Fișă tematică comună

Supravegherea în masă[1]
Jurisprudența Curții Europene a Drepturilor Omului (CEDO) și a Curții de Justiție a Uniunii Europene (CJUE)

(Ultima actualizare: 28.02.2025)

Această fișă tematică a fost întocmită de grefa Curții Europene a Drepturilor Omului („CEDO")[2] și de Agenția pentru Drepturi Fundamentale a Uniunii Europene, în cadrul unui efort de colaborare pentru a evidenția jurisprudența în anumite domenii în care dreptul Uniunii Europene („UE") interacționează cu cel al Convenției europene a drepturilor omului („Convenția europeană" sau „Convenția").

I. Supravegherea în masă

Având în vedere recentele evoluții ale tehnologiei și ale societății în domeniul comunicațiilor electronice, CEDO și CJUE au fost invitate să abordeze problema riscurilor la adresa drepturilor omului care decurg din regimurile de supraveghere în masă, și anume sistemele care permit culegerea pe scară largă, prin mijloace tehnice, a informațiilor[3] din comunicațiile electronice și a informațiilor legate de aceste comunicații.

În epoca actuală, din ce în ce mai digitalizată, marea majoritate a comunicațiilor iau o formă digitală și sunt transmise prin intermediul rețelelor globale de telecomunicații, folosind o combinație a celor mai rapide și mai ieftine căi, fără niciun raport semnificativ cu frontierele naționale. Așadar, supravegherea care nu vizează direct persoane particulare are capacitatea de a avea un domeniu de aplicare foarte larg, atât pe teritoriul statului care efectuează supravegherea, cât și în afara acestuia[4].

Regimurile de supraveghere în masă pot funcționa prin accesarea, folosirea și stocarea unor volume mari de date extrase din rețelele de transmisie a comunicațiilor prin Internet (așa-numita

[1] În sensul prezentei fișe tematice, prin termenul general „supraveghere în masă" trebuie să se înțeleagă „supravegherea generală a comunicațiilor". Terminologia este discutată mai pe larg în raportul din 2017 al Agenției pentru Drepturi Fundamentale a Uniunii Europene (FRA), p. 29 *Supravegherea de către serviciile de informații: garanții și căi de atac privind drepturile fundamentale în Uniunea Europeană – volumul II: perspective dobândite din experiențe practice și observații directe, și actualizare juridică*. A se vedea, de asemenea, raportul FRA privind *Supravegherea de către serviciile de informații: Garanții și căi de atac privind drepturile fundamentale în Uniunea Europeană - actualizare din 2023 | Agenția pentru Drepturi Fundamentale a Uniunii Europene*.

[2] Conținutul acestei fișe tematice nu obligă Curtea.
Prezenta traducere este publicată cu acordul Consiliului Europei și al Curții Europene a Drepturilor Omului și reprezintă responsabilitatea exclusivă a Institutului European din România.

[3] Termenul „informații" este utilizat pentru a face referire nu doar la informații colectate de serviciile de informații, ci și la interceptarea „în masă" de informații în contextul unor proceduri penale.

[4] CEDO, *Big Brother Watch și alții împotriva Regatului Unit* (MC), nr. 58170/13 și alte 2 cereri, pct. 322, 25 mai 2021; și *Centrum för rättvisa împotriva Suediei* (MC), nr. 35252/08, pct. 236, 25 mai 2021.

„interceptare în masă”)[5]. De asemenea, acestea pot solicita furnizorilor de servicii de comunicații electronice („FSC”) să procedeze la păstrarea și stocarea generală a comunicațiilor utilizatorilor și a datelor aferente comunicațiilor[6] și să permită autorităților naționale să aibă acces la datele respective, fie în mod direct și nelimitat[7], fie pe baza unor cereri specifice[8].

Supravegherea în masă poate viza conținutul comunicațiilor electronice și/sau datele aferente comunicațiilor, inclusiv datele cu caracter personal ale abonaților și ale utilizatorilor înregistrați, precum și datele de trafic și datele de localizare. Obținerea de date privind comunicațiile nu este în mod necesar mai puțin intruzivă decât obținerea conținutului comunicațiilor, întrucât datele de trafic și datele de localizare, considerate în ansamblu, pot permite deducerea unor concluzii foarte precise cu privire la viața privată a persoanelor, inclusiv cu privire la obiceiurile acestora, locurile de ședere permanente sau temporare, deplasările zilnice, activitățile desfășurate, relațiile lor personale și mediile sociale frecventate de ele[9]. În ceea ce privește conținutul comunicațiilor electronice, pot apărea o serie de probleme atunci când interceptarea în masă de informații, păstrarea informațiilor și accesul la acestea includ încercări ale autorităților naționale de a decripta mesajele electronice criptate[10].

II. Supravegherea în masă în jurisprudența CJUE

CJUE a examinat regimurile de supraveghere în masă în principal din perspectiva protecției oferite datelor cu caracter personal și dreptului la confidențialitate de Directiva asupra confidențialității și comunicațiilor electronice[11] și de Regulamentul general privind protecția datelor („RGPD”)[12], interpretate în lumina drepturilor fundamentale garantate de articolul 7 (respectarea vieții private și de familie), articolul 8 (protecția datelor cu caracter personal) și articolul 11 (libertatea de exprimare) din Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „Carta”)[13].

În cazuri specifice legate de funcționarea regimurilor de supraveghere în masă, CJUE a furnizat, de asemenea, orientări cu privire la interpretarea altor instrumente juridice ale UE, citite în lumina

[5] A se vedea, de exemplu, *Big Brother Watch*, citată anterior, pct. 15, și, mai general, jurisprudența descrisă mai jos la punctul A.

[6] A se vedea, de exemplu, CEDO, *Podciasov împotriva Rusiei*, nr. 33696/19, 13 februarie 2024 și, mai general, jurisprudența descrisă mai jos la punctul B.

[7] A se vedea, de exemplu, CEDO, *Pietrzak și Bychawska-Siniarska și alții împotriva Poloniei*, nr. 72038/17 și 25237/18, 28 mai 2024.

[8] A se vedea, de exemplu, CEDO, *Ben Faiza împotriva Franței*, nr. 31446/12, 8 februarie 2018, și *Škoberne împotriva Sloveniei*, nr. 19920/20, 15 februarie 2024; CJUE, Hotărârea din 2 martie 2021, *Prokuratuur*, C-746/18, EU:C:2021:152, Hotărârea din 5 aprilie 2022, *Commissioner of An Garda Síochána și alții*, C-140/20, EU:C:2022:258, Hotărârea din 17 noiembrie 2022, *Spetsializirana prokuratura*, C-350/21, EU:C:2022:896.

[9] CJUE, Hotărârea din 8 aprilie 2014, *Digital Rights Ireland și alții*, C-293/12 și C 594/12, EU:C:2014:238, pct. 27; CEDO, *Big Brother Watch*, citată anterior, pct. 342.

[10] CJUE, Hotărârea din 30 aprilie 2024, *M.N. (EncroChat)*, C-670/22, EU:C:2024:372; CEDO, *Podciasov împotriva Rusiei*, citată anterior.

[11] 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.

[12] 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/CE.

[13] Vă rugăm să consultați jurisprudența CJUE descrisă mai jos, în secțiunile C.1 și C.2.

drepturilor fundamentale enumerate mai sus, de exemplu în contextul cooperării judiciare în materie penală și al ordinului european de anchetă[14] sau al combaterii abuzului de piață[15].

III. Supravegherea în masă în jurisprudența Curții Europene a Drepturilor Omului (CEDO)

CEDO a examinat regimurile de supraveghere în masă în principal din perspectiva dreptului la respectarea vieții private[16] și a corespondenței (art. 8 din Convenția europeană), precum și a dreptului la libertatea de exprimare (art. 10 din Convenția europeană), în legătură cu protecția comunicațiilor jurnaliștilor.

În ceea ce privește art. 8 din Convenția europeană, pe baza jurisprudenței sale privind regimurile de supraveghere secretă care permit măsuri de supraveghere specifice[17], CEDO a reiterat faptul că, în contextul special al măsurilor de supraveghere secretă, „previzibilitatea" înseamnă că legislația națională trebuie să fie suficient de clară pentru a oferi cetățenilor indicații adecvate cu privire la circumstanțele și condițiile în care autoritățile publice sunt împuternicite să recurgă la astfel de măsuri și trebuie să indice domeniul de aplicare al marjei de apreciere conferite autorităților și modul de exercitare a acesteia într-un mod suficient de clar încât să ofere persoanelor o protecție adecvată împotriva ingerințelor arbitrare[18].

De asemenea, aceasta a reiterat faptul că, în cazul în care legislația prin care se autorizează supravegherea secretă este contestată în fața CEDO, este oportun să se examineze împreună criteriile potrivit cărora măsura în cauză trebuie să fie „prevăzută de lege" și „necesară". Dreptul intern trebuie să fie nu doar accesibil și previzibil în ceea ce privește aplicarea sa, dar trebuie, în plus, să garanteze că măsurile de supraveghere secretă sunt aplicate numai atunci când sunt „necesare într-o societate democratică", în special prin furnizarea unor garanții suficiente și efective împotriva abuzurilor[19].

În ceea ce privește garanțiile care ar trebui să fie incluse într-un regim de supraveghere în masă conform cu dispozițiile Convenției, CEDO a considerat că este necesar ca garanțiile prevăzute în jurisprudența anterioară cu privire la regimurile de interceptare țintită să fie dezvoltate și adaptate la

[14] Directiva 2014/41/UE a Parlamentului European și a Consiliului din 3 aprilie 2014 privind ordinul european de anchetă în materie penală; a se vedea CJUE, *M.N. (EncroChat)*, citată anterior.

[15] Directiva 2003/6/CE a Parlamentului European și a Consiliului din 28 ianuarie 2003 privind utilizările abuzive ale informațiilor confidențiale și manipulările pieței („Directiva privind abuzul de piață") și Regulamentul (UE) nr. 596/2014 al Parlamentului European și al Consiliului din 16 aprilie 2014 privind abuzul de piață (Regulamentul privind abuzul de piață); a se vedea CJUE, Hotărârea din 20 septembrie 2022, *VD și SR*, C-339/20 și C-397/20, EU:C:2022:703.

[16] Pentru a evalua ingerințele în exercitarea dreptului la respectarea vieții private care decurg din regimurile de supraveghere în masă, Curtea s-a bazat, de asemenea, pe alte instrumente juridice ale Consiliului Europei, cum ar fi Convenția din 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal și Protocolul adițional din 8 noiembrie 2001 la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, cu privire la autoritățile de control și fluxul transfrontalier al datelor; Recomandarea nr. R (95) 4 a Comitetului de Miniștri privind protecția datelor cu caracter personal în domeniul serviciilor de telecomunicații (adoptată la 7 februarie 1995) și Raportul din 2015 al Comisiei Europene pentru Democrație prin Drept privind controlul democratic al serviciilor de informații care folosesc sisteme de colectare a informațiilor de tip SIGINT.

[17] A se vedea, de exemplu, CEDO, *Roman Zaharov împotriva Rusiei* (MC), nr. 47143/06, pct. 227-234, CEDO 2015, și jurisprudența citată.

[18] A se vedea, de exemplu, CEDO, *Big Brother Watch*, citată anterior, pct. 333.

[19] *Ibid.*, pct. 334.

particularitățile interceptării în masă a comunicațiilor[20], precum și la accesul la datele aferente comunicațiilor și păstrarea generală a acestora[21].

În ceea ce privește art. 10 din Convenția europeană, CEDO s-a bazat pe jurisprudența sa existentă cu privire la percheziții efectuate la domiciliul sau locul de muncă al unui jurnalist, adaptând garanțiile materiale și procedurale prevăzute de acest articol la contextul interceptării în masă[22] și al păstrării generale a datelor[23]. Aceasta a făcut distincție, în special, în ceea ce privește garanțiile care ar trebui să fie incluse într-un regim de supraveghere în masă conform cu dispozițiile Convenției, între cazurile în care ingerința în exercitarea de către jurnaliști a libertății de exprimare este intenționată și cazurile în care comunicațiile jurnalistice sau datele aferente comunicațiilor nu au fost selectate în mod deliberat spre examinare, cu condiția să devină evident, în etapa examinării, că respectivele comunicații sau date aferente comunicațiilor conțin materiale jurnalistice confidențiale[24].

