeană admite că Big Data devin şi exercită atribuțiile de „proprietari" ale datelor utilizatorilor: „În anumite cazuri, fabricanții sau furnizorii de servicii pot deveni de facto **„proprietari"** ai datelor generate de calculatoarele sau procesele lor, chiar dacă respectivele calculatoare se află în proprietatea utilizatorului. Un control de facto asupra acestor date poate constitui pentru fabricanți o sursă de diferențiere şi de avantaje concurențiale."

Mai multe instituții şi operatori (GD Connect, ESOMAR etc.) caută să primească de la autoritățile europene răspuns la întrebarea cine este proprietarul datelor. Se pare că instituțiile europene nu sunt încă pregătite să dea un răspuns oficial şi nici entuziasmate de întrebarea vădit incomodă.

De curând, ESOMAR[36] a întocmit un raport[37] pe baza analizelor şi informațiilor şi sondajelor desfăşurate atât în UE, UK cât şi SUA, din care a rezultat ca aproximativ 68% din entitățile intervievate se consideră proprietari ai datelor.

De ce legiuitorul European nu a reglementat şi nu a definit expres cine este proprietarul datelor personale? Este aceasta o omisiune e legiuitorului European? Evident, nu.

Regulamentul este rezultatul unei negocieri şi dezbateri de peste 5 ani şi a trecut prin 2 lecturi în Parlamentul European. Nu încape îndoială că dacă legiuitorul de la Bruxelles nu a recunoscut persoanei vreun drept de proprietate asupra datelor sale, este pentru că nu a dorit acest lucru.

GDPR, de fapt, nu este un instrument prin care să ofere persoanei vreun control real asupra datelor sale. Ci are ca scop să reglementeze un mecanism de control al celor care sunt proprietarii datelor *(Data owner)*, respectiv operatorii şi persoanele împuternicite. *Temeo danones et dona ferentes.* Aceasta se întâmplă în contextul în care giganții *Big data* au acumulat şi au acces la volume uriaşe de date, exercitând nu doar putere economică dar şi politică fără precedent (scandalul Cambridge Analitica, Facebook, Google, Microsoft).

În acest context, legiuitorul European are nevoie de o legislație unitară, eficientă, care să îi asigure un sistem de control al fluxului datelor cu prerogative şi puteri efective şi extinse pe întreg teritoriul UE, inclusiv cu efecte de extrateritorialitate (art. 3 GDPR).

---

[35] Privacy policies etc.

[36] **ESOMAR** https://www.esomar.org/ is a membership organization representing the interests of the data, research and insights profession at an international level. While it started as a European associations, ESOMAR is the global association for the industry, with members based in 130 countries.

[37] Raportul ESOMAR din 2018.

VI. Jurisprudența CEDO şi a CJUE în materia respectării intimității şi protecția datelor. Cauza Schrems

Jurisprudența în protecția vieții private a intimității şi datelor cu caracter personale este creată atât prin hotărârile Curții de la Strasbourg (CEDO) cât şi în special cele ale CJUE.

Amintim printre cele mai relevante, cauzele ale CJUE: Cauza C‑582/14– Patrick Breyer c. Germania, Cauzele C-203/15 şi C-698/15 Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department c. Davis and Others EU:C:2016:970, Szabó şi Vissy c. Ungariei nr. 37138/14 (ECtHR, 12 January 2016) par. 68-70. O decizie cu impact deosebit asupra dreptului persoanei de a îi fi şterse datele sau dreptul persoanei de a fi uitat (right to be forgotten) este Cauza Mario Costeja Gonzalez, C-131/12.

Printre hotărârile CEDO enunțăm, în principal: Weber şi Saravia c. Germaniei nr.54934/00 (CEDO, 29 Junie 2006), Huvig c. Franței nr. 11105/84 (CEDO, 24 Aprilie 1990) par. 34; Kopp v Elveției nr. 23224/94 (CEDO, 25 Martie 1998) par. 55; Amann c. Elveției nr. 27798/95 (CEDO, 16 Februarie 2000) par. 76; Valenzuela Contreras c. Spainiei nr. 27671/95 (CEDO, 30 July 1998) par. 46; Prado Bugallo c. Spainieinr. 58496/00 (CEDO, 18 Februarie 2003) parag.30, Rotaru c. României nr. 28341/95 (CEDO, 4 Mai 2000) par. 55; Huvig c. Franței nr. 11105/84 (CEDO, 24 Aprilie 1990) par. 29; Zakharov c. Rusiei nr. 47143/06 (CEDO, 4 Decembrie 2015).

Geografia cauzelor indică o intoxicare cu abuzuri a întregului spațiu European.

Acest studiu nu va fi complet dacă nu ne facem puțin timp şi loc să discutăm Cauza Schrems.

Vă propun respectuos să ne aplicăm asupra analizei Cauzei studentului austriac Maximilian Schrems C-362/14 împotriva Data Protection Commissioner, Cerere de decizie preliminară formulată de High Court (Irland) – pentru că aceasta este, fără îndoială, cauza care a marcat şi a schimbat fundamental protecția datelor cu caracter personal, şi care a avut cel mai mare răsunet şi cele mai aspre critici din mediul politic, presiuni ale marilor grupuri economice nord americane, dar şi un val fără precedent de admirație şi susținere populară.

Piatra din capul unghiului, pe care nu au luat-o în seamă ziditori[38]. Cauza studentului Maximillian Schrems C-362/14 Schrems a fost buturuga care a răsturnat carul *Safe Harbour*[39], care până la acea data părea imbatabil. Astfel după 6 octombrie 2015

[38] Evanghelia după Matei 21,42.

[39] Acordul UE-SUA elaborat în perioada 1998-2000 având ca obiect reglementarea măsurilor de protecție adecvate în ce priveşte transferul datelor cu caracter personal din UE către SUA. Acest acord reprezintă Decizia privind sfera de siguranță adoptată de către Comisia Europeană în temeiul art. 25 alin. (6) din Directiva 95/46/CE prin care Comisia a atestat în 2000 faptul că principiile sferei de siguranță privind protecția vieții private şi întrebările frecvente aferente publicate de Departamentul Comerțului al SUA asigură un nivel de protecție adecvat în scopul transferurilor de date cu caracter personal din UE3. Drept urmare, a devenit posibil transferul liber al datelor cu caracter personal din

transferurile datelor către companii SUA sunt subiect de dezbatere, critică şi se află sub lupa şi controlul de legalitate a autorităților UE.

În data de 6 octombrie 2015 s-a întâmplat ceea ce părea de necrezut, Curtea de Justiție a Uniunii Europene a declarat invalidă Decizia 2000/520/CE a Comisiei Europene, adoptată în temeiul Directivei 95/46/CE, decizie care reglementa transferul de date cu caracter personal din state membre ale Uniunii Europene către entități din Statele Unite ale Americii, ca urmare a adeziunii acestor entități la principiile acordului *Safe Harbour*. Urmare a hotărârii Curții de Justiție a Uniunii Europene, Decizia 2000/520/CE a Comisiei Europene (Safe Harbour) nu a mai constituit temei legal pentru efectuarea transferurilor de date cu caracter personal în Statele Unite ale Americii.

În încercarea de a salva situația şi a continua afacerile companiilor afectate, Safe Harbour a fost înlocuit cu o nouă decizie privind sfera de siguranță UE-SUA denumită *Privacy Shield*, care niciodată nu a avut o poziție cimentată legal şi fost atacat chiar de la „naştere", inclusiv de către EDPS, prin critici dur exprimate. Principalele atacuri vin de la trei asociații non-profit franceze activiste în zona digitală a protecției drepturilor (La Quadrature du Net, French Data Network and Fédération FDN), dar şi în continuare prin Cauza C-311/18, inițiată iarăşi de insistentul austriac Maximillian Schrems Cauza C-311/18, (care pe lângă acțiunile împotriva Facebook, Google cu prejudicii reclamate de cca €3,9 bilioane din ianuarie 2019 a acționat în justiție inclusiv titani precum Amazon, Apple Music, DAZN, Filmmit, Netflix, SoundCloud, Spotify, and YouTube

Intervenția în viața privată, colectarea masivă a datelor cetățenilor de către sistemele guvernamentale şi monitorizarea permanentă este o realitate. Este peste tot şi în toate, asemenea unui praf impregnat în aer, e*vil dust,* cum a fost denumită de către Julian Assange[40]. Nu o mai putem evita, în societatea modernă. Fenomenul este surprins în lucrarea *Data Protection and Privacy under Pressure* scrisă de către Gert Vermeulen Eva Lievens (Maklu-Publishers, Antwerp, 2017), publicată inclusiv de către Autoritatea Europeană privind Protecția Datelor (EDPS)[41]. Găsim dezvoltată această idee şi de către Profesorul Andrew Bygrave, în *Data Privacy Law. An International Perspective* (OUP 2014) pag. 93-94, precum şi în articolul Susanei Sanchez Ferro „*The Need for an Institutionalized and Transparent Set*

state membre ale UE către societăți din Statele Unite ale Americii care s-au angajat să respecte principiile respective, în pofida faptului că în Statele Unite ale Americii nu există o lege privind protecția datelor în general. Funcționarea mecanismului sferei de siguranță se baza pe angajamentele şi autocertificarea societăților care aderau la acesta. Aşa au stat lucrurile până pe 6 octombrie 2015 când CJUE a invalidat decizia privind sfera de siguranță a Comisiei, respectiv Acord UE-SUA Safe Harbor în Cauza Schrems.

