ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „ALEXANDRU IOAN CUZA" DIN IAȘI
TOMUL LXIV, ȘTIINȚE JURIDICE, 2018, SUPLIMENT

REGIMUL DE SUPRAVEGHERE PRIN INTERMEDIUL INTERNETULUI ȘI DREPTURILE FUNDAMENTALE

MASS SURVEILLANCE VIA INTERNET AND HUMAN RIGHTS

CARMEN MOLDOVAN[1]

Rezumat: Lucrarea își propune să analizeze efectele pe care le poate avea asupra protecției unor drepturi fundamentale (în mod special, dreptul la viață privată și libertatea de informare) interceptarea comunicațiilor, schimbul de informații cu guverne străine și obținerea de informații de la furnizorii de servicii, aspecte analizate în cea mai recentă hotărâre pronunțată de către Curtea Europeană a Drepturilor Omului - *Big Brother Watch and Others v. the United Kingdom (13 septembrie 2018).*
Cuvinte cheie: comunicații electronice, viață privată, garanții procedurale, confidențialitate

Abstract: The paper aims to analyze the effects that the regime of mass surveillance may have on the protection of fundamental rights (in particular the right to privacy and freedom of information) by intercepting communications, exchanging information with foreign governments and obtaining information from service providers, issues analyzed in the most recent judgment of the European Court of Human Rights - *Big Brother Watch and Others v. the United Kingdom* (September 13th, 2018).
Keywords: electronic communications, private life, procedural guarantees, confidentiality

Prezentare generală

Problema supravegherii în masă a persoanelor pune în discuție întinderea prerogativelor statului în asigurarea securității naționale și asigurarea garantării drepturilor fundamentale și a implicațiile asupra acestora.

[1] Lector universitar dr., Universitatea „Alexandru Ioan Cuza" din Iași, Facultatea de Drept, email: carmen.moldovan@hotmail.com.

În spațiul public, imediat după pronunțare, hotărârea Curții Europene a Drepturilor Omului din 13 septembrie 2018[2] a fost văzută ca o mare victorie a asociațiilor pentru drepturile omului asupra practicilor de supraveghere ale statului britanic, însă la o lectură atentă a considerentelor instanței, rezultă că aceasta nu respinge *prima facie* ideea supravegherilor tehnice, ci dimpotrivă, chiar admite această posibilitate[3], ca expresie a marjei sale de apreciere și este destul de nuanțată în stabilirea încălcărilor anumitor prevederi ale Convenției. Însă nu poate fi omisă importanța acestei hotărâri sub aspectul stabilirii faptului că supravegherea în masă poate fi mai intruzivă decât accesul la conținutul comunicațiilor.[4]

Curtea Europeană a Drepturilor Omului a fost sesizată după ce Edward Snowden, fost angajat al *National Security Agency* a Statelor Unite ale Americii, a dezvăluit existența unor programe de supraveghere și informații, administrate de către serviciile de informații din Statele Unite și din Regatul Unit al Marii Britanii.[5]

Sesizarea a fost făcută prin trei cereri conexate de Curte: *Big Brother Watch and Others v. United Kingdom* (în 2013), *Bureau of Investigative Journalism and Alice Ross v. United Kingdom* (în 2014), 10 *Human Rights Organisations and Others v. United Kingdom* (în 2015).

În centrul tuturor cererilor se aflau susținerile părților că natura activităților serviciilor de informații însemna că informațiile cu privire la comunicările electronice și/sau alte comunicări ar putea fi interceptate sau obținute de către serviciile de informații britanice.

---

[2] European Court of Human Rights, *Case of Big Brother Watch and Others v. The United Kingdom* (Applications nos. 58170/13, 62322/14 and 24960/15), Judgement of 13 September 2018. Toate hotărârile Curții Europene a Drepturilor Omului sunt disponibile la adresa: https://hudoc.echr.coe.int.

[3] Th. Christakis, *A Fragmentation of EU/RCHR Law on Mass Surveillance: Initial Thoughts on The Big Brother Watch Judgement*, 20 September 2018, [Online] la http://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment/, accesat 20.10.2018.

