PRINCIPII CONSACRATE ÎN JURISPRUDENȚA CEDO ȘI CJUE ÎN MATERIE DE SECURITATE NAȚIONALĂ

RELEVANT PRINCIPLES IN THE ECHR AND CJEU JURISPRUDENCE REGARDING NATIONAL SECURITY

Mr.drd. Sorina Ana MANEA *

Sistemul european de protecție a drepturilor omului este, astăzi, unul dintre cele mai avansate din lume. Cu toate acestea, există și zone de activitate în care clarificările și perfecționarea reprezintă o constantă. Măsurile de combatere a terorismului luate în considerare sau adoptate în Europa, în special cele care sporesc supravegherea în masă, colectarea și stocarea informațiilor electronice sau protecția datelor cu caracter personal sunt astfel de zone. Unele dintre aceste măsuri acordă puteri mai intruzive serviciilor de informații pentru a canaliza deciziile în direcția puterii executive, fără a fi instituite garanțiile judiciare necesare într-un stat de drept.

The European system ensuring the protection of human rights is nowadays one of the most advanced in the world. However, there are also areas of activity where clarification and improvement are constant demands. Counter-terrorism measures considered or adopted in Europe, in particular those that increase mass surveillance, the collection and storage of electronic information or the protection of personal data are such areas. Some of these measures give more intrusive powers to the intelligence services to channel decisions in the direction of the executive branch, without the necessary judicial guarantees being established in a state governed by the rule of law.

Cuvinte-cheie: drept comunitar; CEDO; CJUE; securitate națională.
Keywords: *community law; ECHR; CJUE; national security.*

Supravegherea electronică pusă în practică de autoritățile naționale de forță este inerent legată de dreptul la viață privată și de protecția datelor cu caracter personal. Astfel de drepturi sunt consacrate în legislația UE, care obligă la respectarea principiului necesității, al proporționalității și al subsidiarității în materie. Problemele legale care decurg din supravegherea electronică, ce pot aduce atingere drepturilor persoanelor, nu sunt supuse controlului Curții de Justiție a UE (CJUE), aceasta fiind competentă să judece cauzele îndreptate împotriva statelor sau instituțiilor pentru neîndeplinirea obligațiilor care le revin, în temeiul dreptului UE, caz în care statul care nu și-a îndeplinit obligațiile este obligat să ia măsuri pentru a pune neîntârziat capăt încălcării normelor legale. Persoanele vătămate, după epuizarea căilor de atac la nivel național, se pot adresa Curții Europene a Drepturilor Omului (CEDO) pentru o decizie finală. Prin urmare, deciziile celor două instanțe internaționale formează jurisprudența, care poate duce la schimbarea procedurilor interne după care funcționează autoritățile statale competente pentru protejarea securității naționale.

Supravegherea electronică în masă a cunoscut, după septembrie 2001, o evoluție fără precedent, ca reacție la agresivitatea cu care fenomenul terorist a început să se manifeste. Tocmai din cauza urgenței cu care au trebuit să acționeze pentru a-și îndeplini obligația de a-și proteja cetățenii în întreaga Uniune Europeană, serviciile de informații, în activitatea lor, au fost susținute de guvernele naționale prin măsuri care au permis o mai mare ușurință în evaluarea modului în care are loc culegerea informațiilor. în special în ceea ce privește mijloacele tehnice și tehnologice utilizate.

Activitatea de informații pentru cunoașterea, prevenirea și contracararea amenințărilor la adresa securității naționale, în special cea realizată prin intermediul mijloacelor de supraveghere la scară largă poate interfera cu drepturile și libertățile

Universitatea Națională de Apărare „Carol I”
e-mail: *sorinaman2@yahoo.com*

fundamentale, în special cu dreptul la viață privată și cu protecția datelor, ceea ce poate conduce la perturbarea statului de drept și a respectării drepturilor și libertăților fundamentale ale cetățenilor.

În urma dezvăluirilor analistului NSA, Edward Snowden[1] și ale presei privind supravegherea electronică în masă, efectuată de serviciile de informații americane, mai mult sau mai puțin cu acordul mai multor state membre ale UE, Parlamentul European a adoptat o rezoluție privind Programul de supraveghere NSA al SUA, privind organismele de supraveghere din diferite state membre (UE)[2] și impactul acestora asupra drepturilor fundamentale ale cetățenilor UE.

