

DREPTUL LA UITARE DIGITALĂ – UNUL DIN DREPTURILE FUNDAMENTALE ALE UTILIZATORILOR DE INTERNET

THE RIGHT TO BE FORGOTTEN – ONE OF THE FUNDAMENTAL RIGHTS OF INTERNET USERS

[https://doi.org/10.52327/1813-8489.2021.4\(112\).04](https://doi.org/10.52327/1813-8489.2021.4(112).04)

CZU: 342.738:004.738.5

Andrei SMOCHINĂ,
doctor habilitat în științe juridice, profesor universitar,
Academia de Administrare Publică

Alexandru ȚĂRNĂ,
doctorand,
Universitatea de Stat din Moldova

SUMMARY

Information technology changed the way we relate to information as any data posted on the Internet can remain accessible indefinitely. This ease of access undoubtedly favored the freedom of information, but the fundamental right to privacy of natural persons seems to be under threat in the absence of adequate legal mechanisms.

Since recently the Court of Justice of the European Union („CJEU”) ruled in two cases (C-136/17 and C-507/17) on a series of questions concerning the implementation of the right to de-referencing (digital right to be forgotten) and its territorial scope, this paper analyses the impact of those two judgments on the effectiveness of the right to be forgotten.

On the one hand, we are witnessing its strengthening, especially as a result of the clarification that, in principle, the operator of a search engine is required to admit a request for de-referencing where the information relates to an earlier stage of a legal proceeding and no longer corresponds to the current situation. On the other hand, we find a limitation of its effectiveness, since, by default, the links removal by the operator of the search engine will only be done on the versions of that search engine corresponding to all member states. However, we must not forget that CJEU emphasized that, in the light of national standards of protection of fundamental rights, a supervisory or judicial authority of a member state remains competent to order, where appropriate, the operator of that search engine to carry out a de-referencing concerning all its versions.

Keywords: *personal data, sensitive data, freedom of expression and information, right to be forgotten, right to de-referencing, right to be delisted, right to de-indexing.*

REZUMAT

Tehnologia informației a schimbat modul în care ne raportăm la informații, întrucât orice date postate în internet pot rămâne accesibile pe o perioadă nedeterminată. Fără îndoială, această ușurință de acces a favorizat libertatea de informare, însă dreptul fundamental la viața privată al persoanelor fizice pare să fie amenințat.

Cum de curând Curtea de Justiție a Uniunii Europene („CJUE”) s-a pronunțat în două cauze (C-136/17 și C-507/17) asupra unor aspecte privind punerea în aplicare a dreptului la înlăturare (dreptul la uitare digitală) și domeniul său de aplicare teritorială, acest articol își propune să analizeze impactul celor două hotărâri asupra efectivității dreptului de a fi uitat.

Pe de o parte, asistăm la o consolidare a acestuia, în special ca urmare a clarificării faptului că, în principiu, operatorul unui motor de căutare este obligat să admită o cerere de înlăturare atunci când aceste informații se referă la o etapă anterioară a unei proceduri judiciare și care nu mai corespund situației actuale. Pe de altă parte, constatăm o limitare a efectivității sale, de vreme ce, în mod implicit, înlăturarea linkurilor urmează a se face de către operatorul motorului de căutare numai în versiunile acestuia care corespund ansamblului statelor membre. Totuși nu trebuie să scăpăm din vedere că CJUE a subliniat că, în lumina standardelor naționale pentru protecția drepturilor fundamentale, autoritățile de supraveghere, precum și cele judiciare din statele membre rămân competente, atunci când este cazul, să impună operatorului unui motor de căutare să procedeze la o înlăturare privind ansamblul versiunilor sale.

Cuvinte-cheie: *date cu caracter personal, date sensibile, libertatea de exprimare și de informare, dreptul de a fi uitat, dreptul la înlăturare, dreptul la delistare, dreptul la dezindexare.*

Preliminarii. Marea majoritate a informațiilor și datelor personale care circulă în mod constant pe web au făcut ca identitatea digitală să se afle mai puțin sub controlul nostru, dar în același timp să aibă repercusiuni semnificative în viața reală de zi cu zi.

Utilizarea constantă a aplicațiilor și a obiectelor conectate la o rețea de calculatoare afectează în mod iremediabil comportamentul oamenilor, care împărtășesc cu ușurință informații personale, fără să se gândească la consecințe și la înlăturarea lor dificilă din lumea virtuală: de fapt odată încărcat, un fișier de pe web

devine aproape imposibil de eliminat complet.

Pentru a proteja drepturile legate de difuzarea necorespunzătoare a acestor date în rețele de calculatoare și pentru a asigura intimitatea fiecărui cetățean a luat naștere așa-numitul „drept la uitare” și anume dreptul unei persoane de a fi uitat și de a nu-i fi aduse aminte fapte care îl privesc. În practică, acest drept este ca o garanție pentru cei care nu doresc să fie expuși pe termen nelimitat la consecințe dăunătoare, care le pot afecta negativ reputația, pentru evenimente care au avut loc în trecut (în special într-o eră digitală ca a noas-

tră, în care cele mai multe informații circulă on-line).

Dreptul de a fi uitat, sau altfel spus, dreptul la ștergerea datelor cu caracter personal reprezintă unul dintre elementele care compun genul proximal al drepturilor privind protecția datelor cu caracter personal, cuprinse în art. 15-22 din Regulamentul (UE) nr. 2016/679 General Data Protection Regulation (GDPR) [24], sau în traducere din engleză – Regulamentul General de Protecție a Datelor (RGPD), dar și în TFUE (art. 16, alin. 1) sau în Carta drepturilor fundamentale a UE (art. 8, alin. 1). Astfel, având în vedere importanța deosebită a dreptului de a fi uitat ca drept la protecția datelor cu caracter personal, ne propunem să investigăm în esența acestui drept.

Importanța cunoașterii dificultăților în asigurarea dreptului omului la la ștergerea datelor cu caracter personal. Din start vom aduce o claritate în terminologia utilizată în legislație și doctrină. Astfel, pot fi întâlnite expresiile: „Dreptul de a fi uitat”, „Dreptul la ștergerea datelor cu caracter personal”, „Dreptul la înlăturare”, „Dreptul la delistare”, „Dreptul la dezindexarea web”. Cu o singură precizare că, spre deosebire de delistarea din lista de rezultate afișată atunci când se utilizează drept cuvânt-cheie numele persoanei vizate, dezindexarea constă în ștergerea linkurilor către paginile web ale terților din însăși baza de date indexate a motorului de căutare, linkurile respective nemaifiind afișate în lista de rezultate indiferent de cuvintele-cheie utilizate.

După cum era și de așteptat, toate aceste noțiuni și termeni derivă de

la sintagma utilizată în limba engleză: „the right to be forgotten”.