IV. Jurisprudența Curții de Justiție a Uniunii Europene (CJUE) și a Curții Europene a Drepturilor omului (CEDO) privind supravegherea în masă

A. Regimuri de interceptare în masă

CJUE, Hotărârea din 6 octombrie 2020, *Privacy International*, C-623/17, EU:C:2020:790

În fapt – La începutul anului 2015, a fost făcută publică existența unor practici de achiziționare și utilizare, de către diverse agenții de securitate și de informații din Regatul Unit, a datelor referitoare la comunicații colectate în masă (*bulk communications data*). În temeiul regimului în litigiu, ministrul (the Secretary of State) putea solicita furnizorilor de servicii de comunicații electronice (FSC), atunci când considera că este necesar în interesul securității naționale sau al relațiilor cu un guvern străin, să transmită agenților de securitate și de informații date referitoare la comunicații colectate în masă (inclusiv date de trafic și date de localizare, precum și informații privind serviciile utilizate). O asemenea comunicare prin transmiterea datelor îi privea pe toți utilizatorii mijloacelor de comunicații electronice. Odată transmise, aceste date erau păstrate de agențiile de securitate și de informații și rămâneau la dispoziția acestora din urmă în scopul desfășurării activităților lor, la fel ca în cazul celorlalte baze de date administrate de aceste agenții. În special, datele astfel colectate, care erau supuse prelucrării și analizelor de masă și automate, puteau fi verificate încrucișat cu alte baze de date care conțineau diferite categorii de date cu caracter personal colectate în masă sau puteau fi divulgate în afara acestor agenții și unor state terțe. Aceste operațiuni nu erau condiționate de autorizarea prealabilă a unei instanțe sau a unei autorități administrative independente și nu implicau informarea în vreun fel a persoanelor vizate.

Privacy International, o organizație neguvernamentală, a sesizat Investigatory Powers Tribunal (Tribunalul cu competențe de investigare, Regatul Unit, denumit în continuare „IPT”) pentru a contesta legalitatea acestor practici. IPT a constatat că, având în vedere declarațiile pârâților din litigiu, în care au recunoscut activitățile agenților de securitate și de informații în cauză, regimul în discuție era conform cu art. 8 din Convenția europeană. Cu toate acestea, instanța a identificat următoarele patru cerințe, care păreau să rezulte din Hotărârea *Tele2 Sverige și Watson și alții*, pronunțată de CJUE, și care păreau să depășească cerințele art. 8 din Convenția europeană: o restricție privind accesul nespecific la date colectate în masă; necesitatea obținerii unei autorizări

[20] CEDO, *Big Brother Watch*, citată anterior, pct. 340-347; *Centrum för rättvisa*, citată anterior, pct. 254-261.
[21] CEDO, *Ekimdjiev și alții împotriva Bulgariei*, nr. 70078/12, pct. 394-395, 11 ianuarie 2022.
[22] CEDO, *Big Brother Watch*, citată anterior, pct. 447-450.
[23] CEDO, *Big Brother Watch*, citată anterior, pct. 524-525 și 528.
[24] CEDO, *Big Brother Watch*, citată anterior, pct. 447.

prealabile (cu excepția cazurilor de urgență stabilite în mod valabil) înainte ca datele să poată fi accesate; dispoziții privind notificarea ulterioară a persoanelor afectate; și păstrarea tuturor datelor în cadrul UE.

La 30 octombrie 2017, IPT a sesizat CJUE cu o cerere de decizie preliminară în scopul de a clarifica măsura în care cerințele din hotărârea *Watson* s-ar putea aplica în cazul în care tehnicile de obținere în masă și de prelucrare automată erau necesare pentru a proteja securitatea națională.

În drept – CJUE a constatat că o reglementare națională care permite unei autorități a statului să impună furnizorilor de servicii de comunicații electronice să transmită agenților de securitate și de informații date de trafic și date de localizare în vederea apărării securității naționale intră în domeniul de aplicare al Directivei asupra confidențialității și comunicațiilor electronice. Interpretarea acestei directive trebuie să țină seama de drepturile garantate de articolele 7, 8 și 11 din Cartă. Restrângerile exercițiului acestor drepturi trebuie să fie prevăzute de lege, să respecte substanța drepturilor respective, să respecte principiul proporționalității, să fie necesare și să răspundă efectiv obiectivelor de interes general recunoscute de Uniune sau necesității protejării drepturilor și libertăților celorlalți. În plus, limitările privind protecția datelor cu caracter personal trebuie să fie aplicate în limitele strictului necesar; și, pentru a respecta cerința proporționalității, reglementarea trebuie să prevadă norme clare și precise care să reglementeze conținutul și aplicarea măsurii respective și să impună o serie de cerințe minime, astfel încât persoanele ale căror date cu caracter personal sunt vizate să dispună de garanții suficiente care să permită protejarea în mod eficient a acestor date împotriva riscurilor de abuz.

În opinia CJUE, o reglementare națională care impune furnizorilor de servicii de comunicații electronice să transmită în mod generalizat și nediferențiat date de trafic și date de localizare agenților de securitate și de informații – transmitere de date care privește în mod global toate persoanele care utilizează servicii de comunicații electronice – depășește limitele strictului necesar și nu poate fi considerată justificată într-o societate democratică, astfel cum se prevede în Directiva asupra confidențialității și comunicațiilor electronice, interpretată în lumina Cartei.

CEDO, *Big Brother Watch și alții împotriva Regatului Unit* (MC), nr. 58170/13 și alte 2, 25 mai 2021

În fapt – Cauza privea compatibilitatea cu art. 8 și 10 din Convenția europeană a regimului de supraveghere secretă din Regatul Unit, astfel cum era în vigoare la 7 noiembrie 2017, care reglementa:

I) interceptarea în masă a conținutului comunicațiilor și a datelor aferente comunicațiilor;

II) primirea de informații de la servicii de informații străine;

III) obținerea de date privind comunicațiile de la FSC.

În drept – **Cu privire la punctul I), art. 8 din Convenția europeană:** reclamanții s-au plâns că interceptarea în masă a comunicațiilor transfrontaliere de către serviciile de informații a încălcat art. 8.

În ceea ce privește existența unei ingerințe, CEDO a considerat interceptarea în masă ca fiind un proces gradual, în care gradul de ingerință în drepturile persoanelor particulare în temeiul art. 8 crește pe măsură ce procesul avansează. Acest proces are patru etape:

(a) interceptarea și păstrarea inițială a comunicațiilor și a datelor aferente comunicațiilor;

(b) aplicarea unor selectori specifici comunicațiilor păstrate/datelor aferente comunicațiilor păstrate;

(c) examinarea de către analiști a comunicațiilor selectate/datelor aferente comunicațiilor selectate;

(d) păstrarea ulterioară a datelor și utilizarea „produsului final”, inclusiv schimbul de date cu terții.

Deși interceptarea inițială, urmată de eliminarea imediată a unor părți ale comunicațiilor, nu a constituit o ingerință deosebit de semnificativă, gradul de ingerință în drepturile persoanelor în temeiul art. 8 a crescut pe măsură ce procesul de interceptare în masă a progresat.

În ceea ce privește principiile relevante aplicabile cauzelor având ca obiect interceptarea în masă, CEDO a făcut referire la jurisprudența sa anterioară cu privire la regimurile de interceptare țintită, afirmând că, deși statele beneficiază de o marjă largă de apreciere pentru a decide ce tip de regim de interceptare este necesar pentru a proteja securitatea națională și alte interese naționale esențiale împotriva amenințărilor externe grave, pentru operarea unui astfel de sistem, marja de apreciere care le este acordată trebuie să fie mai restrânsă și trebuie să existe o serie de garanții. Aceasta a considerat că garanțiile identificate în contextul regimurilor de interceptare țintită trebuie să fie adaptate pentru a reflecta caracteristicile specifice ale unui regim de interceptare în masă și, în special, gradul tot mai mare de intruziune în drepturile persoanelor particulare în temeiul art. 8, pe măsură ce operațiunea trece prin etapele identificate mai sus.

Atunci când a apreciat dacă statele au acționat în limitele marjei lor de apreciere, CEDO a examinat coroborat criteriile conform cărora măsurile trebuie să fie „prevăzute de lege” și „necesare” și a efectuat o evaluare globală pentru a stabili dacă cadrul juridic intern a definit în mod clar:

1. motivele pentru care putea fi autorizată interceptarea în masă;

2. circumstanțele în care comunicațiile unei persoane puteau fi interceptate;

3. procedura care trebuia urmată pentru acordarea autorizației;

4. procedurile care trebuiau urmate pentru selectarea, examinarea și utilizarea materialelor interceptate;

5. măsurile de precauție care trebuiau luate la comunicarea materialelor către alte părți;

6. limitele privind durata interceptării, stocarea materialelor interceptate și circumstanțele în care aceste materiale puteau fi șterse și distruse;

7. procedurile și modalitățile de supraveghere de către o autoritate independentă a respectării garanțiilor de mai sus și competențele acesteia de a soluționa cazurile de nerespectare;

8. procedurile de control *ex post facto* independent al respectării garanțiilor și competențele conferite organului abilitat să soluționeze cazurile de nerespectare.

În special în ceea ce privește măsurile de precauție care trebuie luate atunci când materialele interceptate sunt comunicate altor părți, CEDO a precizat că transmiterea de materiale către state străine sau organizații internaționale ar trebui să se limiteze la materialele colectate și stocate în conformitate cu Convenția și ar trebui să facă obiectul unor garanții suplimentare referitoare la transferul în sine. Mai întâi, circumstanțele în care poate avea loc un astfel de transfer trebuie să fie precizate în mod clar în dreptul intern. În al doilea rând, statul care efectuează transferul trebuie să se asigure că, în cadrul prelucrării datelor, statul destinatar dispune de garanții de natură să prevină abuzurile și ingerințele disproporționate. În special, statul destinatar trebuia să garanteze stocarea în condiții de siguranță a materialelor și să restricționeze divulgarea ulterioară a acestora. Aceasta nu înseamnă neapărat că statul destinatar trebuie să beneficieze de protecție comparabilă cu cea a statului care face transferul și nici nu impune în mod necesar să fie oferită o garanție înainte de fiecare transfer. În al treilea rând, vor fi necesare garanții sporite pentru transmiterea de materiale care necesită o confidențialitate specială, cum ar fi materialele jurnalistice confidențiale.

În plus, transferul de materiale către servicii de informații partenere străine ar trebui, de asemenea, să facă obiectul unui control independent.

În ceea ce privește măsurile de precauție care trebuie luate pentru obținerea datelor aferente comunicațiilor prin interceptarea în masă, CEDO a subliniat că aceste date pot fi analizate și interogate astfel încât să prezinte o imagine intimă a unei persoane prin cartografierea rețelelor de socializare, urmărirea locației, urmărirea navigării pe Internet, cartografierea modelelor de comunicare și cunoașterea persoanelor cu care a interacționat respectiva persoană. Aceasta a considerat că interceptarea, păstrarea și căutarea datelor aferente comunicațiilor trebuie analizată în raport cu aceleași garanții precum cele aplicabile conținutului, chiar dacă dispozițiile legale care reglementează tratamentul acestora nu trebuie în mod necesar să fie identice în toate privințele cu cele care reglementează tratamentul conținutului.