În acest context, CJUE și CEDO au dezvoltat un set de teste de legalitate, transpuse în principii compatibile cu statul de drept.

Astfel, în cauza Digital Rights Ireland Ltd[3], CJUE a anulat directiva UE[4] care prevedea că statele trebuiau să prevadă obligația furnizorilor de telecomunicații de a păstra metadatele pe o perioadă de șase luni (minimum) și de doi ani (maximum) și să le pună la dispoziția organelor de urmărire și de cercetare penală, în cazul investigării infracțiunilor grave. Directiva lăsa la latitudinea statelor să instituie garanții pentru a reglementa accesul la metadate și pentru a preveni abuzul de putere. Cauza nu a dus însă la uniformizarea practicii investigative în materie penală sau de securitate națională în statele UE, acestea preferând să considere că răspunderea, cel puțin în domeniul securității, este exclusiv națională.

În octombrie 2015, în cauza Schrems[5], CJUE a invalidat acordul UE – SUA, numit *The Umbrella Agreement*[6], care a înlocuit *Acordul Safe Harbour*[7] și care permitea companiilor private să transfere date cu caracter personal ale cetățenilor UE pe teritoriul SUA, hotărând că, în lumina dezvăluirilor Snowden, era rezonabil și pertinent raționamentul că legea și practica în vigoare în SUA nu asigurau o protecție adecvată a datelor cu caracter personal, constatând că monitorizarea conținutului e-mailurilor, apelurilor telefonice și al mesajelor textelor, precum și extragerea unui volum mare de metadate privind locația telefonului mobil, navigarea pe Internet, e-mailurile, cărțile de adrese de e-mail etc., nu era protejată împotriva supravegherii ilegale. CJUE a constatat că statele UE nu erau libere să transfere date către state terțe, cu excepția cazului în care aceste state terțe prevedeau standarde de protecție a datelor echivalente celor care se aplică în UE.

În decembrie 2016, în cauza Tele2 Sverige AB[8] referitoare la Directiva 2002/58[9], prin care sunt stipulate regulile aplicabile prelucrării datelor de trafic și localizare, generate de utilizarea serviciilor de comunicații electronice, precum și anonimizarea sau ștergerea acestor date, cu excepții în materie penală și de securitate națională, CJUE a constatat că garanțiile privind păstrarea și accesul sunt sub răspunderea dreptului comunitar. În acest sens, CJUE a statuat că accesul la metadate trebuie să fie condiționat de aprobarea prealabilă a unei instanțe.

CJUE a reținut că stocarea discriminatorie a datelor privind traficul și localizarea, în scopul combaterii infracțiunilor grave la nivelul legislației naționale, poate fi acceptată, ca măsură preventivă, atunci când „această reglementare națională prevede, în primul rând, norme clare și precise care să reglementeze conținutul și aplicarea unei astfel de măsuri de păstrare a datelor și impune un minim de cerințe, astfel încât persoanele ale căror date au fost păstrate să dispună de garanții suficiente care să le permită să protejeze în mod eficient datele lor cu caracter personal împotriva riscurilor de abuz. Aceasta trebuie, în special, să indice în ce împrejurări și în ce condiții poate fi luată, cu titlu preventiv, o măsură de păstrare a datelor, garantând astfel că o asemenea măsură este limitată la strictul necesar (a se vedea, prin analogie, Directiva 2006/24, Hotărârea Digital Rights, punctul 54, și jurisprudența citată)”[10]. De asemenea, „în ceea ce privește condițiile materiale pe care trebuie să le îndeplinească reglementarea națională care permite, în cadrul combaterii infracționalității, păstrarea cu titlu preventiv a datelor de transfer și a datelor de localizare, pentru a garanta că aceasta este limitată la strictul necesar, trebuie să se arate că, deși aceste condiții pot varia în funcție de măsurile adoptate pentru prevenirea, investigarea, detectarea și urmărirea penală a infracțiunilor grave, păstrarea datelor trebuie să răspundă întotdeauna unor criterii obiective, care să stabilească un raport între datele care trebuie păstrate și obiectivul urmărit. În special, astfel de condiții trebuie să se dovedească, în practică, de natură să delimiteze în mod efectiv amploarea măsurii și, în consecință, publicul în cauză”[11].