În doctrină, cu precădere în cea anglosaxonă, dreptul de a fi uitat, este considerat unul din elementele constitutive și fundamentale al exercitării controlului asupra datelor personale de către o persoană [30, p.24]. În esență, acesta reprezintă unul din drepturile pozitive cu referire la protecția datelor cu caracter personal.

Dreptul de a fi uitat, fiind la etapa incipientă de dezvoltare, de consacrare, și-a găsit o reglementare în special în statele dezvoltate, atât la nivel național, cât și pe dimensiunea actelor internaționale, cu precădere în Uniunea Europeană. Totodată, se constată că anume practica judiciară a fost cea care a clarificat modul practic de realizare a dreptului la uitare [8].

Există opinia, conform căreia dreptul la uitare își are originile în ordinele latinoamericane habeas data, prin intermediul cărora persoana obținea dreptul de a solicita accesul la fișierele ce conțineau informații despre ea sau corectarea unor date incorecte [14, p. 2].

Astfel, în general, dreptul de a fi uitat nu conține nimic fundamental nou din punct de vedere juridic. În epoca digitală, importanța acestui drept sporește, pe măsură ce oamenii câștigă noi oportunități aproape nelimitate de diseminare a informațiilor personale confidențiale despre ei și despre ceilalți și adesea fac acest lucru fără să-și dea seama de consecințele, adesea nefaste [25]. Dreptul de a fi uitat permite corectarea consecințelor negative de activitate excesivă pe Internet. În același timp, exercitarea acestui drept

în legătură cu informațiile postate online dă naștere la o serie de probleme datorită naturii tehnice a internetului, care complică implementarea acestuia și necesită o soluție legală.

O problemă gravă este legată de faptul că, din punct de vedere tehnic, informațiile care odată plasate pe Internet nu pot fi șterse complet și definitiv, „informațiile de pe Internet sunt continuu copiate, multiplicare și, prin urmare, devin practic indestructibile” [31, p. 73]. „Internetul înregistrează totul și nu uită nimic” [30, p. 31]. Această problemă este rezolvată prin eliminarea localizatorului de resurse uniform (URL) din indexul motorului de căutare (altfel zis, dezintexare – nota noastră), după care informațiile devin invizibile pentru utilizatorii terți atunci când efectuează o căutare după numele persoanei, dar datele originale rămân disponibile în sursa originală [15]. Informațiile „șterse” sunt stocate pe site-urile corespunzătoare, în documente oficiale, în arhive online, dar le puteți găsi doar din pură întâmplare sau dacă căutați intenționat și știți unde să căutați.

În același timp, doctrinarii identifică originile acestei abordări în prevederile legislației franceze și elvețiene, care oferea unei persoane reabilitate sau unei persoane a cărei antecedente penale au fost stinse, posibilitatea de a obiecta la dezvăluirea faptului condamnării sale. Se prezumă că stigma condamnării nu ar trebui să fie aplicată pentru tot restul vieții. Prin urmare, atât societatea, cât și de fapt, în interes public, nu ar trebui să existe un acces la informații despre circumstanțele comiterii infracțiunii și condamnarea unei

persoane pe o perioadă nedeterminată [30, p. 24].

În dezvoltarea acestei idei, Curtea Constituțională Federală a Germaniei consideră că diseminarea informațiilor care și-au pierdut relevanța cu privire la infracțiunea comisă de o persoană (speța în discuție se referă la difuzarea unui film documentar pe posturile de televiziune) încalcă dreptul unei persoane la dezvoltare, deoarece împiedică reintegrarea sa socială, iar acest drept în contextul dat a fost recunoscut de Curte ca fiind mai semnificativ și prioritar decât libertatea presei [6].

În esență dreptul de a fi uitat este un fel de răspuns legal „la provocarea din partea tehnologiilor digitale” [31, p. 84]. Per ansamblu, „dreptul de a fi uitat” sau „dreptul de a fi șters” este mai degrabă o metaforă frumoasă; în realitate totul se reduce la dreptul de a cere ca accesul la informațiile postate pe internet să fie mai dificil din punct de vedere tehnic și, prin urmare, informațiile relevante să fie mai puțin publice. Dar, probabil, în legătură cu dezvoltarea tehnologiilor de căutare și „autoinstruirea avansată” a „utilizatorului mediu”, dreptul de a fi uitat „va fi uitat în curând” [15].

Este evident că nu împărtășim acest ultim deziderat, pe care îl catalogăm drept unul fie optimist, fie prea pesimist. În realitate, dreptul de a fi uitat este la început de cale în ceea ce privește consacarea și apărarea sa. În acest sens, Republica Moldova ar urma să analizeze cu maximă atenție realitățile din Uniunea Europeană în domeniul protecției datelor cu caracter personal.

La nivelul Uniunii Europene, dreptul de a fi uitat este consacrat în prevede-

rile art. 17 din Regulamentul (UE) nr. 2016/679 și, potrivit doctrinei, își are izvorul în jurisprudența Curții de Justiție a Uniunii Europene (CJUE) [28, nota nr. 21; 26, nota nr. 21], mai exact în cauza Google Spain și Google [7, pp. 18-20]. Din textul art. 17, alin. (1) din RGPD rezultă următoarea definiție: dreptul de a fi uitat este dreptul potestativ pe temeiul căruia persoana vizată obligă operatorul la ștergerea, fără întârzieri nejustificate, a datelor cu caracter personal care o privesc, în condițiile și limitele art. 17 din RGPD.

Acest drept implică obligația corelativă a operatorului de a șterge datele cu caracter personal fără întârzieri nejustificate în cazul în care își găsesc aplicabilitate motivele enumerate limitativ de art. 17, alin. (1), lit. a-f din RGPD. Totodată, în strânsă legătură cu dreptul la ștergerea datelor, dar fără a intra în sfera obligației corelative a acestuia, în sarcina operatorului există și obligația de notificare consacrată în cuprinsul art. 19 din RGPD.

Subiectul dreptului de a fi uitat îl constituie persoana vizată. Respectiv „persoana fizică sau juridică căreia îi aparține dreptul subiectiv”. Această noțiune vizează persoana fizică identificată sau identificabilă a cărei date personale sunt supuse colectării, potrivit art. 4, pct. 1. din RGPD. Desigur, conform art. 1, alin. (1) din RGPD, prevederile regulamentului protejează exclusiv persoanele fizice, deci, pe cale de consecință, persoanele juridice nu pot fi titularii a dreptului de a fi uitat.

Subiectul pasiv al dreptului de a fi uitat, respectiv titularul obligației corelative dreptului, îl constituie operato-

rul, respectiv „persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal” [24, art. 4 pc. 7].