Aplicând aceste principii în speță, CEDO a considerat că regimul de supraveghere secretă din Regatul Unit, în pofida măsurilor de protecție pe care le prevedea, nu conținea suficiente garanții „de la un capăt la altul" (*„end-to-end" safeguards*, măsuri de protecție a datelor în toate etapele utilizării lor) pentru a oferi garanții adecvate și eficiente împotriva arbitrarului și a riscului de abuzuri. Aceasta a identificat următoarele deficiențe fundamentale ale regimului: lipsa unei autorizații independente, neincluderea categoriilor de selectori în cererea de emitere a mandatului și lipsa autorizării interne prealabile a selectorilor legați de o persoană. Aceste deficiențe priveau nu numai interceptarea conținutului comunicațiilor, ci și interceptarea datelor aferente comunicațiilor. Deși Comisarul independent pentru Interceptarea Comunicațiilor („Comisarul IC") asigura o supraveghere independentă și eficientă a regimului, iar IPT oferea o cale de atac solidă oricărei persoane care suspecta că serviciile de informații au interceptat comunicațiile sale, aceste garanții importante nu erau suficiente pentru a contrabalansa deficiențele evidențiate anterior.

Cu privire la punctul I), art. 10 din Convenția europeană: reclamanții s-au plâns că regimul de interceptare în masă încălca art. 10 deoarece avea un efect de descurajare asupra libertății de comunicare a jurnaliștilor.

CEDO a făcut distincție între accesarea intenționată de către serviciile de informații a unor materiale jurnalistice confidențiale, prin utilizarea deliberată a selectorilor sau a termenilor de căutare legați de un jurnalist sau de o organizație de știri, și accesarea neintenționată a unor astfel de materiale, ca o „captură accidentală" a operațiunii de interceptare în masă. În primul scenariu, CEDO a considerat că ingerința ar trebui să fie proporțională cu cea ocazionată de percheziția domiciliului sau a locului de muncă al unui jurnalist și a afirmat că selectorii sau termenii de căutare trebuie să fi fost autorizați de o instanță sau de un alt organ decizional independent și imparțial învestit cu competența de a stabili dacă acestea erau „justificate de o cerință imperativă de interes public" și, în special, dacă o măsură mai puțin intruzivă ar fi fost suficientă pentru a servi interesului public imperativ. În cel de al doilea scenariu, CEDO a considerat că gradul de ingerință în comunicațiile și/sau sursele jurnalistice nu putea fi prevăzut de la bun început. În consecință, nu ar fi posibil ca, în etapa autorizării, o instanță sau un alt organ independent să evalueze dacă o astfel de ingerință ar fi justificată. Cu toate acestea, CEDO a considerat, de asemenea, că, având în vedere evoluțiile tehnologice din ultimii ani, supravegherea care nu vizează direct persoane particulare are capacitatea de a avea un domeniu de aplicare foarte larg. Prin urmare, întrucât examinarea de către un analist a comunicațiilor unui jurnalist sau a datelor aferente comunicațiilor unui jurnalist ar putea conduce la identificarea unor surse, CEDO a considerat că este imperativ ca dreptul intern să conțină garanții solide în ceea ce privește stocarea, examinarea, utilizarea, transmiterea ulterioară și distrugerea unor astfel de materiale confidențiale. În plus, în cazul în care și atunci când devine evident că și comunicațiile sau datele aferente comunicațiilor conțin materiale jurnalistice confidențiale, continuarea stocării și examinării lor de către un analist ar trebui să fie posibilă numai dacă este autorizată de un judecător sau de un alt organ decizional independent și imparțial, abilitat

să stabilească dacă continuarea stocării și examinării este „justificată de o cerință imperativă de interes public”.

Aplicând aceste principii în speță, CEDO a considerat că respectivul cadru juridic al Regatului Unit privind stocarea, transmiterea ulterioară și distrugerea materialelor jurnalistice confidențiale oferea garanții adecvate. Totuși, acesta nu a soluționat deficiențele identificate de CEDO în analiza sa privind regimul în cauză din perspectiva art. 8 și nici nu îndeplinea cerința care impunea ca utilizarea selectorilor sau a termenilor de căutare despre care se știa că aveau legătură cu un jurnalist să fie autorizată de o instanță sau de un alt organ decizional independent și imparțial abilitat să stabilească dacă această utilizare era „justificată de o cerință imperativă de interes public” și dacă o măsură mai puțin intruzivă ar fi putut fi suficientă pentru a servi interesului public imperativ. În plus, nu existau garanții suficiente pentru a se asigura faptul că, odată ce a devenit evident că o comunicație, care nu fusese selectată spre examinare prin utilizarea deliberată a unui selector sau a unui termen de căutare despre care se știa că avea legătură cu un jurnalist, conținea totuși materiale jurnalistice confidențiale, această comunicație putea fi stocată și examinată în continuare de către un analist numai dacă acest lucru era autorizat de o instanță sau de un alt organ decizional independent și imparțial abilitat să stabilească dacă continuarea stocării și examinării comunicației respective era „justificată de o cerință imperativă de interes public”.

Cu privire la punctul II), art. 8: Reclamanții s-au plâns în principal de primirea de către autoritățile naționale, de la servicii de informații străine, a unor materiale interceptate solicitate.

CEDO a considerat că, în cazul în care o cerere de interceptare a unor informații este adresată unui stat necontractant, cererea trebuie să aibă un temei în dreptul intern, iar legea trebuie să fie accesibilă persoanei în cauză și previzibilă în ceea ce privește efectele sale. De asemenea, va fi necesar să existe norme detaliate și clare, care să ofere resortisanților indicații adecvate cu privire la circumstanțele și condițiile în care autoritățile sunt abilitate să facă o astfel de cerere și care să prevadă garanții efective împotriva folosirii acestei competențe pentru a eluda dreptul intern și/sau obligațiile ce revin statelor în temeiul Convenției europene.

În ceea ce privește a doua etapă (primirea materialului interceptat), statul destinatar trebuie să dispună de garanții suficiente pentru examinarea, utilizarea și stocarea acestui material, pentru transmiterea sa ulterioară, precum și pentru ștergerea și distrugerea sa. În plus, orice regim care le permite serviciilor de informații să solicite, din partea statelor necontractante, fie interceptarea unor materiale, fie transmiterea unor materiale interceptate sau accesul direct la astfel de materiale ar trebui să facă obiectul unei supravegheri independente și ar trebui să existe, de asemenea, posibilitatea unui control *ex post facto* independent.

Aplicând aceste principii în speță, CEDO a considerat că, în cadrul juridic al Regatului Unit, existau norme detaliate și clare, care le ofereau resortisanților indicații adecvate cu privire la circumstanțele și condițiile în care autoritățile erau abilitate să adreseze o astfel de cerere unui serviciu de informații străin; dreptul intern conținea garanții efective împotriva utilizării unor astfel de cereri pentru a eluda dreptul intern și/sau dispozițiile Convenției; Regatul Unit a instituit garanții adecvate pentru examinarea, utilizarea, stocarea, transmiterea ulterioară, ștergerea și distrugerea materialelor; și regimul făcea obiectul unei supravegheri independente efectuate de către Comisarul IC și exista posibilitatea unui control *ex post facto,* efectuat de IPT.

Cu privire la punctul II), art. 10: Reclamanții s-au plâns că regimul schimbului de informații le-a încălcat drepturile care le reveneau în temeiul art. 10. CEDO a considerat că acest argument nu ridica nicio problemă separată, în plus față de cea care decurgea din art. 8.

Cu privire la punctul III): a se vedea punctul C de mai jos.

Concluzie – Încălcarea art. 8 și 10 din Convenția europeană în ceea ce privește interceptarea în masă. Neîncălcarea art. 8 și 10 din CEDO în ceea ce privește primirea de informații de la servicii de informații străine.

CEDO, *Centrum för rättvisa împotriva Suediei* (MC), nr. 35252/08, 25 mai 2021

În fapt – Această cauză privea compatibilitatea cu art. 8 a regimului suedez de colectare de informații de tip SIGINT, astfel cum era în vigoare în mai 2018, în special interceptarea în masă a comunicațiilor transfrontaliere, inclusiv a conținutului comunicațiilor și a datelor aferente comunicațiilor.

Reclamanta s-a plâns în principal de faptul că legislația și practicile naționale privind interceptarea în masă a comunicațiilor încălcau art. 8 din Convenția europeană.

În drept – Prin aplicarea principiilor enunțate în hotărârea *Big Brother Watch,* citată anterior, CEDO s-a convins de faptul că principalele caracteristici ale regimului suedez de interceptare în masă îndeplineau cerințele Convenției europene privind accesibilitatea și previzibilitatea legii și a considerat că acest regim funcționa, în majoritatea privințelor, în limitele a ceea ce este „necesar într-o societate democratică”. Totuși, a identificat trei deficiențe ale regimului: absența unei reguli clare privind distrugerea materialelor interceptate care nu conțineau date cu caracter personal; absența, în legislația relevantă, a unei cerințe potrivit căreia, atunci când era luată decizia de a transmite materiale interceptate serviciilor partenere străine, erau luate în considerare interesele legate de viața privată a persoanelor; și absența unui control *ex post facto* efectiv.

Concluzie – Încălcarea art. 8 din Convenția europeană.

CEDO, *Wieder și Guarnieri împotriva Regatului Unit*, nr. 64371/16 și 64407/16, 12 septembrie 2023

În fapt – Reclamanții, persoane particulare cu reședința în afara statului pârât, s-au plâns în principal de compatibilitatea cu art. 8 din Convenția europeană a regimului de interceptare în masă din Regatul Unit.

În drept – Principala problemă juridică ridicată în prezenta cauză a fost aceea de a stabili dacă, în scopul formulării unui capăt de cerere în temeiul art. 8, (se consideră că) persoanele din afara unui stat contractant se află sub jurisdicția teritorială a acestuia în cazul în care comunicațiile electronice ale acestor persoane fac (sau riscă să facă) obiectul unor căutări efectuate de agenții de informații ale acestui stat, care își desfășoară activitatea pe teritoriul acestuia, și sunt (sau riscă să fie) interceptate și examinate de către aceste agenții.

Având în vedere că, în mod evident, ingerința în confidențialitatea comunicațiilor are loc pe teritoriul unde aceste comunicații sunt interceptate, căutate, examinate și utilizate și că atingerea adusă dreptului la viață privată, care rezultă din această ingerință, are loc tot pe teritoriul respectiv, CEDO a considerat că ingerința în drepturile reclamanților prevăzute la art. 8 a avut loc în Regatul Unit și că, prin urmare, intra în jurisdicția teritorială a statului pârât.

În ceea ce privește fondul capătului de cerere, CEDO s-a întemeiat pe concluziile stabilite în hotărârea *Big Brother Watch,* citată anterior.

Concluzie – Încălcarea art. 8 din Convenția europeană.

CJUE, Hotărârea din 30 aprilie 2024, *M.N. (EncroChat)*, C-670/22, EU:C:2024:372

În fapt – În cadrul unei investigații efectuate de autoritățile franceze, s-a constatat că persoanele acuzate foloseau telefoane mobile criptate, care funcționau cu o licență denumită „EncroChat", pentru a săvârși infracțiuni legate în principal de traficul de stupefiante. Aceste telefoane mobile permiteau, datorită unui software special și unui hardware modificat, ca, prin intermediul unui server instalat la Roubaix (Franța), să se stabilească o comunicație criptată „end-to-end", care nu putea fi interceptată prin metode de investigație tradiționale (denumit „serviciul EncroChat"). Cu autorizarea unui judecător, un software de tip „troian" a fost încărcat pe serverul respectiv în primăvara anului 2020 și, de acolo, a fost instalat pe telefoanele mobile menționate, prin intermediul unei actualizări simulate. Din totalul de 66 134 de utilizatori înregistrați, 32 477 de utilizatori, din 122 de țări, dintre care aproximativ 4 600 din Germania, ar fi fost vizați de acest software. Reprezentanții autorităților franceze și neerlandeze i-au informat pe reprezentanții autorităților celorlalte state membre cu privire la investigația pe care o desfășurau. Reprezentanții autorităților germane și-au exprimat interesul pentru datele utilizatorilor germani. Oficiul Federal al Poliției Judiciare (*Bundeskriminalamt*, „BKA") a anunțat că deschide o investigație împotriva unui grup necunoscut de utilizatori ai serviciului EncroChat pentru trafic prezumat de stupefiante în grup organizat și în cantități deloc neglijabile și constituire a unui grup infracțional organizat. La 2 iunie 2020, Parchetul General din Frankfurt a solicitat autorităților franceze, prin intermediul unui prim ordin european de anchetă, autorizarea de a utiliza, în cadrul unei proceduri penale, datele provenite de la serviciul EncroChat.