[4] M. Tzanou, *Big Brother Watch and others v. the United Kingdom: A Victory of Human Rights over Modern Digital Surveillance?*, *VerfBlog*, 2018/9/18, [Online] la https://verfassungsblog.de/big-brother-watch-and-others-v-the-united-kingdom-a-victory-of-human-rights-over-modern-digital-surveillance/, DOI: https://doi.org/10.17176/20180918-125600-0, accesat 20.10.2018.

[5] Open Society Foundation, [Online] la https://www.opensocietyfoundations.org/litigation/big-brother-watch-v-united-kingdom, accesat 20.10.2018.

Cauza privește plângeri ale unor jurnaliști și asociații pentru drepturile omului cu privire la trei regimuri de supraveghere diferite: (1) interceptarea în masă a comunicațiilor; (2) schimbul de informații cu guvernele străine; și (3) obținerea datelor de comunicații de la furnizorii de servicii de comunicații din Marea Britanie.

Măsurile de interceptare în masă și regimul de obținere a datelor de comunicații de la furnizorii de servicii de comunicații au ca temei o lege privind competențele de anchetă adoptată în anul 2000 - *Regulation of Investigatory Powers Act 2000*. Regimul juridic al acestora va fi modificat în mod semnificativ după intrarea în vigoare a legislației specifice adoptate în 2016 - *Investigatory Powers Act 2016*. Curtea a analizat dispozițiile legale în vigoare, respectiv cele din anul 2000.

Reclamanții au invocat încălcarea articolului 8 din Convenție[6], sub aspectul dreptului la viață privată, deoarece regimul juridic al interceptărilor în masă al comunicațiilor, schimbul de informații și obținerea de informații de la furnizorii de servicii de comunicații.

O altă încălcare privea articolul 10 din Convenție[7], care garantează libertatea de exprimare, în legătură cu activitatea de jurnaliști și organizații non - guvernamentale a unora dintre reclamanți.

A treia încălcare privea articolul 6 din Convenție, în legătură cu procedurile interne ce puteau fi folosite pentru a contesta măsurile de supraveghere.

---

[6] Articolul 8 din Convenția europeană a drepturilor omului, intitulat „Dreptul la respectarea vieţii private şi de familie" prevede: „ 1. Orice persoană are dreptul la respectarea vieţii sale private şi de familie, a domiciliului său şi a corespondentei sale. 2. Nu este admis amestecul unei autorități publice în exercitarea acestui drept decât în măsura în care acesta este prevăzut de lege şi constituie, într-o societate democratică, o măsură necesară pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii şi prevenirea faptelor penale, protecția sănătății, a moralei, a drepturilor şi a libertăților altora."

[7] Articolul 10 din Convenția europeană a drepturilor omului, intitulat „Libertatea de exprimare" prevede: „1. Orice persoană are dreptul la libertate de exprimare. Acest drept include libertatea de opinie şi libertatea de a primi sau a comunica informații ori idei fără amestecul autorităților publice şi fără a ține seama de frontiere. Prezentul articol nu împiedică Statele să supună societățile de radiodifuziune, cinematografie sau televiziune unui regim de autorizare. 2. Exercitarea acestor libertăți ce comportă îndatoriri şi responsabilități poate fi supusă unor formalități, condiții, restrângeri sau sancțiuni prevăzute de lege care, într-o societate democratică, constituie măsuri necesare pentru securitatea națională, integritatea teritorială sau siguranța publică, apărarea ordinii şi prevenirea infracțiunilor, protecția sănătății, a moralei, a reputației sau a drepturilor altora, pentru a împiedica divulgarea informațiilor confidențiale sau pentru a garanta autoritatea şi imparțialitatea puterii judecătorești."

A fost de asemenea invocată încălcarea articolului 14 împreună cu articolul 8 și 10, susținându-se că regimul interceptărilor în masă discriminează persoanele din afara Regatului Unit ale căror comunicații erau mult mai probabil să fie interceptate și, dacă ar fi fost interceptate, ar fi fost supuse analizei conținutului. Curtea nu a constatat încălcarea articolului 14 din Convenție, prin urmare prezenta lucrare nu va tratat aspecte legate de acesta.