În doctrină s-a apreciat faptul că dreptul la protecția datelor cu caracter personal, implicit și dreptul de a fi uitat nu se confunda cu dreptul la viață privată, chiar dacă nu de puține ori domeniul lor de incidență se intersectează. Savanții C. Munteanu și O. Ungureanu invocă decizia Tribunalului de primă instanță al CJUE din cauza Bavarian Lager, în care s-a reținut faptul că „nu toate datele cu caracter personal pot, prin natura lor, să aducă atingere vieții private a persoanei vizate” [22, nota nr. 11 și 12]. Credem că adoptarea RGPD tranșează problema autonomiei acestei categorii de drepturi în raport cu dreptul la viață privată, dată fiind consacrarea legislativă expresă a acestora în mod separat, cu stabilirea unor limite și condiții specifice în privința exercitării acestuia. În plus, dreptul la ștergerea datelor protejează adesea și informații cu caracter public, mai ales în contextul dezvoltării accelerate a platformelor de socializare în ultimul deceniu [28, nota nr. 7].

Totodată, dreptul de a fi uitat, asemenea celorlalte drepturi care vizează protecția datelor cu caracter personal, își are izvorul în dreptul la viață privată, dar evoluția tehnologică a domeniului informatic a determinat necesitatea conferirii autonomiei juridice acestui drept, în vederea sporirii standardului de protecție al integrității datelor personale [22, nota nr. 15].

Sub aspect material, art. 17, alin. (1), lit. a-f din RGPD instituie șase temeuri alternative pe care se fundamentează exercitarea dreptului de a fi uitat [23, par. 27]:

(1) scopul procesării a fost deja atins și datele nu mai sunt necesare;

(2) consimțământul a fost retras și nu există alt temei legal pentru procesare;

(3) persoana vizată obiectează conform art. 21, alin. (1) RGPD;

(4) datele au fost procesate ilegal;

(5) ștergerea este necesară pentru executarea unei obligații legale conform dreptului Uniunii sau dreptului național;

(6) procesarea s-a efectuat în baza consimțământului minorului în contextul ofertei de servicii informaționale

1. Scopul procesării a fost deja atins și datele nu mai sunt necesare. În conformitate cu prevederile art. 17, alin. (1), lit. a) din RGPD, ștergerea datelor cu caracter personal poate fi obținută atunci când datele nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate. Potrivit principiului reducerii la minimum a datelor, datele trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate. Astfel, dacă datele nu mai sunt necesare pentru îndeplinirea scopurilor prelucrării, această operațiune nu mai are un temei legitim. Această regulă subliniază importanța stabilirii în mod neechivoc a unui scop al fiecărei prelucrări de date cu caracter personal în parte, scop ce trebuie cunoscut de persoana vizată, astfel încât aceasta să-și poată exer-

cita, de exemplu, dreptul la ștergerea respectivelor date.

2. Consimțământul a fost retras și nu există alt temei legal pentru procesare. În conformitate cu prevederile art. 17, alin. (1), lit. b) din RGPD, ștergerea datelor cu caracter personal poate fi obținută atunci când persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea și nu există niciun alt temei juridic pentru prelucrare. Retragerea consimțământului va lipsi prelucrarea de temeiul juridic necesar, astfel că, de vreme ce datele trebuie prelucrate în mod legal, dacă nu mai există niciun alt temei juridic pentru a continua prelucrarea, operatorul va trebui să dea curs cererii de ștergere a datelor.

Retragerea consimțământului, reprezintă cel mai larg temei pentru exercitarea acestui drept [5, pct.5], nefiind necesar ca persoana vizată să invoce un motiv sau un interes pentru a-și retrage în mod efectiv consimțământul. Sub acest aspect, consimțământul persoanei vizate are un caracter nedefinit, fundamentat pe dreptul discreționar al persoanei vizate de a-și retrage acceptul dat pentru prelucrarea datelor cu caracter personal [5, nota nr.66], deci, odată îndeplinite condițiile materiale, acest drept poate fi exercitat unilateral și neîngrădit. Astfel, exercitarea dreptului pe acest temei relevă în mod univoc caracterul potestativ al acestui drept, necesar în vederea garantării efective a integrității datelor persoanei vizate.

Totodată, în lumina reglementărilor din art. 7, alin. (3) din RGPD, retragerea consimțământului nu afectează legalitatea prelucrării efectuate

pe baza consimțământului înainte de retragerea acestuia. În urma retragerii consimțământului operatorul va putea să continue prelucrarea datelor cu caracter personal spre exemplu în temeiul intereselor sale legitime, adică în baza art. 6, alin. (1), lit. f) din RGPD, caz în care persoana vizată nu va putea obține ștergerea datelor decât în condițiile exercitării dreptului la opoziție prevăzut de art. 21 din RGPD.

3. Persoana vizată obiectează conform art. 21, alin. (1) RGPD. În conformitate cu prevederile art. 17, alin. (1), lit. c) din RGPD, ștergerea datelor cu caracter personal poate fi obținută atunci când persoana vizată și-a exercitat cu succes dreptul la opoziție în temeiul art.21 din RGPD. De vreme ce dreptul de opoziție cu privire la prelucrare nu pare a avea ca efect direct obligația operatorului de a șterge datele, prevederile privind dreptul la ștergerea datelor pot fi interpretate în sensul în care se impune formularea unei cereri exprese privind ștergerea datelor, alături de exprimarea opoziției, cel puțin în situația în care aceasta din urmă nu privește prelucrarea în scop de marketing direct.

4. Datele au fost procesate ilegal. În conformitate cu prevederile art. 17, alin. (1), lit. d) din RGPD, ștergerea datelor cu caracter personal poate fi obținută atunci când datele cu caracter personal au fost prelucrate în mod ilegal. Orice prelucrare a datelor cu caracter personal trebuie, pe de o parte, să fie conformă cu principiile legate de prelucrarea datelor cu caracter personal, enunțate în cadrul art.5 din RGPD, și, pe de altă parte, să respecte unul

dintre criteriile privind legitimitatea prelucrării datelor, enumerate la art.6 din RGPD. Prin urmare, orice prelucrare care nu este conformă acestor prevederi va fi considerată nelegală și va da naștere dreptului de a obține ștergerea datelor respective. Sarcina probei privind justificarea prelucrării datelor revine operatorului de date deoarece acesta este responsabil de legitimitatea prelucrării datelor. În conformitate cu principiul responsabilității, operatorul trebuie, în orice moment, să poată demonstra că există un temei juridic solid pentru prelucrarea datelor, iar în caz contrar procesul trebuie întrerupt.

5. Ștergerea este necesară pentru executarea unei obligații legale conform dreptului Uniunii sau dreptului național. În conformitate cu prevederile art. 17, alin. (1), lit. e) din RGPD, datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se află operatorul. În acest caz dreptul de a obține ștergerea datelor invocat de persoana vizată trebuie să fie prevăzut de alte dispoziții ale dreptului UE sau ale dreptului intern.

6. Procesarea s-a efectuat în baza consimțământului minorului în contextul ofertei de servicii informaționale. În conformitate cu prevederile art. 17, alin. (1), lit. f) din RGPD, ștergerea datelor cu caracter personal poate fi obținută atunci când datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale menționate la art. 8, alin.(1) din RGPD. Potrivit art.