[40] https://www.youtube.com/watch?v=PYZwCllmaZc.

[41] https://edps.europa.eu/sites/edp/files/publication/17-12-18_wiewiorowski_data_protection_and_privacy_under_pressure_en.pdf publicat de către European Data Protection Supervisor-EDPS - Autoritatea Europeană privind Protecția Datelor

of Domestic Legal Rules Governing Transnational Intelligence Sharing in Democratic Societies" în Miller (nr. 5) p. 513, lucrarea Prof. Fred H Cate, James X Dempsey (eds), Bulk Collection: *Systematic Government Access to Private-Sector Data* (Oxford University Press 2017).

De ce este importantă Hotărârea Schrems:

În *Cauza Schrems*, Curtea de Justiție a Uniunii Europene (CJUE) a avut un cuvânt decisiv în cimentarea principiilor de protecție a datelor în cazul transferurilor de date.

- a identificat criterii şi stabilit definiții;
- a susținut şi afirmat explicit d**reptul Autorităților de supraveghere naționale să investigheze** dacă se asigură efectiv un nivel adecvat de protecție a datelor transferate către țări terțe, **chiar şi atunci când Comisia Europeană a emis o Decizie de conformitate** (articolul 45 GDPR);
- a articulat expres standardul de ***„esențialul echivalent"*** al protecției datelor, folosindu-l intenționat pentru a îl opune permisivului standard al *protecției adecvate* preferat de Comisie;
- a clarificat ce anume trebuie să înțelegem prin nivel adecvat de protecție în lumina prevederilor cheie ale Tratatului Privind Funcționarea Uniunii Europene (TFUE) şi în special a Cartei Drepturilor Fundamentale ale UE (Charta). A reiterat şi redat **Chartei** poziția dominantă şi ca **standard minim de referință în protecția datelor**;

De mare interes şi curaj este faptul că în această decizie, Curtea a statuat explicit că o reglementare care le permite autorităților publice accesul în mod generalizat la conținutul comunicărilor electronice aduce atingere substanței dreptului fundamental la respectarea vieții private[42]. Evident referirea viza transferurile masive de date, făcute în afara cadrului legal, de către Facebook şi Google către serviciul național de securitate al SUA, respectiv National Security Agency (NSA), afacere devenită publică după dezvăluire făcute de către Edward Snowden.

Curtea a confirmat că, chiar dacă există o decizie privind caracterul adecvat adoptată de Comisia Europeană în temeiul art. 25 alin. (6) din Directiva 95/46/CE (actualmente Articolul 45 GDPR), autoritățile de supraveghere din statele membre au în continuare competența şi obligația de a examina, în condiții de independență deplină, dacă transferul datelor către o țară terță respectă cerințele impuse de directiva menționată, interpretate în lumina articolelor 7, 8 şi 47 din Carta drep-

[42] Punctul 94 din Hotărârea Schrems: *„În special, trebuie să se considere că o reglementare care permite autorităților publice să acceadă în mod generalizat la conținutul comunicărilor electronice aduce atingere substanței dreptului fundamental la respectarea vieții private, astfel cum este garantat la articolul 7 din Cartă" (a se vedea în acest sens Hotărârea Digital Rights Ireland şi alții, C-293/12 şi C-594/12, EU:C:2014:238, punctul 39).*

turilor fundamentale[43]. Dar a arătat că, totuşi sarcina de a invalida un act al UE, cum ar fi o decizie a Comisiei privind caracterul adecvat, îi revine exclusiv Curții de Justiție a Uniunii Europene.

O valoare deosebită a Hotărârii Schrems este dată de faptul că în considerentele sale CJUE de mai multe ori repetă şi insistă că măsură la care trebuie să ne raportăm când analizăm respectarea dreptului la intimitate şi protecție a datelor este Carta Drepturilor Fundamentale a UE şi a arătat că acesta este şi standardul minim în cazul transferului de date din UE şi că nu va accepta niciun nivel sub cel stabilit şi garantat prin Chartă, chiar şi transferurilor de date. Această constatare este esențială[44].

Carta are rolul de a împiedica o practică de degradare a valorilor în standardele privind drepturile fundamentale, cum ar putea apărea dacă ar fi luate standarde scăzute în anumite state membre ca măsură pentru dreptul fundamental la protecția datelor. În consecință, chiar dacă actualmente competența legislativă în materia securității este apanajul exclusiv al statelor membre, asta nu înseamnă că acolo unde protecția datelor poate interfera cu securitatea statului, statele membre ar dispune de libertate discreționară de a interpreta conceptul de securitate națională pentru a scoate aceste acte de subcontrolul de legalitate al UE, respectiv de a le deturna de sub autoritatea legislației UE privind drepturile fundamentale.

Curajul CJUE este cu atât mai de apreciat cu cât sintagma controversată de criteriului standard „*în esență echivalent*" este folosită de către Curte tocmai pentru a contrabalansa şi confrunta direct criteriul de standard folosit de către Comisia Europeană în elaborarea deciziei Safe Harbour. Şi anume, standardul de criteriu preferat de către Comisie, este termenul special de „*protecție **adecvată***" față de

---

[43] Decizia şi Comunicarea Comisiei către Parlamentul European şi Consiliu privind transferul datelor cu caracter personal dinspre UE către Statele Unite ale Americii în temeiul Directivei 95/46/CE în urma hotărârii pronunțate de Curtea de Justiție în cauza C-362/14 (Schrems) poate fi consultat aici: https://eur-lex.europa.eu/legal-content/RO/TXT/?qid=1561751849927&uri=CELEX:62014CJ0362 şi https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52015DC0566 accesat la data de 01.07.2019.

[44] A se vedea în Hotărârea Schrems: **Paragraful 38** „*Trebuie amintit, cu titlu introductiv, că dispozițiile Directivei 95/46, în măsura în care reglementează prelucrarea unor date cu caracter personal care pot aduce atingere libertăților fundamentale şi în special dreptului la respectarea vieții private, **trebuie interpretate în mod necesar în lumina drepturilor fundamentale garantate de Cartă**…*" Paragraful **67**: „*În astfel de circumstanțe, având în vedere constatările făcute la punctele 60-63 din prezenta hotărâre şi pentru a oferi un răspuns complet instanței menționate, **trebuie să se analizeze dacă această decizie este conformă** cu cerințele care decurg din directiva menționată, **interpretată în lumina Cartei**"*. **Paragraful 78**: „*În această privință, trebuie să se constate că, ținând seama, pe de o parte, de rolul important pe care îl are protecția datelor cu caracter personal în lumina dreptului fundamental la respectarea vieții private şi, pe de altă parte, de numărul important de persoane ale căror drepturi fundamentale sunt susceptibile să fie încălcate în caz de transfer al datelor cu caracter personal către o țară terță care nu asigură un nivel de protecție adecvat, puterea de apreciere a Comisiei cu privire la caracterul adecvat al nivelului de protecție asigurat de o țară terță se dovedeşte redusă, astfel încât este necesară efectuarea unei supravegheri stricte a cerințelor care decurg din cuprinsul articolului 25 din Directiva 95/46, **interpretat în lumina Cartei".***

„protecție ***echivalentă***"[45]. Nuanța fiind nu doar esențială, ci vitală. Ceva ce este *adecvat* (depinde la ce ne raportăm la nivelul țării terțe), poate să nu fie nici pe departe *echivalentă* cu protecția reglementată la nivelul legislației UE.

Dar după ce se iese din holul curților de justiție şi se păşeşte în realitatea cotidiană, se constată că lucrurile stau diferit şi că trăim iluzia protecției efective.

Hotărârea Schrems, oricât de valoroasă, nu poate oferi o protecție completă a transferurilor de date către țări terțe. Acest lucru este ilustrat de faptul că, în ciuda afirmațiilor puternice ale CJEU cu privire la drepturile de protecție a datelor în hotărâre, în viața reală şi cotidiană, respectiv în practica de transfer a datelor acestea au fost pus în executare mult prea puțin, în special ne referim la perioada cuprinsă între invalidarea *Safe Harbor* şi intrarea în vigoare a *Privacy Shield.* Perioadă în care deşi companiile nord americane, mari operatori de date personale pe teritoriul UE (de exemplu Facebook, Google, IBM, Microsoft etc.) nu mai aveau temei legal de a transfera date către SUA, cu toate acestea toate, fără excepție au continuat transferurile. Un astfel de eşec al executării Hotărârii Schrems denotă o lipsă de considerare a legislației UE privind protecția datelor.

