



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

CURTEA EUROPEANĂ A DREPTURILOR OMULUI

MAREA CAMERĂ

CAUZA BIG BROTHER WATCH ȘI ALȚII ÎMPOTRIVA REGATULUI UNIT

(Cererile nr. 58170/13, 62322/14 și 24960/15)

HOTĂRÂRE

Art. 8 • Viață privată • Conformitatea cu Convenția a unui regim de supraveghere secretă care include interceptarea în masă a comunicațiilor și schimbul de informații • Necesitatea dezvoltării jurisprudenței în lumina diferențelor importante dintre interceptarea țintită și interceptarea în masă • Criteriu adaptat pentru examinarea regimurilor de interceptare în masă printr-o evaluare globală • Accentul pus pe „garanții de la un capăt la altul” pentru a ține seama de gradul crescut de intruziune în dreptul la viață privată, pe măsură ce procesul de interceptare în masă trece prin diferite etape • Deficiențe fundamentale prezente în regimul de interceptare în masă, ca urmare a lipsei unei autorizații independente, neincluderea unor categorii de selectori în cererea de emitere a unui mandat și neincluderea unor selectori legați de o persoană înainte de autorizarea prealabilă internă • Previzibilitate și garanții suficiente în regimul primirii de informații de la servicii de informații străine • Regim de obținere a datelor de comunicații de la furnizorii de servicii de comunicații care nu este „prevăzut de lege”

Art. 10 • Libertatea de exprimare • Protecția insuficientă a materialelor confidențiale ale jurnaliștilor în cadrul schemelor de supraveghere electronică

STRASBOURG

25 mai 2021

Prezenta hotărâre este definitivă, dar poate suferi modificări de formă.

În cauza Big Brother Watch și alții împotriva Regatului Unit,

Curtea Europeană a Drepturilor Omului, reunită în Marea Camera compusă din:

Robert Spano, *Președinte*,
Jon Fridrik Kjølbro,
Angelika Nußberger,
Paul Lemmens,
Yonko Grozev,
Vincent A. De Gaetano,
Paulo Pinto de Albuquerque,
Faris Vehabović,
Iulia Antoanella Motoc,
Carlo Ranzoni,
Mărtiș Mits,
Gabriele Kucsko-Stadlmayer,
Marko Bošnjak,
Tim Eicke,
Darian Pavli,
Erik Wennerström,
Saadet Yüksel, *judecători*,

și Søren Prebensen, *grefier-adjunct al Marii Camere*,

după ce a deliberat în camera de consiliu, la 11 iulie 2019, 4 și 6 septembrie 2019 și 17 februarie 2021,

pronunță prezenta hotărâre, adoptată la aceeași dată:

PROCEDURA

1. La originea cauzei se află trei cereri (nr. 58170/12, nr. 62322/12 și nr. 24969/12) îndreptate împotriva Regatului Unit al Marii Britanii și al Irlandei de Nord prin care companiile, organizațiile de caritate, persoanele fizice și juridice enumerate în anexă („părțile reclamante”), au sesizat Curtea la 4 septembrie 2013, 11 septembrie 2014, respectiv la 20 mai 2015, în temeiul art. 34 din Convenția pentru apărarea drepturilor omului și libertăților fundamentale („Convenția”).

2. Părțile reclamante au fost reprezentate de domnul D. Carey, din partea Deighton Pierce Glynn Solicitors, doamna R. Curling, din partea Leigh Day and Co. Solicitors, și doamna E. Norton, din partea Liberty. Guvernul Regatului Unit („Guvernul”) a fost reprezentat de agentul său guvernamental, domnul P. McKell, din cadrul Ministerului Afacerilor Externe și Commonwealth-ului (Foreign and Commonwealth Office).

3. Părțile reclamante s-au plâns de domeniul de aplicare și de amploarea programelor de supraveghere electronică operate de Guvernul Regatului Unit.

4. Cererile au fost comunicate Guvernului la 7 ianuarie 2014, 5 ianuarie 2015 și 24 noiembrie 2015. În prima cauză, cererea de a interveni a fost admisă pentru terții Human Rights Watch, Access Now, Dutch Against

Plasterk, Centrul pentru Democrație și Tehnologie (*Center For Democracy & Technology*), Rețeaua Europeană a Instituțiilor Naționale pentru Drepturile Omului (*European Network of National Human Rights Institutions*) și Comisia pentru Egalitatea și Drepturile Omului (*Equality and Human Rights Commission*), Fundația Helsinki pentru Drepturile Omului, Comisia Internațională a Juriștilor, Open Society Justice Initiative, The Law Society of England and Wales și Project Moore. În cea de-a doua cauză, a fost admisă cererea de a interveni pentru terții Center For Democracy & Technology, Fundația Helsinki pentru Drepturile Omului, Comisia Internațională a Juriștilor, Uniunea Națională a Jurnaliștilor (*National Union of Journalists*) și Asociația Avocaților de Mass-media (*Media Lawyers' Association*). În cea de-a treia cauză, cererea de a interveni a fost admisă pentru terții Grupul Articolul 19 (*Article 19*), Centrul Electronic de Informare cu privire la Viața Privată (*Electronic Privacy Information Center*) și Comisia pentru Egalitate și Drepturile Omului (*Human Rights Commission*).

5. La 4 iulie 2017, o cameră a Secției întâi a decis să conexeze cererile și să organizeze o audiere. Audierea a avut loc la 7 noiembrie 2017 în clădirea Curții Europene a Drepturilor Omului din Strasbourg. La 13 septembrie 2018, o cameră a secției respective, compusă din Linos-Alexandre Sicilianos, Kristina Pardalos, Aleš Pejchal, Ksenija Turković, Armen Harutyunyan, Pauliine Koskelo și Tim Eicke, judecători, și Abel Campos, grefier de secție, a pronunțat o hotărâre. Camera a declarat în unanimitate inadmisibile capetele de cerere formulate de părțile reclamante din cea de-a treia din cauzele conexate în ceea ce privește art. 6 și art. 10, în măsura în care părțile reclamante au invocat statutul lor de ONG-uri, și art. 14, și a declarat admisibile celelalte capete de cerere. Cu majoritate de voturi, Camera a declarat admisibile capetele de cerere formulate de părțile reclamante în prima și în cea de-a doua din cauzele conexate. Tot cu majoritate de voturi, a hotărât că au fost încălcate art. 8 și 10 din Convenție atât în ceea ce privește regimul prevăzut la art. 8 alin. (4) din Legea din 2000 privind competențele de investigare (*Regulation of Investigatory Powers Act 2000*, „RIPA”), cât și regimul prevăzut la Capitolul II din legea respectivă, și a hotărât că nu a fost încălcat art. 8 din Convenție în ceea ce privește regimul schimbului de informații. Au fost anexate la hotărâre opinia parțial concordantă și parțial dizidentă a doamnei judecător Koskelo, la care a subscris doamna judecător Turković, precum și opinia comună parțial concordantă și parțial dizidentă a domnilor judecători Pardalos și Eicke.

6. La 12 decembrie 2018, respectiv la 11 decembrie 2018, părțile reclamante din prima și din cea de-a treia cauză conexate au solicitat trimiterea cauzei în fața Marii Camere, în conformitate cu art. 43 din Convenție. La 4 februarie 2019, colegiul Marii Camere a admis cererea.

7. Compunerea Marii Camere a fost stabilită în conformitate cu dispozițiile art. 26 § 4 și 5 din Convenție și art. 24 din Regulamentul Curții.

8. Părțile reclamante și Guvernul au prezentat fiecare observații (art. 59 § 1) cu privire la admisibilitatea și fondul cauzei.

9. Președintele Marii Camere a admis cererea de a interveni în cadrul procedurii scrise, în conformitate cu art. 36 § 2 din Convenție și art. 44 § 3 din Regulament, pentru Guvernele Franței, Norvegiei și Țărilor de Jos, precum și pentru Raportorul special al Organizației Națiunilor Unite pentru promovarea și protecția dreptului la libertatea de opinie și de exprimare.

10. La 10 iulie 2019, a avut loc o ședință publică în clădirea Curții Europene a Drepturilor Omului din Strasbourg.

Au compărut în fața Curții:

a) *pentru Guvern*

domnul C. WICKREMASINGHE, *agent*,

domnul J. EADIE Q.C. ȘI

domnul J. MITFORD, *consilier*,

domnul R. YARDLEY,

doamna L. MORGAN,

domnul H. MAWBY,

domnul T. RUTHERFORD ȘI

domnul J. KEAY-BRIGHT, *consilieri*;

b) *pentru părțile reclamante*

domnul B. JAFFEY Q.C.,

doamna H. MOUNTFIELD Q.C.,

domnul MCCARTHY,

domnul R. MEHTA,

doamna G. SARATHY ȘI

domnul D. HEATON, *consilier*,

domnul D. CAREY ȘI

doamna R. CURLING, *consilieri*.

11. Curtea a audiat declarațiile domnilor Eadie, Jaffey și Mountfield, precum și răspunsurile acestora la întrebări.

ÎN FAPT

I. CONTEXTUL CAUZEI

12. Cele trei cereri au fost introduse în urma dezvăluirilor făcute de Edward Snowden cu privire la programele de supraveghere electronică operate de serviciile de informații din Statele Unite ale Americii și din Regatul Unit.

13. Părțile reclamante, enumerate în anexă, consideră că, având în vedere natura activităților lor, este probabil ca comunicațiile lor electronice să fi fost

interceptate de serviciile de informații din Regatul Unit, obținute de aceste servicii după ce au fost interceptate de guverne străine și/sau obținute de autoritățile din Regatul Unit de la furnizorii de servicii de comunicații („FSC”).

II. SISTEMELE DE SUPRAVEGHERE SECRETĂ PE INTERNET RELEVANTE PENTRU CAUZA DE FAȚĂ

14. Comunicațiile pe Internet sunt transportate în principal prin cabluri de fibră optică submarine operate de FSC. Fiecare cablu poate conține mai multe canale de transmisie (*bearers*), existând aproximativ 100 000 de astfel de canale de transmisie la nivel global, acestea constituind Internetul. O singură comunicație prin Internet este împărțită în „pachete” (unități de date) care pot fi transmise separat prin mai multe canale de transmisie. Aceste pachete circulă printr-o combinație a celor mai rapide și mai ieftine căi. În consecință, unele sau toate pachetele unei anumite comunicații trimise de la o persoană la alta, fie în Regatul Unit, fie la nivel transfrontalier, pot fi transmise prin una sau mai multe alte țări, dacă aceasta este calea optimă pentru FSC implicați.