1, alin. (1), lit. b) din Directiva (UE) 2015/1535, prin aceste servicii ale societății informaționale înțelegem orice serviciu prestat în mod normal în schimbul unei remunerații, la distanță, prin mijloace electronice și la solicitarea individuală a beneficiarului serviciului.

Situația în care operatorul a făcut publice datele cu caracter personal, este prevăzută de art. 17, alin. (2) din RGPD și de jurisprudența CJUE, respectiv cauza Google Spain și Google [10, nota nr. 3], în care Curtea a reținut că, în anumite condiții, „operatorul unui motor de căutare este obligat să elimine de pe lista de rezultate, afișată în urma unei căutări efectuate plecând de la numele unei persoane, linkurile către paginile web publicate de terți și care conțin informații referitoare la această persoană” [7, pct.3 din partea dispozitivă a hotărârii].

Pe de altă parte, art. 17, alin. (3), lit. a-e din RGPD reglementează cinci situații derogatorii, a căror incidență are ca efect blocarea exercitării dreptului de a fi uitat. Scopul acestor derogări îl constituie asigurarea echilibrului între dreptul la ștergerea datelor și unele drepturi subiective sau interese legitime ale operatorului ori ale societății. Textul legal stabilește în terminis și limitativ care sunt aceste drepturi sau interese preeminente în raport cu dreptul de a fi uitat: dreptul la liberă exprimare și la informare; respectarea unei anumite obligații legale în sarcina operatorului; interesul public în domeniul sănătății publice; arhivare în interes public, cercetare, ori scopuri statistice; ori pentru constatarea, exercitarea

sau apărarea unui drept în instanță.

Potrivit art. 51 din RGPD, în fiecare stat membru UE se înființează o autoritate independentă de supraveghere a prelucrării datelor. Spre exemplu, în România – stat membru, a fost înființată Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), care reprezintă o autoritate publică, autonomă și independentă a cărei obiectiv este apărarea drepturilor și libertăților fundamentale ale persoanelor fizice, în special a dreptului la viață intimă, familială și privată, în legătură cu prelucrarea datelor cu caracter personal și cu libera circulație a acestor date, conform art. 1, alin. (1) și (2) din Legea nr. 102/2005 privind înființarea, organizarea și funcționarea ANSPDCP.

Cu referire la cauza Google Spain și Google [7, pp. 18-20], este lesne să menționăm că respectiva cauză privește un cetățean spaniol care dorește ca un articol din ziarul spaniol La Vanguardia Ediciones să fie șters, sau, dacă acest lucru nu este posibil, atunci solicită ca articolul să nu mai apară pe lista rezultatelor de căutare a Google [7]. Acesta susține că informația pe care o dorește ștersă se referă la o datorie veche, pe care a plătit-o demult. Solicitățile sale au fost respinse și de publicație și de Google Spania, care a argumentat că cererea trebuie înaintată sediului principal al Google din SUA. Drept urmare, cetățeanul a depus o plângere la autoritatea spaniolă de supraveghere a datelor personale, care a respins solicitarea cu privire la ștergerea informațiilor de către publicație, dar a emis, în schimb, un ordin adresat Google Spa-

nia „pentru a lua toți pașii necesari în retragerea datelor vizate din indexările sale și să facă imposibil accesul la aceste date în viitor” [2].

Deși cadrul legal actual pentru garantarea dreptului la ștergere a fost considerat „inadecvat” în doctrina din acea perioadă (anii 2012-2013) [3, p. 145], această cauză arată că prevederile directivei protecției datelor pot fi interpretate fără o dificultate ridicată în sensul existenței deja a unui drept de a fi uitat, care are însă o structură fragmentară și care are nevoie de o interpretare dinamică pentru a fi aplicat eficient. O asemenea interpretare a fost făcută deja de către autoritatea spaniolă de supraveghere a protecției datelor, și a convins o curte supremă a unui stat membru UE să ridice întrebări detaliate și clare în fața CJUE în problema motoarelor de căutare ca facilitatori ai uitării informațiilor. Cu toate acestea, a devenit clar că Uniunea Europeană nu conține un drept general și explicit de a fi uitat [1, p.7] și drept urmare, ar trebui să adopte un cadru legal de consfințire a dreptului de a fi uitat, fapt care s-a și produs peste cinci ani.

Într-un final, Curtea de Justiție a Uniunii Europene a publicat în mai 2014 o hotărâre defavorabilă Google, consecința fiind că utilizatorii pot cere motoarelor de căutare - în anumite condiții - să șteargă informații care încalcă dreptul la viața privată și dreptul la protecția datelor cu caracter personal.

După cum este și firesc, Decizia CJUE din 2014, prescurtată în presa internațională sub exprimarea „right to be forgotten” (dreptul la uitare) a stârnit multe controverse între cei care

susțin libertatea de exprimare și cei care susțin dreptul la viață privată.

Practica judiciară a fost cea care a dezvoltat conceptul de drept la uitare și i-a fixat anumite limite, atunci când este vorba de aplicarea sa.

În esență, Curtea de Justiție a Uniunii Europene nu a consacrat pe cale jurisprudențială uitarea în sine, ci un drept a cărui exercitare creează premisele uitării naturale, fenomen inerent oricărei ființe umane, însă căruia tehnologia i se opune. Practic, s-a impus motoarelor de căutare obligația de a șterge legătura care unește anumite date de numele persoanei vizate, legătură ce decurge din modul de funcționare al motorului de căutare și datorită căreia, în lista de rezultate afișată în urma unei căutări efectuate plecând de la numele acelei persoane, figurează linkuri către paginile web publicate de terți, pagini web ce conțin informații referitoare la această persoană [27, p. 63].

Unul din cele mai relevante exemple în acest sens este Hotărârea Curții de Justiție a Uniunii Europene (Marea Cameră) C-507/17 din 24 septembrie 2019 „Trimitere preliminară – Date cu caracter personal – Protecția persoanelor fizice în ceea ce privește prelucrarea acestor date – Directiva 95/46/CE – Regulamentul (UE) 2016/679 – Motoare de căutare pe internet – Prelucrarea datelor care figurează pe pagini web – Întinderea teritorială a dreptului la dezindexare”, cauza Google LLC împotriva Commission nationale de l’informatique et des libertés (CNIL – Consiliul Național de Informații și Libertăți, Franța) și Conseil d’État (Consiliul de Stat, Franța) [16].

Fondul problemei relevă faptul că printr-o decizie din 21 mai 2015, președinta CNIL a pus în întârziere Google ca, atunci când admite cererea unei persoane fizice având ca obiect eliminarea din lista de rezultate, afișată în urma unei căutări efectuate plecând de la numele său, a unor linkuri care duc spre pagini web, să aplice această eliminare în privința tuturor extensiilor numelui de domeniu al motorului său de căutare.