În cadrul procedurii penale inițiate împotriva lui M.N., instanța națională a solicitat pronunțarea unei decizii preliminare cu privire la mai multe aspecte procedurale și materiale ale compatibilității acestor ordine europene de anchetă cu dreptul Uniunii Europene, inclusiv să se stabilească dacă și, după caz, în ce condiții articolul 6 alineatul (1) din Directiva privind ordinul european de anchetă (în materie penală) se opunea ca un procuror să adopte un ordin european de anchetă care viza transmiterea de probe aflate deja în posesia autorităților competente ale statului executant, atunci când aceste probe au fost obținute în urma interceptării de către aceste autorități, pe teritoriul statului emitent, a telecomunicațiilor tuturor utilizatorilor de telefoane mobile care permiteau, datorită unui software special și unui hardware modificat, o comunicație criptată end-to-end.

În drept – CJUE a statuat că legalitatea ordinelor europene de anchetă în discuție era supusă aceloraşi condiții precum cele aplicabile, dacă era cazul, transmiterii unor astfel de date într-o situație pur internă din statul emitent. În consecință, dacă dreptul statului emitent condiționa această transmitere de existența unor indicii concrete privind săvârșirea unor infracțiuni grave de către persoana acuzată sau de admisibilitatea probelor reprezentate de datele în cauză, adoptarea unui ordin european de anchetă era supusă tuturor acestor condiții. În schimb, articolul 6 alineatul (1) litera (b) din Directiva privind ordinul european de anchetă nu impunea, nici într-o situație precum cea în discuție în litigiul principal, în care datele în cauză au fost colectate de autoritățile competente ale statului executant de pe teritoriul statului emitent și în interesul acestuia, ca emiterea unui ordin european de anchetă care vizează transmiterea de probe aflate deja în posesia autorităților competente ale statului executant să fie supusă aceloraşi condiții de fond precum cele aplicate în statul emitent în materie de strângere a acestor probe.

CJUE a remarcat în această privință că ordinul european de anchetă este un instrument care ține de cooperarea judiciară în materie penală și care se întemeiază pe principiul recunoașterii reciproce a hotărârilor judecătorești și a deciziilor judiciare, precum și pe prezumția refragabilă că celelalte state membre respectă dreptul Uniunii Europene și în special drepturile fundamentale. Prin urmare, autoritatea care emite un ordin european de anchetă nu este autorizată să controleze regularitatea procedurii distincte prin care statul executant a strâns probele a căror transmitere se solicită.

CJUE a reamintit, de asemenea, că, în temeiul articolului 14 alineatul (1) din Directiva 2014/41 , statele membre se asigură că măsurilor de investigare indicate în ordinul european de anchetă le sunt aplicabile căile de atac echivalente celor disponibile într-o cauză internă similară și, în acest context, instanța competentă trebuie să verifice dacă sunt îndeplinite condițiile pentru emiterea unui ordin european de anchetă, și anume dacă emiterea ordinului este necesară și proporțională față de scopul procedurilor penale inițiate în statul emitent și dacă măsurile de investigare indicate în ordinul european de anchetă ar fi putut fi dispuse în aceleași condiții într-o cauză internă similară.

În cele din urmă, CJUE a statuat că, în cadrul unei proceduri penale inițiate împotriva unei persoane bănuite de acte de infracționalitate, judecătorul penal național trebuie să înlăture informațiile și probele obținute prin intermediul ordinului european de anchetă dacă respectiva persoană nu este în măsură să pună în discuție în mod eficient aceste informații și aceste probe și dacă ele pot influența în mod preponderent aprecierea faptelor.

CEDO, *A.L. și E.J. împotriva Franței (dec.)*, nr. 44715/20 și 47930/21, 24 septembrie 2024

În fapt – Cererile se referă la colectarea de către autoritățile franceze a datelor privind utilizatorii de telefoane mobile criptate, care funcționau cu o licență denumită „EncroChat", și la transmiterea acestora către autoritățile de aplicare a legii din Regatul Unit. Reclamanții au făcut obiectul unor proceduri penale în Regatul Unit, în două cauze separate în care au fost acuzați că au utilizat EncroChat. Aceștia au invocat art. 8, separat și coroborat cu art. 13 și art. 6 din Convenție.

În drept – Pornind de la principiile enunțate în hotărârea *Wieder și Guarnieri,* citată anterior, CEDO a statuat că colectarea, stocarea și transmiterea datelor către autoritățile britanice au avut loc în Franța și, prin urmare, ingerința în drepturile reclamanților prevăzute la art. 8 intra în jurisdicția teritorială a statului pârât. CEDO a constatat că această concluzie era conformă cu jurisprudența CJUE [Hotărârea *M.N. (EncroChat),* citată anterior], în temeiul căreia principiul recunoașterii reciproce a hotărârilor judecătorești și a deciziilor judiciare împiedica autoritatea emitentă a unui ordin european de anchetă să controleze regularitatea procedurii distincte prin care statul executant a strâns probele a căror transmitere se solicită.

În ceea ce privește epuizarea căilor de atac interne, CEDO a considerat că nici faptul că reclamanții locuiau în afara teritoriului francez, nici faptul că aceștia nu au ales în mod voluntar să se plaseze sub jurisdicția acestui stat nu îi scutea de obligația de a epuiza căile de atac interne disponibile în statul respectiv. CEDO a constatat că, în ordinea juridică internă, existau dispoziții de punere în aplicare a articolului 14 din Directiva 2014/41, potrivit căruia statele membre trebuie să se asigure că măsurilor de investigare indicate în ordinul european de anchetă le sunt aplicabile căile de atac echivalente celor disponibile într-o cauză internă similară, și a subliniat că aceste dispoziții par să fie conforme cu jurisprudența CJUE, potrivit căreia statele membre sunt obligate să asigure respectarea dreptului la o cale de atac efectivă, consacrat la articolul 47 din Cartă, în contextul procedurii de emitere și de executare a unui ordin european de anchetă. Întrucât, în temeiul dreptului intern, o persoană anchetată putea contesta includerea în dosarul procedurii penale a probelor obținute în cadrul unei proceduri separate, inclusiv prin invocarea unei încălcări a drepturilor garantate de Convenție, această cale de atac era deschisă și reclamanților, care ar fi putut solicita anularea măsurii de punere în aplicare a ordinului european de anchetă în aceleași condiții și în același mod ca și în cazul unei persoane anchetate în Franța, inclusiv prin invocarea art. 8 din Convenție.

Pentru a ajunge la concluzia că reclamanții au avut la dispoziție o cale de atac efectivă, CEDO a subliniat de asemenea că, în temeiul articolului 14 alineatul (7) din Directiva 2014/41, statul emitent trebuia să țină seama de faptul că un ordin european de anchetă fusese contestat cu succes. Prin urmare, întrucât procedurile penale îndreptate împotriva reclamanților erau încă pendinte, instanțele penale din Regatul Unit ar fi trebuit să ia în considerare un posibil rezultat favorabil al procedurilor desfășurate în fața instanțelor franceze.

Concluzie – Capetele de cerere formulate în temeiul art. 8 din Convenție au fost declarate inadmisibile pentru neepuizarea căilor de atac interne, iar capetele de cerere formulate în temeiul art. 6 și 13 din Convenție au fost declarate inadmisibile ca fiind în mod vădit nefondate.

B. Obligațiile FSC privind păstrarea datelor și accesul specific al autorităților naționale

B. 1. Date privind abonații

CJUE, Hotărârea din 2 octombrie 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788

În fapt – Poliția spaniolă, în cursul unei investigații privind furtul unui portofel și al unui telefon mobil, a solicitat judecătorului de instrucție să îi acorde acces la datele de identificare a utilizatorilor numerelor de telefon activate cu telefonul furat, pe parcursul unei perioade de douăsprezece zile de la furt. Judecătorul de instrucție a respins cererea, printre altele, pentru motivul că faptele care făceau obiectul anchetei penale nu constituiau o infracțiune „gravă".

Ulterior, instanța de trimitere a solicitat îndrumări din partea CJUE cu privire la stabilirea pragului de gravitate (a unei infracțiuni) pentru care poate fi justificată o ingerință în drepturile fundamentale.

În drept – CJUE a hotărât că articolul 15 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice, citit în lumina articolelor 7 și 8 din Cartă, trebuie interpretat în sensul că accesul unor autorități publice la date care vizează identificarea titularilor cartelelor SIM activate cu un telefon mobil furat, cum ar fi numele, prenumele și, dacă este cazul, adresa acestor titulari, implică o ingerință în drepturile fundamentale ale acestora din urmă, consacrate la articolele menționate din Cartă, care nu prezintă o asemenea gravitate încât să fie necesar ca acest acces să fie limitat, în materie de prevenire, de investigare, de detectare și de urmărire penală a infracțiunilor, la combaterea infracționalității grave. În special, aceasta a precizat că, în conformitate cu principiul proporționalității, o ingerință gravă nu poate fi justificată, în materie de prevenire, de investigare, de detectare și de urmărire penală a infracțiunilor, decât prin obiectivul privind combaterea infracționalității care trebuie calificată drept „gravă". În schimb, dacă ingerința pe care o implică un asemenea acces nu este gravă, respectivul acces este susceptibil să fie justificat de un obiectiv privind prevenirea, investigarea, detectarea și urmărirea penală a unor „infracțiuni" în general. CJUE a considerat că accesul la datele care făceau obiectul cererii nu constituia o ingerință deosebit de gravă întrucât permitea doar ca respectivele cartele SIM activate cu telefonul mobil furat să fie asociate, pe o perioadă determinată, cu identitatea titularilor acestor cartele. Fără o verificare încrucișată a datelor aferente comunicațiilor efectuate cu respectivele cartele SIM și a datelor de localizare, aceste date nu permiteau să se cunoască nici data, ora, durata și destinatarii comunicațiilor efectuate cu cartela sau cu cartelele SIM în cauză, nici locurile în care aceste comunicații au avut loc sau frecvența acestora cu anumite persoane într-o perioadă determinată. Prin urmare, aceste date nu permiteau să se tragă concluzii precise cu privire la viața privată a persoanelor ale căror date erau vizate.

CEDO, *Breyer împotriva Germaniei*, nr. 50001/12, 30 ianuarie 2020

În fapt – Reclamanții s-au plâns în principal, în temeiul art. 8 din Convenția europeană (dreptul la respectarea vieții private), că, în calitate de utilizatori de cartele SIM preplătite pentru telefoane mobile, anumite date cu caracter personal (numărul de telefon, numele și adresa, data nașterii și data încheierii contractului) au fost stocate de furnizorii lor de servicii de comunicații electronice, ca urmare a unei obligații legale în vigoare la 1 ianuarie 2008.

În drept – CEDO a reamintit jurisprudența sa consacrată privind ingerințele în dreptul la respectarea vieții private, prevăzut la art. 8, ca urmare a stocării, prelucrării și utilizării datelor cu caracter personal (inclusiv hotărârea *Ben Faiza împotriva Franței* nr. 31446/12, 8 februarie 2018).

În ceea ce privește justificarea ingerinței, CEDO a constatat că stocarea contestată avea un temei în dreptul intern, care era suficient de clar și de previzibil. În plus, durata și aspectele tehnice ale stocării erau clar stabilite. În ceea ce privește necesitatea ingerinței într-o societate democratică, CEDO a recunoscut că preînregistrarea abonaților la serviciile de telefonie mobilă simplifica și accelera considerabil anchetele efectuate de organele de aplicare a legii și, prin urmare, puteau

contribui la aplicarea eficientă a legii, la apărarea ordinii și la prevenirea faptelor penale. De asemenea, aceasta a reiterat faptul că, în materie de securitate națională, autoritățile naționale beneficiau de o anumită marjă de apreciere în privința alegerii mijloacelor adecvate pentru atingerea unui scop legitim și a subliniat că nu exista un consens între statele membre privind păstrarea informațiilor referitoare la abonații care dețineau cartele SIM preplătite. Având în vedere această marjă de apreciere, obligația de stocare a informațiilor privind abonații constituia, în general, un răspuns adaptat la evoluția comportamentului în materie de comunicare și a mijloacelor de telecomunicații. În cadrul evaluării proporționalității obligației legale contestate, CEDO a făcut distincție între cauza în discuție și cauzele referitoare la stocarea de informații foarte personale (de exemplu, hotărârea *Ben Faiza,* citată anterior) și, bazându-se, de asemenea, pe hotărârea CJUE în cauza *Ministerio fiscal,* citată anterior, a constatat că ingerința a avut un caracter limitat.

