

SUPRAVEGHEREA DIGITALĂ DE CĂTRE SERVICIILE DE INFORMAȚII: STATELE TREBUIE SĂ IA MĂSURI PENTRU A PROTEJA MAI BINE PERSOANELE

Olga BENEȘ, master în drept, lector universitar (ORCID: 0000-0001-7853-9557)

DIGITAL SURVEILLANCE BY INFORMATION SERVICES: STATES NEED TO TAKE MEASURES TO BETTER PROTECT PEOPLE

States are called upon to strengthen the protection of personal data in the context of digital surveillance by intelligence services. Countries need to agree internationally on the authorized scope of digital surveillance by intelligence services, the conditions under which it is conducted and its safeguards, including effective and independent control.

Keywords: *personal data, digital surveillance, intelligence services.*

Statele sunt chemate să consolideze protecția datelor cu caracter personal în contextul supravegherii digitale efectuate de serviciile de informații. Țările trebuie să găsească acord la nivel internațional cu privire la domeniul de aplicare autorizat al supravegherii digitale efectuate de serviciile de informații, condițiile în care se desfășoară cât și garanțiile acesteia, inclusiv un control efectiv și independent.

Cuvinte cheie: *date cu caracter personal, supraveghere digitală, serviciile de informații.*

Într-o lume în continuă schimbare, în care datele au devenit aurul negru al secolului 21, transformarea digitală, pentru care securitatea cibernetică este un imperativ pentru succes, pătrunde profund procesele și activitățile de afaceri ale persoanelor din toate țările.

Într-o declarație comună¹, președintele Comitetului „Convenției 108” pentru protecția datelor² al Consiliului Europei, Alessandra Pierucci, și comisarul Consiliului Europei pentru protecția datelor, Jean-Philippe Walter, au solicitat statelor să consolideze protecția datelor cu caracter personal în contextul supravegherii digitale efectuate de serviciile de informații, prin aderarea la convenția Consiliului Europei privind protecția datelor, numită „Convenția 108+”, și prin promovarea unui nou

1 Déclaration conjointe par Alessandra Pierucci, Présidente du Comité de la Convention 108 et Jean-Philippe Walter, Commissaire à la protection des données du Conseil de l'Europe „Mieux protéger les personnes dans un contexte de flux international de données: La nécessité d'une supervision démocratique et effective des services de renseignement.» <https://rm.coe.int/declaration-conjointe-schrems-ii-finale/16809f79ca>

2 Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal din 28 ianuarie 1981. <https://www.coe.int/fr/web/data-protection/convention108-and-protocol>

instrument juridic internațional care să asigure garanții eficiente și democratice în acest domeniu.

Deschisă pentru semnare la 28 ianuarie 1981, Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, a fost primul instrument juridic internațional obligatoriu în domeniul protecției datelor. În temeiul Convenției, părțile trebuie să ia măsurile necesare în dreptul intern în vederea aplicării principiilor acesteia pentru a asigura, pe teritoriul lor, respectarea drepturilor fundamentale ale omului în ceea ce privește aplicarea protecției datelor.

Convenția are ca scop protejarea persoanelor fizice, respectarea în mod special a dreptului la viața privată, față de procesarea datelor cu caracter personal, acestea fiind definite la articolul 2 ca „orice informație privind o persoană fizică identificată sau identificabilă”³.

Convenția privind protecția datelor este primul instrument internațional obligatoriu care are ca scop protejarea persoanelor împotriva utilizării abuzive a prelucrării automate a datelor cu caracter personal și care reglementează fluxurile de date transfrontaliere. Pe lângă garanțiile oferite pentru prelucrarea automată a datelor cu caracter personal, interzice prelucrarea datelor „sensibile” referitoare la originea rasială, opiniile politice, sănătatea, religia, viața sexuală, condamnări penale etc., în absența garanțiilor oferite de legislația internă. Convenția garantează, de asemenea, dreptul persoanelor vizate de a cunoaște informațiile stocate despre acestea și de a solicita rectificări acolo unde este necesar. Singura restricție a acestui drept: atunci când sunt în joc interesele majore ale statului (securitate publică, apărare etc.). Convenția impune, de asemenea, restricții asupra fluxurilor de date transfrontaliere în statele în care nu există o protecție echivalentă.