Google a refuzat să se conformeze acestei puneri în întârziere, limitându-se la eliminarea linkurilor în cauză doar din rezultatele afișate ca răspuns la căutări efectuate, plecând de la numele de domeniu care corespund declinărilor motorului său de căutare în statele membre [16, pct. 31].

Pe de altă parte, CNIL a considerat insuficientă propunerea complementară denumită de „geoblocare” făcută de Google după expirarea termenului punerii în întârziere, constând în eliminarea posibilității de acces, de la o adresă IP (Internet Protocol) considerată a fi localizată în statul de reședință al persoanei vizate, la rezultatele în litigiu în urma unei căutări efectuate, plecând de la numele acesteia, indiferent de declinarea motorului de căutare solicitată de utilizatorul de internet [16, pct. 32].

După ce a constatat că Google nu s-a conformat punerii în întârziere menționate în termenul acordat, CNIL, printr-o deliberare din data de 10 martie 2016, a aplicat acestei societăți o sancțiune de 100 000 de euro, care a fost adusă la cunoștința publicului [16, pct. 33].

Prin cererea formulată în fața Conseil d'État (Consiliul de Stat, Franța),

Google solicită anularea acestei delibere.

În fața Conseil d'État (Consiliul de Stat), Google susține că sancțiunea în litigiu se întemeiază pe o interpretare eronată a dispozițiilor Legii din 6 ianuarie 1978, care transpun articolul 12, litera (b) și articolul 14, primul paragraf, litera (a) din Directiva 95/46, în temeiul cărora Curtea a recunoscut, în Hotărârea din 13 mai 2014, Google Spain și Google (C 131/12, EU:C:2014:317), un „drept la dezindexare”. Google arată că acest drept nu implică în mod necesar eliminarea linkurilor în litigiu, fără limitare geografică, din ansamblul numerelor de domeniu ale motorului său. În plus, reținând o astfel de interpretare, CNIL ar fi încălcat principiile curtoaziei și neamestecului recunoscute de dreptul internațional public și ar fi adus o atingere disproporționată libertății de exprimare, de informare, de comunicare și a presei garantate în special de articolul 11 din cartă [16, pct. 38].

Întrucât a constatat că această argumentație ridică mai multe dificultăți serioase de interpretare a Directivei 95/46, Conseil d'État (Consiliul de Stat) a hotărât să suspende judecarea cauzei și să adreseze Curții de Justiție a Uniunii Europene trei întrebări preliminare de ordin magistral, prin care urmărea să se stabilească dacă normele dreptului Uniunii de protecție a datelor cu caracter personal [9 și 24] trebuie interpretate în sensul că, atunci când operatorul unui motor de căutare admite o cerere de dezindexare, el este obligat să efectueze această dezindexare în ansamblul versiunilor motorului său sau dacă, dimpotrivă, este obligat

să o realizeze doar în versiunile acestuia care corespund ansamblului statelor membre sau chiar numai în versiunea care corespunde statului membru de reședință al beneficiarului dezindexării.

La modul concret, aceste 3 întrebări preliminare abordează următoarele probleme [16, pct. 39]:

1. „Dreptul la dezindexare”, astfel cum a fost consacrat de [Curte] prin Hotărârea din 13 mai 2014 [Google Spain și Google (C 131/12, EU:C:2014:317)] în temeiul dispozițiilor articolului 12, litera (b) și ale articolului 14 [primul paragraf], litera (a) din Directiva [95/46], trebuie interpretat în sensul că operatorul unui motor de căutare are obligația, în cazul în care admite o cerere de dezindexare, să efectueze această dezindexare din toate numele de domeniu ale motorului său de căutare, astfel încât linkurile în litigiu să nu mai fie afișate indiferent de locul de unde este lansată căutarea privind numele solicitantului, inclusiv atunci când acest loc se află în afara domeniului de aplicare teritorial al Directivei [95/46]?

2. În cazul unui răspuns negativ la această primă întrebare, „dreptul la dezindexare”, astfel cum a fost consacrat de [Curte] prin hotărârea citată anterior, trebuie interpretat în sensul că operatorul unui motor de căutare are obligația, în cazul în care admite o cerere de dezindexare, să elimine linkurile în litigiu din lista rezultatelor afișate în urma unei căutări efectuate, plecând de la numele solicitantului doar din numele de domeniu corespunzător statului în care se consideră că s-a efectuat căutarea sau, în sens mai general, din numele de domeniu ale motorului de

căutare corespunzătoare extensiilor naționale ale acestui motor în toate statele membre [...]?

3. În plus, pe lângă obligația menționată [în cea de-a doua întrebare], „dreptul la dezindexare”, astfel cum a fost consacrat de [Curte] prin hotărârea citată anterior, trebuie interpretat în sensul că operatorul unui motor de căutare are obligația, în cazul în care admite o cerere de dezindexare, să elimine prin tehnica denumită de „geoblocare”, pornind de la o adresă IP considerată a fi localizată în statul de reședință al beneficiarului „dreptului la dezindexare”, rezultatele în litigiu ale căutărilor efectuate plecând de la numele acestui beneficiar sau chiar, în sens mai general, de la o adresă IP considerată a fi localizată în unul dintre statele membre care intră sub incidența Directivei [95/46], indiferent de numele de domeniu folosit de utilizatorul de internet care efectuează căutarea?

La examinarea fondului cauzei, CJUE a făcut referințe la mai multe prevederi din Regulamentul (UE) 2016/679 General Data Protection Regulation [24], considerate a fi relevante speței. Vom examina minuțios unele dintre ele, considerate a fi de importanță magistrală pentru cercetarea noastră.

Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este un drept fundamental. Articolul 8, alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene („carta”) și articolul 16, alineatul (1) [TFUE] prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc [24, art. 1].

Prelucrarea datelor cu caracter personal ar trebui să fie în serviciul cetățenilor. Dreptul la protecția datelor cu caracter personal nu este un drept absolut; acesta trebuie luat în considerare în raport cu funcția pe care o îndeplinește în societate și echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporționalității. Prezentul regulament respectă toate drepturile fundamentale și libertățile și principiile recunoscute în cartă astfel cum sunt consacrate în tratate, în special respectarea vieții private și de familie, [...] a protecției datelor cu caracter personal, a libertății de gândire, de conștiință și de religie, a libertății de exprimare și de informare, a libertății de a desfășura o activitate comercială, [...] [24, art. 4].

Directiva 95/46 [...] nu a prevenit fragmentarea modului în care protecția datelor este pusă în aplicare în Uniune [...]. Diferențele dintre nivelurile de protecție [...] din statele membre pot împiedica libera circulație a datelor cu caracter personal în întreaga Uniune. Aceste diferențe pot constitui, prin urmare, un obstacol în desfășurarea de activități economice la nivelul Uniunii [...] [24, art. 9].

Pentru a se asigura un nivel consecvent și ridicat de protecție a persoanelor fizice și pentru a se îndepărta obstacolele din calea circulației datelor cu caracter personal în cadrul Uniunii, nivelul protecției drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea unor astfel de date ar trebui să fie echivalent în toate statele membre. [...] [24, art. 10].