CEDO a observat, de asemenea, că, deși reclamanții s-au plâns doar cu privire la stocarea informațiilor lor cu caracter personal, aceasta nu putea să examineze proporționalitatea ingerinței fără să analizeze îndeaproape posibilul acces pe viitor la aceste informații și posibila utilizare viitoare a acestora. Aceasta a considerat că accesul la date era limitat la un anumit număr de autorități (care erau fie enumerate în mod explicit, caz în care accesul era permis prin intermediul unei proceduri centralizate și automatizate, fie identificate cu referire la sarcinile pe care le îndeplineau, caz în care accesul putea fi solicitat prin intermediul unei cereri scrise). În plus, accesul făcea obiectul unei serii de garanții, inclusiv garanția potrivit căreia doar Agenția Federală a Rețelelor (*Bundesnetzagentur*) sau respectivul furnizor de servicii de comunicații electronice putea divulga datele; accesul era limitat la datele necesare; acest criteriu al necesității era garantat prin impunerea unei obligații generale ca autoritățile respective care au obținut informațiile să șteargă, fără întârzieri nejustificate, orice date de care nu aveau nevoie; în contextul urmăririi penale a infracțiunilor, trebuia să existe cel puțin o suspiciune inițială. În ceea ce privește posibilitățile existente în materie de examinare și monitorizare a solicitărilor de informații, CEDO a făcut distincție între această cauză și hotărârile anterioare cu privire la diferite ingerințe în dreptul prevăzut la art. 8, considerând că astfel de garanții trebuie considerate un element important, dar nu decisiv, pentru evaluarea proporționalității, având în vedere setul limitat de date implicat. În această privință, CEDO a considerat că respectivul cadru juridic relevant oferea garanții suficiente, deoarece orice extragere de date și informațiile relevante privind extragerea erau înregistrate în scopul supravegherii protecției datelor, efectuată de autorități independente pentru protecția datelor, care puteau fi sesizate de orice persoană care considera că i-au fost încălcate drepturile.

Concluzie – Neîncălcarea art. 8 din Convenția europeană.

B. 2. Date de trafic și localizare

CJUE, Hotărârea din 8 aprilie 2014, *Digital Rights Ireland și alții*, C-293/12 și C 594/12, EU:C:2014:238

În fapt – La originea cauzei se află două cereri de decizie preliminară cu privire la validitatea Directivei 2006/24/CE privind păstrarea datelor, formulate în contextul unei proceduri interne în care legalitatea măsurilor legislative și administrative naționale referitoare la păstrarea unor date privind comunicațiile electronice a fost pusă în discuție în raport cu drepturile privind protecția datelor, prevăzute de Legea constituțională federală și de legislația Uniunii Europene.

În drept – CJUE a declarat că obligația furnizorilor de servicii de comunicații electronice de a păstra datele referitoare la viața privată a unei persoane și la comunicațiile sale, precum și accesul ulterior al autorităților naționale la aceste date constituia o ingerință în drepturile garantate de articolele 7 și 8 din Cartă. Ingerința a fost considerată deosebit de gravă și susceptibilă să genereze, în mintea persoanelor vizate, sentimentul că viața lor privată făcea obiectul unei supravegheri constante.

CJUE a statuat că aprecierea proporționalității includea o analiză (i) a caracterului adecvat și (ii) a necesității măsurilor contestate, în lumina obiectivelor acestora. Bazându-se, de asemenea, pe principiile stabilite în jurisprudența CEDO privind marja de apreciere, CJUE a hotărât că întinderea puterii de apreciere a legiuitorului Uniunii putea fi limitată în funcție de o serie de elemente, inclusiv domeniul vizat, natura dreptului în cauză, natura și gravitatea ingerinței, precum și finalitatea ingerinței și că, în speță, această putere de apreciere era redusă ca urmare a importanței protecției datelor cu caracter personal și a gravității ingerinței.

Deși măsurile contestate puteau fi considerate adecvate, având în vedere importanța în creștere a mijloacelor de comunicare electronică și utilitatea acestora ca instrument valoros pentru desfășurarea anchetelor penale, CJUE a considerat că Directiva privind păstrarea datelor nu se limitează la ceea ce este strict necesar pentru atingerea obiectivelor sale, din următoarele motive.

Pe de o parte, aceasta acoperă, în mod generalizat, toate persoanele și toate mijloacele de comunicare electronică, precum și toate datele de trafic, fără a face vreo diferențiere, limitare sau excepție în funcție de obiectivul de combatere a infracțiunilor grave. Aceasta nu se limitează la datele aferente unei anumite perioade de timp și/sau unei anumite zone geografice și se aplică și persoanelor în privința cărora nu există dovezi de natură să sugereze că comportamentul lor poate avea o legătură cu infracțiuni grave.

În al doilea rând, aceasta nu conține condiții materiale și procedurale care să reglementeze accesul autorităților naționale competente la date și utilizarea lor ulterioară. Limitându-se la a face trimitere, în general, la infracțiunile grave, astfel cum sunt definite de fiecare stat membru în dreptul său intern, directiva nu prevede niciun criteriu obiectiv care să permită stabilirea infracțiunilor care pot fi considerate suficient de grave pentru a justifica o ingerință atât de amplă în drepturile fundamentale consacrate la articolele 7 și 8 din Cartă. În plus, accesul autorităților naționale competente la datele păstrate nu este condiționat de un control prealabil efectuat de o instanță sau de o entitate administrativă independentă, prin a cărei decizie se urmărește limitarea accesului la date și a utilizării acestora la ceea ce este strict necesar.

În al treilea rând, aceasta impune ca toate datele să fie păstrate pentru o perioadă de cel puțin șase luni, fără a se face vreo distincție între categoriile de date în funcție de utilitatea lor eventuală în scopul realizării obiectivului urmărit sau în funcție de persoanele vizate. CJUE a concluzionat că directiva implică o ingerință de o mare amploare și de o gravitate deosebită în drepturile fundamentale consacrate la articolele 7 și 8 din Cartă, fără ca o astfel de ingerință să fie încadrată în mod precis de dispoziții care să permită asigurarea faptului că aceasta se limitează efectiv la ceea ce este strict necesar. CJUE a subliniat, de asemenea, că directiva nu prevede garanții suficiente, prin intermediul unor măsuri tehnice și organizaționale, care să permită asigurarea unei protecții eficiente a datelor păstrate împotriva riscurilor de abuz și împotriva oricărui acces și a oricărei utilizări ilicite a acestor date. Aceasta nu garantează nici distrugerea iremediabilă a datelor la sfârșitul duratei de păstrare a datelor și nici nu impune ca datele în cauză să fie păstrate pe teritoriul Uniunii Europene.

CJUE, Hotărârea din 21 decembrie 2016, *Tele2 Sverige și Watson și alții*, C-203/15 și C-698/15, EU:C:2016:970

În fapt – La originea cauzei se află două cereri de decizie preliminară privind compatibilitatea cu dreptul Uniunii a unei reglementări naționale care prevedea păstrarea generalizată a tuturor datelor de trafic și de localizare în scopul combaterii criminalității.

În drept – CJUE a statuat că articolul 15 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din Cartă, trebuie interpretat în sensul că se opune unei reglementări naționale:

1) care prevede, în scopul combaterii infracționalității, o păstrare generalizată și nediferențiată a ansamblului datelor de trafic și al datelor de localizare ale tuturor abonaților și utilizatorilor înregistrați în ceea ce privește toate mijloacele de comunicare electronică.

În special, CJUE s-a bazat pe Hotărârea *Digital Rights Ireland și alții,* citată anterior, și a precizat că păstrarea datelor trebuie limitată la strictul necesar în ceea ce privește categoriile de date care trebuie păstrate, mijloacele de comunicare vizate, persoanele în cauză, precum și perioada de păstrare reținută. Pentru a îndeplini aceste cerințe, reglementarea națională trebuie, în primul rând, să prevadă norme clare și precise, care să reglementeze conținutul și aplicarea unei astfel de măsuri de păstrare a datelor și să impună garanții minime. În al doilea rând, aceasta trebuie să prevadă condiții materiale pentru păstrarea datelor, astfel încât să se mențină o legătură între datele care trebuie păstrate și obiectivul urmărit.

2) care reglementează protecția și securitatea datelor de trafic și a datelor de localizare și în special accesul autorităților naționale competente la datele păstrate, în cazul în care (i) obiectivul urmărit de acest acces, în cadrul combaterii criminalității, nu este limitat numai la combaterea infracțiunilor grave, (ii) accesul nu este supus unui control prealabil din partea unei instanțe sau a unei autorități administrative independente și (iii) nu există nicio cerință care impune ca datele în cauză să fie păstrate pe teritoriul Uniunii.

CEDO, *Ben Faiza împotriva Franței*, nr. 31446/12, 8 februarie 2018

În fapt – Cauza privea în principal compatibilitatea cu art. 8 din Convenția europeană a accesului poliției judiciare, cu autorizarea procurorului, la datele de trafic și de localizare păstrate de furnizorii de servicii de comunicații electronice.

În drept – CEDO a considerat că accesul autorităților naționale la datele de trafic și de localizare a constituit o ingerință în dreptul reclamantului prevăzut la art. 8.

În ceea ce privește justificarea ingerinței, CEDO a considerat că accesul avea un temei în dreptul intern și era previzibil. În ceea ce privește garanțiile împotriva arbitrariului, CEDO a observat că poliția judiciară putea avea acces la datele aferente comunicațiilor cu autorizarea procurorului. În plus, accesul era supus unui control judiciar *ex post facto* în contextul unei proceduri penale îndreptate împotriva persoanei în cauză, în cadrul căreia instanțele puteau să controleze legalitatea accesului și, în cazul în care constatau nelegalitatea acestuia, puteau să excludă din procesul penal probele astfel obținute. CEDO a subliniat, de asemenea, că garanțiile prevăzute pentru accesul la datele aferente comunicațiilor erau mai puțin stricte decât cele prevăzute pentru geo-localizarea în timp real, dar a considerat că această diferențiere era justificată de natura mai puțin gravă a ingerinței.

În ceea ce privește necesitatea ingerinței într-o societate democratică, CEDO a considerat că era necesară împiedicarea unei operațiuni majore de trafic de droguri. În plus, informațiile obținute au fost utilizate în cadrul unui proces penal în care reclamantul a beneficiat de un control efectiv, conform cu statul de drept, și care a fost de natură să limiteze ingerința în cauză la ceea ce era necesar într-o societate democratică.

Concluzie – Neîncălcarea art. 8 din Convenția europeană.

CJUE, Hotărârea din 16 iulie 2020, *Facebook Ireland și Schrems*, C-311/18, EU:C:2020:559

În fapt – În urma hotărârii pronunțate de CJUE la 6 octombrie 2015, în cauza *Schrems*, C-362/14, EU:C:2015:650, cu privire la nevaliditatea Deciziei privind sfera de siguranță (2000/520/CE), în cadrul căreia Comisia Europeană a considerat că Statele Unite au asigurat un nivel adecvat de protecție a datelor cu caracter personal transferate, domnul Schrems a contestat din nou transferul datelor sale de către Facebook Ireland către Statele Unite și păstrarea datelor sale pe servere situate în această țară. El s-a plâns că dreptul Statelor Unite impunea societății Facebook Inc. să pună datele cu caracter personal care i-au fost transferate la dispoziția anumitor autorități americane, cum ar fi Agenția Națională de Securitate (National Security Agency) și Biroul Federal de Investigații (Federal Bureau of Investigation). Domnul Schrems a susținut că, întrucât aceste date au fost utilizate în cadrul mai multor programe de supraveghere într-un mod incompatibil cu articolele 7, 8 și 47 din Cartă, Decizia 2010/87/UE nu putea justifica transferul acestor date către Statele Unite.