A. Regatul Unit

1. Interceptarea în masă

15. Dezvăluirile făcute de Edward Snowden în 2013 indicau faptul că Cartierul General pentru Comunicații al Guvernului (*Government Communications Headquarters*, „GCHQ”, unul dintre serviciile de informații din Regatul Unit) derula operațiunea cu numele de cod „TEMPORA”, care îi permitea să acceseze și să stocheze volume uriase de date extrase din canalele de transmisie. Autoritățile britanice nu au confirmat, nici nu au negat existența unei operațiuni cu nume de cod TEMPORA.

16. Cu toate acestea, conform Raportului din martie 2015 al Comisiei pentru Informații și Securitate a Parlamentului (*Intelligence and Security Committee*) („raportul ISC” – infra, pct. 142-149), GCHQ opera două sisteme majore de prelucrare pentru interceptarea în masă a comunicațiilor.

17. Primul dintre cele două sisteme de prelucrare la care se făcea referire în raportul ISC viza un procent foarte mic de canale de transmisie. Pe măsură ce comunicațiile au circulat între canalele de transmisie vizate, sistemul compara traficul cu o listă de „selectorii simpli”. Aceștia erau identificatori specifici (de exemplu, o adresă de e-mail) referitori la o țintă cunoscută. Erau colectate toate comunicațiile care se potriveau cu selectorii simpli; cele care nu se potriveau erau eliminate automat. Analistii efectuau apoi un „proces de triaj” în ceea ce privește comunicațiile colectate pentru a stabili care erau cele mai valoroase informații și, prin urmare, trebuiau să fie deschise și citite. În practică, doar o foarte mică parte din elementele colectate în cadrul acestui

proces erau deschise și citite de analiști. Potrivit raportului ISC, GCHQ nu avea capacitatea de a citi toate comunicațiile.

18. Al doilea sistem de prelucrare viza un număr și mai redus de canale de transmisie (un subansamblu dintre cele accesate prin procesul descris la punctul de mai sus) care erau vizate în mod deliberat ca fiind cele mai susceptibile să efectueze comunicații de interes ca informație. Acest al doilea sistem se desfășura în două etape: în primul rând, aplicarea inițială a unui set de „reguli de prelucrare” destinate eliminării materialelor cel mai puțin importante și, în al doilea rând, aplicarea unor interogări complexe aplicate materialelor selectate pentru a stabili care sunt cele ar putea avea cea mai mare valoare ca informație. Aceste căutări generau un index și numai elementele din acest index puteau fi examinate de analiști. Toate comunicațiile care nu figurau în index trebuiau să fie eliminate.

19. Cadrul juridic pentru interceptarea în masă în vigoare la momentul faptelor este prezentat în detaliu în secțiunea „Dreptul intern relevant” de mai jos. Pe scurt, art. 8 alin. (4) din Legea din 2000 de reglementare a competențelor de investigare („RIPA” – infra, pct. 72) permitea ministrului să emită mandate pentru „interceptarea comunicațiilor externe”, dar, în temeiul art. 16 din RIPA (infra, pct. 84-92), materialele interceptate nu puteau fi selectate pentru a fi citite, examinate sau ascultate, „potrivit unui factor care are legătură cu o persoană despre care se cunoaște că se află pentru moment în Insulele Britanice”.

2. Schimbul de informații

20. Capitolul 12 din Codul de bune practici în interceptarea comunicațiilor (*Interception of Communications Code* – „Codul IC” – infra, pct. 116) stabilea condițiile în care serviciile de informații din Regatul Unit puteau solicita informații de la servicii de informații străine, precum și procedurile care trebuiau urmate pentru a formula o astfel de cerere. Capitolul 12 a fost adăugat la Codul IC după ce Tribunalul cu Competențe de Investigare (*Investigatory Powers Tribunal*, „IPT”) a dispus ca serviciile de informații să divulge procedurile lor de a face schimb de informații în cadrul procedurii inițiate de părțile reclamante în cea de-a treia din cauzele conexe („procedura *Liberty*” – infra, pct. 28-60).

3. Obținerea datelor de comunicații de la FSC

21. Capitolul II din RIPA și Codul de bune practici privind obținerea datelor de comunicații aferente reglementau procesul prin care anumite autorități publice puteau solicita date de comunicații de la FSC (infra, pct. 117-121).

B. Statele Unite ale Americii

22. Agenția Națională de Securitate („NSA”) a recunoscut existența a două operațiuni cu nume de cod PRISM și Upstream.

1. PRISM

23. PRISM era un program prin care Guvernul Statelor Unite ale Americii obținea materiale de informații (cum ar fi comunicații) de la furnizorii de servicii de internet („FSI”). Accesul în cadrul PRISM era specific și ținut (în contrast cu capacitatea amplă de „extragere a datelor”). Administrația Statelor Unite ale Americii a declarat că programul era reglementat de Legea privind supravegherea activităților străine de spionaj (*Foreign Intelligence Surveillance Act* – „FISA”) și toate cererile de acces la materiale în cadrul PRISM trebuiau să fie aprobate de Curtea de Supraveghere a Activităților Străine de Spionaj (*Foreign Intelligence Surveillance Court* – „FISC”).

24. Documentele NSA divulgate de Edward Snowden sugerau că GCHQ a avut acces la PRISM din iulie 2010 și l-a utilizat pentru a genera rapoarte de informații. GCHQ a recunoscut că a primit informații de la Statele Unite ale Americii care fuseseră obținute prin intermediul PRISM.

2. Upstream

25. Potrivit documentelor divulgate, programul Upstream permitea colectarea de date referitoare la conținut și date de comunicații provenite din infrastructura și cablurile de fibră optică deținute de FSC din Statele Unite ale Americii. Acest program a avut acces larg la date globale, în special ale resortisanților care nu erau americani, care au putut fi ulterior colectate, stocate și examinate utilizând cuvinte-cheie (pentru detalii suplimentare, infra, pct. 261-264).

III. PROCEDURILE INTERNE DIN PRIMA ȘI DIN CEA DE-A DOUA DIN CAUZELE CONEXATE

26. Părțile reclamante din prima din cauzele conexate (cererea nr. 58170/13) au transmis Guvernului, la 3 iulie 2013, o scrisoare de protocol anterioară sesizării instanței în care își enunțau plângerile și solicitau autorităților să declare că art. 1 și 3 din Legea din 1994 privind serviciile de informații (*Intelligence Services Act* 1994 – „ISA” – infra, pct. 108 și 110), art. 1 din Legea privind serviciile de securitate din 1989 (*Security Services Act* 1989 – „SSA” – infra, pct. 106) și art. 8 din RIPA (infra, pct. 66) erau incompatibile cu Convenția. În răspunsul său din 26 iulie 2013, Guvernul a afirmat că art. 65 alin. (2) din RIPA avea ca efect excluderea competenței *High Court* în ceea ce privește plângerile referitoare la drepturile omului formulate împotriva serviciilor de informații, dar că plângerile părților

reclamante puteau fi formulate în fața IPT. IPT era un tribunal specializat înființat în temeiul RIPA pentru a examina plângerile formulate de resortisanți care se considerau victime ale unei ingerințe ilicite din partea autorităților în comunicațiile lor ca urmare a unei activități reglementate de respectiva lege și avea competență exclusivă pentru a investiga orice plângere privind interceptarea comunicațiilor unei persoane și, în cazul în care o asemenea interceptare a avut loc, pentru a examina baza în care a fost efectuată (infra, pct. 122-133). Cu toate acestea, părțile reclamante nu au întreprins demersuri suplimentare.

27. Părțile reclamante din cea de-a doua din cauzele conexe (cererea nr. 62322/14) nu au inițiat nicio procedură internă, întrucât au considerat că nu dispuneau de o cale de atac efectivă pentru plângerile formulate în temeiul Convenției.

IV. PROCEDURI INTERNE ÎN CEA DE-A TREIA DIN CAUZELE CONEXATE

28. Cele zece organizații pentru drepturile omului care sunt reclamante în cea de-a treia din cauzele conexe (cererea nr. 24960/15) au formulat fiecare plângere în fața IPT între iunie și decembrie 2013 („procedura *Liberty*”). Acestea au susținut că serviciile de informații, ministrul internelor și ministrul afacerilor externe au acționat prin încălcarea art. 8, 10 și 14 din Convenție: (i) accesând sau primind de la Guvernul Statelor Unite ale Americii comunicații și date de comunicații interceptate în temeiul programelor PRISM și Upstream („plângerea legată de PRISM”); și (ii) interceptând, inspectând și păstrând comunicațiile și datele lor de comunicații în cadrul programului TEMPORA [„plângerea legată de art. 8 alin. (4)”].

29. La 14 februarie 2014, IPT a dispus conexarea celor zece cauze. Ulterior, a desemnat avocatul de pe lângă IPT (infra, pct. 132), însărcinat cu asistarea IPT în orice mod i se solicita, inclusiv prin prezentarea de observații cu privire la aspecte în legătură cu care nu toate părțile puteau fi reprezentate (de exemplu, din motive de securitate națională).

30. În răspunsul său la plângerile părților reclamante, Guvernul a adoptat o abordare de tipul „nu putem confirma sau nega”, și anume a refuzat să confirme sau să nege dacă comunicațiile părților reclamante fuseseră cu adevărat interceptate. Prin urmare, s-a convenit că IPT va examina aspectele legale pe baza faptelor prezumate că NSA a obținut comunicațiile și datele de comunicații ale părților reclamante prin intermediul PRISM sau Upstream și le-a transferat către GCHQ, unde acestea au fost reținute, păstrate, stocate, analizate și partajate, precum și că comunicațiile și datele de comunicații ale părților reclamante au fost interceptate de GCHQ în cadrul programului TEMPORA și au fost reținute, păstrate, analizate și partajate. Întrebarea era dacă, pe baza acestor fapte prezumate, interceptarea, păstrarea, stocarea și

schimbul de date erau compatibile cu art. 8 și 10, considerate separat și coroborate cu art. 14 din Convenție.

A. Audierea

31. IPT, compus din doi judecători ai High Court, un judecător regional (*circuit judge*) și doi avocați pledanți experimentați (*senior barristers*), a organizat o audiere publică de cinci zile, în perioada 14-18 iulie 2014. Guvernul a solicitat o audiere cu ușile închise suplimentară pentru a permite IPT să examineze procedurile interne nepublice ale GCHQ – descrise în cursul audierii publice ca fiind „sub linia de plutire” („nepublice”) – de prelucrare a materialelor interceptate. Părțile reclamante au obiectat, susținând că organizarea unei audieri cu ușile închise nu era justificată și că faptul că nu le-au fost divulgate procedurile era contrar legii.