Mult mai grav este faptul că după Hotărârea Schrems şi criticile aduse modului în care Comisia Europeană a tratat protecția transferurilor datelor, la doar câteva luni (iulie 2016), Comisia Europeană, sfidând aceste critici a aprobat şi validat următorul acord de transfer de date UE-SUA, *Privacy Shield*, care nu diferă fundamental de predecesorul său Safe Harbor şi nu remediază efectiv deficiențele acestuia. Comisia a ignorat de această data şi criticile ridicate de EDPS cu privire la nivel necorespunzător de protecție a datelor de către Privacy Shield. În consecință, astăzi, iarăşi CJUE este chemată să se pronunțe asupra legalității acestui acord (Privacy Shield) în Cauza C-311/18, cu primul termen de audiere în fața CJUE în data de 9 iulie, 2019.

Ca urmare a hotărârii lui Schrems, unii comentatori (în special cei din SUA) au susținut că este o ipocrizie pentru factorii politici din UE şi respective CJUE să se preocupe de standardele de protecție a datelor pentru supravegherea exercitată de serviciilor de informații din afara UE, atât timp cât când standardele aplicabile unor astfel de servicii în interiorul UE prezintă mari deficiențe şi nu asigură cu nimic un nivel mai ridicat de protecție decât cel imputat omologilor săi din SUA.

În plus, este falsă afişarea preocupării pentru protecția datelor de către autoritățile UE, cât timp la nivelul statelor membre ale UE, este practicată împărtăşirea şi distribuirea largă a informațiilor şi datelor de către agențiile de informații ale statelor membre către serviciile guvernamentale SUA, inclusiv prin rețeaua de

[45] În mod just Dl. Prof. Kuner arată că Termenul „*esențial echivalent*" pare să implice o comparație între standardele privind protecția datelor ale țărilor terțe unde se urmăreşte transmiterea datele privind protecția datelor şi standardele UE, o sarcină dificil de realizat în practică. Întrucât, judecățile privind protecția datelor şi viața privată impun aprecieri „legate de context şi legate de cultură", ceea ce face din aceste standarde, instrumente de analiză comparativă dificil de gestionat. KUNER German Law Journal Vol. 18, nr. 04 https://germanlawjournal.com/volume-18-no-04/.

partajare a informațiilor „*Five Eyes*" (care include Australia, Canada, Noua Zeelandă, Marea Britanie şi SUA) şi în cadrul unor acorduri bilaterale care implică state membre, cum ar fi Marea Britanie, Franța şi Germania.

Cu alte cuvinte ce ni se reproşează este că CJUE se preocupă să repare o „țeavă" (de scurgere ilegală a datelor din UE către SUA), în timp ce se acceptă tacit şi se închid ochii pe „canale şi cascade" (ex: *Five Eyes*) de torente de curgere a datelor către agențiile SUA.

Greu de combătut aceste critici, pentru că sunt adevărate. Şi pentru că ating în mod just punctul nevralgic al vulnerabilității noastre în UE, pe care încă justiția UE nu este pregătită să le provoace.

Totuşi, strict vorbind, standardele de protecție a datelor ale agențiilor de informații ale statelor membre chiar compromise fiind, rămân totuşi irelevante pentru a aprecia nivelul de protecție oferit de țările terțe. Iar o încălcare a drepturilor fundamentale de către o țară terță nu poate fi scuzată prin faptul că standardele statelor membre ar prezenta deficiență sau ar fi compromise definitiv. O ilegalitate nu se poate scuza prin altă nelegalitate.

Altfel spus, faptul că avem „canale şi cascade" de scurgere ilegală a datelor, nu înseamnă că nu trebuie să reparăm „țevile" de scurgere ilegală. Şi că tolerarea unora şi a celorlalte este la fel de reprobabilă şi acuzabilă.

Cauza Schrems a deschis Cutia Pandorei şi a scos în mod oficial în dezbaterea publică, obligând autoritățile să vorbească despre aceste abuzuri care treceau nespuse şi asupra cărora autoritățile de supraveghere naționale (DPAs) nu îndrăzneau să se pronunțe.

Într-un sens moral şi politic, legitimitatea protecției drepturilor fundamentale în UE este subminată dacă UE este privită ca solicitând țărilor terțe standard de protecție a datelor cu caracter personal pe care ea însăşi nu este dispusă să le respecte. UE va căpăta realmente legitimitate în ochii autorităților statelor terțe, abia atunci când guvernele statelor membre vor accepta să îşi supusă şi să analizeze politicile sale de securitate națională cu legislația drepturilor fundamentale UE. Lucru care pare încă departe de a se realiza, neexistând suficientă voință politică în acest sens. Dar gheața a fost spartă…

Dacă avem pretenția că suntem o uniune şi state de drept, democratice, nu ne mai este permis să ignorăm incoerența juridică şi logică a reglementării transferului de date sau să se pretindă de către instituțiile UE (Comisie, în special) că poate fi atins un nivel adecvat de protecție a datelor la nivel mondial doar prin măsuri formale.

VII. GDPR – Noua legislație care revoluționează noțiunea intimității

Aşa cum am analizat mai sus, intervenția în viața privată, colectarea masivă a datelor cetățenilor de către sistemele guvernamentale şi monitorizarea permanentă

este o realitate. Este peste tot şi în toate, asemenea unui praf impregnat în aer, e*vil dust,* cum a fost denumită de către Julian Assange[46]. Nu o mai putem evita, în societatea modernă. Fenomenul este surprins în lucrarea *Data Protection and Privacy under Pressure* (trad. „Protecția Datelor şi Viața Privată sub Presiune") scrisă de către Gert Vermeulen Eva Lievens (Maklu-Publishers, Antwerp, 2017), publicată inclusiv de către Autoritatea Europeană privind Protecția Datelor (EDPS)[47].

Găsim dezvoltată această idee şi de către Profesorul Andrew Bygrave, în *Data Privacy Law. An International Perspective* (OUP 2014) pag. 93-94, precum şi în articolul Susanei Sanchez Ferro „*The Need for an Institutionalized and Transparent Set of Domestic Legal Rules Governing Transnational Intelligence Sharing in Democratic Societies*" în Miller (nr. 5) pag.513, lucrarea Prof. Fred H Cate, James X Dempsey (eds), Bulk Collection: *Systematic Government Access to Private-Sector Data* (Oxford University Press 2017).

Astfel probabil, a mai discuta astăzi despre protecția datelor personale şi intimitate însăşi (privacy, intimité) în sensul original al Convenției 108, CEDO[48], ține de trecut. Sau cel puțin, nu mai emulează cu aceeaşi putere cu care a fost învestită la origini sau la care ne-am aştepta. Azi, intimitatea este o noțiune convențională, subiectivă şi cu certitudine o chestiune circumstanțială. Nu mai putem, cu sinceritate avea şi nici pretinde realist **intimitatea**, în accepțiunea şi percepția clasică a termenului, a Dreptului de a fi lăsat în pace (Right to be left alone)[49].

---

[46] https://www.youtube.com/watch?v=PYZwCllmaZc accesat la data de 01.07.2019.

[47]https://edps.europa.eu/sites/edp/files/publication/17-12- accesat la data de 01.07.201918_ wiewiorowski_data_protection_and_privacy_under_pressure_en.pdf accesat la data de 01.07.2019publicat de către European Data Protection Supervisor-EDPS - Autoritatea Europeană privind Protecția Datelor.

[48] *Curtea Europeană a Drepturilor Omului* (CEDO), adesea numită informal „Curtea de la Strasbourg" https://www.echr.coe.int/Documents/Convention_RON.pdf.

[49] *Right to be left alone* - pentru prima data o fost articulat în anul 1834 de către Judecătorul Curşii Supreme din SUA (SCotUS) Dl. Justice Cooley, care într-o cauză privind drepturile reale, consemnat în considerente inclusiv prima definiție a dreptului la intimidate şi autodeterminare – dreptul de a fi lăsat în pace, dreptul la intimitate, prin următoarele considerente: «*right to one's person may be said to be a right of complete immunity: the right to be let alone*». Ulterior, peste mai bine de 50 de ani, definiția academică a intimității ca drept (privacy) a fost reținută în lucrările doctrinare a doi iluştri profesori şi judecători a SCotUS SUA, Judecătorul Samuel Warren şi Judecătorul Louis Brandeis https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf
https://fee.org/articles/the-right-to-be-left-alone/ Această definiție a fost lansată în 1890 şi îşi are originea în cauza care a implicat-o pe soția judecătorului Samuel Warren ale cărei poze au fost publicate de către societatea nou înființată Kodak, fără acordul acesteia. A. RENGEL, *Privacy in the 21st century, Studies in Intercultural Human.*

rights, Leiden-Boston, 2013; K. LACHANA, *Elements of convergence in the historical origins and ideological.*

foundations of the US and European privacy law: the nexus between the „right to be let alone" and continental.

De ce are nevoie sistemul instituțional de GDPR?

Presiunea pieței digitale, aşa cum am arătat în capitolele anterioare, au obligat instituțiile europene să ia atitudine şi să îşi securizeze poziția lor, prin adoptarea unei legislații în acest domeniul care să permit controlul instituțiilor UE. Aşa a fost adoptat Regulamentul GDPR. Naşterea lui a fost anevoioasă şi presiunile din partea celor 7 titani ai social media SUA, au fost exercitate la puterea lor maximă.