În octombrie 2020, Marea Cameră a CJUE a pronunțat două hotărâri[12] privind păstrarea datelor,

securitatea națională și drepturile fundamentale, prin care interzice statelor membre ale UE să adopte legislație menită să aducă atingere domeniului de aplicare a obligațiilor sale de confidențialitate în domeniul datelor referitoare la trafic și locație, cu excepția cazului în care respectă principiile generale ale dreptului comunitar, în special principiul proporționalității, precum și drepturile fundamentale, prevăzute de Carta drepturilor fundamentale a UE.

În cauzele conexate C-511/18 și C-512/18, a fost supusă judecății situația cu privire la legalitatea legislației naționale care impune furnizorilor de servicii de comunicații să transmită utilizatorilor date de trafic și date de localizare către o autoritate publică, sau să păstreze aceste date într-un mod general ori nediscriminatoriu. Instanțele naționale au trimis cazurile CJUE pentru a clarifica dacă activitățile serviciilor naționale de securitate – spre deosebire de organele penale – intră în domeniul de aplicare a legislației UE și dacă păstrarea nediscriminatorie a datelor, pentru securitatea națională, este compatibilă cu legislația UE.

CJUE a decis că analiza automatizată și colectarea în timp real a datelor de trafic, a datelor de localizare sau colectarea în timp real a datelor referitoare la localizarea dispozitivelor sunt autorizate dacă analiza automată este limitată la cazurile în care statul membru se confruntă cu o amenințare gravă, autentică și prezentă sau previzibilă pentru securitatea națională, iar colectarea în timp real este limitată la persoanele suspectate în mod valid de a fi implicate în activități teroriste. În ambele cazuri, gravitatea amenințării și pericolul reprezentat de persoana suspectată trebuie să facă obiectul unei verificări prealabile efectuate de o instanță sau de un organism administrativ independent a cărui decizie este obligatorie.

În cele din urmă, judecății CJUE i-a fost supusă situația în care este posibil să se mențină temporar efectele unei dispoziții naționale care încalcă legislația UE, pentru a evita incertitudinea juridică și pentru a utiliza datele colectate și păstrate anterior. Cu privire la această problemă, CJUE a considerat că directiva, citită în lumina Cartei, nu permite unei instanțe naționale să aplice temporar o dispoziție de drept intern, care, de altfel, este incompatibilă cu dreptul UE. În special, CJUE a interzis instanțelor naționale să aplice o dispoziție națională care solicită furnizorilor să păstreze, într-o manieră generalizată și nediscriminatorie, datele de trafic și localizare, chiar dacă obiectivul dispoziției atacate este de a proteja securitatea națională și de a preveni infracțiunile grave.

Hotărârea CJUE are un rol important în reglementarea activităților de securitate națională și a activității de informații în statele membre ale UE. În acest sens, inclusiv Avocatul General Campos Sanchez-Bordona, în Opinia formulată, în ianuarie 2020[13], cu privire la cazurile sus-menționate, a susținut existența unei distincții între activitatea de informații executată pentru a proteja securitatea națională și legislația adoptată pentru protecția securității naționale, care impune indivizilor obligații care le afectează drepturile comunitare. Această noutate relativă se reflectă în cadrul legal al UE, unde securitatea națională, în ciuda integrării europene, a rămas în mod explicit în responsabilitatea statelor membre.

Și CEDO joacă un rol activ în asigurarea respectării drepturilor și libertăților fundamentale ale omului împotriva folosirii arbitrare a puterii statului. În acest sens, CEDO a statuat, în materie de interceptare a comunicațiilor de orice fel, faptul că, atunci când un stat ia măsuri de supraveghere, este posibil ca persoanele vizate să fie tratate într-un mod contrar articolului 8 din Convenție, fără ca respectivele persoane să fie conștiente de acest lucru și, prin urmare, fără a putea obține o cale de atac la nivel național sau în fața instituțiilor Convenției. Prin urmare, Curtea a acceptat că o persoană poate, în anumite condiții, să pretindă că este victima unei încălcări, cauzate de simpla existență a unor măsuri secrete sau a unei legislații care permite măsuri secrete, fără a fi nevoie să pretindă că astfel de măsuri i-au fost aplicate. Condițiile relevante trebuie stabilite în fiecare caz, în conformitate cu prevederile Convenției sau cu drepturile presupus a fi fost încălcate, cu caracterul secret al măsurilor contestate și cu legătura dintre persoana care se consideră lezată în drepturile sale și acele măsuri. De asemenea, Curtea a reținut că posibilitatea de supraveghere în secret a unor cetățeni este admisă, în temeiul Convenției, numai ca măsură strict necesară pentru protejarea instituțiilor democratice. „Constatând însă că, în prezent, societățile democratice sunt amenințate de forme extrem de sofisticate de spionaj și de terorism, ceea ce impune ca statul să fie capabil să contracareze efectiv astfel de amenințări chiar și prin supravegherea în secret a