Instanța națională a adresat CJUE o serie de întrebări preliminare, solicitând, printre altele, să se stabilească dacă dreptul Uniunii se aplică transferului de date de la o societate privată dintr-un stat membru al UE către o societate privată dintr-o țară terță; și dacă nivelul de protecție acordat de Statele Unite a respectat esența dreptului garantat prin articolul 47 din Cartă.

În drept – CJUE a statuat că RGPD se aplică unui transfer de date cu caracter personal în scopuri comerciale de către un operator economic stabilit într-un stat membru către un alt operator economic stabilit într-o țară terță, în pofida faptului că, în cursul sau în urma transferului menționat, datele respective sunt susceptibile de a fi prelucrate de autoritățile țării terțe în cauză în scopuri de siguranță publică, de apărare și de securitate a statului. În plus, garanțiile adecvate, drepturile opozabile și căile de atac eficiente prevăzute de RGPD trebuie să asigure faptul că persoanele ale căror date cu caracter personal sunt transferate către o țară terță în temeiul unor clauze standard de protecție a datelor beneficiază de un nivel de protecție în esență echivalent cu cel garantat în cadrul UE. În acest scop, evaluarea nivelului de protecție asigurat în contextul unui astfel de transfer trebuie în special să ia în considerare atât stipulațiile contractuale convenite între operator sau persoana împuternicită de operator stabiliți în Uniune și destinatarul transferului stabilit în țara terță în cauză, cât și, în ceea ce privește un eventual acces al autorităților publice ale acestei țări terțe la datele cu caracter personal astfel transferate, elementele relevante ale sistemului juridic al acesteia.

În plus, cu excepția cazului în care există o decizie privind caracterul adecvat al nivelului de protecție, adoptată în mod valabil de Comisie, autoritatea de supraveghere competentă este obligată să suspende sau să interzică un transfer de date către o țară terță, atunci când această autoritate de supraveghere consideră, în lumina tuturor împrejurărilor proprii transferului menționat, că respectivele clauze standard de protecție a datelor adoptate de Comisie nu sunt sau nu pot fi respectate în țara terță respectivă și că protecția datelor transferate (impusă de dreptul Uniunii) nu poate fi asigurată prin alte mijloace.

Adoptarea de către Comisie a unei decizii privind caracterul adecvat al nivelului de protecție necesită constatarea că țara terță în cauză asigură, în temeiul legislației interne sau al angajamentelor sale internaționale, un nivel de protecție a drepturilor fundamentale în esență echivalent cu cel garantat în ordinea juridică a Uniunii. În opinia CJUE, Decizia privind sfera de siguranță era nevalidă. Dispoziția relevantă nu evidenția în niciun mod existența unor limitări ale abilitării pe care o presupunea pentru punerea în aplicare a programelor de supraveghere în scopul informării externe și nici existența unor garanții pentru persoane, care nu erau cetățeni americani, potențial vizate de programele menționate. În aceste condiții, aceasta nu putea asigura un nivel de protecție în esență echivalent cu cel garantat de Cartă. În plus, în ceea ce privește programele de supraveghere, era clar că acest decret nu conferea drepturi opozabile autorităților americane în fața instanțelor judecătorești americane.

CJUE, Hotărârea din 6 octombrie 2020, *La Quadrature du Net și alții*, C-511/18, C-512/18 și C-520/18, EU:C:2020:791

În fapt – La originea cauzei se află trei cereri de decizie preliminară privind aplicarea Directivei asupra confidențialității și comunicațiilor electronice în cazul unei reglementări naționale care impunea furnizorilor de servicii de comunicații electronice obligații privind:

(i) stocarea generalizată și nediferențiată a datelor de trafic și a datelor de localizare în scopul protejării securității naționale și al combaterii terorismului.

(ii) punerea în aplicare, în rețelele lor, a unor măsuri care permiteau, pe de o parte, analiza automatizată, precum și colectarea în timp real a datelor de trafic și a datelor de localizare și, pe de altă parte, colectarea în timp real a datelor tehnice referitoare la localizarea echipamentelor terminale utilizate.

În drept – CJUE a subliniat că obiectivul de protejare a securității naționale nu a fost încă examinat în mod specific de CJUE în hotărârile sale de interpretare a Directivei asupra confidențialității și comunicațiilor electronice. Aceasta a confirmat că, deși directiva menționată, interpretată în lumina Cartei, se opunea unor măsuri legislative care prevedeau stocarea generalizată și nediferențiată a datelor de trafic și a datelor de localizare, în cazul în care un stat membru se confrunta cu o amenințare gravă la adresa securității naționale, care se dovedea reală și actuală sau previzibilă, nu exista niciun obstacol în calea unor măsuri legislative care impuneau furnizorilor de servicii de comunicații electronice stocarea generalizată și nediferențiată a datelor de trafic și de localizare pentru o perioadă limitată în timp la strictul necesar, dar care putea fi reînnoită în cazul menținerii acestei amenințări. Într-un astfel de caz, decizia prin care se impunea o astfel de obligație trebuia să facă obiectul unui control efectiv, fie de către o instanță, fie de către o entitate administrativă independentă, a cărei decizie avea efect obligatoriu, scopul acestui control fiind de a verifica existența uneia dintre aceste situații și respectarea condițiilor și a garanțiilor care trebuiau să fie prevăzute. În scopul combaterii infracționalității grave și al prevenirii amenințărilor grave la adresa siguranței publice, un stat membru putea de asemenea să prevadă – dacă această măsură era limitată în timp la strictul necesar – o stocare direcționată a datelor de trafic și a datelor de localizare, care să fie delimitată, pe baza unor elemente obiective și nediscriminatorii, în funcție de categoriile de persoane vizate sau prin intermediul unui criteriu geografic, sau stocarea adreselor IP atribuite sursei unei conexiuni (la Internet). De asemenea, un stat membru putea efectua o stocare generalizată și nediferențiată a datelor referitoare la identitatea civilă a utilizatorilor mijloacelor de comunicații electronice, fără să prevadă un termen specific pentru această stocare.

În plus, Directiva asupra confidențialității și comunicațiilor electronice, interpretată în lumina Cartei, nu se opunea unei reglementări naționale care impunea furnizorilor de servicii de comunicații electronice să recurgă, pe de o parte, la analiza automatizată și la colectarea în timp real a datelor de trafic și a datelor de localizare și, pe de altă parte, la colectarea în timp real a datelor tehnice privind localizarea echipamentelor terminale utilizate, în cazul în care recurgerea la analiza automatizată se limita la situațiile în care un stat membru se confrunta cu o amenințare gravă la adresa securității naționale, care era reală și actuală sau previzibilă, și în condițiile în care recurgerea la o astfel de analiză putea face obiectul unui control efectiv fie de către o instanță, fie de către o entitate administrativă independentă, a cărei decizie avea efect obligatoriu.

CJUE, Hotărârea din 2 martie 2021, *Prokuratuur*, C-746/18, EU:C:2021:152

În fapt – La originea cauzei se află o cerere de decizie preliminară privind aplicarea Directivei asupra confidențialității și comunicațiilor electronice în cazul unei reglementări naționale care permitea

accesul la datele stocate de furnizorii de servicii de comunicații electronice în contextul unei proceduri penale.

În drept – CJUE a reiterat faptul că articolul 15 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice permite accesul la datele de trafic sau de localizare stocate în scopul combaterii infracționalității numai în cazul infracțiunilor grave sau al amenințărilor grave la adresa siguranței publice, indiferent de întinderea perioadei pentru care se solicită accesul și de volumul sau de natura datelor disponibile pentru o astfel de perioadă.

CJUE a hotărât, de asemenea, că nu putea fi acordată Ministerului Public competența de a examina cererile de acces, având în vedere că sarcinile acestuia de a conduce procedura de urmărire penală și de a exercita acțiunea puteau afecta independența acestuia față de părțile din procedura penală.

CEDO, *Big Brother Watch și alții împotriva Regatului Unit* (MC), citată anterior

În fapt – A se vedea caseta dedicată de la punctul B de mai sus.

În drept – Reclamanții s-au plâns că regimul de obținere a datelor aferente comunicațiilor de la furnizorii de servicii de comunicații era incompatibil cu drepturile lor prevăzute la art. 8 și 10 din Convenția europeană. Marea Cameră a confirmat concluziile Camerei în privința ambelor capete de cerere (formulate în temeiul art. 8 și 10):

În ceea ce privește art. 8, la data examinării cauzei de către Cameră, era pendinte o procedură internă privind noua lege care reglementa păstrarea datelor aferente comunicațiilor de către furnizorii de servicii de comunicații. În cursul acestei proceduri, Guvernul Regatului Unit a admis că dispozițiile legale relevante erau incompatibile cu dreptul Uniunii și, în consecință, instanțele naționale le-au considerat incompatibile cu drepturile fundamentale, astfel cum sunt garantate de dreptul Uniunii.

Având în vedere atât supremația dreptului Uniunii asupra dreptului Regatului Unit la momentul respectiv, cât și aspectele recunoscute de Guvern în cadrul procedurii interne, CEDO a considerat că era clar că dreptul intern impunea ca orice regim care permitea autorităților să acceseze datele păstrate de furnizorii de servicii de comunicații să limiteze accesul la scopul combaterii „infracțiunilor grave” și că accesul ar trebui să facă obiectul unei examinări prealabile de către o instanță sau de către un organ administrativ independent. Întrucât regimul anterior fusese afectat de aceleași deficiențe ca și succesorul său, CEDO a constatat că nu se putea considera că acesta era prevăzut de lege, în sensul art. 8 din Convenția europeană.

În ceea ce privește art. 10, CEDO a admis că regimul în litigiu oferea o protecție sporită în cazul în care datele erau solicitate în scopul identificării sursei unui jurnalist. Cu toate acestea, dispozițiile în cauză nu se aplicau în toate cazurile în care exista o cerere care viza datele aferente comunicațiilor unui jurnalist sau în care era probabil să se producă o astfel de intruziune colaterală. În plus, nu existau dispoziții speciale care să limiteze accesul la datele aferente comunicațiilor unui jurnalist la scopul combaterii „infracțiunilor grave”. În consecință, CEDO a considerat că regimul respectiv nu era prevăzut de lege în sensul art. 10 din Convenția europeană.

Concluzie – Încălcarea art. 8 și 10 din Convenția europeană în ceea ce privește regimul de obținere a datelor aferente comunicațiilor de la furnizorii de servicii de comunicații.

CEDO, *Ekimdjiev și alții împotriva Bulgariei*, nr. 70078/12, 11 ianuarie 2022

În fapt – Cauza a avut ca obiect compatibilitatea cu art. 8 a legilor și practicilor bulgare privind păstrarea datelor aferente comunicațiilor și accesul la acestea. Reclamanții, doi avocați și două

organizații neguvernamentale, au afirmat că natura activităților lor îi expunea riscului ca datele aferente comunicațiilor acestora să fie accesate de autorități.

În drept – Reclamanții s-au plâns că sistemul de păstrare a datelor aferente comunicațiilor și de accesare ulterioară a acestora (datele privind abonații, datele de trafic și datele de localizare) nu îndeplinea cerințele art. 8 din Convenția europeană.

Bazându-se pe jurisprudența sa anterioară (*Breyer*, *Centrum för rättvisa* și *Big Brother Watch*, toate citate anterior), CEDO a considerat că:

a) simpla stocare a acestor date a constituit o ingerință în dreptul reclamanților individuali la respectarea vieții private și a corespondenței, precum și în dreptul organizațiilor reclamante la respectarea corespondenței;

(b) accesul autorităților la datele păstrate referitoare la comunicații a constituit o altă ingerință în drepturile prevăzute la art. 8.