Probabil că unul din motivele determinante este însăşi natura specifică a datelor. Şi anume, vestea proastă cu datele este că ele nu pot fi realmente monopolizate, prin însăşi natura lor. Este simplu cu gazele, petrolul, electricitatea, aurul etc. Dar datele plutesc cu uşurință peste tot. Fără hotare. Fără limite. Oamenii cu uşurință îşi dezvăluie datele şi informațiile personale (mai cu seamă în mediu online), aproape oricui este suficient de inteligent să le ofere sau promită un avantaj în schimb (încărcarea „gratuită" a unui app, softwear etc.).

Mase întregi de persoane, fără nicio constrângere împărtăşesc zilnic online (facebook, wase, skype etc.) zeci de date cu privire la persoana lor, rude, apropiați, prieteni, exprimă opinii şi preferințe, publică poze, accesează social media şi încarcă aplicații cu funcții de geolocalizare (wase, google search, inclusiv aplicațiile online ale magazinelor online etc.). Telefoanele sunt conectate la internet şi se interconectează automat prin setări automate, nelimitat, prin bluetooth şi wireless cu mii de alte dispozitive prin care are loc un schimb intens de date. Aceste operațiuni au loc în încăperi private, pe stradă, în cafenele, în universitate, la serviciu, inclusiv în parcuri, spații de joacă pentru copii, biblioteci publice şi orice alte locații fie spații private sau publice, prin sisteme wifi care fie că necesită sau nu identificare colectează multiple datele cu privire la utilizatorii dispozitivelor (ex: geolocalizare), inclusiv prin urmărirea IP-ului dinamic (Case 582/14 – Patrick Breyer v Germany[50]). Sute de mii de accesări pe oră, miliarde pe zi.

Fluxul de date este gigantic.

Astfel, această marfă (datele), dacă nu sunt controlate, au potențial real să fie acumulate masiv de către oricine şi mai ales folosite în orice scop, riscând să compromită şi erodeze sistemul guvernamental instituțional, aşa cum îl cunoaştem azi.

Astfel EDPS îşi reafirmă expres interesul de a deține (prelua) controlul asupra deținătorilor fluxurilor masive ale datelor p. 4 Op3/2018: „Respectul pentru drepturile fundamentale, inclusiv un drept la protecția datelor, este crucial pentru a asigura corectitudinea alegerilor, mai ales că ne apropiem de alegerile din 2019 pentru Parlamentul European. În primul rând, avizul va rezuma procesul prin care datele cu caracter personal alimentează şi determină ciclul predominant de urmărire digitală, țintire cu exactitate şi manipulare. Apoi, va lua în considerare rolurile diferitelor entități din ecosistemul de informații digitale. În încheiere va

jurisdictions, M. BOTTIS (ed.), *Privacy and Surveillance, Current aspects and future perspectives*, Athene, 2013.

[50] http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN.

avertiza că problema manipulării online cel mai probabil se va agrava, că o singură abordare de reglementare nu va fi suficientă în sine şi că, prin urmare, autoritățile de reglementare vor fi nevoite să colaboreze de urgență pentru a aborda nu numai abuzurile localizate, ci şi distorsiunile structurale cauzate de concentrarea excesivă a pieței"[51].

În consecință, dacă sistemul guvernamental nu poate monopoliza datele, el în mod disperat are nevoie să exercite controlul asupra acestora. De fapt, să **controleze stăpânii datelor**. În esență, despre asta este GDPR-ul - **reglementarea unui cadrul legal** structurat, **învestit cu putere centrală care** (inclusiv prin *consistency mechanism*[52]) să implementeze un **sistem de control al stăpânilor datelor** (celor care le acumulează şi dețin date).

GDPR instituie un sistem de control al entităților care colectează şi prelucrează date, stabilindu-le limite legale şi un control instituțional riguros. Operatorii de date pentru a putea să mai continue activități de prelucrare a datelor trebuie să implementeze codul de reguli stabilite prin GDPR, iar autoritățile de supraveghere naționale au fost învestite cu puteri extinse pentru a asigura implementarea corespunzătoare (art. 58 GDPR).

În 2016, Comisia Europeană a decis să preia controlul datelor şi a pieței digitale în spațiul European şi a lansat Proiectul Digital Single Market 2020 (DSM)[53], trasând prin planul aprobat Strategia DSM2020 publicată în 10 mai 2017 şi a stabilit 7 obiective a fi atinse. În descrierea obiectivelor transpar şi scopuri care au determinat GDPR, *causa remota*, precum:

- *„Noi vrem să ştim ce se întâmplă cu datele noastre şi noi trebuie să ştim că regulile jocului sunt aceleaşi în toate țările Uniunii Europene".*

- *„Noi trebuie să ajungem din urmă principalii noştri competitor din Tehnologia de Comunicații prin Interment (ICT), cercetare şi inovație digitală"*[54] *We must catch up with our main competitors in ICT research and digital innovation*[55]*".*

---

[51] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_summary_ro.pdf.

[52] Art.63 GDPR / mecanismlegal de asigurare a aplicării coerente, unitare şi uniforme a controlului pe întreg teritoriul Uniunii Europene prin autorități de supraveghere locale (art.51) şi la nivel european întrunindu-se lunar Comitetul european pentru protecția datelor (format din președinții autorităților locale de supraveghere) pentru trasarea şi aplicarea unitară a politicilor şi soluțiilor GDPR.

[53]https://ec.europa.eu/digital-single-market/en/europe-2020-strategy accesat la data de 01.07.2019.

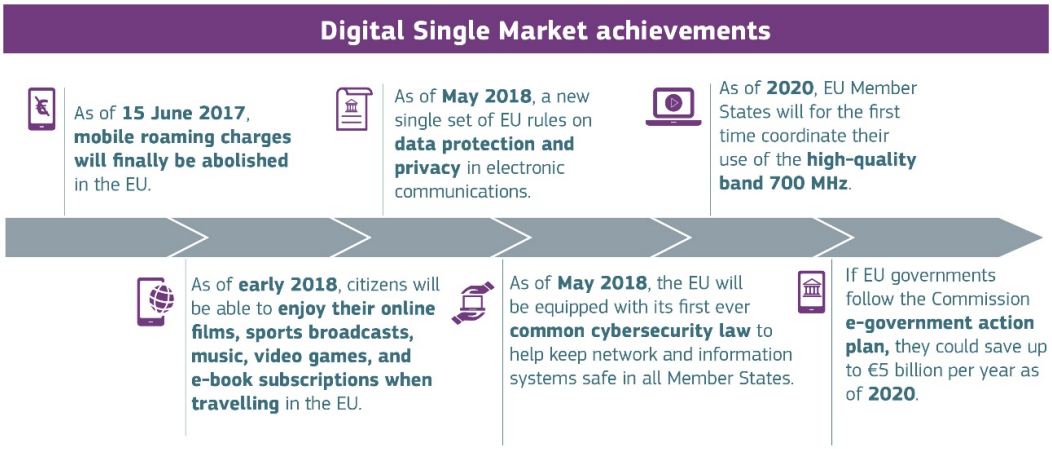
https://ec.europa.eu/digital-single-market/en/news/digital-single-market-mid-term-review accesat la data de 01.07.2019.

[54] Strategia DSM2020 publicată în 10 mai 2017:*"We want to know what's happening to our personal data, and we need to know that the rules of the game are the same in all countries of the EU.""We must catch up with our main competitors in ICT research and digital innovation".*

[55] https://ec.europa.eu/digital-single-market/en accesat la data de 01.07.2019. Traducere:

„– Vrem să ştim ce se întâmplă cu datele noastre personale şi trebuie să ştim că regulile jocului sunt aceleaşi în toate țările UE".

GDPR face parte din politicile şi legislaţia reglementată de 1-ul obiectiv al DSM2010 şi este o realizare marcata ca atare de către Comisia Europeană privind realizările DSM în 2017-2020[56]:



GDPR oferă sistemului instrumente şi pârghii legale cară să asigure controlul efectiv al fluxului de date:

- Dacă până la intrarea în vigoare a GDPR, puteam doar imagina volumul real de date care se colectau şi nu aveam informaţii unde acestea se află şi nici pârghii legale de acces. Odată cu intrarea în vigoare, GDPR instituie norme obligatorii privind evidenţa fluxului datelor, registrul operaţiunilor de prelucrare a datelor (art. 30, 10-22 GDPR), solicitând atât operatorilor cât şi persoanelor împuternicite în orice moment să fie capabili (inclusiv tehnologic – art. 32 GDPR) să indice ce date colectează/prelucrează şi câte date colectează şi unde le stochează, locaţia efectivă a acestora. Precum şi obligaţia de a le pune la dispoziţia autorităţii şi a prezenta autorităţii (art. 5, *accountability*). Şi toate aceste măsuri de asigurare a controlului sunt impuse pe cheltuiala deloc neglijabilă a operatorului/persoanei împuternicite însăşi, aceştia fiind obligaţi să avanseze toate costurile şi să investească în tehnologii care să asigure controlul fluxului datelor, securitatea precum şi trasabilitatea şi reconstituirea datelor (art. 32, art. 25 şi urm. GDPR). Şi toate acestea trebuie executate şi menţinute la cel mai înalt nivel care să satisfacă aşteptările autorităţii (*state of art*, art. 25 GDPR) şi într-o manieră documentată, care să permită autorităţii să verificare mijloacele implementării adecvate (accountability art. 5 alin. 2 GDPR). În caz contrar, dacă aceste condiţii nu sunt

„– Trebuie să ne apropiem de principalii noştri concurenţi în domeniul cercetării în domeniul TIC şi inovării digitale"

56 https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market#The Pillars accesat la data de 01.07.2019

îndeplinite la nivelul aşteptărilor autorității de supraveghere, aceasta are puterea nu doar de a dispune amenzi uriaşe (până la 20 milioane euro, art. 83 pct. 5 GDPR), dar şi să suspenda sau să bloca activitatea (art. 58 alin. 2 pct. f GDPR).