32. Cererea de audiere cu ușile închise a fost admisă în temeiul art. 9 din Regulamentul de procedură al IPT (infra, pct. 129). La 10 septembrie 2014, a avut loc o audiere cu ușile închise, în cadrul căreia IPT a fost „asistat prin participarea deplină, perceptivă și neutră [...] a avocatului de pe lângă Tribunal”, care a îndeplinit următoarele roluri: (i) identificarea documentelor, a părților din documente sau a elementelor care puteau fi divulgate în mod adecvat; (ii) depunerea acestor observații în favoarea divulgării informațiilor ca fiind în interesul părților reclamante și al unei justiții deschise; și (iii) garantarea faptului că toate argumentele relevante (din perspectiva părților reclamante) în fapt și în drept sunt prezentate în fața IPT.

33. În cadrul audierii cu ușile închise, IPT a examinat procedurile interne („nepublice”) care reglementau activitatea și practica serviciilor de informații. La 9 octombrie 2014, a comunicat părților reclamante că aprecia că existau anumite materiale confidențiale care puteau fi divulgate. IPT a explicat că a invitat Guvernul să divulge materialele și că Guvernul a fost de acord să facă acest lucru. În consecință, materialele au fost furnizate părților reclamante într-o notă („nota de divulgare din 9 octombrie”), iar părțile au fost invitate să prezinte observații în fața IPT cu privire la materialele divulgate.

34. Părțile reclamante au solicitat informații privind contextul și sursa elementelor divulgate, dar IPT a refuzat să furnizeze detalii suplimentare. Părțile reclamante au prezentat observații în ceea ce privește nota de divulgare.

35. Ulterior, părțile reclamante au modificat și completat materialele divulgate.

36. În urma divulgărilor finale din 12 noiembrie 2014, nota de divulgare din 9 octombrie indica următoarele:

„Guvernul SUA a recunoscut public că sistemul Prism și programul Upstream [...] permit obținerea de comunicații către, dinspre sau cu privire la anumiți selectori legați de persoane care nu sunt americane despre care se crede în mod rezonabil că se află în

afara Statelor Unite ale Americii pentru a obține informații operative străine. În măsura în care serviciile de informații sunt autorizate de Guvernul SUA să solicite materiale obținute în cadrul sistemului Prism (și/sau [...] în cadrul programului Upstream), aceste cereri pot fi formulate numai pentru comunicațiile interceptate neanalizate (și datele de comunicații aferente) obținute în acest mod.

1. Serviciile de informații nu pot formula o cerere către guvernul unei țări sau al unui teritoriu din afara Regatului Unit decât pentru comunicații interceptate neanalizate (și datele de comunicații aferente), în alte cazuri decât conform unui acord internațional de asistență judiciară reciprocă, dacă:

- a. un mandat de interceptare relevant în temeiul [RIPA] a fost deja emis de ministru, asistența guvernului străin fiind necesară pentru obținerea comunicărilor în cauză deoarece nu pot fi obținute în temeiul mandatului de interceptare respectiv și obținerea lor de către serviciile de informații este necesară și proporțională cu scopul urmărit; sau
- b. cererea de obținere a acestor comunicații, în lipsa unui mandat de interceptare relevant în temeiul RIPA nu reprezintă o eludare deliberată a RIPA și nici nu este contrară principiului consacrat în *Padfield împotriva Ministrului Agriculturii, Pescuitului și Alimentației* [1968] AC 997 [o instituție publică are obligația de a-și exercita puterile discreționare pentru a promova (și nu pentru a eluda) politica și obiectele legislației prin care i-au fost conferite aceste puteri] (de exemplu, pentru că nu este posibilă din punct de vedere tehnic obținerea comunicărilor prin intermediul interceptării în temeiul RIPA) și este necesar și proporțional ca serviciile de informații să obțină comunicațiile respective. În aceste condiții, ministrul va examina și va decide personal cu privire la oportunitatea formulării cererii. Acest tip de cerere va fi făcută numai în circumstanțe excepționale, și nicio astfel de cerere nu a fost formulată la data prezentei declarații.

[...]

2. În cazul în care serviciile de informații primesc conținutul comunicațiilor interceptate sau date de comunicații de la guvernul unei țări sau al unui teritoriu din afara Regatului Unit, indiferent dacă acestea sunt solicitate sau nesolicitate, dacă conținutul este analizat sau nu sau dacă datele de comunicații sunt asociate sau nu cu conținutul comunicațiilor, conținutul și datele de comunicații sunt, în temeiul «procedurilor» interne, supuse aceluiași norme și garanții interne ca și aceleași categorii de conținut sau de date care sunt obținute direct de serviciile de informații ca urmare a interceptării în temeiul RIPA.

3. Serviciile de informații care primesc materiale interceptate neanalizate și date de comunicații aferente interceptării pe baza unui mandat emis în temeiul art. 8 alin. (4) stabilesc «proceduri» interne care impun crearea unei înregistrări, explicând de ce este necesar accesul la materialele interceptate neanalizate, înainte ca o persoană autorizată să poată accesa astfel de materiale în temeiul art. 16 din RIPA.

4. «Procedurile» interne ale serviciilor de informații care primesc materiale interceptate neanalizate și date de comunicații aferente interceptării pe baza unui mandat emis în temeiul art. 8 alin. (4) stabilesc (sau necesită să fie stabilite, pentru fiecare sistem în parte) perioadele maxime de păstrare pentru diferite categorii de astfel de date, care reflectă natura și caracterul intruziv al datelor specifice în discuție. Perioadele astfel specificate (sau stabilite) nu depășesc în mod normal 2 ani și, în anumite cazuri, sunt semnificativ mai scurte (rapoartele de informații care se bazează pe astfel de date sunt tratate ca o categorie separată și sunt păstrate pentru o perioadă mai lungă). Datele pot fi păstrate pentru o perioadă mai lungă decât perioada maximă

de păstrare aplicabilă numai în cazul în care a fost obținută o autorizare prealabilă din partea unui înalt funcționar din cadrul serviciului de informații în cauză, pe baza faptului că păstrarea continuă a datelor specifice în discuție a fost evaluată ca fiind necesară și proporțională (dacă păstrarea în continuare a acestor date nu mai îndeplinește criteriile necesității și proporționalității, aceste date sunt șterse). În măsura posibilului, toate perioadele de păstrare sunt implementate printr-un proces de ștergere automată care se declanșează odată ce a fost atinsă perioada maximă de păstrare aplicabilă pentru datele în discuție. Perioadele maxime de păstrare sunt monitorizate de Comisar și convenite cu acesta. În ceea ce privește în special datele de comunicații aferente, Sir Anthony May a făcut o recomandare serviciilor de informații care primesc materiale interceptate neanalizate și date de comunicații aferente interceptării pe baza unui mandat emis în temeiul art. 8 alin. (4), iar Comisarul interimar (Sir Paul Kennedy) s-a exprimat recent ca fiind mulțumit de modul în care a fost implementată recomandarea respectivă.

5. «Procedurile interne» ale serviciilor de informații în temeiul Legii privind serviciile de securitate din 1989, Legii privind serviciile de informații din 1994 și al art. 15-16 din RIPA sunt revizuite periodic pentru a se asigura că sunt actualizate și efective. În plus, serviciile de informații analizează, în continuare, în cursul unor astfel de revizuii periodice, dacă mai multe dintre aceste proceduri interne ar putea fi plasate în mod sigur și util în domeniul public (de exemplu, prin includerea într-un cod de bune practici relevant).»

B. Prima hotărâre a IPT din 5 decembrie 2014

37. IPT a pronunțat prima sa hotărâre la 5 decembrie 2014. Hotărârea privea procedurile în materie de interceptare a comunicațiilor și de obținere a comunicațiilor interceptate de la servicii de informații străine.

1. Plângerea legată de PRISM

38. IPT a acceptat că plângerea legată de PRISM angajează art. 8 din Convenție, deși la un „nivel inferior” față de regimul examinat în *Weber și Saravia împotriva Germaniei* (dec.), nr. 54934/00, CEDO 2006-XI. În consecință, trebuia ca autoritățile implicate în prelucrarea comunicațiilor primite de la serviciile de informații străine să respecte cerințele art. 8, în special în ceea ce privește stocarea, partajarea, păstrarea și distrugerea acestora. În opinia IPT, bazându-se pe concluziile din *Bykov împotriva Rusiei* (MC), nr. 4378/02, pct. 76 și 78, 10 martie 2009 și *Malone împotriva Regatului Unit*, 2 august 1984, Seria A nr. 82, pentru ca ingerința să poată fi considerată „prevăzută de lege”, nu putea exista o marjă de apreciere nelimitată acordată acțiunii executivului, ci mai degrabă trebuia ca natura normelor să fie clară, iar domeniul de aplicare al normelor trebuia, în măsura posibilului, să fie în spațiul public. Cu toate acestea, a considerat evident că, în domeniul securității naționale, era necesară o expunere mai redusă în spațiul public și să se reducă gradul de previzibilitate prevăzut la art. 8, pentru că, în caz contrar, întregul scop al măsurilor luate pentru a proteja securitatea națională ar fi pus în pericol (citând *Leander împotriva Suediei*, 26 martie 1987, pct. 51, Seria A nr. 116).

39. IPT a continuat:

„41. Considerăm că este necesar indicarea suficientă a normelor sau a procedurilor, în măsura în care acestea nu sunt divulgate [...] Avem convingerea că, în domeniul schimbului de informații, nu se poate aștepta ca normele să fie conținute în statut (*Weber*) sau într-un cod (așa cum a solicitat Curtea în hotărârea pronunțată în cauza *Liberty [împotriva Regatului Unit*, nr. 58243/00, 1 iulie 2008]). În opinia noastră, este suficient:

i) să existe norme sau proceduri adecvate a căror existență să fie făcută public și recunoscută, conținutul acestora fiind suficient divulgat astfel încât să se știe în ce constau (vezi hotărârea *Malone*).

ii) să facă obiectul unui control corespunzător.”

40. IPT a observat că modalitățile privind schimbul de informații erau prevăzute în cadrul legal stabilit în Legea din 1989 privind serviciile de securitate (infra, pct. 105-106) și în Legea din 1994 privind serviciile de informații (infra, pct. 107-110). A făcut referire, de asemenea, la o declarație dată în calitate de martor în cauza *Liberty* sus-menționată de Charles Farr, directorul general al Oficiului pentru Securitate și Combaterea Terorismului („OSCT”) din cadrul Ministerului Internelor, care a explicat că cadrul legislativ prevăzut de respectivele acte era susținut de orientări interne detaliate, inclusiv de proceduri care să garanteze că serviciile obțineau doar informațiile necesare pentru îndeplinirea adecvată a funcțiilor lor. Acesta a indicat, de asemenea, că personalul beneficia de formare obligatorie cu privire la cadrul juridic și politic în care își desfășura activitatea, inclusiv instrucțiuni clare cu privire la necesitatea respectării stricte a legii și orientărilor interne. În sfârșit, a afirmat că detaliile complete ale procedurilor erau confidențiale, întrucât nu puteau fi publicate în siguranță fără a aduce atingere intereselor securității naționale.