Protecția efectivă a datelor cu caracter personal în întreaga Uniune necesită nu numai consolidarea și stabilirea în detaliu a drepturilor persoanelor vizate și a obligațiilor celor care prelucrează și decid prelucrarea datelor cu caracter personal, ci și competențe echivalente pentru monitorizarea și asigurarea conformității cu normele de protecție a datelor cu caracter personal și sancțiuni echivalente pentru infracțiuni în statele membre [24, art. 11].

Modalități de depășire a dificultăților în asigurarea dreptului la uitare digitală. În vederea asigurării unui nivel uniform de protecție pentru persoanele fizice în întreaga Uniune și a preîntâmpinării discrepanțelor care împiedică libera circulație a datelor în cadrul pieței interne, este necesar un regulament în scopul de a furniza securitate juridică și transparență pentru operatorii economici, [...] precum și de a oferi persoanelor fizice în toate statele membre același nivel de drepturi, obligații și responsabilități opozabile din punct de vedere juridic pentru operatori și persoanele împuternicite de aceștia, pentru a se asigura o monitorizare coerentă a prelucrării datelor cu caracter personal, sancțiuni echivalente în toate statele membre, precum și cooperarea eficace a autorităților de supraveghere ale diferitelor state membre. Pentru buna funcționare a pieței interne, este necesar ca libera circulație a datelor cu caracter personal în cadrul Uniunii să nu fie restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal. [...] [24, art. 13].

Orice prelucrare a datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator din Uniune ar trebui efectuată în conformitate cu prezentul regulament, indiferent dacă procesul de prelucrare în sine are loc sau nu în cadrul Uniunii. [...] [24, art. 22].

Pentru a se asigura că persoanele fizice nu sunt lipsite de protecția la care au dreptul în temeiul prezentului regulament, prelucrarea datelor cu caracter personal ale persoanelor vizate care se află pe teritoriul Uniunii de către un operator sau o persoană împuternicită de acesta care nu își are sediul în Uniune ar trebui să facă obiectul prezentului regulament în cazul în care activitățile de prelucrare au legătură cu oferirea de bunuri sau servicii unor astfel de persoane vizate, indiferent dacă acestea sunt sau nu legate de o plată. Pentru a determina dacă un astfel de operator sau o astfel de persoană împuternicită de operator oferă bunuri sau servicii unor persoane vizate care se află pe teritoriul Uniunii, ar trebui să se stabilească dacă reiese că operatorul sau persoana împuternicită de operator intenționează să furnizeze servicii persoanelor vizate din unul sau mai multe state membre din Uniune. [...] [24, art. 23].

Prelucrarea datelor cu caracter personal ale persoanelor vizate care se află pe teritoriul Uniunii de către un operator sau o persoană împuternicită de acesta care nu își are sediul în Uniune ar trebui, de asemenea, să facă obiectul prezentului regulament în cazul în care este legată de monitorizarea com-

portamentului unor astfel de persoane vizate, în măsura în care acest comportament se manifestă pe teritoriul Uniunii. Pentru a se determina dacă o activitate de prelucrare poate fi considerată ca „monitorizare a comportamentului” persoanelor vizate, ar trebui să se stabilească dacă persoanele fizice sunt urmărite pe internet, inclusiv posibila utilizare ulterioară a unor tehnici de prelucrare a datelor cu caracter personal care constau în crearea unui profil al unei persoane fizice, în special în scopul de a lua decizii cu privire la aceasta sau de a analiza sau de a face previziuni referitoare la preferințele personale, comportamentele și atitudinile acestora [24, art. 24].

În cazul în care dreptul unui stat membru se aplică în temeiul dreptului internațional public, prezentul regulament ar trebui să se aplice, de asemenea, unui operator care nu este stabilit în Uniune, ci, de exemplu, într-o misiune diplomatică sau într-un oficiu consular al unui stat membru [24, art. 25].

O persoană vizată ar trebui să aibă [...] „dreptul de a fi uitată”, în cazul în care păstrarea acestor date încalcă prezentul regulament sau dreptul Uniunii sau dreptul intern sub incidența căruia intră operatorul [...]. Cu toate acestea, păstrarea în continuare a datelor cu caracter personal ar trebui să fie legală în cazul în care este necesară pentru exercitarea dreptului la libertatea de exprimare și de informare [...]” [24, art. 65].

În urma examinării cauzei, CJUE a invocat mai multe argumente, de natură să influențeze consacrarea și apărarea dreptului la uitare. Printre cele mai rele-

vante atât studiului de față, cât și practicienilor din Republica Moldova, ar fi:

În hotărârea sa, CJUE începe prin a aminti că a statuat deja [7] că operatorul unui motor de căutare este obligat să elimine de pe lista de rezultate, afișată în urma unei căutări efectuate plecând de la numele unei persoane, linkurile către paginile de internet publicate de terți și care conțin informații referitoare la această persoană și în ipoteza în care acest nume sau aceste informații nu sunt șterse în prealabil sau simultan de pe paginile de internet respective, iar aceasta, dacă este cazul, chiar dacă publicarea lor în sine pe paginile menționate este legală.

Curtea subliniază că, într-o lume globalizată, accesul utilizatorilor de internet, în special al celor care se află în afara Uniunii, la indexarea unui link care trimite la informații cu privire la o persoană al cărei centru de interes este situat în Uniune este astfel susceptibil să producă asupra acesteia efecte imediate și substanțiale chiar în cadrul Uniunii, astfel încât o dezindexare mondială ar fi de natură să satisfacă pe deplin obiectivul de protecție vizat de dreptul Uniunii. Ea precizează însă că numeroase state terțe nu cunosc dreptul la dezindexare sau adoptă o abordare diferită față de acest drept.

Pe de altă parte, dreptul la protecția datelor cu caracter personal nu este un drept absolut, ci trebuie luat în considerare în raport cu funcția pe care o îndeplinește în societate și trebuie echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporționalității [17, pct. 48; 4, pct. 136]. La aceasta se adaugă faptul că

echilibrul dintre dreptul la respectarea vieții private și la protecția datelor cu caracter personal, pe de o parte, și libertatea de informare a utilizatorilor de internet, pe de altă parte, este susceptibil să varieze în mod semnificativ la nivel mondial [16, pct. 60].

De altfel, în timp ce Regulamentul 2016/679 furnizează, la articolele 56 și 60-66 din acesta, autorităților de supraveghere din statele membre instrumentele și mecanismele care le permit, dacă este cazul, să coopereze pentru a ajunge la o decizie comună întemeiată pe o evaluare comparativă între dreptul persoanei vizate la respectarea vieții sale private și la protecția datelor cu caracter personal care o privesc și interesul publicului din diferite state membre de a avea acces la o informație, trebuie să se constate că dreptul Uniunii nu prevede în prezent asemenea instrumente și mecanisme de cooperare în ceea ce privește extinderea unei dezindexări în afara Uniunii [16, pct. 63].