- Sistemul instituțional de supraveghere şi control la nivel teritorial (local)[57] şi cel la nivel European[58], instituite prin GDPR prin Capitolul VII Cooperare şi coerență şi în special Mecanismul pentru asigurarea coerenței (art. 63 GDPR) etc. Aceste instituții învestite cu puteri considerabile, fără precedent[59] (cu dreptul de a organiza raiduri inopinate, ridica dispozitive şi calculatoare, inspecta inopinat şi fără mandat orice locații, inclusiv ale persoanelor fizice, identifica la locație orice persoane şi a audia persoane ad-hoc etc.) au autoritatea şi acum şi baza legală[60] de a asigura implementarea controlului.

Iar la nivel European, instituțiile precum Comitetul european pentru protecția datelor (art. 68 GDPR) şi Autoritatea Europeană pentru Protecția Datelor (EDPS) prin intermediul mecanismului de cooperare şi coerență *(Consistency mechanism)* asigura aplicarea unitară şi coerentă pe întreg teritoriul European.

Sunt încă mulți care au vie amintirea regimul epocii '20-'90, în care instituții precum KGB sau alte organizații de securitate cheltuiau imense resurse financiare, utilizând teroarea, opresiunea, şantajul şi tortura pentru a-şi spiona populația, a obține informații privind populația şi eventualii oponenți ai regimului. Unele lucruri se schimbă, altele nu se schimbă…

VIII. De ce GDPR pentru instituțiile Uniunii Europene? Criza legitimității şi deficitul de democrație a instituțiilor UE

GDPR pentru cetățeni?

Uniunea Europeană şi instituțiile, agențiile şi departamentele create în susținerea sistemului său au luat naştere nu pe care federativă, ci ca un cartel economic (al industriei grele a cărbunelui şi oțelului, atrăgând mai târziu şi fermierii) care trebuia să susțină organizatoric şi administrativ cooperarea Germano-Franceză, având bazele aşezate pe convertibilitatea dolarului american conform înțelegerii de la Bretton Wood (iulie 1944), dezvoltat prin programul Marshall pentru reconstrucția Europei.

Instituțiile europene nici la origine (şi nici azi) nu reprezintă un sistem decizional cu baze pur democratice transparente. Sistemul European decizional este încă opac, cu tendințe de de-politizare în favoarea tehnocrației susținute de interese economice, respectiv grupuri instituționalizate de interese economice.

---

[57] Prin autoritățile de supraveghere (art. 51 GDPR).

[58] Prin Comitetul european pentru protecția datelor (art. 68 GDPR) şi Autoritatea Europeană pentru Protecția Datelor (EDPS).

[59] Poate pe alocuri uşor comparabile cu cele ale Consiliului concurenței.

[60] Art. 51 GDPR, Decizia nr. 161/2018 ANSPDCP.

Instituțiile centrale de conducere respectiv Comisia cât şi Consiliul European şi Consiliul de Miniştri au ca reprezentanți persoane numite, nu alese (comisari, reprezentanți naționali, şefii statelor, prim miniştri şi miniştri de resort), iar Parlamentul European, paradoxal față de ce ar sugera denumirea sa, nu are realmente puteri legislative, ci preponderent consultative (un handicap puternic pentru sistemul democratic european) şi în continuare nu i se recunoaşte inițiativă de a propune legislație, în ciuda faptului că este singura instituției europeană ale ai cărei membri sunt direct aleşi de către cetățenii europeni, prin scrutin.

Eşecul democratizării UE, chiar şi după reformele aduse prin Tratatul de la Maastrich (1992), este una din cauzele majore ale crizei sistemului instituțional al UE pe care îl trăim în prezent, aşa cum o recunosc şi oficialitățile[61].

În special după decizia Marii Britanii de părăsire a Uniunii Europene (Brexit), la nivel european se fac tot mai auzite vocile care pun în dezbatere publică *legitimitatea instituțiilor europene* şi în special a Comisiei Europene şi a Consiliului UE (cunoscut şi sub denumirea de Consiliul de Miniştri), aşa cum a sintetizat grupul academic Jaques Delors Instituit în Raportul din 5 ianuarie 2018 *(„A more democratic European Union. Propositions and scope for political action").*

Un semnal pozitiv este că în dezbaterile restructurării pro-democratizării europene au participat ca şi actori principali Preşedintele Comisiei Europene Dl. Jean-Claude Juncker, Preşedintele Franței Dl. Emmanuel Macron[62] şi Preşedintele Consiliului European Dl. Donald Tusk.

Din „Carta Alba privind viitorului Europei şi calea de urmat" prezentată de către Dl. Jean Claude Junker se desprinde concluzia că oficialitățile nu doar recunosc că UE se află între-o criză instituțională, dar şi că această criză pentru a fi depăşită implică acțiuni comune de democratizare, implicare a cetățeanului european în mecanismele decizionale la nivelul UE. Lucru care nu se poate realiza, decât dacă există pârghiile legale şi o conştiință europeană. Trebuie creată legătură şi relația dintre instituție, funcționar şi cetățean european. Este singura cale de legitimizare a instituțiilor europene.

Alegerile electorale, reprezintă singurul mijloc autentic prin care cetățenii îşi cunosc şi îşi aleg direct conducătorii, creând între aceştia relații de încredere şi asumare directă a răspunderii politice. Este şi singura ocazie când cetățeanul poate să îşi exprime direct poziția şi imediat preferința sau să sancționeze politic clasa politică.

---

[61] Sunt fireşte şi alte cauze puternice, precum lipsa unui sistem de apărarea europeană comun (eşecul PESC), criza financiară globală, criza euro etc.

[62] De mare interes este discursul Dl Preşedinte Emmanuel Macron pro-european şi pro reforme instituționale europene care a ținut să sublinieze public că „Pentru a lucra mai bine, această Uniune Europeană nu poate să mai evite chestiunea delicata a instituțiilor sale" (trad. „In order to work better, this European Union cannot escape the issue of its institutions"). Discursul complet de o tehnică oratorică excepțională poate fi consultat aici https://www.diplomatie.gouv.fr/IMG/pdf/english_version_transcript_-_initiative_for_europe_–_speech_by_the_president_of_the_french_republic_cle8de628.pdf accesat la data de 01.07.2019.

Delegarea excesivă a puterii erodează relaţia dintre cetăţean şi conducătorii săi (cetăţeanul ajunge să nu cunoască efectiv cine îi sunt comisarii naţionali, cine sunt membrii Consiliului UE sau când au loc întrunirile, ce se discută etc.) relaţia dintre cetăţean şi reprezentantul naţional este diluată până la inexistenţă. Un alt efect şi mai nociv al delegării excesive a puterii este atrofierea simţul şi răspunderii civice a cetăţenilor.

Şi anume: odată ales de către cetăţean un parlament (mecanismul alegerilor parlamentare) acesta automat deleg dreptul unor parlamentari de a desemna miniştri naţionali, care la rândul lor desemnează comisarul european şi reacţia delegaţională se declanşează în lanţ.

Moment de la care cetăţeanul, nu mai are nu doar controlul, dar nici reprezentarea reală şi obiectivă a mecanismelor politice. Ceea ce duce la pierderea interesului civic şi a prezenţei sale civice în mecanismul puterii şi construirii politicilor (naţionale şi europene).

Or, nu asta este esenţa unui stat democratic? Participarea nemijlocită şi efectivă a cetăţeanului la viaţa cetăţii? Cetăţeanul se vede pe sine pe o parte a baricadei, iar instituţiile UE îi apar ca fiind factori de putere care nu doar că se situează şi funcţionează într-o sferă depărtată (şi empatic, şi geografic, deopotrivă), dar şi independent de voinţa sa (şi chiar de interesele sale), ceea ce este şi mai regretabil.

Apatia cetăţenilor statelor membre faţă de participarea la viaţa publică şi civică europeană, se datorează lipsei informării adecvate şi lipsa implicării directe a acestora în mecanismul decizional european, ceea ce evident se manifestă prin lipsa unei identităţi europene. Cetăţeanul român continuă să se vadă pe sine pe o poziţie de adversitate, tip noi-şi-ei.