41. IPT a recunoscut că, întrucât procedurile nu au fost aduse la cunoștința publicului, nici măcar sub formă de rezumat, nu erau accesibile. Cu toate acestea, IPT a considerat că este semnificativ faptul că procedurile au făcut obiectul controlului și investigării de către Comisia pentru Informații și Securitate a Parlamentului (*Intelligence and Security Committee of Parliament* – „ISC”) și de către Comisarul independent pentru Interceptarea Comunicațiilor (*Interception of Communications Commissioner* – „Comisarul IC”). Pe de altă parte, IPT era în măsură să asigure controlul, să aibă acces la toate informațiile secrete și să suspende ședința publică pentru a organiza o audiere cu ușile închise pentru a aprecia dacă procedurile menționate de domnul Farr existau și erau de natură să asigure protecția individuală împotriva ingerințelor arbitrare.

42. După ce a luat în considerare procedurile „nepublice”, IPT a concluzionat că nota de divulgare din 9 octombrie (astfel cum a fost modificată ulterior – supra, pct. 33 și 36) oferea un rezumat clar și exact al acelei părți a probelor prezentate în cadrul audierii cu ușile închise și că restul probelor prezentate în cadrul audierii respective erau prea sensibile pentru a

fi divulgate fără riscuri pentru securitatea națională sau pentru principiul „nu putem confirma sau nega”. În plus, a considerat că precondițiile pentru solicitarea de informații de la Guvernul Statelor Unite ale Americii erau clare: era necesar să existe fie un mandat emis în temeiul art. 8 alin. (1), fie un mandat în temeiul art. 8 alin. (4) care să acopere comunicațiile țintei vizate, și, în cazul în care se știa că persoana se află în Insulele Britanice, un act modificator în temeiul art. 16 alin. (3) (infra, pct. 86). Orice cerere formulată în temeiul PRISM sau Upstream cu privire la comunicațiile interceptate sau datele de comunicații era, prin urmare, supusă regimului RIPA, cu excepția cazului în care se încadra în scenariul cu totul excepțional prezentat la pct. 1 lit. b) privind materialele divulgate după prima audiere. Cu toate acestea, nu a fost formulată niciodată o cerere în temeiul pct. 1 lit. b).

43. IPT a identificat însă următoarele „subiecte de îngrijorare”:

„Deși este adevărat că orice solicitare sau primire de comunicații interceptate sau date de comunicații prin intermediul Prism și/sau Upstream este supusă, în mod normal, aceluiași garanții ca în cazul în care datele de comunicații sau interceptate sunt obținute direct de către pârâți, în cazul în care există o cerere în temeiul pct. 1 lit. b), chiar dacă o astfel de cerere trebuie adresată ministrului și orice materiale astfel obținute trebuie tratate în conformitate cu RIPA, există posibilitatea ca protecția prevăzută la art. 16 să nu se aplice. Astfel cum s-a arătat deja, pct. 1 lit. b) nu a fost niciodată invocat și, prin urmare, până în prezent nu a existat nicio problemă. Cu toate acestea, avem convingerea că ar trebui introdusă o procedură prin care orice astfel de cerere, dacă este adresată ministrului, trebuie să abordeze chestiunea art. 16 alin. (3).”

44. Cu toate acestea, sub rezerva menționată, IPT a ajuns la următoarele concluzii:

„(i) Având în vedere procedurile nepublice, astfel cum sunt ele descrise în prezenta hotărâre, considerăm că există proceduri adecvate pentru a asigura conformitatea cu cadrul legal și cu art. 8 și 10 din Convenție, în ceea ce privește primirea datelor interceptate prin intermediul Prism și/sau Upstream.

(ii) Desigur, acest lucru nu este în sine suficient, întrucât procedurile trebuie să fie suficient accesibile publicului. Considerăm că acestea sunt suficient semnalate în virtutea cadrului legal la care am făcut trimitere și a declarațiilor ISC și ale Comisarului, citate mai sus, și, la fel ca în prezent, în urma celor două audieri cu ușile închise pe care le-am organizat, au fost făcute publice de către pârâți și înregistrate în prezenta hotărâre.

(iii) Aceste proceduri fac obiectul unui control.

(iv) Întinderea puterii discreționare conferite pârâților pentru a primi și a gestiona materialele interceptate și datele de comunicații și [sub rezerva aspectelor care privesc art. 8 alin. (4) menționate mai jos]] modalitatea de exercitare a acestei puteri sunt, în consecință (și în conformitate cu *Bykov* – supra, pct. 37), accesibile cu suficientă claritate pentru a oferi fiecărei persoane o protecție adecvată împotriva oricărei ingerințe arbitrară.”

45. În sfârșit, IPT a răspuns unui argument invocat doar de Amnesty International, și anume acela că Regatul Unit avea o obligație pozitivă în temeiul art. 8 din Convenție de a preveni sau de a împiedica ca Statele Unite ale Americii să intercepteze comunicații, inclusiv obligația de a nu accepta o

astfel de interceptare prin primirea produsului său. Cu toate acestea, IPT, invocând *M. și alții împotriva Italiei și Bulgariei*, nr. 40020/03, pct. 127, 31 iulie 2012, menționa că „organele Convenției au afirmat în mod repetat că aceasta nu conține un drept care impune unei înalte părți contractante să exercite protecție diplomatică, să invoce plângerile unui reclamant în temeiul dreptului internațional sau să intervină în alt mod în relația cu autoritățile altui stat, în numele acestuia”. Prin urmare, IPT a respins acest argument.

2. Plângerea legată de art. 8 alin. (4)

46. IPT a formulat patru întrebări la care era necesar să se răspundă pentru a se stabili dacă regimul prevăzut la art. 8 alin. (4) (care prevedea cadrul juridic al interceptării în masă a comunicațiilor externe) era compatibil cu Convenția:

„(1) Este contrară art. 8 § 2 din Convenție dificultatea de a stabili diferența dintre comunicațiile externe și cele interne [...] astfel încât regimul prevăzut la art. 8 alin. (4) să fie privat de bază legală?

(2) În măsura în care art. 16 din RIPA este necesar drept o garanție pentru ca ingerința în dreptul prevăzut la art. 8 să fie prevăzută de lege, este această garanție suficientă?

(3) Respectă acest regim, în prezența sau în lipsa art. 16, cerințele *Weber*, în măsura în care acest fapt este necesar pentru a fi prevăzut de lege?

(4) Art. 16 alin. (2) constituie o discriminare indirectă, în sensul art. 14 din Convenție, și, în cazul unui răspuns afirmativ, poate fi el justificat?”

47. În ceea ce privește prima întrebare, părțile reclamante au susținut că, în urma „schimbărilor decisive în domeniul tehnologiei începând cu anul 2000”, tot mai multe comunicații erau în prezent externe, astfel încât distincția comunicații interne/externe prevăzută la art. 8 alin. (4) nu mai era „adevătată scopului”. Deși IPT a admis că schimbările tehnologice erau substanțiale și că era imposibil să se facă diferența, în etapa interceptării, între comunicațiile externe și cele interne, a constatat că diferențele în ceea ce privește definiția exactă a „comunicațiilor externe” nu fac, în sine, ca regimul prevăzut la art. 8 alin. (4) să fie incompatibil cu art. 8 § 2 din Convenție. În această privință, a considerat că dificultatea de a face distincție între comunicațiile „interne” și cele „externe” exista încă din momentul adoptării RIPA și că schimbările tehnologice nu modificaseră semnificativ cantitatea sau proporția comunicațiilor care puteau sau nu puteau fi diferențiate ca fiind externe sau interne la momentul interceptării. În cel mai rău caz, „au accelerat procesul care făcea ca mai multe lucruri din această lume, pe baza unei analize veritabile, depășeau cadrul frontierelor naționale”. În orice caz, distincția era relevantă doar în etapa interceptării. „Povara cea mai grea” era dusă de art. 16 din RIPA, care nu permitea ca materialul interceptat selectat să fie citit, examinat sau ascultat „în conformitate cu un factor care are legătură cu o persoană despre care se cunoaște că se află pentru moment în Insulele Britanice” (infra, pct. 84-92). În plus, toate comunicațiile

interceptate pe baza unui mandat emis în temeiul art. 8 alin. (4) puteau fi examinate numai în raport cu art. 16.

48. În ceea ce privește cea de-a doua întrebare, IPT a hotărât că garanțiile prevăzute la art. 16, care nu se aplicau decât materialelor interceptate, nu și datelor de comunicații aferente, erau suficiente. Deși a concluzionat că criteriile *Weber* se extindeau și la datele de comunicații, a considerat că există protecție și garanții adecvate prin trimitere la art. 15 din RIPA (infra, pct. 77-82). În plus, în măsura în care art. 16 asigura o protecție mai mare pentru conținutul comunicațiilor decât pentru datele de comunicații, diferența era justificată și proporțională, întrucât datele de comunicații erau necesare pentru identificarea persoanelor ale căror materiale interceptate erau protejate de art. 16 (și anume, persoanele despre care se știa că se află în Insulele Britanice).

49. Abordând cea de a treia întrebare, IPT a concluzionat că regimul prevăzut la art. 8 alin. (4) respectă în mod suficient criteriile *Weber* (și anume criteriile stabilite în *Weber și Sarabia*, citată anterior, pct. 95; de asemenea, infra, pct. 274 și 335) și că, în orice caz, era „prevăzut de lege”. În ceea ce privește primele două cerințe, IPT a considerat că trimiterea la „securitatea națională” era suficient de clară [citând *Esbestor împotriva Regatului Unit* (dec.), nr. 18601/91, 2 aprilie 1993, și *Kennedy împotriva Regatului Unit*, nr. 26839/05, 18 mai 2010]; lipsa țintirii în etapa interceptării era acceptabilă și inevitabilă, la fel ca în *Weber*; în viziunea IPT, dispozițiile pct. 5.2 din Codul IC, coroborate cu pct. 2.4, 2.5, 5.3, 5.4, 5.5 și 5.6 (infra, pct. 96), erau satisfăcătoare; nu era necesară includerea cuvintelor de căutare în cererea de emitere a mandatului sau în mandatul propriu-zis, întrucât acest lucru ar fi afectat și ar fi limitat în mod inutil executarea mandatului și ar fi putut să fie un lucru total nerealist; nu exista nicio cerință ca mandatul să trebuiască să primească autorizare judiciară.