Prin hotărârea pronunțată de Cameră la 13 septembrie 2018, Curtea Europeană a Drepturilor Omului a decis, cu cinci voturi la două, că: regimul de interceptare în masă a încălcat articolul 8 al Convenției Europene a Drepturilor Omului (dreptul la respectarea vieții private și familiale/și a comunicărilor) deoarece a existat o insuficientă supraveghere atât asupra selecției intermediarilor serviciilor de internet pentru interceptare, cât și asupra filtrării, căutării și selecției comunicațiilor interceptate pentru examinare, de asemenea și garanțiile privind alegere „datelor de comunicare asociate" pentru examinare au fost neadecvate sau insuficiente.

Curtea a constatat că funcționarea unui regim de interceptare în masă nu a încălcat per *se* Convenția, dar a reținut că un astfel de regim trebuia să respecte criteriile stabilite în jurisprudența sa. De asemenea, Curtea a hotărât, cu șase voturi la unul că:regimul de obținere a datelor de comunicații de la furnizorii de servicii de comunicații a încălcat articolul 8 deoarece nu era în conformitate cu legea; și că atât regimul de interceptare în masă, cât și regimul de obținere a datelor de comunicații de la furnizorii de servicii de comunicații au încălcat articolul 10 din Convenție, deoarece nu existau garanții suficiente în ceea ce privește materialele jurnalistice confidențiale.

De asemenea, a constatat că regimul juridic al schimbului de informații cu guvernele străine nu a încălcat nici articolul 8, nici articolul 10. Curtea a respins în mod unanim plângerile formulate de al treilea set de solicitanți în temeiul articolului 6 (dreptul la un proces echitabil), procedura internă de contestare a măsurilor de supraveghere secrete și articolul 14 (interzicerea discriminării).

Hotărârea din 13 septembrie 2018 este prima în care Curtea a analizat problema schimbului de informații între servicii de informații din state diferite și a concluzionat în sensul că acesta nu contravine Convenției.

Aspectele pentru care s-a constatat încălcarea articolului 8 din Convenție

În ceea ce privește încălcarea articolului 8 din Convenție, Curtea a analizat mecanismul de interceptare masivă instituit de articolul 8 alin. (4) din legea din anul 2000 (*Regulation on Investigatory Powers Act*) și a constatat că *per se*, mecanismul creat pentru interceptarea masivă a comunicațiilor nu este în contradicție cu dispozițiile Convenției, deoarece statele dispun de o marjă mare de discreție în a stabili astfel de mijloace în scopul protejării securității naționale.

Articolul 8 alin. (4) din Legea din anul 2000 prevedea patru etape de operare: interceptarea comunicațiilor electronice transmise; folosirea unor selectoare pentru a filtra și a șterge în timp real acele comunicații care nu conțineau deloc sau conțineau prea puține informații; interceptarea comunicațiilor rămase; examinarea de către un analist, a materialelor reținute.

În analiza implicațiilor măsurilor de supraveghere secretă asupra vieții private, Curtea a făcut trimitere la principiile generale referitoare la măsurile de supraveghere secretă, inclusiv interceptarea comunicațiilor stabilite în jurisprudența sa ca cerințe minime ce trebuie respectate în cadrul legislației naționale[8]: natura infracțiunilor care ar putea reclama un mandat de interceptare; definirea categoriilor de persoane supuse interceptării convorbirilor; stabilirea unei limite a duratei de interceptare; procedura care trebuie urmată pentru examinarea, utilizarea și stocarea datelor obținute; măsurile de precauție care trebuie luate la comunicarea datelor către alte părți; circumstanțele în care datele interceptate pot sau trebuie să fie șterse sau distruse.

Cu privire la aceste cerințe minime, reclamanții au afirmat că ele ar trebui actualizate, în sensul includerii cerințelor privind dovezile obiective de bănuială rezonabilă în privința persoanelor pentru care s-au cerut informații, autorizarea judiciară independentă prealabilă a mandatelor de interceptare și notificările ulterioare ale subiectului supus supravegherii.

În analiza Curții, aceasta a reținut că metodele de interceptare în masă constituie un mijloc important pentru atingerea obiectivelor legitime urmărite, în special în contextul nivelului actual al pericolului generat de

[8] European Court of Human Rights, *Weber and Saravia v. Germany* (Application no. 54934/00), Decision on admisibility, 29 June 2006.

actele de terorism cât și de infracțiunile grave. Măsurile de interceptare aveau caracter general, iar necesitatea existenței unei bănuieli rezonabile ar face imposibilă funcționarea unui astfel de sistem. De asemenea, includerea unei cerințe de notificare ulterioară ar presupune existența unor obiective de supraveghere clar definite, fapt care nu era suficient în cazul unui regim de interceptare în masă.