elementelor subversive care operează în jurisdicția sa, Curtea a considerat că existența unei anumite legislații care acordă competența de a supraveghea în secret corespondența, comunicările prin poștă și telecomunicațiile este, în condiții excepționale, necesară într-o societate democratică, în interesul securității naționale și/sau pentru a preveni dezordinea sau faptele penale”[14].

Prin urmare, această hotărâre, reflectând prevederile convenționale, instituie principiile testului de legalitate privind punerea în practică a măsurilor restrictive temporar ale drepturilor și libertăților fundamentale, mai exact dreptul la viață privată, la libertate de exprimare, accesul la justiție și dreptul la un proces corect, precum și drepturile corelative acestora.

Curtea a considerat că stocarea de date referitoare la viața privată a unei persoane de către o autoritate publică este o interferență cu dreptul la viață privată, indiferent de utilizarea ulterioară a informațiilor sau dacă informațiile colectate au lezat ori nu persoana vizată[15]. Inclusiv informațiile publice colectate și stocate în mod sistematic de autorități intră în sfera vieții private, mai ales în situația în care informațiile privesc trecutul îndepărtat al unei persoane, iar o parte dintre aceste informații ar fi fost declarate false, existând probabilitatea să aducă atingere reputației persoanei vizate[16].

Conform jurisprudenței Curții, cerința ca orice ingerință să fie în conformitate cu legea „este îndeplinită atunci când măsura atacată trebuie să aibă o bază în dreptul intern, iar legea în cauză trebuie să fie accesibilă persoanei în cauză și să aibă consecințe previzibile[17]. În cazul Rotaru împotriva României[18], Curtea a examinat legislația română privind măsurile de supraveghere secretă legate de securitatea națională și a concluzionat că legislația privind culegerea și stocarea informațiilor nu a oferit garanțiile necesare. Instanța a reiterat această constatare în hotărârile sale cu privire la cauzele Dumitru Popescu împotriva României, nr. 2, 2007 și Asociația „21 decembrie 1989”și alții împotriva României, 2011.

Interesul statului de a-și proteja securitatea națională trebuie să fie proporțional cu gravitatea ingerinței în dreptul persoanei supravegheate de a-i fi respectată viața privată. Astfel, în cauza Kennedy împotriva Marii Britanii, Curtea a considerat că puterea de a institui supravegherea cetățenilor este tolerată numai în conformitate cu prevederile convenției, în măsura în care aceasta a fost strict necesară pentru protejarea instituțiilor democratice, cu alte cuvinte există garanții adecvate și eficiente împotriva abuzului.

Concluzii

Activitatea CJUE și CEDO formulează cadrul democratic de desfășurare a activității de informații la nivel legislativ și, ca rezultat al controlului de constituționalitate, dar mai ales al apartenenței României la UE, la nivel executiv și judecătoresc. Dacă în 1990 activitatea de informații, desfășurată pentru realizarea securității naționale era învăluită de secret și inaccesibilitate, astăzi și, cu siguranță, pe viitor aceasta va avea drept coordonate respectarea drepturilor omului și jurisprudența instanțelor comunitare.