Tratatul de la Maastrich (1992) a încercat să mai îndrepte puţin lucrurile şi a acordat anumite prerogative legislative Parlamentului, cu caracter mai degrabă de veto, în anumite domenii limitativ stabilite, care se adoptă pe calea Procedurii Legislative Ordinare[63]. În continuare *Parlamentului European nu îi este recunoscută iniţiativă legislativă*, respectiv dreptul de a propune sau amenda legi. Un handicap uriaş, căci ce fel de legiuitor (parlament) este acela care nu are şi dreptul de a propună legi şi iniţieze mecanismul legislativ.

De asemenea, nu putem să trecem sub tăcere faptul că în continuare sunt domenii de interes major strategic în care Parlamentului European nu i se recunosc prerogative decizionale legislative, rolul Parlamentului fiind în continuare limitat (Procedura specială).

[63] Procedura de codecizie respectiv de implicare în procesul legislativ şi a Parlamentului, a fost introdusă târziu şi la presiunile grupurilor de pro-democratizare, abia în 1992 prin Tratatul de la Maastrich, iar folosirea sa generalizat în 1999, odată cu aprobarea Tratatului de la Lisabona, codecizia a fost redenumită procedura legislativă ordinară, devenind principala procedura decizională folosită pentru adoptarea actelor legislative ale UE. Aproximativ 85 domenii de politică intră sub incidenţă sa.

Într-o astfel de structură instituțională, jocul politic este cel determinat de actorii săi (instituțiile UE), dictat de interesele şi prioritățile sale. În consecință, nu ar trebui să ne surprindă faptul că Regulamentul privind protecția datelor personale (GDPR), ca şi element de realizare a Politicilor Strategice Digitale, este o reglementare care deserveşte şi este orientată cu precădere către interesele instituționale şi nu către cele ale cetățeanului. Cu alte cuvinte GDPR prin concepție este destinat să servească interesului instituțional.

Criticii privind deficitului democratic şi legitimității instituțional nu mai sunt subiecte tabu, devenind o prioritate în dezbaterea europeană. Astfel, în februarie 2017, Parlamentul European a elaborat programul agendă „Carta Alba privind viitorului Europei şi calea de urmat[64]" prin care a descris cinci posibile scenarii.

Legislația europeană are grijă atunci când intensifică controlul prin crearea unor instrumente noi, să creeze fireşte un număr nou de locuri pentru funcționari şi recruți ai sistemului birocratic care să le implementeze[65]. GDPR ca şi Regulamentul UE 2018/1725, prin reglementarea obligației numirii Reprezentantului privind protecția datelor – DPO (Data Protection Officier), atât de către instituțiile publice, inclusiv europene, şi un număr larg de societăți şi entități private (art. 35 GDPR).

Doar în anul 2018, cifra de DPO necesari se ridica către 75.000[66] potrivit estimărilor IAPP (International Association of Privacy Professionals). O cifra uriaşă de noi funcționari. Ceea ce determină alocații semnificative în budget. Căci cineva trebuie să plătească aceste noi funcții şi funcționari. Noi venituri din consultanță în mediu privat etc. Cine suportă costul acestor noi cheltuieli, sau în buzunarul cui se răsfrâng acestea? Fireşte că în ale cetățeanului european.

Este cetățeanul informat în acest sens? Are el motive a se plânge sau a fi nemulțumit de GDPR?

De facto, niciun comunicat al Comisiei europene nu a vorbit despre costuri şi bugete, dar au curs comunicate şi programe vaste de informare către cetățenii europeni prin care aceştia erau asigurați că GDPR aduce un nou capitol (art. 12-22 GDPR) de drepturi pentru persoana vizată. În mediul guvernamental şi academic se scrie încă prea puțin despre aceste costuri şi controlul adus de GDPR. În schimb

---

64 https://ec.europa.eu/commission/future-europe/white-paper-future-europe-and-way-forward accesat la data de 01.07.2019.

65 De exemplu privind implementarea DSM 2020 se anunță oficial: „DSM creates opportunities for new startups and allows existing companies to reach a market of over 500 million people. Completing a DSM can contribute EUR 415 billion per year to Europe's economy, create jobs and transform our public services". https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market#ThePillars accesat la data de 01.07.2019.

66 https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/ - „More than 28,000 will be needed in Europe and U.S. and as many as 75,000 around the globe as a result of GDPR, the International Association of Privacy Professionals" accesat la data de 01.07.2019.

în 2018 s-a scris substanțial cu privire la drepturile persoanei vizate în lumina GDPR, susținându-se că au fost îmbunătățite față de Directiva anterioară[67]. Dar oare sunt?

Este poate GDPR un Cal Troian pentru cetățeanul European?

IX. Lacunele GDPR privind drepturile persoanei vizate. Analiza. Critici şi perspective

De la început, remarcăm că orice legislație opresivă se lansează cu o motivare pro cetățean, prezentându-se ca o măsură să apere interesul cetățeanului. GDPR a fost lansat ca un regulament care sporeşte drepturile individului. Mai înainte de toate, pentru că sună foarte democratic a susține – mai multe drepturi pentru *demos*.

Cu cât se vor acorda mai multe „drepturi" cu atât mai multă legitimitate democratica va putea pretinde măsura. Pentru acceptarea măsurilor de constrângere ca fiind necesare şi chiar benefice, acestea sunt îmbrăcate în drepturi pentru cetățeni, atunci când analiza conținutului trădează exact opusul. Deghizarea controlului este diversiunea de bază. Asemenea parabolei dintr-o splendidă legendă de la începutul secolului XIX despre adevărul gol[68] şi minciuna deghizată, subiect al picturii lui Jean-Léon Gérôme *„La Vérité sortant du puits armée de son martinet pour châtier l'humanité"*[69], 1896. Aşa cum o indică şi fondul pe care vine şi conținutul, Regulamentul (GDPR) este asimilabil Calului Troian. Aidoma GDPR, Calul Troian nu ar fi intrat în Troia, dacă nu era atât de „frumos" şi atât de „gratuit".

GDPR şi-a făcut intrarea într-un marş a drepturilor noi extinse pentru persoane. Când o lege se prezintă atât de generos, cetățenii nu se mai apleacă asupra substanței, vigilența fiindu-le inhibată.

---

[67] Directiva 95/46/CE privind protecția datelor.

[68] Conform unei legende din secolul 19, Adevărul şi Minciuna se întâlnesc într-o zi. Minciuna îi spune Adevărului: „Astăzi este o zi minunată!", Adevărul se uită pe cer şi constată că ziua chiar era minunată. Ei petrec ceva timp împreună, ca mai apoi să ajungă la o fântână. Minciuna îi spune adevărului: „Apa este foarte bună, hai să facem o baie împreună". Adevărul, din nou suspect, verifică apa şi descoperă într-adevăr că aceasta este foarte bună. Se dezbracă amândoi şi încep să facă baie. Deodată, Minciuna iese afară din apă, se îmbracă cu hainele Adevărului şi fuge. Furios, Adevărul iese afară din fântână şi merge să caute Minciuna pentru a-şi recupera hainele. Lumea, văzând Adevărul gol-goluț, îşi mută privirea cu ură şi dispreț. După un timp, bietul Adevăr se întoarce în fântână şi dispare pe vecie, ascunzându-şi ruşinea.

De atunci, Minciuna face înconjurul lumii, îmbrăcată ca Adevărul, satisfăcând nevoia societății, pentru că, Lumea, în orice caz, nu are nicio dorință să vadă Adevărul gol-goluț. Pictură faimoasă: *„Adevărul ieşind din fântână"* de către Jean-Léon Gérôme, 1896.

[69] https://en.wikipedia.org/wiki/Truth_Coming_Out_of_Her_Well accesat la data de 01.07.2019.

Avem dreptul să solicităm informații cu privire la prelucrarea datelor noastre? Da, cu limitele stabilite expres. Sistemul instituțional are drept de acces nelimitat, dreptul de a cunoaşte toate prelucrările datelor noastre şi a le monitoriza gestiunea. Ca orice drept el are o obligație corelativă. Şi anume, prin legalizarea dreptului individului de a solicita entităților informații cu privire la prelucrarea datelor sale personale, se legalizează evident obligația entităților private de a structura şi păstra evidențe ale acestor operațiuni în mod controlat.

În consecință, sistemul instituțional pentru prima data urmează să aibă imaginea completă asupra volumului de date deținute şi gestionate de către entitățile private şi astfel şanse în a ține sub control Big Data. Prin exercitarea de către indivizi a acestor drepturi față de entități, se exercită de fapt controlul instituțional. Căci entitățile care nu se conformează sunt denunțate Autorității de Supraveghere prin plângerile puse la dispoziție persoanei vizate de către autorități, inclusiv online. Astfel, persoanele vizate, sunt chiar ele însele cele care veghează funcționarea sistemului de control instituțional.

Avem dreptul la portarea datelor? Un drept, de fapt, foarte util sistemului, care pentru a asigura o piață digitală controlată trebuie să se asigure de accesibilitatea formatului în care se păstrează şi clasifică datele, dar mai ales de disponibilitatea transmiterii acestora (accesibilitatea) prin portare. Costurile tehnologice şi întreaga investiție este chiar prin lege în sarcina operatorului (art. 25 GDPR). Privit din perspectiva persoanei, cele mai multe persoane probabil nu fac uz de acest drept. Sistemul instituțional efectuează operațiuni de portare a datelor în mod sistematic.