50. Examinând cele de-al treilea, al patrulea, al cincilea și al șaselea criterii *Weber*, IPT a ținut seama de garanțiile prevăzute la art. 15 și 16 din RIPA, Codul IC și procedurile „nepublice”. IPT nu a considerat necesar ca detaliile exacte ale tuturor garanțiilor să fie publicate sau incluse în statut sau în codul de bune practici. În special în domeniul securității naționale, ar putea fi luate în considerare proceduri administrative nedivulgate, care, prin definiție, ar putea fi modificate de executiv, fără a se face trimitere la Parlament, sub rezerva ca ceea ce este divulgat să indice întinderea puterii discreționare și modul de exercitare a acesteia. Acest lucru era valabil, în special, atunci când, precum în speță, Codul IC făcea trimitere la proceduri și exista un sistem de control (exercitat de Comisarul IC, IPT însuși și ISC), prin care se asigura că procedurile sunt supuse controlului. IPT a constatat cu satisfacție că, în urma audierii cu ușile închise, nu fusese creată o bază mare de date de comunicații și că existau proceduri adecvate cu privire la durata păstrării datelor și distrugerea acestora. Ca și în cazul plângerii legate de PRISM, IPT a considerat că regimul prevăzut la art. 8 alin. (4) a fost semnalat în mod

suficient în statut, în Codul IC, în rapoartele Comisarului IC și, acum, în propria sa hotărâre.

51. În ceea ce privește cele de-a patra și ultima întrebare, IPT nu a clarificat aspectul cu privire la existența efectivă a unei discriminări indirecte bazate pe originea națională ca urmare a regimurilor diferite aplicabile persoanelor aflate în Insulele Britanice și celor situate în afara acestora, considerând că orice discriminare indirectă era suficient de justificată, pe motiv că era mai dificil să fie investigate amenințările teroriste și infracționale din străinătate. Având în vedere că scopul accesului la comunicații externe era în principal acela de a obține informații despre persoanele din străinătate, consecințele eliminării distincției ar fi fost necesitatea de a obține un certificat în temeiul art. 16 alin. (3) din RIPA [care permitea în mod excepțional accesul la materiale privind persoanele din Insulele Britanice interceptate pe baza unui mandat emis în temeiul art. 8 alin. (4) – infra, pct. 86) în aproape orice caz, ceea ce ar fi subminat radical eficacitatea regimului prevăzut la art. 8 alin. (4).

52. În sfârșit, părțile reclamante au susținut că protecția conferită de art. 10 din Convenție se aplica ONG-urilor care realizau investigații în același mod în care se aplica jurnaliștilor. Amnesty International a susținut inițial în fața IPT că era posibil să nu existe proceduri adecvate pentru materialele protejate de secretul profesional al avocaților, plângere care, ulterior, a fost „transferată” în cauza *Belhadj* (infra, pct. 99-101), în care Amnesty International s-a alăturat ca parte reclamantă suplimentară. Nu a fost prezentat niciun argument similar în ceea ce privește confidențialitatea datelor ONG-urilor până la 17 noiembrie 2014 (după prima și a doua audiere deschisă publicului). Întrucât IPT a considerat că acest argument ar fi putut fi invocat în orice moment, în hotărâre a concluzionat că a fost invocat „extrem de tardiv” pentru a fi inclus în cadrul procedurii.

53. În ceea ce privește celelalte capete de cerere formulate în temeiul art. 10, IPT a observat că nu există niciun argument separat în plus față de cel care fusese invocat în temeiul art. 8. În pofida faptului că IPT a avut în vedere *Sanoma Uitgevers B.V. împotriva Țărilor de Jos* (MC), nr. 38224/03, 14 septembrie 2010, a subliniat că speța părților reclamante nu privea supravegherea ținută a jurnaliștilor sau a organizațiilor neguvernamentale. În orice caz, în opinia sa, în contextul monitorizării neținute pe baza unui mandat emis în temeiul art. 8 alin. (4), ar fi „în mod clar imposibil” să se anticipeze o autorizare judiciară înainte de emiterea mandatului, limitată la ceea ce s-ar putea dovedi a avea un impact asupra art. 10. Deși IPT a admis că ar putea apărea o problemă în cazul în care, în cursul examinării conținutului, ar apărea o anumită problemă de confidențialitate jurnalistică, Codul IC conținea garanții suplimentare în ceea ce privește tratamentul unor astfel de materiale.

54. În urma publicării hotărârii, părțile au fost invitate să prezinte observații cu privire la conformitatea, înainte de divulgarea către IPT, a regimului juridic în vigoare în ceea ce privește întrebarea dacă plângerea

legată de PRISM este conformă cu art. 8 și 10, precum și cu privire la proporționalitatea și legalitatea oricărei preținse interceptări a comunicațiilor lor. IPT nu a considerat necesară prezentarea de informații suplimentare cu privire la proporționalitatea regimului prevăzut la art. 8 alin. (4) în ansamblul său.

C. Cea de-a doua hotărâre a IPT din 6 februarie 2015

55. În cea de-a doua hotărâre din 6 februarie 2015, IPT a examinat dacă, înainte de hotărârea sa din decembrie 2014, procedurile privind PRISM sau Upstream au încălcat art. 8 și/sau 10 din Convenție.

56. A admis că numai prin raportare la nota de divulgare din 9 octombrie, astfel cum a fost modificată (supra, pct. 33 și 36), regimul era „prevăzut de lege”. Opinia IPT a fost că, în lipsa divulgărilor, nu ar fi existat o semnalizare adecvată, astfel cum era prevăzut la art. 8 și 10. Prin urmare, a declarat că, înainte de divulgarea informațiilor:

„23. [...] [r]egimul care reglementează solicitarea, primirea, stocarea și transmiterea de către autoritățile din Regatul Unit a comunicațiilor private ale persoanelor aflate în Regatul Unit, care au fost obținute de autoritățile SUA în cadrul Prism și/sau [...] Upstream, a încălcat art. 8 sau 10 din CEDO, dar acum îl respectă.”

D. Cea de-a treia hotărâre a IPT din 22 iunie 2015, astfel cum a fost modificată prin scrisoarea sa din 1 iulie 2015

57. Cea de-a treia hotărâre a IPT, publicată la 22 iunie 2015, a examinat dacă comunicațiile părților reclamante obținute prin intermediul PRISM sau Upstream fuseseră solicitate, primite, stocate sau transmise de autoritățile britanice cu încălcarea art. 8 și/sau 10 din Convenție și dacă comunicațiile părților reclamante au fost interceptate, examinate, depozitate sau transmise de autoritățile britanice astfel încât să constituie o activitate ilegală sau contrară art. 8 și/sau 10.

58. IPT a respins opt dintre cele zece plângeri ale părților reclamante. În linie cu practica sa obișnuită în asemenea cazuri, IPT nu a confirmat dacă comunicațiile acestora au fost interceptate sau nu. Cu toate acestea, IPT a efectuat aprecieri cu privire la două dintre părțile reclamante. Identitatea uneia dintre organizații a fost înscrisă greșit în hotărâre, iar eroarea a fost corectată prin scrisoarea IPT din 1 iulie 2015.

59. În privința Amnesty International, IPT a constatat că comunicațiile electronice fuseseră interceptate și accesate în mod legal și proporțional în temeiul art. 8 alin. (4) din RIPA, dar că termenul de păstrare permis de politicile interne ale GCHQ fusese trecut cu vederea și, prin urmare, materialele au fost păstrate pentru o perioadă mai lungă de timp decât cea admisă. Cu toate acestea, IPT a avut convingerea că materialele nu au fost accesate după expirarea termenului de păstrare relevant și că încălcarea putea

fi calificată drept una tehnică. Cu toate acestea, a fost încălcat art. 8 și s-a dispus ca GCHQ să distrugă oricare dintre comunicațiile care au fost păstrate pentru o perioadă mai lungă de timp decât perioada relevantă și să transmită o copie tipărită a documentelor în termen de șapte zile Comisarului IC, care să le păstreze pe o perioadă de cinci ani, în cazul în care acestea ar fi necesare pentru orice proceduri judiciare ulterioare. S-a dispus, de asemenea, ca GCHQ să prezinte un raport confidențial, în termen de paisprezece zile, care să confirme distrugerea documentelor. Nu s-au acordat despăgubiri.

60. În privința Centrului de Resurse Juridice, IPT a constatat că comunicațiile de la o adresă de e-mail asociată reclamantei fuseseră interceptate și selectate spre examinare pe baza unui mandat emis în temeiul art. 8 alin. (4). Deși a considerat că interceptarea a fost legală și proporțională și că selecția făcută spre examinare a fost proporțională, IPT a constatat că procedura internă de selecție nu fusese urmată. Prin urmare, a avut loc o încălcare a drepturilor Centrului de Resurse Juridice prevăzute la art. 8. Cu toate acestea, IPT a considerat că datele nu au fost utilizate și că nu a fost păstrată nicio înregistrare, astfel încât reclamanta nu a suferit niciun prejudiciu, moral sau material. Prin urmare, decizia sa a constituit o reparație echitabilă și nu a fost acordată nicio despăgubire.

CADRUL JURIDIC ȘI PRACTICA RELEVANTĂ

I. DREPTUL INTERN RELEVANT

A. Interceptarea comunicațiilor

1. Mandatele: dispoziții generale

61. Art. 1 alin. (1) din RIPA 2000 (care a fost înlocuit de Legea privind competențele de investigare din 2016) consideră ilegală interceptarea oricărei comunicații în cursul transmiterii sale prin intermediul unui serviciu poștal public sau al unui sistem public de telecomunicații, cu excepția cazului în care a avut loc în baza unui mandat emis în temeiul art. 5 („mandat de interceptare”).

62. Art. 5 alin. (2) permitea ministrului să autorizeze emiterea unui mandat de interceptare în cazul în care considera că acest lucru era necesar din motivele prevăzute la art. 5 alin. (3), și anume că era în interesul securității naționale, în scopul prevenirii sau al detectării infracțiunilor grave sau al protejării bunăstării economice a Regatului Unit (în măsura în care aceste interese sunt relevante și pentru interesele securității naționale - pct. 3.5 și 6.11 din Codul IC, infra, pct. 96); iar activitatea autorizată prin mandat era proporțională cu ceea ce se urmărea a fi atins prin respectiva activitate. Pentru evaluarea necesității și a proporționalității, trebuia să se ia în considerare dacă informațiile solicitate în temeiul mandatului puteau fi obținute în mod rezonabil prin alte mijloace.