Importanța celor două izvoare de reglementare a unora dintre metodele de lucru ale serviciilor de informații este potențată, mai ales dacă regulile și testele, stabilite pe cale jurisprudențială, ar fi preluate ca standarde de performanță a activității menționate. Spre exemplu, pentru a preveni terorismul, statele pot lua măsuri care interferează cu dreptul la respectarea vieții private, a libertății de exprimare sau a dreptului de asociere, însă supremația legii nu dă statelor mână liberă să interfereze cu drepturile celor din jurisdicția lor. Guvernele vor avea întotdeauna nevoie să demonstreze că măsurile pe care le-au luat pentru contracararea amenințărilor la adresa securității naționale au fost justificate, în lumina textului convenției și a interpretărilor date de cele două instanțe comunitare prin hotărârile sale.

NOTE:

1 Edward Joseph, avertizor de integritate nord-american, care a făcut public programul clasificat de supraveghere în masă, desfășurat de SUA prin NSA.

2 *** *Rezoluţia Parlamentului European*, din 12 martie 2014, referitoare la programul de supraveghere al Agenției Naționale de Securitate (NSA) a SUA, la organismele de supraveghere din diferite state membre și la impactul acestora asupra drepturilor fundamentale ale cetățenilor UE și asupra cooperării transatlantice în materie de justiție și de afaceri interne (2013/2188(INI)), https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52014IP0230&from=RO, accesat la 12.02.2021.

3 *** *Hotărârea Curții (Marea Cameră),* din 8 aprilie 2014, C-293/12 și C-594/12 Digital Rights Ireland, EU:C:2014:238, http://curia.europa.eu/juris/liste.jsf?num=C-293/12, accesat la 12.02.2021.

4 *** *Directiva 2006/24/EC privind reținerea datelor generate sau prelucrate în legătură cu furnizarea de servicii de comunicații electronice accesibile publicului sau a rețelelor de comunicații publice și de modificare a Directivei 2002/58 / CE*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2006.105.01.0054.01.ENG&toc=OJ%3AL%3A2006%3A105%3ATOC, accesat la 12.02.2021.

5 *** *Hotărârea Curții (Marea Cameră)*, din 6 octombrie 2015, C-362/14 Maximillian Schrems împotriva Data Protection Commissioner, http://curia.europa.eu/juris/liste.jsf?num=C-362/14, accesat la 12.02.2021.

6 *** *Decizia Consiliului (UE) 2016/920, din 20 mai 2016, privind semnarea, în numele Uniunii Europene, a Acordului dintre Statele Unite ale Americii și Uniunea Europeană privind protecția informațiilor personale referitoare la prevenire, investigație, detectare și urmărirea penală a infracțiunilor*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016D0920, accesat la 12.02.2021.

7 *** *Decizia 2000/520*, O.J. L 215/7 (2000), https://eur-lex.europa.eu/legal content/en/ALL/?uri=CELEX%3A32000D0520, accesat la 12.02.2021.

8 *** *Hotărârea Curții (Marea Cameră)*, din 21 decembrie 2016, Tele2 Sverige AB (C 203/15) v Post-och telestyrelsen, și Secretarul de Stat al Departamentului de Interne (C 698/15) împotriva Tom Watson, Peter Brice și Geoffrey Lewis, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:62015CJ0203&from=EN, accesat la 12.02.2021.

9 *** *Directiva 2002/58/CE, din 12 iulie 2002, privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice* (Directiva privind confidențialitatea și comunicațiile electronice), https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32002L0058&from=EN, accesat la 12.02.2021.

10 *** *Hotărârea Curții (Marea Cameră)*, din 21 decembrie 2016, Tele2 Sverige AB (C 203/15), paragraful 109.

11 *Ibidem*, paragraful 110.

12 http://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=6166350și cauza C-623/17 Privacy International, lahttp://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=6063852, accesat la 12.02.2021.

13 https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:62018CC0511, accesat la 12.02.2021.

14 *Klass și alții împotriva Germaniei*, 6 septembrie 1978, paragraful 34 și urm., https://hudoc.echr.coe.int/eng#{%22dmdocnumber%22:[%22695387%22],%22itemid%22:[%22001-57510%22]}, accesat la 13.02.2021.

15 *Amann împotriva Elveției*, 2000, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58497%22]},accesat la 13.02.2021.

16 *Rotaru împotriva României*, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-148906%22]}, accesat la 13.02.2021.