Curtea a considerat că prevederea legală era suficient de clară și furniza persoanelor indicii adecvate cu privire la circumstanțele și condițiile în care ar putea fi emis un mandat în temeiul articolului 8 alin. (4) și că nu au fost furnizate probe din care să rezulte că autoritățile naționale au autorizat emiterea de mandate în lipsa unei analize corecte și adecvate. Curtea a considerat că erau suficient de clare și acordau garanții adecvate împotriva abuzurilor o serie de prevederi relevante: referitoare la durata și reînnoirea mandatelor de interceptare, a celor referitoare la stocarea, accesarea, analiza și utilizarea datelor de comunicație interceptate, a celor referitoare la procedura ce trebuie urmată pentru comunicarea datelor interceptate către părți și a celor referitoare la ștergerea și distrugerea materialului interceptat.

În ceea ce privește sistemul de selectare a comunicațiilor pentru analiză, Curtea a reținut că aceasta presupunea într-o primă etapă aplicarea automată, prin intermediul computerului, a unor criterii de sortare simple cum sunt adresele de e-mail sau numerele de telefon și a unor criterii inițiale de căutare, iar ulterior, utilizarea unor căutări mai complexe. Criteriile de căutare și cele de selectare nu erau făcute publice și nici nu trebuiau să fie menționate în mandatul de interceptare, însă acestea ar fi trebuit să fie supuse unui control independent, garanție care în aparență lipsea din articolul 8 alin. (4). Conform legislației aplicabile, controlul asupra procesului de filtrare și de selectare a comunicațiilor și datelor interceptate era unul *post factum* și se făcea prin audit al Comisarului pentru Interceptarea Comunicațiilor sau al instanței cu competențe de investigare (*Investigatory Powers Tribunal*). Curtea a subliniat că în privința unui regim de supraveghere și interceptare în masă, în care discreția autorităților era foarte extinsă și nu era restricționată în mod semnificativ de condițiile mandatului, garanțiile aplicabile etapei de filtrare și de selectare a comunicațiilor trebuie să fie mai puternice.

În această privință, Curtea a reținut că serviciile de informații din Regatul Unit iau foarte în serios obligațiile ce le revin și nu abuzează de prerogativele pe care le au în temeiul dispozițiilor legale. Cu toate acestea,

după analiza regulilor concrete de funcționare a mecanismului de interceptare a comunicațiilor electronice, instanța a ajuns la concluzia că nu există o supraveghere independentă a proceselor de selectare și căutare implicate, în mod special în cazurile în care este vorba despre intermediarii de servicii de internet și în alegerea criteriilor de selectare și căutare pentru a filtra și selecta comunicațiile interceptate pentru analiză.

Mai mult, Curtea a constatat că nu erau prevăzute în legislație garanții concrete, efective aplicabile comunicațiilor aflate în legătură cu cele selectate pentru analiză. Din acest motiv, poate apărea problema dacă unele dintre acestea ar putea dezvălui mai multe informații cu privire la obiceiurile unei persoane și contactele acesteia.

În opinia Curții, aceste lipsuri ale legislației au legătură cu cerințele de „calitate a legii", astfel cum rezultă din jurisprudența sa și în consecință, nu ar putea întruni condițiile de necesitate într-o societate democratică.

În ceea ce privește regimul juridic al schimbului de informații între serviciile de informații, Curtea a reținut că ingerința în discuție nu este reprezentată de interceptarea convorbirilor propriu-zise, ci de recepționarea materialului interceptat și stocarea, analizarea și utilizarea ulterioară de către serviciile de informații ale statului solicitat. În scopul evitării abuzurilor în această privință, se subliniază că dreptul național trebuie să prevadă circumstanțele în care pot fi solicitate materialele interceptate de către serviciile de informații străine.

Instanța europeană a constatat existența unei baze legale pentru solicitarea de informații din partea serviciilor străine și de asemenea, că aceasta era suficient de accesibilă și urmărea mai multe scopuri legitime, iar procedura ce trebuia urmată pentru solicitarea interceptărilor și pentru transmiterea informațiilor, era prevăzută cu suficientă claritate. Pentru aceste considerente, s-a constatat neîncălcarea Convenției în această privință.