63. Art. 81 alin. (2) lit. b) din RIPA definea „infracțiunea gravă” drept infracțiunea care îndeplinea unul dintre următoarele criterii:

„a) infracțiunea sau una dintre infracțiunile care este sau ar fi constituită din fapta care reprezintă o infracțiune pentru care se poate aștepta în mod rezonabil ca o persoană care a împlinit vârsta de douăzeci și unu de ani și care nu a fost condamnată anterior să fie condamnată la pedeapsa cu închisoarea pentru o perioadă de cel puțin trei ani;

b) fapta să implice utilizarea violenței, să aibă ca rezultat un câștig financiar substanțial sau să fie o faptă a unui număr mare de persoane care urmăresc un scop comun.”

64. Art. 81 alin. (5) prevedea:

„În sensul prezentei legi, prin detectarea infracțiunilor se înțelege:

a) stabilirea de către cine, în ce scop, prin ce mijloace și în ce condiții a fost săvârșită o infracțiune; și

b) arestarea persoanei care a săvârșit orice infracțiune;

orice trimitere din prezenta lege la prevenirea sau depistarea infracțiunilor grave se interpretează în consecință [...]

65. Art. 6 prevedea că, în ceea ce privește serviciile de informații, numai directorul general al MI5, șeful MI6 și directorul GCHQ puteau solicita emiterea unui mandat de interceptare.

66. Existau două tipuri de mandat de interceptare cărora li se aplicau art. 5 și 6: un mandat țintit, astfel cum prevedea art. 8 alin. (1), și un mandat nețintit, astfel cum prevedea art. 8 alin. (4).

67. În temeiul art. 9 din RIPA, un mandat emis în interesul securității naționale sau al protejării bunăstării economice a Regatului Unit înceta să mai producă efecte la sfârșitul unei perioade de șase luni, iar un mandat emis în scopul depistării infracțiunilor grave înceta să mai producă efecte după trei luni. În orice moment înainte de expirarea acestor termene, ministrul putea reînnoi mandatul (pentru perioade de șase, respectiv de trei luni) în cazul în care considera că mandatul continua să fie necesar pentru motive care intrau sub incidența art. 5 alin. (3). Ministrul era obligat să anuleze un mandat de interceptare în cazul în care era convins că mandatul nu mai era necesar din motive care intrau sub incidența art. 5 alin. (3).

68. Conform art. 5 alin. (6), activitatea autorizată printr-un mandat de interceptare trebuia să includă interceptarea comunicațiilor care nu au fost identificate de mandat, dacă era necesar pentru a face ceea ce a fost autorizat sau impus în mod expres de mandat; și obținerea datelor de comunicații aferente.

69. Art. 21 alin. (4) definea „datele de comunicații” ca fiind:

(a) „orice date de trafic incluse în sau atașate la o comunicație (fie de către expeditor, fie în alt mod) pentru orice serviciu poștal sau sistem de telecomunicații, prin intermediul căruia este transmisă sau poate fi transmisă;

- (b) orice informații care nu includ nimic din conținutul unei comunicații [cu excepția oricăror informații care intră sub incidența lit. a)] și care se referă la utilizarea lor de către orice persoană:
 - i. orice serviciu poștal sau serviciu de telecomunicații; sau
 - ii. în legătură cu furnizarea sau cu utilizarea de către orice persoană a oricărui serviciu de telecomunicații sau a oricărei părți a sistemului de telecomunicații;
- (c) orice informație care nu intră sub incidența lit. a) sau b), care este deținută sau obținută, în legătură cu persoanele cărora le furnizează serviciul, de către o persoană care furnizează un serviciu poștal sau de telecomunicații.”

70. Codul de bune practici privind achiziționarea și divulgarea datelor de comunicații din martie 2015 făcea referire la aceste trei categorii ca „date de trafic”, „informații privind utilizarea serviciilor” și „informații privind abonații”. Art. 21 alin. (6) din RIPA definea în detaliu „datele de trafic” ca fiind datele care identificau persoana, aparatul, localizarea sau adresa către sau de la care a fost transmisă o comunicație, precum și informațiile cu privire la un fișier sau program informatic accesat sau rulat în cursul trimiterii sau primirii unei comunicații.

71. Potrivit art. 20 din RIPA, „datele de comunicații aferente”, în legătură cu o comunicație interceptată în cursul transmiterii sale prin intermediul unui serviciu poștal sau al unui sistem de telecomunicații, înseamnă „atât de multe date de comunicații câte au fost obținute prin sau în legătură cu interceptarea”; și legate de „comunicația sau expeditorul ori destinatarul sau destinatarul preconizat al comunicației”.

2. *Mandate: art. 8 alin. (4)*

(a) **Autorizare**

72. „Interceptarea în masă” a comunicațiilor era efectuată pe baza unui mandat emis în temeiul art. 8 alin. (4). Art. 8 alin. (4) și (5) din RIPA permitea ministrului să emită un mandat pentru „interceptarea comunicațiilor externe în cursul transmiterii acestora prin intermediul unui sistem de telecomunicații”.

73. La momentul emiterii unui mandat în temeiul art. 8 alin. (4), ministrul era, de asemenea, obligat să emită un certificat care să conțină o descriere a materialelor interceptate pe care considera necesar să le examineze și care să indice că examinarea materialelor respective era considerată necesară din motivele prevăzute la art. 5 alin. (3) (și anume, că era necesară în interesul securității naționale, în scopul prevenirii sau al depistării infracțiunilor grave sau al protejării bunăstării economice a Regatului Unit – în măsura în care aceste interese de securitate națională erau, de asemenea, relevante pentru interesele securității naționale; a se vedea pct. 3.5 și 6.11 din Codul IC, infra, pct. 96).

(b) Comunicații „externe”

74. Art. 20 definea „comunicațiile externe” ca fiind „comunicații trimise sau primite în afara Insulelor Britanice”.

75. În cursul procedurii *Liberty*, Charles Farr, directorul general al OSCT, a indicat că două persoane din Regatul Unit care își trimiteau reciproc e-mailuri se angajau în „comunicații interne”, chiar dacă serviciul de e-mail era găzduit pe un server din Statele Unite ale Americii; cu toate acestea, comunicația respectivă putea fi interceptată drept „captură accidentală” a unui mandat care ținea comunicațiile externe. Pe de altă parte, o persoană din Regatul Unit care comunica cu ajutorul unui motor de căutare din străinătate participa la o comunicație externă, precum o persoană din Regatul Unit care publica un mesaj public (cum ar fi un mesaj Tweeter sau o actualizare a statusului pe Facebook), cu excepția cazului în care toți destinatarii acestui mesaj se aflau în Insulele Britanice.

76. În declarația dată în fața ISC în octombrie 2014, ministrul afacerilor externe și al Commonwealth-ului considera că:

„În ceea ce privește un e-mail, în cazul în care unul sau ambii expeditori sau destinatari se află în străinătate, atunci aceasta ar fi o comunicație externă.

În ceea ce privește navigarea pe Internet, dacă o persoană citește site-ul Internet al Washington Post, atunci aceasta a «comunicat» cu un server web situat în străinătate și, prin urmare, aceasta este o comunicație externă.

În ceea ce privește platformele de comunicare socială, dacă o persoană postează ceva pe Facebook, întrucât serverul web are sediul în străinătate, postarea ar fi tratată ca o comunicație externă.

În ceea ce privește stocarea în cloud (de exemplu, fișiere încărcate în Dropbox), acestea sunt tratate drept comunicații externe, deoarece au fost trimise pe un server web în străinătate.”

3. Garanții specifice în temeiul RIPA**(a) Art. 15**

77. Potrivit art. 15 alin. (1), ministrul avea obligația să se asigure, în ceea ce privește toate mandatele de interceptare, că sunt în vigoare procedurile pe care le considera necesare pentru ca cerințele prevăzute la alin. (2) și (3) să fie îndeplinite în ceea ce privește materialele interceptate și orice date de comunicații aferente; și, în cazul mandatelor pentru care existau certificatele prevăzute la art. 8 alin. (4), că cerințele prevăzute la art. 16 erau, de asemenea, îndeplinite.

78. Art. 15 alin. (2) prevedea:

„Cerințele prezentului articol sunt îndeplinite în ceea ce privește materialele interceptate și orice date de comunicații aferente dacă fiecare dintre următorii factori este limitat la minimul necesar pentru îndeplinirea scopurilor autorizate:

- a. numărul de persoane cărora le sunt divulgate sau puse la dispoziție oricare dintre materiale sau date este accesibil;

- b. măsura în care oricare dintre materiale sau date este divulgată sau altfel accesibilă;
- c. măsura în care oricare dintre materiale sau date sunt copiate și
- d. numărul de copii făcute.”

79. Art. 15 alin. (3) prevedea:

„Cerințele prezentului articol sunt îndeplinite în ceea ce privește materialele interceptate și orice date de comunicații aferente în cazul în care fiecare copie a oricăruia dintre materiale sau a oricăreia dintre date (dacă nu au fost distruse mai devreme) este distrusă de îndată ce nu mai există motive pentru păstrarea acestora, dacă este cazul, pentru îndeplinirea oricărui dintre scopurile autorizate.”

80. Potrivit art. 15 alin. (4), era necesar în scopurile autorizate dacă și numai dacă continua să fie, sau putea deveni necesar, astfel cum se menționează la art. 5 alin. (3) din lege (adică necesar în interesul securității naționale, cu scopul prevenirii sau detectării infracțiunilor grave; cu scopul protejării bunăstării economice a Regatului Unit (în măsura în care aceste interese sunt relevante și pentru interesele securității naționale – pct. 3.5 și 6.11 din Codul IC, infra, pct. 96); sau cu scopul punerii în aplicare a prevederilor oricărui acord internațional de asistență reciprocă); era necesar pentru a facilita îndeplinirea oricăreia dintre funcțiile de interceptare ale ministrului; era necesar pentru a facilita îndeplinirea oricărei funcții a Comisarului IC sau a IPT; era necesar pentru a se asigura că o persoană care desfășoară urmărirea penală dispune de informațiile necesare pentru a stabili ce este de datoria sa spre a asigura echitatea urmăririi penale; sau era necesar pentru îndeplinirea oricărei obligații impuse oricărei persoane în temeiul legislației referitoare la arhivele publice.

81. Art. 15 alin. (5) impunea ca procedurile în vigoare pentru a asigura respectarea art. 15 alin. (2) să includă măsurile pe care ministrul le considera necesare pentru a se asigura că fiecare copie a materialelor sau a datelor care se făcea era stocată, atât timp cât era păstrată, în condiții de siguranță.