În ceea ce privește justificarea ingerinței, întemeindu-se pe hotărârile *Centrum för rättvisa* și *Big Brother Watch,* ambele citate anterior, CEDO a considerat că obținerea acestor date prin interceptarea în masă ar putea fi la fel de intruzivă ca obținerea în masă a conținutului comunicațiilor. Prin urmare, ar trebui să se aplice aceleași garanții precum cele aplicabile conținutului comunicațiilor. CEDO a adăugat că, în mod similar, păstrarea generală a datelor aferente comunicațiilor de către furnizorii de servicii de comunicații și accesarea acestora de către autorități în cazuri individuale trebuie să fie însoțite, *mutatis mutandis,* de aceleași garanții ca și supravegherea secretă (s-a întemeiat în special pe hotărârea *Roman Zaharov,* citată anterior).

După ce a aplicat aceste principii în speță și a apreciat o serie de elemente (accesibilitatea legii; nivelul de protecție a datelor păstrate asigurat de furnizorii de servicii de comunicații; analizarea motivelor pentru care datele păstrate pot fi accesate de către autorități; procedurile de obținere a accesului; durata stocării și utilizării datelor accesate care nu au fost utilizate ulterior în cadrul unor proceduri penale; și analizarea procedurilor de stocare, accesare, examinare, utilizare, comunicare și distrugere a datelor accesate de autorități; mecanismul de supraveghere; notificarea persoanelor interesate; căile de atac disponibile), CEDO a concluzionat că respectivul cadru juridic nu respecta garanțiile minime împotriva arbitrarului și a abuzurilor, prevăzute la art. 8 din Convenția europeană, în următoarele privințe:

(a) procedura de autorizare nu părea de natură să garanteze că datele păstrate referitoare la comunicații erau accesate de autorități numai atunci când acest lucru era „necesar într-o societate democratică”;

(b) nu au fost stabilite termene clare pentru distrugerea datelor accesate de autorități în cursul procedurilor penale;

(c) nu existau norme accesibile publicului privind stocarea, accesarea, examinarea, utilizarea, comunicarea și distrugerea datelor aferente comunicațiilor accesate de autorități;

(d) sistemul de supraveghere nu părea de natură să asigure verificarea eficientă a existenței unor abuzuri;

(e) sistemul de notificare era prea limitat;

(f) nu exista nicio cale de atac efectivă.

Concluzie – Încălcarea art. 8 din Convenția europeană în ceea ce privește sistemul de păstrare a datelor aferente comunicațiilor și de accesare ulterioară a acestora.

CJUE, Hotărârea din 5 aprilie 2022, *Commissioner of An Garda Síochána și alții*., C-140/20, EU:C:2022:258

În fapt – La originea cauzei se află o cerere de decizie preliminară privind aplicarea Directivei asupra confidențialității și comunicațiilor electronice în cazul unei legislații naționale care permitea accesul la datele păstrate de furnizorii de servicii de comunicații electronice în contextul unei proceduri penale.

În drept – CJUE și-a confirmat jurisprudența constantă potrivit căreia dreptul Uniunii se opune unei reglementări naționale care prevede păstrarea generalizată și nediferențiată a datelor de trafic și a datelor de localizare referitoare la comunicațiile electronice ca măsură preventivă în scopul combaterii criminalității grave și al prevenirii amenințărilor grave la adresa siguranței publice. Cu toate acestea, CJUE a considerat că dreptul Uniunii nu se opune:

– păstrării direcționate a datelor de trafic și a datelor de localizare pentru o perioadă limitată de timp și care este delimitată pe baza unor elemente obiective și nediscriminatorii;

– păstrării generalizate și nediferențiate a adreselor IP atribuite sursei unei conexiuni (la Internet) pentru o perioadă limitată;

– păstrării generalizate și nediferențiate a datelor referitoare la identitatea civilă a utilizatorilor de mijloace de comunicații electronice; și

– impunerii unei obligații furnizorilor de servicii de comunicații electronice, prin intermediul unei decizii a autorității competente supuse unui control jurisdicțional efectiv, de a efectua, pentru o perioadă determinată, păstrarea rapidă a datelor de trafic și a datelor de localizare de care dispun acești furnizori de servicii,

cu condiția ca aceste măsuri să garanteze, prin norme clare și precise, că păstrarea datelor în cauză este subordonată respectării condițiilor materiale și procedurale aferente și că persoanele vizate dispun de garanții efective împotriva riscurilor de abuz.

În plus, CJUE a considerat că dreptul Uniunii se opune unei legislații naționale în temeiul căreia prelucrarea centralizată a cererilor de acces la date păstrate de furnizorii de servicii de comunicații electronice, care provin de la poliție în cadrul investigării și al urmăririi penale a infracțiunilor grave, revine unui funcționar al poliției, asistat de o unitate instituită în cadrul poliției, care beneficiază de un anumit grad de autonomie în exercitarea misiunii sale, și ale cărui decizii pot face ulterior obiectul unui control jurisdicțional.

CJUE, Hotărârea din 20 septembrie 2022, *SpaceNet și Telekom Deutschland*, C-793/19 și C-794/19, EU:C:2022:702

În fapt – La originea cauzei se află două cereri de decizie preliminară privind aplicarea Directivei asupra confidențialității și comunicațiilor electronice în cazul unei reglementări naționale care impunea furnizorilor de servicii de comunicații electronice păstrarea generalizată și nediferențiată a celei mai mari părți a datelor de trafic și a datelor de localizare ale utilizatorilor finali ai acestor servicii (inclusiv date referitoare la site-urile internet consultate și date privind serviciile de poștă electronică), prevăzând o perioadă de păstrare de mai multe săptămâni, precum și norme prin care se urmărea garantarea unei protecții eficiente a datelor păstrate împotriva riscurilor de abuz și împotriva oricărui acces ilicit la aceste date.

În drept – CJUE a confirmat jurisprudența sa constantă împotriva păstrării generalizate și nediferențiate a datelor de trafic și a datelor de localizare în scopul combaterii criminalității grave sau al prevenirii amenințărilor grave la adresa siguranței publice (a se vedea *La Quadrature du Net* și *Commissioner of An Garda Síochána,* ambele citate anterior). Aceasta a constatat că legislația națională în cauză nu era conformă cu dreptul Uniunii, în pofida existenței unor garanții și a unei perioade de păstrare mai scurte decât în cauzele anterioare. CJUE a statuat, de asemenea, că păstrarea datelor respective și accesul la acestea constituiau ingerințe distincte în drepturile fundamentale ale persoanelor vizate, ingerințe care necesitau o justificare distinctă, și că, în consecință, legislația națională care asigura respectarea deplină a condițiilor rezultate din jurisprudența privind accesul la datele păstrate nu putea fi susceptibilă, prin însăși natura sa, nici să limiteze și nici măcar să remedieze ingerința gravă în drepturile persoanelor vizate, care ar fi rezultat din păstrarea generalizată a datelor respective.

CJUE, Hotărârea din 20 septembrie 2022, *VD și SR*, C-339/20 și C-397/20, EU:C:2022:703

În fapt – La originea cauzei se află două cereri de decizie preliminară privind interpretarea dispozițiilor Uniunii Europene privind abuzul de piață, coroborate cu articolul 15 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice. Aceste cereri au fost formulate în cadrul procedurilor penale inițiate împotriva lui VD și a lui SR pentru utilizări abuzive ale informațiilor confidențiale, tăinuire a unor utilizări abuzive a informațiilor confidențiale, complicitate, corupție și spălare de bani.

În drept – CJUE a hotărât că Directiva privind abuzul de piață și Regulamentul privind abuzul de piață, coroborate cu Directiva asupra confidențialității și comunicațiilor electronice și în lumina articolelor 7, 8 și 11 din Cartă, nu autorizează o păstrare generalizată și nediferențiată a datelor de trafic de către furnizorii de servicii de comunicații electronice pentru o perioadă de un an de la data înregistrării, în vederea combaterii infracțiunilor de abuz de piață.

CJUE a statuat, de asemenea, că dreptul Uniunii se opunea ca o instanță națională să limiteze în timp efectele unei declarații de nevaliditate pe care avea obligația să o efectueze, în temeiul dreptului național, în privința dispozițiilor naționale care, pe de o parte, impuneau operatorilor de servicii de comunicații electronice o păstrare generalizată și nediferențiată a datelor de transfer și, pe de altă parte, permiteau comunicarea unor asemenea date autorității competente în materie financiară, fără autorizarea prealabilă a unei instanțe sau a unei autorități administrative independente, ca urmare a incompatibilității acestor dispoziții cu articolul 15 alineatul (1) din Directiva asupra confidențialității și comunicațiilor electronice, interpretat în lumina Cartei Admisibilitatea elementelor de probă obținute în aplicarea dispozițiilor legislative naționale incompatibile cu dreptul Uniunii intrau în sfera de aplicare a dreptului național, în conformitate cu

principiul autonomiei procedurale a statelor membre, sub rezerva respectării, printre altele, a principiilor echivalenței și efectivității.

CJUE, Hotărârea din 17 noiembrie 2022, *Spetsializirana prokuratura*, C-350/21, EU:C:2022:896

În fapt – La originea cauzei se află o cerere de decizie preliminară privind aplicarea Directivei asupra confidențialității și comunicațiilor electronice în lumina articolelor 7, 8, 11 și 52 din Cartă în cazul unei legi naționale:

(i) care impunea furnizorilor de servicii de comunicații electronice obligația stocării generalizate și nediferențiate a tuturor datelor de trafic și de localizare ale utilizatorilor finali ai acestor servicii, în scopul combaterii criminalității grave, stabilind o perioadă de stocare de șase luni și norme menite să asigure o serie de garanții.

(ii) care nu limita accesul la datele respective la ceea ce era strict necesar și care nu prevedea nici dreptul persoanelor fizice de a fi informate cu privire la acest acces, în cazul în care informarea acestora nu împiedica procedura penală, și nici dreptul la o cale de atac împotriva unui acces ilicit.

În drept – CJUE a confirmat jurisprudența sa constantă împotriva păstrării generalizate și nediferențiate a datelor de trafic și a datelor de localizare în scopul combaterii criminalității grave (a se vedea *La Quadrature du Net* și *Commissioner of An Garda Síochána,* ambele citate anterior). Aceasta a constatat că legea națională în cauză nu era conformă cu dreptul Uniunii, în pofida existenței unor garanții și a unei perioade de stocare de șase luni. În ceea ce privește garanțiile procedurale împotriva unui acces ilicit, CJUE a statuat că o autorizație judiciară (acordată de o instanță națională) nu era suficientă în sine pentru a asigura o protecție eficientă a persoanelor vizate împotriva riscurilor de abuzuri și de acces ilicit la datele referitoare la acestea, atunci când, precum în speță, legea națională în cauză prevedea că o astfel de autorizație era acordată exclusiv pe baza unei cereri formulate de organele naționale de urmărire penală, fără ca persoanele vizate să fi fost audiate și, în consecință, fără ca instanța competentă să emită o astfel de autorizație să fi putut ține seama de eventualele obiecții ale acestor persoane.

CEDO, *Škoberne împotriva Sloveniei*, nr. 19920/20, 15 februarie 2024

În fapt – Datele de trafic și de localizare ale reclamantului – care au fost păstrate de furnizorii de servicii de comunicații electronice pentru o perioadă de paisprezece luni ca parte a unei măsuri sistemice – au fost obținute de autoritățile de aplicare a legii în temeiul unor hotărâri judecătorești care s-au bazat pe motive de suspiciune că reclamantul ar fi săvârșit infracțiunea de luare de mită. Cauza privește compatibilitatea cu art. 8 din Convenția europeană a unei reglementări care permitea păstrarea datelor privind telecomunicațiile reclamantului și utilizarea acestora de către autorități în cadrul procesului îndreptat împotriva sa.

În drept – Pentru a aprecia dacă regimul de păstrare a datelor era necesar într-o societate democratică, CEDO a ținut seama de (i) gradul de ingerință; (ii) întinderea marjei de apreciere și (iii) dacă s-a asigurat un „just echilibru”.