În schimb, Curtea nu s-a pronunțat cu privire la aplicarea Convenției măsurilor de supraveghere extrateritorială, respectiv a persoanelor aflate în afara teritoriului Regatului Unit care sunt supuse măsurilor de supraveghere și interceptare[9].

În privința regimului din capitolul II al legii care permitea anumitor autorități să obține datele convorbirilor de la furnizorii de serviciului de

[9] M. Milanovic, *ECtHR Judgement in Big Brother Watch v. UK*, *17* September 2018, EJIL: Talk!, [Online] la https://www.ejiltalk.org/ecthr-judgment-in-big-brother-watch-v-uk/ accesat 20.10.2018.

comunicații, în analiza efectuată, Curtea a reținut că dreptul intern, prin perspectiva în care a fost interpretat de autoritățile naționale în baza hotărârilor pronunțate de Curtea de Justiție a Uniunii Europene, impunea ca orice regim care permite autorităților să acceseze datele deținute, să aibă un acces limitat la combaterea infracțiunilor grave, iar accesul să fie supus unei analize prealabile de către un tribunal sau autoritate administrativă independentă.

Aspectele pentru care s-a constatat încălcarea articolului 10 din Convenție

Reclamanții din cea de a doua cerere formulată în anul 2014, un jurnalist și o agenție de știri, au invocat existența unei ingerințe cu privire la confidențialitatea materialelor jurnalistice, din cauza regimului de prevăzut de articolului 8 alin. (4) și de Capitolul II al dispozițiilor interne.

Curtea a apreciat că măsurile de supraveghere prevăzute nu vizau monitorizarea jurnaliștilor sau dezvăluirea surselor lor de informare. Interceptarea unor comunicații ale jurnaliștilor nu poate fi caracterizată, în sine ca una deosebit de gravă în libertatea de exprimare, deoarece autoritățile află că anumite comunicații aparțin jurnaliștilor doar după ce acestea au fost deja interceptate și sunt supuse analizei.

În ceea ce privește aspectele care încalcă articolul 10 din Convenție, instanța a făcut trimitere la principiile generale în materia libertății de exprimare din jurisprudența sa și la faptul că „protejarea surselor jurnalistice constituie una dintre pietrele de temelie ale libertății presei. În lipsa unei astfel de protecții, sursele pot fi descurajate să sprijine presa în informarea publicului asupra problemelor de interes general (...)”[10].

De asemenea, Curtea a reiterat că „întotdeauna a supus garanțiile pentru respectarea libertății de exprimare unui control special. Având în vedere importanța protecției surselor jurnalistice pentru libertatea presei într-o societate democratică, o ingerință nu poate fi compatibilă cu articolul 10 din Convenție decât dacă este justificată de o cerință imperativă de interes general (...)”.[11]

[10] European Court of Human Rights, *Case of Big Brother Watch and Others v. The United Kingdom*, § 487.

[11] European Court of Human Rights, *Case of Big Brother Watch and Others v. The United Kingdom*, § 488.

În cuprinsul considerentelor, instanța a subliniat existența unei „diferențe fundamentale" între ordinul autorităților ca un jurnalist să dezvăluie identitatea surselor sale și realizarea de percheziții la domiciliul ziaristului sau la locul de muncă cu scopul de a afla identitatea surselor și a apreciat că cea din urmă măsură, chiar dacă este fără rezultat, este mai severă decât ordinul de a divulga identitatea sursei, deoarece anchetatorii care descind la locul de muncă al jurnalistului au acces la întreaga documentație a acestuia[12].