Dreptul de a obiecta (de a formula obiecțiuni). Dreptul de acționa în instanță. Dreptul de a depune plângeri şi sesizări. Toate fiind forme de reacție *post factum*[70], față de o acțiune abuzivă privind datele. Marea parte a acestora existau şi înainte[71], fiind reiterate.

Este de remarcat faptul că GDPR nu oferă persoanei instrumentul legal de a bloca *a priori* vânzarea, comercializarea sau valorifica sub orice formă datelor lor personale de către entitățile operatoare. Sistemul decizional European rămâne în continuare opac, iar protecția intimității şi datelor persoanelor rămâne în continuare utopică pentru persoană. În esență, GDPR instituie un sistem de control instituțional concentrat asupra entităților, nu de protecție a intimității persoanei. Persoanei nu îi este reglementat niciun control asupra datelor sale, nefiindu-i nici recunoscută calitatea de proprietar asupra acestora sau atributul de a dispune de datele sale.

---

[70] Este importantă această atenționare, întrucât în GDPR nu oferă individului dreptul de a se pronunța *a priori* asupra vânzării datelor sale, spre deosebire de legislația Californiană (CCPA) care reglementează acest drept ca şi condiție ce se impune a se întruni *a priori*. A preveni un abuz, este fireşte mult mai eficient decât a-i îndepărta efectele.

[71] Directiva 95/46/CE privind protecția datelor cu caracter personal.

X. GDPR şi comercializarea datelor cu caracter personal. Intimitatea de vânzare?

Un raport McKinsey din 2015 descrie cele trei moduri în care companiile accesează date cu caracter personal[72]. În primul rând, datele cu caracter personal pot fi *cumpărate*. Companii precum Experian sau Acxiom oferă spre vânzare baze largi de consumatori care pretind că conțin informații despre obiceiurile, stilul de viață şi atitudinile de cumpărare ale clienților. Acestea pot fi potrivite cu bazele de date interne ale companiei prin identificatori cum ar fi detaliile cărților de credit sau numerele de telefon. Date de panel, de la companii cum ar fi Nielsen şi Compete, oferă contra cost, acces la activitățile a 2 milioane de consumatori, oferind viziuni granulare asupra comportamentului persoanelor, cum ar fi înregistrările paginilor web vizitate şi achizițiile efectuate de consumatori într-o anumită perioadă de timp.

Datele „de călătorie" din programul „AdSense" al Google construiesc o amprentă digitală pentru consumatori, bazată pe datele lor de conectare la site-uri populare (de exemplu, pe site-urile aeriene sau pe Facebook). Odată ce clientul se conectează, cookie-ul urmăreşte acest client pe alte site-uri web. Companiile agregatoare, cum ar fi Datalogix, combină aceste date cu sute de date de conectare şi le adaptează într-o bază de date cu peste 100 de milioane de aparținători.

În al doilea rând, companiile pot *obține gratuit* date de la clienți. McKinsey îi sfătuieşte pe comercianții cu amănuntul să „încurajeze clienții să se autoidentifice prin conectarea la site-ul web, folosind un card de loialitate în magazin sau identificându-se atunci când apelează la îngrijirea clienților".

În cele din urmă, companiile *fac schimb* sau îşi *împărtăşesc reciproc* sau chiar *aduc ca aport în afacere* date cu caracter personal, printr-un parteneriat agreat. De exemplu, Visa a încheiat un parteneriat cu comercianții cu amănuntul pentru a introduce consumatori pe baza de localizări extrem de direcționate în timp ce fac achiziții – „scanați-vă Visa la o distanță pentru a efectua o achiziție şi obțineți oferte pe smartphone-ul pentru comercianții cu amănuntul la distanță de mers pe jos".

Schimburile de date de multe ori se tranzacționează în cantități uriaşe de date. BlueKai Exchange, care este gestionat de Oracle şi este considerate cea mai mare piață de date din lume, oferă „date despre peste 300 de milioane de utilizatori care oferă spre tranzacționare în spor comercial peste 30.000 de atribute de date". Procesul de schimb are peste 750 de milioane de evenimente şi tranzacționează peste 75 de milioane de licitații pe zi[73]. Aceasta formă de afacere este adesea menționată ca *publicitate programatică* – o metodă nouă, automatizată de cumpărare

[72] McKinsey & Company (2015), „Marketing & Sales Big Data, Analytics, and the Future of Marketing & Sales", Available from: www.mckinsey.com.

[73] OECD (2015), 'Data-Driven Innovation: big data for growth and well-being', http://dx.doi.org/10.1787/9789264229358-en accesat la data de 01.07.2019/

şi plasare a anunțurilor pe suporturi digitale, folosind procese algoritmice pentru a găsi şi viza un client oriunde merge[74].

Potrivit raportului publicat de către Forrester[75], *publicitate programatică* va atrage majoritatea cheltuielilor de publicitate digitală în următorii câțiva ani. Procesul implică „licitații" în timp real care apar în milisecunde, permițând ofertanților să „afişeze un anunț unui anumit client, într-un anumit context".

În ciuda existenței unor platforme mari de tranzacționare a datelor, datele personale utile agenților de publicitate sunt adesea colectate şi stocate de companii, mai degrabă decât tranzacționate în mod deschis. Aceste „silozuri de date" sunt în mod obişnuit controlate de companii mari *Big data,* cum ar fi Facebook, Microsoft şi IBM, care au avut tendința de a valorifica datele fără să vândă datele în sine, ci, în schimb, comercializându-le prin permiterea accesul indirect şi temporar la date şi la concluziile rezultate din analiza, compilarea sau urmărirea efectuată asupra datelor şi respectiv a persoanelor vizate.

Unele achiziții (preluări) de afaceri sau fuziuni care au avut loc în ultimii ani, se presupune că au fost determinate de valoarea datelor deținute de acele companii care au fost preluate. Cum ar fi achiziționarea de către Microsoft a LinkedIn la sfârşitul anului 2016[76].

Vânzarea şi comercializarea sub toate formele a datelor cu caracter personal este o realitate. Datele personale sunt petrolul erei noastre digitale (new gold).

Legiuitorul American a urmărit să reglementeze această realitate economică. California Consumer Privacy Act[77] (CCPA – iunie 2018), reprezentă Legea Statului California (SAU) privind reglementarea cadru a protecției datelor cu caracter personal, echivalentul GDPR în Europa în virtutea tradiției nord americane, legiuitorul nord American datelor le recunoaşte caracterul pecuniar şi bun de comerț, defineşte persoana vizată, '[consumator](#)[78]' căreia îi recunoaşte în mod expres Dreptul de a se opune *vânzării datelor* sale personale.

Potrivit Cal. Civ. Code § [1798.120](#) *„Un consumator are dreptul, în orice moment, de a se adresa unui comerciant care comercializează date personale ale consumatorului,*

---

[74] J Chester and K Montgomery (2017), „The role of digital marketing in political campaigns", Internet Policy Review, Volume 6, Issue 4.

[75] R Allen (2016), „What is Programmatic Marketing?", disponibil: www.smartinsights.com accesat la data de 01.07.2019.

[76] The Economist (2017), „Data is giving rise to a new economy", disponibil: www.economist.com accesat la data de 01.07.2019.

[77] https://oag.ca.gov/privacy/ccpa accesat la data de 01.07.2019.

[78] Definiție şi termen care în legislația europeană are aplicabilitate doar în materia Concurenței şi Protecției consumatorului. În timp de Protecția datelor s-a născut ca un derivat al dreptului fundamental la viață privată, intimitate, demnitate, a determinat legiuitorul european să urmărească intenționat să se distanțeze de această ramura comercială a dreptului, dorind a plasa în continuarea reglementarea acestor drepturi în zona drepturilor fundamentale nemateriale, în ciuda realităților economice.

*somându-I **să nu vândă** informațiile personale ale consumatorului*[79]*."* Definiția „Vânzării" datelor personale este definită de în CCPA *„vânzarea, punerea la dispoziție, comunicarea, difuzarea, diseminarea, transferarea sau comunicarea orală, în scris, sau prin mijloace electronice sau prin alte mijloace, a informațiilor personale ale unui consumator unei alte întreprinderi sau unei terțe părți în schimbul **banilor** sau altor **beneficii evaluabile în bani***[80]*."* (Cal. Civ. Code § 1798.140(t)(1).

Legiuitorul nord american, capitalist până în măduva oaselor, nu a avut nicio urmă de ezitare în a legifera dreptul „consumatorului" de a se opune *vânzării* datelor sale, recunoscând evident caracterul economic al acestora („monetary or other valuable consideration" – Cal. Civ. Code § 1798.140(t)(1)). Fără îndoială, inima şi sufletul pieței digitale sunt datele personale, bun de comerț deosebit de valoros şi de interes în toate zonele de comerț, industrie şi viață politică, definit în literatura de specialitate ca fiind 'noul petrol' (*new oil*[81]). Tranzacționat, fără hotare.