Rezultă că, în stadiul actual, nu există pentru operatorul unui motor de căutare care admite o cerere de dezindexare formulată de persoana vizată, eventual ca urmare a unei somații a unei autorități de supraveghere sau a unei autorități judiciare dintr-un stat membru, o obligație care decurge din dreptul Uniunii de a efectua o asemenea dezindexare în ansamblul versiunilor motorului său [16, pct. 64].

Ținând seama de ansamblul acestor considerații, operatorul unui motor de căutare nu poate fi obligat, în temeiul articolului 12, litera (b) și al articolului 14, primul paragraf, litera (a) din

Directiva 95/46, precum și al articolului 17, alineatul (1) din Regulamentul 2016/679, să efectueze o dezindexare în ansamblul versiunilor motorului său [16, pct. 65].

În ceea ce privește aspectul dacă o asemenea dezindexare trebuie să se efectueze în versiunile motorului de căutare care corespund statelor membre sau numai în versiunea acestui motor ce corespunde statului membru de reședință al beneficiarului dezindexării, rezultă în special din faptul că legiuitorul Uniunii a ales în prezent să stabilească normele în materie de protecție a datelor prin intermediul unui regulament, care este direct aplicabil în toate statele membre, și aceasta, astfel cum subliniază considerentul (10) al Regulamentului 2016/679, pentru a se asigura un nivel consecvent și ridicat de protecție în întreaga Uniune și pentru a se înlătura obstacolele din calea circulației datelor din cadrul acesteia, că se presupune că dezindexarea în cauză este în principiu efectuată pentru ansamblul statelor membre [16, pct. 66].

Revine, în plus, operatorului motorului de căutare sarcina de a lua, dacă este necesar, măsuri suficiente de eficiente pentru a asigura o protecție efectivă a drepturilor fundamentale ale persoanei vizate [16, pct.70]. Aceste măsuri trebuie, ele însele, să îndeplinească toate cerințele legale și să aibă ca efect împiedicarea sau, cel puțin, descurajarea în mod serios a utilizatorilor de internet din statele membre de la a avea acces la linkurile în cauză plecând de la o căutare efectuată pe baza numelui acestei persoane [18, pct. 62; 19, pct. 96].

În sfârșit, trebuie să se sublinieze că, deși, astfel cum s-a arătat la punctul 64 din prezenta hotărâre, dreptul Uniunii nu impune, în stadiul actual, ca dezindexarea care s-ar admite să privească ansamblul versiunilor motorului de căutare în cauză, nici nu o interzice [16, pct. 72]. Prin urmare, o autoritate de supraveghere sau o autoritate judiciară dintr-un stat membru rămâne competentă să efectueze, în raport cu standardele naționale de protecție a drepturilor fundamentale [20, pct. 29; 21, pct. 60], o evaluare comparativă între, pe de o parte, dreptul persoanei vizate la respectarea vieții sale private și la protecția datelor cu caracter personal care o privesc și, pe de altă parte, dreptul la libertatea de informare și, în urma acestei evaluări comparative, să impună, dacă este cazul, operatorului acestui motor de căutare să procedeze la o dezindexare privind ansamblul versiunilor acestui motor.

În cele din urmă, Curtea de Justiție a Uniunii Europene vine cu o concluzie fundamentală, specificând expres că legislația Uniunii Europene în domeniul protecției dreptului la uitare trebuie interpretată în sensul că, atunci când operatorul unui motor de căutare admite o cerere de dezindexare în temeiul acestor dispoziții, el nu este obligat să efectueze această dezindexare în ansamblul versiunilor motorului său, ci în versiunile acestuia care corespund ansamblului statelor membre, iar aceasta, dacă este necesar, în combinație cu măsuri care, îndeplinind totodată cerințele legale, permit efectiv să îi împiedice sau, cel puțin, să îi descurajeze în mod serios pe utilizatorii de internet

care efectuează o căutare pe baza numelui persoanei vizate din unul dintre statele membre de la a avea acces, prin intermediul listei de rezultate afișate în urma acestei căutări, la linkurile care fac obiectul acestei cereri [16, concluzia finală].

Așa cum s-a afirmat în doctrina românească – „...În privința efectivității dreptului la uitare digitală, asistăm la o consolidare a acestuia în special ca urmare a clarificării faptului că, în principiu, operatorul unui motor de căutare este obligat să admită o cerere de înlăturare, atunci când aceste informații se referă la o etapă anterioară a unei proceduri judiciare și care nu mai corespund situației actuale sau cel puțin are obligația să organizeze lista de rezultate, astfel încât imaginea globală privind persoana vizată ce este prezentată utilizatorului de internet să reflecte situația judiciară actuală, iar aceasta întrucât, prin intermediul listei de rezultate, internauții obțin o imagine de ansamblu structurată a informațiilor referitoare la persoana vizată care pot fi găsite pe internet, ceea ce le permite să stabilească un profil mai mult sau mai puțin detaliat al acesteia...” [29, p. 90].

Concluzii și recomandări. Pornind de la ideile sus menționate, considerăm că cele mai importante concluzii de ordin teoretic și practic, cu rezonanțe deosebite în actualitate, sunt următoarele:

- „Dreptul de a fi uitat” a fost creat pentru a apăra drepturile legate de folosirea ilegală a datelor personale pe internet și pentru a garanta intimitatea fiecărui cetățean. În acest sens, la data de 3 decembrie 2015, Curtea de

la Roma cu sentința nr. 23771 a reiterat faptul că dreptul la uitare nu este altceva decât o expresie aparte a dreptului la viață privată (de asemenea, exprimată la nivel european în articolele 7 și 8 din Carta drepturilor fundamentale).

- Concluziile desprinse din această hotărâre arată că trebuie să fie clar că faptul pe care intenționați să-l faceți uitat nu trebuie să fie recent și că nu este de interes public. În echilibrarea intereselor care stau la baza legii în cauză, în lipsa unei legislații italiene aparte, trebuie remarcat modul în care interesul public joacă un rol-cheie în decizie. Astfel, se recomandă ca ziariștii să evite să facă referire la anumite fapte din trecut, cu excepția cazului în care acestea sunt esențiale pentru caracterul complet al informării.

- Prin reglementarea sa în cadrul art. 17 din Regulamentul general privind protecția datelor la nivelul Uniunii Europene s-a urmărit crearea cadrului prin care persoana vizată poate interveni direct asupra prelucrării, iar alin.(1) enumeră cele șase situații în care persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, operatorul având obligația de a șterge acele date fără întârzieri nejustificate. Persoana vizată nu va trebui să justifice în vreun fel cererea de ștergere a datelor cu caracter personal, dincolo de identificarea unuia din cele șase temeuri.