În analiza cerinței caracterului necesar al ingerințelor, Curtea a reiterat regula generală potrivit căreia o ingerință în dreptul la protejarea surselor jurnalistice poate fi compatibilă cu articolul 10 din Convenție doar dacă este justificată de o exigență superioară în interes public. Sub acest aspect, a reținut că măsurile de supraveghere prevăzute de articolul 8 (4) nu au ca scop monitorizarea surselor sau expunerea surselor jurnalistice și că, potrivit regulilor de funcționare a mecanismului de interceptare, autoritățile ar afla doar în momentul analizării interceptărilor comunicărilor dacă astfel de comunicații au fost interceptate. Prin urmare, interceptarea unor comunicațiilor ce constituie surse de informare nu poate, prin ea însăși, să fie caracterizată ca o ingerință deosebit de gravă asupra libertății de exprimare. Cu toate acestea, ingerința va fi mai gravă dacă aceste comunicații vor fi selectate pentru analiză și, în opinia Curții, ar putea fi justificate de o cerință imperativă de interes public doar dacă,, este însoțită de garanții suficiente referitoare atât la circumstanțele în care au fost în mod intenționat selecționate pentru a fi analizate, cât și la protejarea confidențialității în cazul în care au fost selectate, în mod intenționat sa nu, pentru a fi analizate. "[13].

După aplicarea principiilor generale ce rezultă din jurisprudența sa în această materie, Curtea a făcut legătura cu criticile deja exprimare față de lipsa de transparență și insuficiența criteriilor pentru căutarea și selectarea comunicațiilor pentru analiză. În contextul articolului 10, instanța a apreciat că este deosebit de îngrijorător că nu există reguli– și nici măcar cerințe «deasupra liniei de plutire» care fie să reglementeze competența serviciilor de informații de a căuta materiale confidențiale jurnalistice sau alte materiale (spre exemplu, prin folosirea adresei de e-mail a jurnalistului drept criteriu

[12] European Court of Human Rights, *Case of Big Brother Watch and Others v. The United Kingdom*, § 489.

[13] European Court of Human Rights, *Case of Big Brother Watch and Others v. The United Kingdom*, § 493.

de selectare), fie să solicite pentru persoanele care analizează materialele, să acorde o atenție deosebită dacă astfel de materiale sunt sau ar putea fi implicate. Prin urmare, pare că analiștii pot căuta și examina fără restricții atât conținutul cât și datele conexe comunicațiilor interceptate. În ceea ce privește stocarea materialelor confidențiale, odată ce au fost identificate, există garanții.[14]. Cu toate acestea, având în vedere potențialul efect inhibitor al oricărei ingerințe asupra confidențialității comunicațiilor și în mod special asupra surselor și, în absența unor reglementări care să limiteze posibilitatea serviciilor secrete de a căuta și analiza astfel de materiale, altele decât cele «justificate de o cerință imperativă de interes general», Curtea a constatat că este încălcat (și) articolul 10 din Convenție.[15]

În ceea ce privește regimul juridic al obținerii datelor de comunicații de la furnizorii de servicii de comunicații, Curtea a constatat că încalcă articolul 10 din Convenție, deoarece, chiar dacă sunt prevăzute garanții pentru situațiile în care datele sunt căutate în scopul identificării surselor jurnalistului, acestea se aplică doar pentru aceste situații, în care scopul este de a identifica o sursă; „prin urmare, nu se aplică în toate cazurile în care există o solicitare pentru datele de comunicații ale unui jurnalist sau pentru situațiile în care o ingerință colaterală este posibilă. Mai mult, în cazurile referitoare la accesul la datele de comunicații ale jurnaliștilor nu există prevederi speciale care să limiteze accesul în scopul comiterii «infracțiunilor grave». În consecință, Curtea consideră că regimul juridic nu este «în conformitate cu legea» în sensul cererii cu privire la articolul 10.”[16]

Diferențe între prezenta hotărâre și alte hotărâri

Poziția Curții Europene este mult diferită de interpretarea dată de Curtea Europeană de Justiție în 2015 în cauza *Schrems*[17], în care această instanță a stabilit că „legislația care permite autorităților naționale să aibă acces la conținutul comunicațiilor electronice trebuie să fie văzută ca

[14] European Court of Human Rights, *Case of Big Brother Watch and Others v. The United Kingdom*, § 494.
[15] European Court of Human Rights, *Case of Big Brother Watch and Others v. The United Kingdom*, § 495.
[16] European Court of Human Rights, *Case of Big Brother Watch and Others v. The United Kingdom*, §§ 496- 500.
[17] European Court of Justice, *Judgment of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v. Data Protection Commissione*r, [Online] la https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362, accesat 20.10.2018.

aducând atingere esenței dreptului fundamental la respectarea vieții private, astfel cum este garantat de articolul 7 din Carta drepturilor fundamentale a Uniunii Europene.