Oare instituțiile europene, care reglementează piața digitală, elaborând *Strategia Pieței Digitale Comune*, sunt ignorante cu privire la valoarea economică a datelor? De ce GDPR în definiția data datelor personale (art. 4 pct. 1 GDPR) omite caracterul economic şi evaluabil în bani al acestora? De ce GDPR omite să indice cine este proprietarul datelor, cel care poate dispune economic de acestea şi singurul care poate autoriza vânzarea? De ce GDPR, aparent atât de generos şi doritor să „extindă" şi protejeze drepturile persoanei, nu reglementează expres dreptul persoanei de a se opune şi de a bloca (a priori) vânzarea datelor sale personale?

Sunt aceste scăpări nevinovate sau omisiuni intenționate?

Răspunsul îl putem găsi inclusiv în documentele de lucru ale instituțiilor europene, schimbul de opinii şi negocieri purtate de-a lungul dezbaterilor legislative privind DSM2010 şi GDPR.

Față de propunerea *Directivei privind anumite aspecte referitoare la contractele de furnizare de conținut digital* AEPD (EDPS) a emis avizul său prin Opinia nr. 4/2017 emisă către Comisia Europeană prin care AEPD a criticat sintagmele care recunosc datele personale ca monedă de plată pentru servicii digitale, recunoscându-le explicit valoarea pecuniar-economică.

Prin Opinia nr. 4/2017 către Autoritatea Europeană de Protecție a Datelor (EDPS) critică vehement în pct.9-10 Capitolul 2 (pana la pct. 34) exprimarea de „plata prin *contraprestație cu datele personale*", solicitând înlocuirea cu alt text, care

---

[79] Textul original: „A *consumer shall have the right, **at any time**, to direct a business that sells personal information about the consumer to third parties **not to sell** the consumer's personal information"*.

[80] Textul original *„selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information to another business or a third party for monetary or other valuable consideration"*.

[81] https://www.forbes.com/sites/bernardmarr/2018/03/05/heres-why-data-is-not-the-new-oil/#15afa8903aa9, accesat la data de 01.07.2019.

nu schimbă natura tranzacției, dar evită sintagma deranjantă. Iată şi argumentele EDPS, pct. 11 ad seq. din Opinia nr.4/2017:

Directiva propusă se aplică "oricărui contract în care furnizorul furnizează servicii digitale conținutul pentru consumator sau se angajează să facă acest lucru *„în schimbul unui preț, dar şi atunci când „consumatorul oferă în mod activ* ***în contra-prestație****, altfel decât banii,* ***sub formă de date cu caracter personal*** *sau orice alte date*".

Domeniul de aplicare al directivei este definit astfel încât să asigure că acele contracte care sunt aparent „gratuite" să poată beneficia, de asemenea, de anumită protecție a directivei propuse. Servicii în general considerate „gratuite", se bazează în general pe un model economic în care primesc în contraprestație date cu caracter personal, colectate de furnizori pentru a crea valoare (comercială) din datele procesate (s.n.).

AEPD recunoaşte importanța economiei digitale în Uniune şi valoarea datelor în mediul digital[82]. Prin urmare, AEPD salută inițiativele Comisiei cu privire la utilizarea datelor (personale şi non-personale) şi pentru a favoriza economia bazată pe date (s.n.). Noul cadru de protecție a datelor, care va fi aplicabil începând cu data de 25 Mai 2018, a fost reproiectat pentru a aborda oportunitățile şi provocările UE utilizarea datelor într-un astfel de context. În acest context, misiunea AEPD este să ajute legiuitorul abordează reglementarea acestei piețe, luând în considerare implicațiile pentru indivizilor în ceea ce priveşte dreptul lor fundamental la protecția datelor cu caracter personal.

AEPD salută intenția legiuitorului de a se asigura că şi în cazul aşa-numitor „servicii gratuite" consumatorului să i se asigure aceleiaşi protecție, precum cea din cazul serviciilor pentru care se plăteşte un preț pentru un serviciu (în bani – s.n.). Cu toate acestea, datele personale nu pot fi comparate cu un preț sau cu bani. Informațiile personale sunt legate de un drept fundamental şi nu pot fi considerate ca fiind o marfă.

Pornind de la această ipoteză, următoarele secțiuni prezintă motivele pentru care AEPD recomandă *evitarea utilizării noțiunii de date plătite în contra-prestație* (s.n.). şi prezintă opțiuni alternative pentru a înlocui utilizarea unei astfel de noțiuni (s.n.)".

Ca urmare a acestor critici şi solicitării de înlocuire a termenului de „contra-prestație", versiunea amendată pusă în dezbatere în Parlamentul European în martie 2019 maschează acest termen prin descrierea tranzacțiilor, dar evită cuvântul scandalos.

Din analiza acestor acte şi documente de lucru inter-instituționale, observăm că aceste aspecte spinoase privind recunoaşterea datelor personale caracterul

[82] A se vedea şi Comunicatul Comisiei către Parlamentul European, Consiliu, Comitetului Economic European al Regiunilor, „*Towards a thriving data-driven economy*", COM (2014) 442 final.

evaluabil în bani, marfă de schimb au făcut obiectul unor *dezbateri intense*. Regulamentul GDPR intenționat evită să reglementeze caracterul evaluabil în bani al datelor personale, deşi reglementează tranzacționarea datelor personale pe piața digitală.

Ca o consecință, GDPR *intenționat nu a reglementat* dreptul persoanei de a se *opune vânzării datelor sale personale*. GDPR nu a omis o astfel de reglementare, pe care legiuitorul Californian a recunoscut-o prin CCPA. Căci a recunoaşte dreptul de a se opune vânzării datelor, implicit ar fi reprezentat recunoaşterea ca datele sunt marfa. Ce ceea ar fi scandalizat cetățeanul european, al cărui drept la intimitate şi date personale este reglementat prin Carta Europeană a Drepturilor Fundamentale (art. 8) ca drept şi libertate fundamentală (neevaluabile în bani), alături de dreptul la viață, la demnitate umană, viață de familie etc.

Sistemul instituțional European lasă sub tăcere recunoaşterea valorii economice a datelor, disimulând prin tehnici de redactare legislativă realitatea, îmbrăcând noțiunile în fraze semantice echivalente şi redactare obscură. Sunt de asemenea lăsate cu intenție nereglementate aspecte esențiale şi de bază precum proprietatea asupra datelor personale, dreptul exclusiv de a dispune cu privire la date, dreptul persoanei de a interzice vânzarea datelor. Realitatea economică a pieței datelor s-a impus de mai bine de două decenii, fiind azi într-o accesiune fără precedent şi a dus în desuetudine intimitatea persoanei. Datele persoanele, identitatea cu urmărirea emoțiilor şi trăirilor sunt valori comerciale într-o societate a pieței digitale.

Dacă intimitatea şi astfel şi demnitatea devin valori vandabile, mai) trăim într-un sistem democratic autentic?

Urmare acestei evocări fugitive a considerentelor, revine şi persistă incomoda şi retorica întrebare *Cui prodest*?

"Can't you see? It all makes perfect sense
Expressed in dollars and cents
Pounds, shillings and pence
Can't you see? It all makes perfect sense"[83]

XI. Concluzii şi perspective

Articolul nu se doreşte un epitaf, ci un apel de conştientizare a realității. Demnitatea, intimitatea ca şi democrația nu sunt un *dat*, pentru eternitate. Ci sunt valori foarte fragile, care nu se câştigă odată pentru totdeauna şi se îmbracă în

[83] Versuri ale lui Roger Water cântecul „Perfect sense" https://www.youtube.com/watch?v=SUGwHOAdwBw.

forme reci[84] pentru păstrare spre veşnicie, în sălile universităților sau palatele parlamentelor, în statui înalte şi reci. Nu este suficientă o recunoaştere într-o Cartă sau constituție.

Ele trebuie zi de zi exercitate, trăite şi mai ales protejate şi prin solidaritate activă de abuzuri instituționale, de lăcomia mediului economic-financiar-bancar. Altfel, aceste valori devin scripte formale şi desuete, depărtându-se de realitate. Democrația este cea mai fragilă dintre flori[85]. Nu doar că uităm, dar uităm mult prea repede, prețul plătit de generațiile anterioare ale acestui continent cu istorie tumultoasă. Într-o Europă, leagăn al democrației cu fundație creştină, obligația esențială pe care o are fiecare generație este să se responsabilizeze cu privire la păstrarea acestor valori, spre a le transmite.

[84] Cu deosebită frumusețe spus de către Costache Ioanid în poezia creştină „Nu-i Iuda singur vinovat" https://www.youtube.com/watch?v=qw4iwVU9jAg , https://www.resursecrestine.ro/poezii/31904/nu-i-singur-iuda-vinovat accesat la data de 01.07.2019.

[85] https://journals.sagepub.com/doi/abs/10.1177/0032329202030001003, https://www.independent.ie/opinion/editorial/democracy-is-a-fragile-flower-26898688.html accesat la data de 01.07.2019.