- Mai nou, dreptul la uitare digitală este invocat de foștii deținuți. Astfel, un fenomen care ia amploare este invocarea dreptului la uitare digitală, materializat prin solicitarea îndepărtării articolelor scrise în mediul online, des-

pre persoane care au fost condamnate penal. Respectivele persoane invocă dreptul la viață privată și dreptul la uitare, menționând printre altele, că și-au ispășit pedeapsa și că ar avea dreptul la o nouă șansă. Acest fapt ne demonstrează cu prisosință caracterul complex și extrem de important al dreptului de a fi uitat în mediul Internet.

- Venim cu recomandarea adresată instituțiilor din Republica Moldova cu atribuții în domeniul protecției drepturilor persoanelor în Internet de a prelua legislația, experiența și bunele practici ale Uniunii Europene în acest domeniu, inclusiv pe dimensiunea gestionării situațiilor legate de demersurile privind consacrarea și apărarea dreptului la uitare.

BIBLIOGRAFIE

1. Ambrose M. and Ausloos J. The right to be forgotten across the pond, Telecommunications Policy Research Conference, 2012.
2. Audiencia Nacional, Recurso 725/2010, Sala de lo Contencioso-Administrativo. Sección 1ª, din 2 februarie 2012 (t.a.).
3. Ausloos J. The Right to be Forgotten - Worth Remembering?, Computers Law and Security Review nr. 28, 2012.
4. Avizul 1/15 (Acordul PNR UE Canada) din 26 iulie 2017, EU:C:2017:592, punctul 136.
5. Bercea L. Standardul „consumatorului mediu” și consimțământul pentru prelucrarea datelor cu caracter personal, RRDP nr. 1/2018.
6. BVerfGE35, 202 - Lebach. In the: <http://www.servat.unibe.ch/dfr/bv035202.html> (visited on 04.09.2021).
7. C-131/12, Google Spain și Google, Hotărârea din 13 mai 2014, ECLI:EU:C:2014:317. În: https://ec.europa.eu/anti-fraud/sites/default/files/case-law_2001_2015_en.pdf
8. CJEU. Grand Chamber. Case C-131/12. Google Spain SL and Google Inc.v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez. Judgment of 13 May 2014.
9. Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (JO 1995, L 281, p. 31, Ediție specială, 13/vol. 17, p. 10) (abrogată).
10. Duțu A. Uniunea Europeană: dreptul la eliminarea datelor personale din motoarele de căutare, P.R. nr. 12/2015. Nota nr. 3.
11. ECtHR. Khelili v. Switzerland. Application no. 16188/07. Judgment of 18 October 2011.
12. ECtHR. M. L. and W. W. v. Germany. Applications nos. 60798/10 and 65599/10. Judgment of 28 June 2018.
13. ECtHR. Pihl v. Sweden. Application no. 74742/14. Decision of 7 February 2017.

14. Ekmekdjian M. A., Calogero P. Habeas data: El derecho a la intimidad frente a la revolucion informatica. Buenos Aires, 1996.

15. Gstrein O. J. The Judgment That Will Be Forgotten: How the ECJ Missed an Opportunity in Google vs CNIL (C-507/17) // Verfassungsblog. 25 September 2019. În: <https://verfassungsblog.de/the-judgment-that-will-be-forgotten/> (visited on 02.09.2021).

16. Hotărârea Curții de Justiție a Uniunii Europene (Marea Cameră) C-507/17 din 24 septembrie 2019 „Trimitere preliminară – Date cu caracter personal – Protecția persoanelor fizice în ceea ce privește prelucrarea acestor date – Directiva 95/46/CE – Regulamentul (UE) 2016/679 – Motoare de căutare pe internet – Prelucrarea datelor care figurează pe pagini web – Întinderea teritorială a dreptului la dezindexare”, cauza Google LLC împotriva Commission nationale de l’informatique et des libertés (CNIL – Consiliul Național de Informații și Libertăți, Franța) și Conseil d’État (Consiliul de Stat, Franța). În: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=RO&mode=req&dir=&occ=first&part=1&cid=2120718> (vizitat la 21.09.2021).

17. Hotărârea din 9 noiembrie 2010, Volker und Markus Schecke și Eifert, C 92/09 și C 93/09, EU:C:2010:662, punctul 48.

18. Hotărârea din 27 martie 2014, UPC Telekabel Wien, C 314/12, EU:C:2014:192, punctul 62

19. Hotărârea din 15 septembrie 2016, Mc Fadden, C 484/14, EU:C:2016:689, punctul 96.

20. Hotărârea din 26 februarie 2013, Åkerberg Fransson, C 617/10, EU:C:2013:105, punctul 29.

21. Hotărârea din 26 februarie 2013, Melloni, C 399/11, EU:C:2013:107, punctul 60.

22. Munteanu C., Ungureanu O. Dreptul la protecția datelor cu caracter personal, un drept autonom?, RRDP nr. 1/2014, nota nr. 11 și 12.

23. Popa I.F. Impactul Regulamentului privind protecția datelor cu caracter personal asupra răspunderii civile, RRDP nr. 1/2018, par. 27.

24. Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46 (Regulamentul general privind protecția datelor) (JO 2016, L 119, p. 1, rectificare în JO 2018, L 127, p. 2). Forma prescurtată utilizată în acte și doctrină - General Data Protection Regulation (GDPR).

25. Steyer J. Why Kids Need an Eraser Button // Common Sense Media. 2013. În: <http://www.commonsensemedia.org/blog/why-kids-need-aneraser> (visited on 02.09.2021).

26. Șandru A. M. Inovări și reevaluări în privința drepturilor persoanei vizate în Regulamentul nr. 2016/679, RRDA nr. 4/2018, nota nr. 21.

27. Șchiopu S. D. Aplicarea teritorială a dreptului la uitare digitală (dreptul la înlăturare) in lumina cererii de decizie preliminară introdusă de Conseil d’Etat

(Franța) la 21 august 2017 - Google Inc./CNIL [Cauza C-507/17], P.R., nr. 1/2018.

28. Șchiopu S. D. Perspectivele dreptului de a fi uitat, în Dreptul nr. 5/2019, nota nr. 10;

29. Șchiopu S. D. Spre o reconfigurare a dreptului la uitare digitală ulterior hotărârilor Curții de Justiție a Uniunii Europene în cauzele GC și alții (C-136/17) și Google (C-507/17). Revista Română de Drept European nr. 4/2019. pp.82-94.

30. Zeller B., Trakman L., Walters R., Rosadi S.D. The Right to Be Forgotten - The EU and Asia Pacific Experience (Australia, Indonesia, Japan and Singapore) // European Human Rights Law Review, 2019. Iss. 1. p. 24.

31. Войниканис Е. А. Право быть забытым: правовое регулирование и его теоретическое осмысление//Известия высших учебных заведений. Правоведение. 2016, № 3.

Prezentat: 12.10.2021.

E-mail: studii_juridice@yahoo.com

tarna-alex@mail.ru