Protocolul adițional⁴, deschis spre semnare la 8 noiembrie 2001 la Strasbourg, impune părților să înființeze autorități de supraveghere, care să-și exercite funcțiile în deplină independență și care reprezintă un element al protecției efective a persoanelor în ceea ce privește prelucrarea datelor personale. Odată cu creșterea schimbului de date cu caracter personal dincolo de frontierele naționale, este necesar să se asigure protecția eficientă a drepturilor omului și a libertăților fundamentale și, în special, dreptul la viața privată în legătură cu astfel de schimburi de date cu caracter personal.

Dreptul de a proteja sfera privată a unei persoane fizice împotriva intruziunii din partea altora, în deosebi din partea statului este consfințit pentru prima dată în Declarația Universală a Drepturilor Omului din 1948, care în articolul 12 garantează respectarea vieții private și de familie. Alte documente au consfințit și ele în conținutul

3 Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal din 28 ianuarie 1981. <https://www.coe.int/fr/web/data-protection/convention108-and-protocol>

4 Protocolul adițional la Convenția Consiliului Europei pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de supraveghere și fluxul transfrontalier al datelor din 08 noiembrie 2001. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800805d3>

lor dreptul la respectarea vieții private și de familie care include în conținutul său dreptul de protecție împotriva colectării și utilizării datelor cu caracter personal, acest drept făcând parte din articolul 8 al CEDO-Dreptul la respectarea vieții private și de familie, a domiciliului și a corespondenței, care totodată stabilește condițiile de bază care permit limitările acestui drept⁵.

Și dreptul Uniunii Europene a recunoscut protecția datelor cu caracter personal ca drept fundamental, protecția căruia pentru prima dată s-a înscris în 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,⁶ datorită imposibilității de a realiza cu succes libera circulație a mărfurilor, capitalurilor, serviciilor și persoanelor în cadrul pieței interne fără o viziune comună a statelor referitor la protecția la un nivel înalt al fluxurilor de date.

Au urmat o serie de alte instrumente menite să stabilească protecția datelor cu caracter personal nu doar de către state dar și de către instituțiile și organismele UE, în acest cadru putem nominaliza atât Regulamentul nr.45/2001 privind protecția persoanelor fizice cu privire a prelucrarea datelor cu caracter personal de către organele și instituțiile comunitare și privind libera circulație a acestor date⁷ cât și directivele 2002/58/CE⁸ și Directiva 2006/24/CE⁹ cu referință la sectorul comunicațiilor publice și comunicațiile electronice.

O contribuție deosebită în protecția și garantarea acestui drept o are Carta Drepturilor Fundamentale a Uniunii Europene care nu doar asigură respectarea vieții private și de familie (art.7) dar stabilește și dreptul la protecția datelor și totodată face referire la principiile cheie privind protecția datelor (art.8), în acest sens fiind creată o autoritate competentă independentă în scopul controlului respectării principiilor enunțate (art.9)¹⁰.

5 Convenția Europeană a Drepturilor Omului, adoptată la Roma la 04.11.1950. https://www.echr.coe.int/documents/convention_ron.pdf

6 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. <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:31995L0046>

7 Regulamentul nr.45/2001 privind protecția persoanelor fizice cu privire a prelucrarea datelor cu caracter personal de către organele și instituțiile comunitare și privind libera circulație a acestor date.

8 Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice). <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32002L0058>

9 Directiva 2006/24/CE a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE. <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32006L0024>

10 Carta Drepturilor Fundamentale a Uniunii Europene, 2012/C 326/02. <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:12012P/TXT>

Dacă e să analizăm caracterul dreptului enunțat, atunci putem observa că dreptul la protecția datelor cu caracter personal nu are un caracter absolut și toate aceste instrumente enunțate conțin o serie de restrângeri care „...trebuie să fie prevăzute de lege și să respecte substanța acestor drepturi și libertăți. Prin respectarea principiului proporționalității, pot fi impuse restrângeri numai în cazul în care acestea sunt necesare și numai dacă răspund efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți”¹¹. Același articol stipulează convergența acestor restrângeri cu cele prevăzute de CEDO : “ În măsura în care prezenta carte conține drepturi ce corespund unor drepturi garantate de Convenția europeană pentru apărarea Drepturilor Omului și a Libertăților fundamentale, înțelesul și întinderea lor sunt aceleași ca și cele prevăzute de convenția menționată”¹².