82. Potrivit art. 15 alin. (6), procedurile la care face referire art. 15 alin. (1) nu erau necesare pentru a se asigura că cerințele prevăzute la art. 15 alin. (2) și (3) erau îndeplinite în măsura în care făceau referire la oricare dintre materialele interceptate sau la datele de comunicații aferente sau la orice copie a unor astfel de materiale sau date a căror posesie a fost predată oricărei autorități a unei țări sau a unui teritoriu din afara Regatului Unit. Cu toate acestea, astfel de proceduri erau necesare pentru a garanta, în cazul fiecărui astfel tip de mandat, că materialele și datele interceptate, precum și copiile materialelor sau datelor nu au fost predate autorităților unei țări sau ale unui teritoriu din afara Regatului Unit decât dacă erau îndeplinite cerințele prevăzute la art. 15 alin. (7). Art. 15 alin. (7) prevedea:

„Cerințele prezentului articol sunt îndeplinite în cazul în care ministrul consideră că:

- a. cerințele corespunzătoare celor prevăzute la alin. (2) și (3) se aplică, eventual în măsura pe care ministrul o consideră adecvată, în ceea ce privește oricare

dintre materialele interceptate sau datele de comunicații aferente a căror posesie sau ale cărei copii sunt predate autorităților în cauză; și

- b. sunt în vigoare restricții care ar împiedica, eventual în măsura pe care ministrul o consideră adecvată, efectuarea oricărei acțiuni, în scopul sau în legătură cu orice procedură desfășurată în afara Regatului Unit, care ar conduce la o astfel de divulgare, astfel încât, în temeiul art. 17, nu ar putea fi efectuată în Regatul Unit.”

83. Art. 17 din RIPA prevedea ca regulă generală că nu se pot prezenta probe, nu se pot face divulgări sau alte elemente de probă în legătură cu procedurile judiciare care ar divulga conținutul sau datele de comunicații aferente unei comunicații interceptate.

(b) Art. 16

84. Art. 16 stabilea garanții suplimentare în ceea ce privește interceptarea comunicațiilor „externe” în temeiul art. 8 alin. (4). Art. 16 alin. (1) prevedea că materialele interceptate pot fi citite, examinate sau ascultate de către persoanele cărora le-au fost puse la dispoziție în temeiul mandatului numai dacă și în măsura în care au fost certificate ca materiale a căror examinare era necesară, astfel cum se menționa la art. 5 alin. (3) din lege, și intrau sub incidența art. 16 alin. (2). Art. 20 definea „materialele interceptate” ca fiind conținutul oricăror comunicații interceptate printr-o interceptare în cadrul mandatului.

85. Art. 16 alin. (2) prevedea:

„Sub rezerva art. (3) și (4), materialele interceptate intră sub incidența prezentului articol numai în măsura în care sunt selectate pentru a fi citite, examinate sau ascultate altfel decât în funcție de un factor care:

- a. are legătură cu o persoană despre care se cunoaște că se află pentru moment în Insulele Britanice; și
- b. are ca scop sau unul dintre scopuri identificarea materialelor conținute în comunicațiile pe care le trimite sau care îi sunt destinate.”

86. Potrivit art. 16 alin. (3), materialele interceptate intrau sub incidența art. 16 alin. (2), sub rezerva faptului că erau selectate prin referire la unul dintre factorii menționați la articolul respectiv, dacă ministrul certifica, în sensul art. 8 alin. (4) din lege, că examinarea materialelor selectate potrivit factorilor care aveau legătură cu persoana în cauză era necesară, astfel cum se menționa la art. 5 alin. (3) din lege; și materialul avea legătură numai cu comunicațiile trimise pe parcursul unei perioade specificate în certificat, care nu putea depăși durata maximă admisă.

87. „Durata maximă admisă” era definită la art. 16 alin. (3) lit. a) după cum urmează:

„(a) șase luni, în cazul materialelor a căror examinare este certificată în sensul art. 8 alin. (4), după caz, în interesul securității naționale; și

(b) trei luni, în orice alt caz.”

88. Potrivit art. 16 alin. (4), materialele interceptate intrau, de asemenea, sub incidența art. 16 alin. (2), chiar dacă erau selectate prin referire la unul dintre factorii menționați în articolul respectiv, în cazul în care persoana căreia i se adresa mandatul considera, pe baza unor motive întemeiate, că circumstanțele erau de așa natură încât materialele ar intra sub incidența acestui articol; sau condițiile prevăzute la art. 16 alin. (5) erau îndeplinite în ceea ce privește selecția materialelor.

89. Art. 16 alin. (5) prevedea:

„Aceste condiții sunt îndeplinite în ceea ce privește selectarea materialelor interceptate, în cazul în care:

- a) persoanei căreia îi este adresat mandatul constată că a avut loc o astfel de schimbare relevantă a circumstanțelor, întrucât, în lipsa art. (4) lit. b), materialele interceptate nu ar intra sub incidența art. (2);
- b) în urma acestei constatări, un înalt funcționar a autorizat în scris citirea, examinarea sau ascultarea materialelor; și
- c) selecția este făcută înainte de încetarea perioadei admise.”

90. Potrivit art. 16 alin. (5A), prin „perioada admisă” se înțelege:

- „a) în cazul materialelor a căror examinare este certificată în sensul art. 8 alin. (4) ca fiind necesară în interesul siguranței naționale, perioada care încetează la sfârșitul celei de-a cincea zile lucrătoare de la prima constatare, astfel cum se menționează la alin. (5) lit. a), persoanei căreia îi este adresat mandatul; și
- b) în orice alt caz, perioada care încetează la sfârșitul primei zile lucrătoare după prima constatare a respectivei persoane.”

91. Art. 16 alin. (6) a precizat că o „modificare relevantă a circumstanțelor” însemna că persoana în cauză a intrat în Insulele Britanice; sau exista convingerea că persoana căreia i s-a emis mandatul a crezut din greșeală că individul se află în afara Insulelor Britanice.

92. În declarația în fața ISC în octombrie 2014, ministrul afacerilor externe și al Commonwealth-ului explica faptul că:

„Atunci când un analist selectează pentru examinare comunicațiile care au fost interceptate în baza unui mandat emis în temeiul art. 8 alin. (4), nu contează forma de comunicare utilizată de o persoană sau dacă celelalte comunicații ale sale sunt stocate pe un server de e-mail dedicat sau în memoria cloud situată fizic în Regatul Unit, în S.U.A. sau oriunde altundeva (și, în practică, utilizatorul individual al serviciilor de cloud nu va ști unde este stocat). În cazul în care se știe că se află în Insulele Britanice, nu este permisă căutarea comunicațiilor sale prin utilizarea numelui, a adresei de e-mail sau a oricărui alt identificator personal.”

4. Codul de bune practici privind interceptarea comunicațiilor

93. Art. 71 din RIPA prevedea adoptarea unor coduri de bune practici de către ministrul în legătură cu exercitarea și ducerea la îndeplinire a competențelor și atribuțiilor sale, în temeiul legii. Proiectele de coduri de

bune practici trebuiau să fie prezentate Parlamentului și erau documente publice. Acestea puteau intra în vigoare numai prin ordin al ministrului. Ministrul putea emite un astfel de ordin numai dacă proiectul de ordin era prezentat Parlamentului și aprobat printr-o rezoluție a fiecărei Camere.

94. Conform art. 72 alin. (1) din RIPA, o persoană care exercita sau ducea la îndeplinire o competență sau o obligație referitoare la interceptarea comunicațiilor trebuia să țină seama de dispozițiile relevante ale unui cod de bune practici. Dispozițiile unui cod de bune practici puteau, în circumstanțe adecvate, să fie luate în considerare de către instanțe în temeiul art. 72 alin. (4) din RIPA.

95. Codul IC a fost adoptat în temeiul art. 71 din RIPA. Versiunea codului în vigoare la momentul faptelor datează din 2016.

96. În măsura în care este relevant, Codul IC prevedea:

„3.2. Există un număr limitat de persoane care pot depune o cerere pentru un mandat de interceptare sau pot delega competența de a face o asemenea cerere. Acestea sunt:

- Directorul general al Serviciului de Securitate.
- Șeful Serviciului Secret de Informații.
- Directorul Cartierului General pentru Comunicații al Guvernului (GCHQ).
- Directorul general al Agenției Naționale pentru Combaterea Criminalității (ANCC gestionează interceptarea în numele organelor de aplicare a legii din Anglia și Țara Galilor).
- Șeful serviciului de poliție din Scoția.
- Comisarul poliției din Metropolis (Comandamentul poliției metropolitane de combatere a terorismului gestionează interceptarea în numele unităților de combatere a terorismului, al sucursalelor speciale și al unor unități specializate ale forțelor de poliție din Anglia și Țara Galilor).
- Șeful serviciului de poliție din Irlanda de Nord.
- Comisarii Maiestății Sale pentru administrație fiscală și vamă (*The Commissioners of Her Majesty's Revenue & Customs* – HMRC).
- Șeful Serviciului de Informații al Armatei.
- Orice persoană care, în sensul unui acord internațional de asistență reciprocă, reprezintă autoritatea competentă a unei țări sau a unui teritoriu din afara Regatului Unit.

3.3. Orice cerere depusă în numele uneia dintre persoanele de mai sus trebuie să fie făcută de o persoană care deține o funcție în cadrul Coroanei.

3.4. Toate mandatele de interceptare sunt emise de ministrul. Chiar și atunci când se aplică procedura de urgență, ministrul autorizează personal mandatul, chiar dacă este semnat de un înalt funcționar.

Necesitate și proporționalitate

3.5. Obținerea unui mandat în temeiul RIPA va asigura faptul că interceptarea autorizată reprezintă o ingerință justificabilă în drepturile unei persoane în temeiul art. 8 (dreptul la respectarea vieții private și de familie) din Convenția europeană a drepturilor

omului (CEDO) numai dacă este necesară și proporțională pentru ca interceptarea să aibă loc. RIPA recunoaște acest lucru solicitând în primul rând ca ministrul să fie încredințat că autorizația este necesară pentru unul sau mai multe dintre următoarele temeuri legale:

- în interesul securității naționale;
- pentru prevenirea sau depistarea infracțiunilor grave;
- pentru protejarea bunăstării economice a Regatului Unit, în măsura în care aceste interese sunt relevante și pentru interesele securității naționale.