În ceea ce privește punctul (i), CEDO a făcut o distincție între această speță și cauza *Breyer,* citată anterior, subliniind că, în speță, ingerința a fost mai gravă, întrucât s-a extins la datele privind comunicațiile.

În ceea ce privește punctul (ii), CEDO s-a întemeiat pe jurisprudența sa anterioară pentru a reitera faptul că lupta împotriva infracționalității, garantarea siguranței publice și protecția cetățenilor constituie „nevoi sociale imperioase” și că autoritățile naționale beneficiază de o anumită marjă de apreciere în privința alegerii mijloacelor adecvate pentru atingerea acestui obiectiv legitim. Cu toate

acestea, marja tinde să fie mai restrânsă în cazul în care – precum în prezenta speță – dreptul în cauză este esențial pentru exercitarea efectivă de către individ a unor drepturi intime sau fundamentale, ori în cazul în care ingerința a fost amplă.

În ceea ce privește punctul (iii), CEDO a considerat că garanțiile aplicabile păstrării generale a datelor aferente comunicațiilor de către furnizorii de servicii de comunicații și accesării acestor date de către autorități în cazuri individuale ar trebui să fie aceleași, *mutatis mutandis,* ca și în cazul supravegherii secrete.

Aceasta a constatat că respectivul cadru juridic în litigiu nu conținea nicio dispoziție care să delimiteze domeniul de aplicare și aplicarea măsurii în raport cu ceea ce era necesar pentru atingerea scopurilor pentru care trebuiau păstrate datele privind telecomunicațiile. Întemeindu-se, de asemenea, pe hotărârea CJUE în cauza *Digital Rights Ireland,* citată anterior, CEDO a constatat că dreptul național ar trebui să definească domeniul de aplicare al măsurii în cauză și să prevadă proceduri adecvate pentru dispunerea și/sau controlarea acesteia în vederea menținerii sale în limitele a ceea ce este necesar. Simpla limitare a păstrării datelor la o perioadă de paisprezece luni nu putea să afecteze această concluzie. CEDO a considerat, de asemenea, că faptul că regimul de păstrare a datelor a fost declarat nevalid de CJUE și de Curtea Constituțională, după ce datele în cauză au fost accesate, nu putea fi interpretat în sensul că acesta a respectat art. 8 la momentul faptelor.

CEDO a observat, de asemenea, că, în pofida faptului că reclamantul a susținut în mod clar că datele aferente comunicațiilor sale au fost păstrate cu încălcarea dreptului său la respectarea vieții sale private, instanțele naționale și-au limitat aprecierea aproape exclusiv la motivele pentru care hotărârile judecătorești au autorizat accesul la datele păstrate – chiar dacă aceste motive nu au fost contestate de reclamant. CEDO a subliniat că, în pofida faptului că accesul la datele reclamantului a fost însoțit de anumite garanții (cum ar fi supravegherea judiciară), aceste garanții, deși se numărau printre criteriile care trebuiau îndeplinite, nu erau suficiente în sine pentru ca regimul de păstrare a datelor să fie conform cu art. 8 din Convenția europeană. Aceasta s-a întemeiat, de asemenea, pe hotărârea CJUE *SpaceNet și Telekom Deutschland,* citată anterior.

În ceea ce privește obținerea și utilizarea datelor reclamantului în cadrul procedurii interne, întemeindu-se pe hotărârea CJUE *Commissioner of An Garda Síochána și alții,* citată anterior, CEDO a considerat că, atunci când se constată că păstrarea datelor aferente comunicațiilor încalcă art. 8, deoarece nu respectă cerința „calității legii" și/sau principiul proporționalității, nu se putea considera, din același motiv, că accesul la astfel de date, precum și prelucrarea și stocarea ulterioară a acestora de către autorități, respectau art. 8.

Concluzie – Încălcarea art. 8 din Convenția europeană.

CEDO, *Pietrzak și Bychawska-Siniarska și alții împotriva Poloniei*, nr. 72038/17 și 25237/18, 28 mai 2024

În fapt – Cauza privea compatibilitatea cu art. 8 a regimului polonez de supraveghere secretă, care reglementa stocarea și prelucrarea datelor aferente comunicațiilor[25]. Reclamanții nu s-au plâns de faptul că au fost plasați efectiv sub supraveghere, ci de riscul de a fi supusă unor astfel de măsuri.

Reclamanții s-au plâns de asemenea, în temeiul aceleiași dispoziții, cu privire la controlul operațional desfășurat în cadrul activităților polițienești și al măsurilor de supraveghere secretă, în contextul luptei împotriva terorismului, prin intermediul unor tehnici care includeau interceptarea convorbirilor telefonice sau a corespondenței și înregistrarea conținutului acestora, efectuate prin intermediul rețelelor de telecomunicații și de comunicații digitale. Această parte a hotărârii nu va fi analizată întrucât sistemul contestat, care permitea măsuri de supraveghere specifice, nu intră în domeniul de aplicare al prezentei fișe tematice.

Reclamanții s-au plâns de faptul că sistemul de păstrare a datelor aferente comunicațiilor și de accesare ulterioară a acestora (datele de trafic și de localizare, precum și datele referitoare la căutările pe Internet) nu îndeplinea cerințele art. 8 din Convenția europeană.

În drept – Întemeindu-se pe hotărârea *Ekimdjiev*, citată anterior, CEDO a considerat că păstrarea datelor aferente comunicațiilor și accesarea ulterioară a acestora constituiau ingerințe distincte în art. 8 și că păstrarea generală a datelor aferente comunicațiilor de către furnizorii de servicii de comunicații și accesarea acestora de către autorități în cazuri individuale trebuiau să fie însoțite, *mutatis mutandis*, de aceleași garanții ca și supravegherea secretă.

CEDO a făcut distincție între această speță și cauza *Ekimdjiev,* citată anterior, subliniind că regimul contestat permitea autorităților naționale să aibă acces permanent, direct și nelimitat la datele aferente comunicațiilor, fără ca furnizorii de servicii de comunicații să aibă măcar cunoștință de acest lucru și fără nicio intervenție din partea lor. Ingerințele în cauză au fost considerate foarte grave. În plus, deși hotărârea în cauza *Ekimdjiev,* citată anterior, privea un regim de păstrare a datelor aferente comunicațiilor similar celui în discuție în prezenta cauză, CEDO nu s-a pronunțat cu privire la conformitatea respectivului regim în sine cu cerințele art. 8, ci s-a concentrat mai degrabă asupra garanțiilor referitoare la accesul la datele colectate și la stocarea acestora.

Bazându-se, de asemenea, pe jurisprudența CJUE (*Digital Rights Ireland și alții*, *Privacy International*, *Commissioner of An Garda Síochána și alții*, citate anterior, și *La Quadrature du Net și alții*[26]), CEDO a constatat că regimul în litigiu impunea o păstrare generalizată și nediferențiată a datelor aferente comunicațiilor tuturor utilizatorilor de servicii de comunicații, afectând persoane care nu se aflau, nici măcar indirect, într-o situație de natură să conducă la punerea în mișcare a unei acțiuni penale. În plus, acest regim permitea accesul poliției și al serviciilor de informații în orice scop relevant pentru îndeplinirea obligațiilor lor legale respective. În aceste condiții, garanțiile împotriva eventualelor abuzuri, inclusiv controlul judiciar *ex post facto,* erau insuficiente pentru ca regimul în cauză să fie considerat conform cu cerințele art. 8.

Concluzie – Încălcarea art. 8 din Convenția europeană în ceea ce privește sistemul de păstrare a datelor aferente comunicațiilor și de accesare a acestora.

B.3 Conținutul comunicațiilor

CEDO, *Podciasov împotriva Rusiei*, nr. 33696/19, 13 februarie 2024

În fapt – Reclamantul, utilizator al Telegram, s-a plâns cu privire la compatibilitatea cu art. 8 din Convenția europeană a obligației legale impuse „organizatorilor de comunicații prin Internet” (OCI) de a stoca toate datele aferente comunicațiilor pentru o perioadă de un an și conținutul tuturor comunicațiilor pentru o perioadă de șase luni, precum și de a prezenta aceste date autorităților de aplicare a legii sau serviciilor de securitate, în circumstanțele prevăzute de lege, împreună cu informațiile necesare pentru decriptarea mesajelor electronice, în cazul în care acestea erau criptate.

În drept – CEDO s-a întemeiat pe jurisprudența sa anterioară (hotărârile *Breyer, Ekimdjiev și Roman Zaharov,* toate citate anterior), pentru a constata că stocarea continuă de către Telegram a comunicațiilor prin Internet ale reclamantului și a datelor aferente comunicațiilor acestuia, precum și potențialul acces al autorităților la aceste date au constituit o ingerință în drepturile reclamantului prevăzute la art. 8. În ceea ce privește obligația impusă Telegram de a furniza autorităților chei de criptare care să le permită să decripteze comunicațiile criptate end-to-end, CEDO a admis argumentul reclamantului potrivit căruia era imposibil din punct de vedere tehnic să li se furnizeze

[26] Hotărârea din 6 octombrie 2020, *La Quadrature du Net și alții*, C-511/18, C-512/18 și C-520/18, EU:C:2020:791.

autorităților chei de criptare asociate anumitor utilizatori ai Telegram fără ca acest lucru să afecteze toți utilizatorii serviciilor Telegram. Prin urmare, CEDO a admis că reclamantul a fost afectat și de această dispoziție legală.

CEDO a constatat că, deși cauza trebuia examinată în primul rând din punctul de vedere al stocării datelor cu caracter personal ale reclamantului (la fel ca în cauzele *Breyer și Ekimdjiev,* citate anterior), aceasta trebuia de asemenea să fie examinată, după caz, în lumina jurisprudenței sale privind supravegherea secretă (*Roman Zaharov,* citată anterior, *Big Brother Watch,* citată anterior).

În ceea ce privește stocarea comunicațiilor prin Internet și a datelor aferente comunicațiilor, CEDO a subliniat amploarea considerabilă a obligației de păstrare a datelor impusă de legislația atacată, subliniind că aceasta includea păstrarea conținutului tuturor comunicațiilor prin Internet și a datelor aferente comunicațiilor, afectând toți utilizatorii comunicațiilor prin Internet, chiar și în lipsa unei suspiciuni rezonabile cu privire la implicarea în activități infracționale sau în activități care puneau în pericol securitatea națională sau a oricăror alte motive pentru a se considera că păstrarea datelor putea contribui la combaterea infracțiunilor grave sau la protejarea securității naționale și fără nicio delimitare a domeniului de aplicare al măsurii în ceea ce privește aplicarea teritorială sau în timp, ori categoriile de persoane susceptibile să facă obiectul stocării datelor cu caracter personal. Aceasta a constatat că ingerința în cauză era extrem de amplă și gravă.

În ceea ce privește potențialul acces la datele stocate în scopul supravegherii secrete specifice, CEDO a constatat că dreptul intern nu impunea autorităților de aplicare a legii să prezinte furnizorilor de servicii de comunicații o autorizație judiciară (acordată de o instanță) înainte de a obține accesul la comunicațiile unei persoane. În plus, OCI erau obligați să instaleze echipamente care să ofere serviciilor de securitate acces direct la datele stocate, astfel încât acestea să dispună de mijloacele tehnice necesare pentru a eluda procedura de autorizare și pentru a accesa comunicațiile prin Internet stocate și datele aferente acestor comunicații, fără să obțină o autorizare prealabilă de către o instanță judecătorească. De asemenea, CEDO a reiterat constatările sale privind lipsa unor garanții adecvate și suficiente împotriva abuzurilor, făcute în hotărârea *Roman Zaharov,* citată anterior, în care același regim juridic a fost examinat în contextul interceptării comunicațiilor de telefonie mobilă.

În sfârșit, în ceea ce privește obligația legală de a decripta comunicațiile, CEDO a considerat că aceasta era disproporționată în raport cu scopurile legitime urmărite, întrucât, deși a admis că era posibil ca și infractorii să utilizeze criptarea, dispoziția atacată risca să slăbească mecanismul de criptare pentru toți utilizatorii.

Concluzie – Încălcarea art. 8 din Convenția europeană.