17 *Kennedy împotriva Marii Britanii*, 2010, paragraful 151; *Rotaru împotriva României*, 2020, paragraful 52; *Amann împotriva Elveției*, 2000, paragraful 50; *Kruslin împotriva Franței*, 1990, paragraful 27; *Malone împotriva Marii Britanii*, 1984, paragrafele 67 and 68; *Leander împotriva Suediei*, 1987, paragraful 51 etc.

18 *Rotaru împotriva României*, http://legislatie.just.ro/Public/DetaliiDocumentAfis/25965, accesat la 13.02.2021.

BIBLIOGRAFIE

*** *Decizia 2000/520*, O.J. L 215/7 (2000), https://eur-lex.europa.eu/legalcontent/en/ALL/?uri=CELEX%3A32000D0520

*** *Decizia Consiliului (UE) 2016/920, din 20 mai 2016, privind semnarea, în numele Uniunii Europene, a Acordului dintre Statele Unite ale Americii și Uniunea Europeană privind protecția informațiilor personale referitoare la prevenire, investigație, detectare și urmărirea penală a infracțiunilor*,https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016D0920.

*** *Directiva 2002/58/CE, din 12 iulie 2002, privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice* (Directiva privind confidențialitatea și comunicațiile electronice), https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32002L0058&from=EN.

*** *Directiva 2006/24/EC privind reținerea datelor generate sau prelucrate în legătură cu furnizarea de servicii de comunicații electronice accesibile publicului sau a rețelelor de comunicații publice și de modificare a Directivei 2002/58 / CE*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2006.105.01.0054.01.ENG&toc=OJ%3AL%3A2006%3A105%3ATOC.

*** *Hotărârea Curții (Marea Cameră)*, din 21 decembrie 2016, Tele2 Sverige AB (C 203/15) v Post-och telestyrelsen, și Secretarul de Stat al Departamentului de Interne (C 698/15) împotriva Tom Watson, Peter Brice și Geoffrey Lewis, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:62015CJ0203&from=EN.

*** *Hotărârea Curții (Marea Cameră)*, din 21 decembrie 2016, Tele2 Sverige AB (C 203/15), paragraful 109.

*** *Hotărârea Curții (Marea Cameră)*, din 6 octombrie 2015, C-362/14 Maximillian Schrems împotriva Data Protection Commissioner, http://curia.europa.eu/juris/liste.jsf?num=C-362/14.

*** *Hotărârea Curții (Marea Cameră),* din 8 aprilie 2014, C-293/12 și C-594/12 Digital Rights Ireland, EU:C:2014:238, http://curia.europa.eu/juris/liste.jsf?num=C-293/12.

*** *Rezoluţia Parlamentului European*, din 12 martie 2014, referitoare la programul de supraveghere al Agenției Naționale de Securitate (NSA) a SUA, la organismele de supraveghere din diferite state membre și la impactul acestora asupra drepturilor fundamentale ale cetățenilor UE și asupra cooperării transatlantice în materie de justiție și de afaceri interne (2013/2188(INI)), https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52014IP0230&from=RO.

[Consiliul Europei], *Manual de legislație europeană privind protecția datelor*, Agenția pentru Drepturi Fundamentale a Uniunii Europene, 2014.

Ausloos J., *The Right to Erasure in EU Data Protection Law*, Editura Oxford University Press, 2020.

Bîrsan C., *Convenția europeană a drepturilor omului. Comentariu pe articole*, Ediția 2, Editura C.H. Beck, 2010.

Bradford Anu, *The Brussels Effect. How the European Union Rules the World*, Editura Oxford University Press, 2020.

Deleanu I., „Accesibilitatea şi previzibilitatea legii în jurisprudenţa Curţii Europene a Drepturilor Omului şi a Curţii Constituţionale a României”, *Dreptul* nr. 8, 2011.

Duminică R., *Criza legii contemporane*, C.H. Beck, Bucureşti, 2014.

Solove D., Schwarts P., *Privacy Law Fundamentals*, Ediția 4, Editura International Association of Privacy Professionals (IAPP), 2017.

http://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=6166350și cauza C-623/17 Privacy International, lahttp://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=6063852

https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58497%22]}

https://hudoc.echr.coe.int/eng#{%22dmdocnumber%22:[%22695387%22],%22itemid%22:[%22001-57510%22]}

http://legislatie.just.ro/Public/DetaliiDocumentAfis/25965

https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-148906%22]}