Curtea Europeană de Justiție s-a pronunțat și anterior în sensul că natura nediscriminatorie și foarte generală a colectării în masă și a procesării datelor personale, chiar dacă este făcută pentru a proteja împotriva infracțiunilor grave, prezintă riscuri semnificative pentru drepturile omului și libertățile fundamentale și, prin urmare, se impune ca „derogările și limitările în legătură cu protejarea datelor personale trebuie aplicate doar dacă sunt strict necesare". Pare că în analiza caracterului necesar al unei restricții contând în supravegherea în masă, instanța de la Luxemburg a adoptat o abordare mai restrictivă decât instanța de la Strasbourg în hotărârea supusă analizei.

Chiar și Curtea Europeană a Drepturilor Omului a pronunțat anterior, în 2016 o hotărâre împotriva Ungariei (*Szabo c. Ungaria*)[18], în care accentul a fost pus mai mult pe ideea protejării drepturilor fundamentale în Ungaria, care avea legislație cu privire la supravegherea secretă în scopul combaterii terorismului.

În această hotărâre, Curtea Europeană a Drepturilor Omului a reținut că atât Curtea Europeană de Justiție, cât și Raportorul Special al ONU consideră că măsurile de supraveghere secretă trebuie să respecte condiția strictă a necesității. În acest context apare întrebarea firească dacă instanța de contencios al drepturilor omului și-a modificat aprecierea în privința măsurilor de supraveghere în masă ale statelor și a acceptat posibilitatea restricționării drepturilor fundamentale.

În cauza *Big Brother* din 2018, Curtea a furnizat o interpretare diferită cu privire la necesitatea notificării supravegherii, în sensul că respinge această idee ca fiind incompatibilă cu un sistem de supraveghere generală. Anterior, în anul 2016, în hotărârea contra Ungariei, a fost considerată legată în mod inextricabil de cerința existenței unor remedii procedurale efective și a unor garanții efective împotriva abuzurilor autorităților care monitorizează procesul de supraveghere, astfel că se impune comunicarea de informații către persoana în cauză, imediat ce se

[18] European Court of Human Rights, *Case of Szabo and Vissy v. Hungary* (Application no. 37138/14), Judgement, 12 January 2016, § 73.

poate realiza notificarea fără a pune în pericol scopul restricției după terminarea măsurilor de supraveghere[19].

Concluzii

Hotărârea pronunțată la 13 septembrie 2018 trasează o situație echilibrată între protejarea securității naționale și protejarea drepturilor fundamentale, în care esențială este prevederea unor garanții suficiente la nivel național.

Considerentele Curții sunt destul de nuanțate și în unele privințe, semnificativ diferite față de jurisprudența sa anterioară. În același timp, trebuie subliniat faptul că în cursul lunii iunie a acestui an, într-o hotărâre împotriva Suediei[20], Curtea a constatat că regimul juridic instituit de legislația suedeză și practica autorităților naționale suedeze în materia interceptărilor și a supravegherii nu a încălcat Convenția și a prevăzut garanții suficiente și adecvate împotriva arbitrarului.

Relevanța deosebită a interpretării date de către Curte rezultă nu doar din faptul că este prima hotărâre pronunțată cu privire la un regim de supraveghere generală, ci și din perspectiva implicațiilor pe care le va produce în viitor, la nivelul reglementărilor interne ce ar putea fi adoptate de state, cât și al soluțiilor pe care le va pronunța această instanță[21] și cea din cadrul Uniunii Europene, cu privire la cauze în care sunt incidente și aspecte legate de datele personale.

[19] European Court of Human Rights, *Case of Szabo and Vissy v. Hungary*, § 86.

[20] European Court of Human Rights, *Case of Centrum För Rättvisa v. Sweden* (Application no. 35252/08), Judgement, 19 June 2018.

[21] Pe rolul instanței de la Strasbourg sunt înregistrate mai multe cauze care au ca obiect analizarea măsurilor de supraveghere în masă , împotriva Franței - *Assosciation confraternelle de la presse judiciaire c. France* și încă 11 cereri care privesc legislația franceză în materia măsurilor de supraveghere electronică; împotriva Austriei și împotriva Germaniei.