Articolul 8 al Convenției europene a Drepturilor Omului, consfințind dreptul la protecția datelor cu caracter personal, și el la rândul său, vine să impună anumite condiții la restrângerea drepturilor garantate de către state, enunțând că: „Nu este admis amestecul unei autorități publice în exercitarea acestui drept decât în măsura în care acesta este prevăzut de lege și constituie, într-o societate democratică, o măsură necesară pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protecția sănătății, a moralei, a drepturilor și a libertăților altora”¹³.

Astfel, nu întâmplător în Declarația oficialilor europeni enunțată mai sus „statele sunt chemate să consolideze protecția datelor cu caracter personal în contextul supravegherii digitale efectuate de serviciile de informații. Țările trebuie să găsească acord la nivel internațional cu privire la domeniul de aplicare autorizat al supravegherii digitale efectuate de serviciile de informații, condițiile în care se desfășoară cât și garanțiile acestora, inclusiv un control eficient și independent, având la bază multiplele criterii dezvoltate în jurisprudența Curții Europene a Drepturilor Omului și a Curții Supreme a Statelor Unite”¹⁴.

Conform jurisprudenței Curții Europene a Drepturilor Omului cu privire la articolul 8 care garantează dreptul la respectarea vieții private și de familie „simpla înregistrare a datelor referitoare la viața privată a unui individ constituie o încălcare a acestui articol. Cu toate acestea, pentru a stabili dacă informațiile personale stocate de autorități implică orice aspect al vieții private [...] Curtea va ține cont în mod corespunzător de contextul specific în care informațiile în litigiu au fost înregistrate și

11 Ibidem, art.52 (1)

12 Ibidem, art.52 (2)

13 Convenția Europeană a Drepturilor Omului, adoptată la Roma la 04.11.1950. https://www.echr.coe.int/documents/convention_ron.pdf

14 Déclaration conjointe par Alessandra Pierucci, Présidente du Comité de la Convention 108 et Jean-Philippe Walter, Commissaire à la protection des données du Conseil de l'Europe „Mieux protéger les personnes dans un contexte de flux international de données: La nécessité d'une supervision démocratique et effective des services de renseignement.» <https://rm.coe.int/declaration-conjointe-schrems-ii-finale/16809f79ca>

reținute, natura înregistrărilor, modul în care sunt utilizate și prelucrate respectivele înregistrări și rezultatele care pot fi obținute.¹⁵

Cu privire la acest aspect al articolului 8 CEDO, jurisprudența Curții Europene a Drepturilor Omului a evoluat începând cu hotărârea din 1978 *Klass c. Germaniei*, cu privire la interceptarea comunicațiilor, relevând pe parcurs mai multe aspecte, și anume: informațiile privind ADN-ul și amprentele digitale (*S. și Marper c. Regatului Unit* nr.30562/04 și 30566/04), informațiile obținute prin plasarea sistemului GPS (*Ben Faiza c. Franței* nr.31446/12), colectarea datelor medicale (*L.H. c. Letoniei* nr.5201907), prelevarea eșantioanelor de salivă (*Dragan Petrović c. Serbiei* nr.75229/10), preluarea eșantioanelor vocale (*P.G et J.H. c. Regatului-Unit* nr. 44787/98), monitorizarea utilizării calculatorului de către angajați (*Bărbulescu c. României* nr.61496/08), supravegherile video (*Lopez Ribalda c. Spaniei* nr. 1874/13), stocarea și utilizarea datelor cu caracter personal în contextul sistemului de justiție penală (*Perry c. Regatului Unit* nr.63737/00), în procedurile din domeniul asigurărilor sociale (*Vucota-Bojic c. Elveției* nr.61838/10), stocarea în registre secrete (*Leander c. Suediei* nr.9248/81), divulgarea datelor cu caracter personal (M.S. c. Suediei nr.2037/92), accesul la date cu caracter personal (*Gaskin c. Regatului Unit* nr.10454/83), stocarea în registre secrete și ștergerea sau distrugerea datelor cu caracter personal (*Rotaru c. României* nr. 28341/95).

Digitalizarea în masă a activităților noastre, amplificată în special de actuala criză de sănătate necesită o atenție sporită pe măsură ce viața noastră devine din ce în ce mai digitalizată iar serviciile oferite on-line se împletesc la nivel internațional iar datele noastre personale trec granițele naționale sau regionale și în consecință protecția noastră eficientă devine tot mai greu de realizat. Nu întâmplător, jurisprudența cu privire la articolul 8 CEDO a dezvoltat anumite exigențe pentru a stabili dacă imixtiunile în dreptul la viața privată sau corespondență sunt necesare într-o societate democratică și dacă se ajunge la un echilibru echitabil între diferitele interese în joc, CtEDO examinând de fiecare dată dacă imixtiunea este conformă cu legea, urmărește un scop legitim și este necesară și proporțională cu scopul urmărit. Ea a dezvoltat astfel garanții și condiții specifice pe care serviciile de informații trebuie să le respecte. Încă în hotărârea *S. și Marper c. Regaului Unit* din 4 decembrie 2008, CtEDO a enunțat regula că: „Protecția datelor cu caracter personal are un rol fundamental în exercitarea de către o persoană a dreptului său la respectarea vieții private și de familie, astfel cum este garantat de art.8 din Convenție. Dreptul intern trebuie să ofere garanții adecvate pentru a preveni orice utilizare a datelor cu caracter personal care ar putea fi incompatibilă cu garanțiile prevăzute de acest articol [...]. Necesitatea unor astfel de garanții este cu atât mai mare în cazul protecției datelor cu caracter personal care constituie obiectul prelucrării automate, în special atunci când aceste date sunt utilizate în scopuri polițienești. Dreptul intern ar trebui să se asigure că aceste date sunt relevante și nu sunt excesive în raport cu scopurile pentru

15 CEDO, S și Marper c.Regatului Unit, hot. din 04.12.2008. <https://hudoc.echr.coe.int/eng#%7B%22languageisocode%22:%5B%22FRE%22%5D,%22appno%22:%5B%2230562%2F04%22,%2230566%2F04%22%5D,%22documentcollectionid%22:%5B%22GRANDCHAMBER%22%5D,%22itemid%22:%5B%22001-90052%22%5D%7D>

care sunt înregistrate, și că ele sunt păstrate într-o formă care să permită identificarea persoanelor vizate o perioadă nu mai lungă decât este necesar pentru scopurile pentru care acestea sunt înregistrate [...]. [Acesta] trebuie să ofere, de asemenea, garanții adecvate, că datele cu caracter personal care au fost înregistrate au fost protejate în mod eficient împotriva utilizării necorespunzătoare și abuzului [...].¹⁶

Recent, și Curtea de Justiție a Uniunii Europene a reiterat importanța crucială, la nivel internațional a garanțiilor adecvate, a drepturilor executorii și a căilor de atac eficiente atunci când datele cu caracter personal sunt prelucrate în scopul securității publice, apărării sau securității statului.

Hotărârea CJUE Schrems II din 16 iulie 2020¹⁷ ridică probleme mai largi cu privire la transferurile internaționale, oferind astfel o nouă oportunitate de a consolida cadrul universal de protecție a datelor și de a răspunde necesității unui instrument internațional universal privind serviciile de informații. Curtea a reafirmat că datele cu caracter personal transferate în afara Uniunii Europene trebuie să beneficieze de un nivel de protecție echivalent cu cel garantat în cadrul Uniunii Europene de Regulamentul General cu privire la protecția datelor¹⁸, în corespundere cu Carta drepturilor fundamentale, acest Regulament stabilind în mod precis condițiile în care un astfel de transfer poate avea loc în lipsa unei decizii de conformitate sau a garanțiilor adecvate. Curtea specifică faptul că evaluarea unui astfel de nivel de protecție trebuie să ia în considerare atât dispozițiile contractuale convenite între exportatorul de date stabilit în Uniunea Europeană cât și destinatarul transferului stabilit în țara terță respectivă, în ceea ce privește un eventual acces al autorităților acestei țări terțe la datele astfel transferate și elementele relevante ale sistemului juridic al țării terțe respective. În ceea ce privește obligațiile ce revin autorităților de supraveghere în contextul unui astfel de transfer, Curtea consideră că, cu excepția cazului când există o decizie de conformitate adoptată de Comisie, aceste autorități sunt în special obligate să suspende sau să interzică transferul de date cu caracter personal către o țară terță atunci când consideră, că în circumstanțele acestui transfer, clauzele standard de protecție a datelor nu sunt sau nu pot fi respectate în țara respectivă și că protecția datelor transferate impusă de legislația Uniunii, nu poate fi asigurată prin alte mijloace. Dar, aceasta nu se poate spune în cazul Privacy Shield încheiat între UE și Guvernul Statelor Unite ale Americii¹⁹ deoarece limitările

16 CtEDO, hot. S. și Marper c. Regatului Unit nr.30562/04 și 30566 din 4 decembrie 2008.

17 CJCE, affaire 311/18, Data Protection Commissioner contre Facebook Ireland Ltd, Maximillian Schrems, arrêt du 16 juillet 2020. <http://curia.europa.eu/juris/document/document.jsf?jsessionid=6E6216390C271A22797F9C678D67F033?text=&docid=228677&pageIndex=0&doclang=RO&mode=lst&dir=&occ=first&part=1&cid=840756>

18 Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679>

19 Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la

protecției datelor cu caracter personal transferate din Uniunea Europeană-care rezultă din legislația internă a SUA privind accesul și utilizarea acestor date de către autoritățile publice și instituțiile de aplicare a legii din SUA-nu erau încadrate într-un mod care să îndeplinească cerințe în mod substanțial echivalente cu cele impuse, în dreptul Uniunii, de principiul proporționalității, prin faptul că programele de supraveghere fondate în baza acestei reglementări nu sunt limitate la strictul necesar²⁰.

La nivelul Organizației Națiunilor Unite, statele membre au reamintit în Rezoluția 68/167 privind dreptul la viața privată în era digitală că „supravegherea ilegală sau interceptarea comunicațiilor, precum și colectarea ilegală sau arbitrară a datelor cu caracter personal, care reprezintă acte extrem de intruzive, încalcă dreptul al viața privată și libertatea de exprimare și vin în contradicție cu principiile oricărei societăți democratice“, și au chemat toate statele să „creeze condiții care permit revenirea lor, în deosebi vechind la aceea ca legislația națională să respecte obligațiile impuse de dreptul internațional al drepturilor omului.“²¹

Deci, statele trebuie să găsească soluții comune nu doar la măsura în care supravegherea efectuată de serviciile de informații poate fi autorizată, dar de asemenea și la condițiile, garanțiile acordate și controlul independent și efectiv al instanțelor în cazul încălcării lor.

Având în vedere recenta evoluție a evenimentelor în domeniul dat cât și jurisprudența instanțelor internaționale, Declarația oficialilor europeni menționează că Convenția modernizată pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, ar putea constitui acel document solid cu caracter juridic obligatoriu pentru protecția vieții private și a datelor cu caracter personal la nivel mondial, îndeosebi în ceea ce privește fluxul transfrontalier de date cu caracter personal. Prin conținutul său, această Convenție prezintă un cadru juridic internațional de importanță majoră, în special cu privire la necesitatea unei examinări independente și eficiente și a unei supravegheri a limitărilor dreptului la protecția datelor cu caracter personal, justificate prin imperative de securitate națională sau de apărare. Actualizată prin Protocolul din 2018 care nu a intrat încă în vigoare, Convenția garantează că principiile de protecție a datelor sunt întotdeauna adaptate instrumentelor și practicilor actuale, întărește mecanismul de supraveghere, iar elaborarea unui document internațional în domeniul dat s-ar putea baza pe numeroasele criterii deja dezvoltate de instanțele atât europene cât și Curtea Supremă a Statelor Unite.

protection assurée par le bouclier de protection des données UE-États-Unis. <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016D1250>

20 CJUE, Communiqué de presse n°91/20. Arrêt dans l'affaire C-311/18Data Protection Commissioner/Maximillian Schrems et Facebook Ireland. <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091fr.pdf>

21 Résolution adoptée par l'Assemblée générale le 18 décembre 2013. 68/167. Le droit à la vie privée à l'ère du numérique. <https://undocs.org/fr/A/RES/68/167>