3.6. Aceste scopuri sunt prevăzute la art. 5 alin. (3) din RIPA. Ministrul trebuie, de asemenea, să fie încredințat că interceptarea este proporțională cu ceea ce se urmărește prin respectiva activitate. Orice evaluare a proporționalității implică punerea în balanță a gravității intruziunii în viața privată sau atingerea adusă bunurilor subiectului operațiunii (sau a oricărei alte persoane care ar putea fi afectată) cu necesitatea activității din punctul de vedere al investigării, al operării sau al capacității. Mandatul nu va fi proporțional dacă este excesiv în circumstanțele generale ale cazului. Fiecare acțiune autorizată trebuie să aducă un beneficiu preconizat investigației sau operației și nu trebuie să fie disproporționată sau arbitrară. Faptul că există o amenințare potențială la adresa securității naționale (de exemplu) nu permite ca acțiunile cele mai intruzive să fie proporționale. Nicio ingerință trebuie considerată proporțională, în cazul în care informațiile solicitate ar putea fi obținute în mod rezonabil prin alte mijloace mai puțin intruzive.

3. NORME GENERALE PRIVIND INTERCEPTAREA CU MANDAT

[...]

3.7. Trebuie luate, prin urmare, în considerare următoarele elemente de proporționalitate:

- punerea în balanță a dimensiunii și a domeniului de aplicare al ingerinței propuse cu ceea ce se dorește a fi obținut;
- explicarea modului și a motivelor pentru care metodele care urmează să fie adoptate vor provoca cea mai mică intruziune posibilă în ceea ce privește subiectul și alte persoane;
- analizarea măsurii în care activitatea constituie o utilizare adecvată a legislației și o modalitate rezonabilă, după analizarea tuturor alternativelor rezonabile, de a obține rezultatul necesar;
- precizarea, în măsura în care este rezonabil din punct de vedere practic, a altor metode care au fost luate în considerare și care fie nu au fost puse în aplicare, fie au fost utilizate, dar care sunt evaluate ca fiind insuficiente pentru îndeplinirea obiectivelor operaționale fără adăugarea materialelor interceptate vizate.

[...]

Durata mandatelor de interceptare

3.18. Mandatele de interceptare emise pentru infracțiuni grave sunt valabile pentru o perioadă inițială de trei luni. Mandatele de interceptare emise din motive de securitate națională/bunăstare economică a Regatului Unit sunt valabile pentru o perioadă inițială de șase luni. Un mandat emis în cadrul procedurii de urgență (din orice motiv) este valabil timp de cinci zile lucrătoare de la data emiterii, cu excepția cazului în care este reînnoit de către ministru.

3.19. La reînnoire, mandatele emise pentru infracțiuni grave sunt valabile pentru o perioadă suplimentară de trei luni. Mandatele reînnoite emise din motive de securitate națională/bunăstare economică a Regatului Unit sunt valabile pentru o perioadă de șase luni. Aceste date încep să curgă de la data actului de reînnoire.

3.20. În cazul în care se aduc modificări unui mandat de interceptare, data expirării mandatului rămâne neschimbată. Cu toate acestea, în cazul în care modificarea are loc în temeiul dispozițiilor privind urgența, actul de modificare expiră după cinci zile lucrătoare de la data emiterii, cu excepția cazului în care este reînnoit în conformitate cu procedura ordinară.

3.21. În cazul în care o modificare a circumstanțelor determină agenția de interceptare să considere că nu mai este necesar, proporțional sau practic, ca un mandat să fie în vigoare, agenția trebuie să adreseze ministrului o recomandare de anulare cu efect imediat.

[...]

4. NORME SPECIALE PRIVIND INTERCEPTAREA CU MANDAT

Intruziunea colaterală

4.1. Trebuie să se ia în considerare orice ingerință în viața privată a persoanelor care nu fac obiectul interceptării vizate, în special în cazul în care pot fi implicate comunicații referitoare la materiale religioase, medicale, jurnalistice sau care fac obiectul secretului profesional al avocaților sau în cazul în care pot fi implicate comunicații între un membru al Parlamentului și o altă persoană cu privire la aspecte legate de circumscripții sau comunicații între un membru al Parlamentului și un denunțator. O cerere de emitere a unui mandat de interceptare trebuie să precizeze dacă este posibil ca interceptarea să conducă la un anumit grad de încălcare colaterală a vieții private. Persoana care solicită emiterea unui mandat de interceptare trebuie, de asemenea, să ia în considerare măsuri, inclusiv utilizarea de sisteme automatizate, pentru a reduce amploarea intruziunii colaterale. În cazul în care acest lucru este posibil, cererea trebuie să specifice măsurile respective. Aceste circumstanțe și măsuri vor fi luate în considerare de către ministru atunci când examinează o cerere de emitere a unui mandat formulată în temeiul art. 8 alin. (1) din RIPA. În cazul în care o operațiune de interceptare ajunge la punctul în care alte persoane decât obiectul autorizației sunt identificate ca ținte de investigație în nume propriu, trebuie să se ia în considerare solicitarea emiterii unor mandate separate, care să acopere persoanele respective.

Informații confidențiale

4.2. Trebuie, de asemenea, să se acorde o atenție deosebită cazurilor în care subiectul interceptării ar putea să se aștepte în mod rezonabil să aibă un nivel ridicat de confidențialitate sau în care sunt implicate informații confidențiale. Sunt incluse cazurile în care comunicațiile au legătură cu materiale care sunt acoperite de secretul profesional al avocaților; atunci când poate fi implicat material jurnalistice confidențial; atunci când interceptarea ar putea implica comunicații între un profesionist din domeniul sănătății sau ministrul cultelor și o persoană, referitoare la sănătatea sau

bunăstarea spirituală a acestora din urmă; sau atunci când pot fi implicate comunicații între un membru al Parlamentului și o altă persoană, cu privire la activitățile din circumscripție.

4.3. Materialul jurnalistic confidențial include materialele dobândite sau create în scopuri jurnalistice și deținute sub rezerva angajamentului de a le păstra confidențialitatea, precum și comunicațiile care au drept rezultat dobândirea de informații în scopuri jurnalistice și deținerea lor sub rezerva unui astfel de angajament. A se vedea, de asemenea, punctele 4.26 și 4.28–4.31 pentru garanții suplimentare care trebuie aplicate în ceea ce privește materialele jurnalistice confidențiale.

[...]

Comunicații care implică materiale jurnalistice confidențiale, informații personale confidențiale și comunicații între un membru al Parlamentului și o altă persoană, cu privire la activitățile din circumscripție

4.26. Trebuie, de asemenea, să se acorde o atenție deosebită interceptării comunicațiilor care implică materiale jurnalistice confidențiale, informații personale confidențiale sau comunicații între un membru al Parlamentului și o altă persoană, cu privire la activitățile din circumscripție. Materialele jurnalistice confidențiale sunt explicate la punctul 4.3. Informațiile personale confidențiale sunt informații confidențiale cu privire la o persoană (vie sau decedată) care poate fi identificată pe baza acestora, iar materialele în cauză au legătură cu sănătatea sa fizică sau mentală ori consilierea spirituală. Astfel de informații pot include atât comunicații verbale, cât și scrise. Astfel de informații, astfel cum sunt descrise mai sus, sunt confidențiale dacă sunt deținute sub rezerva unui angajament explicit sau implicit de a le păstra confidențialitatea sau dacă fac obiectul unei restricții privind divulgarea sau al unei obligații de confidențialitate prevăzute de legislația în vigoare. De exemplu, informațiile personale confidențiale pot include consultări între un cadru medical și un pacient sau informații din dosarele medicale ale pacientului.

[...]

4.28. Atunci când intenția este de a obține informații personale confidențiale, motivele trebuie să fie documentate în mod clar, iar necesitatea specifică și proporționalitatea acestei intenții trebuie analizate cu atenție. În cazul în care obținerea de informații personale confidențiale este posibil să se producă, dar nu este intenționată, trebuie avute în vedere orice măsuri de atenuare a acestui risc posibil și, în cazul în care nu sunt disponibile, trebuie să se analizeze dacă se impun modalități speciale de tratare a informațiilor în cadrul agenției de interceptare.

4.29. Materialele care au fost identificate drept informații confidențiale trebuie păstrate numai în cazul în care acest lucru este necesar și proporțional pentru unul sau mai multe dintre scopurile autorizate prevăzute la art. 15 alin. (4). Acestea trebuie să fie distruse în siguranță atunci când păstrarea lor nu mai este necesară în acest scop. În cazul în care aceste informații sunt păstrate, trebuie să existe sisteme adecvate de gestionare a informațiilor pentru a se asigura că păstrarea continuă rămâne necesară și proporțională pentru scopurile legale autorizate.

4.30. În cazul în care informațiile confidențiale sunt păstrate sau transmise unui organ extern, trebuie luate măsuri rezonabile pentru a marca caracterul confidențial al informațiilor. În cazul în care există îndoieli cu privire la legalitatea prelucrării sau transmiterii propuse a informațiilor confidențiale, trebuie să se solicite consiliere din partea unui consilier juridic din cadrul agenției de interceptare relevante și înainte ca orice transmitere ulterioară a materialelor să se producă.

4.31. Orice situație în care sunt păstrate informații confidențiale trebuie notificată Comisarului pentru interceptarea comunicațiilor cât mai curând posibil, astfel cum s-a convenit cu Comisarul. Orice material care a fost păstrat trebuie să fie pus la dispoziția Comisarului, la cerere.

4.32. Garanțiile prevăzute la pct. 4.28–4.31 se aplică, de asemenea, oricăror materiale de la art. 8 alin. (4) (a se vedea Capitolul 6) care sunt selectate spre examinare și care constituie informații confidențiale.

[...]

6. MANDATE DE INTERCEPTARE [ART. 8 ALIN. (4)]

6.1. Prezentul punct se aplică interceptării comunicațiilor externe prin intermediul unui mandat emis în conformitate cu art. 8 alin. (4) din RIPA.

6.2. Spre deosebire de art. 8 alin. (1), un mandat emis în temeiul art. 8 alin. (4) nu trebuie să numească sau să descrie subiectul interceptării sau un set de spații în legătură cu care urmează să aibă loc interceptarea. De asemenea, art. 8 alin. (4) nu impune o limitare expresă a numărului de comunicații externe care pot fi interceptate. De exemplu, dacă sunt îndeplinite cerințele prevăzute la art. 8 alin. (4) și (5), atunci interceptarea tuturor comunicațiilor transmise pe o anumită rută sau pe un anumit cablu sau transportate de un anumit FSC poate, în principiu, să fie autorizată în mod legal. Aceasta reflectă faptul că interceptarea în temeiul art. 8 alin. (4) constituie o capacitate de a colecta informații, în timp ce interceptarea în temeiul art. 8 alin. (1) constituie, în primul rând, un instrument de investigare care este utilizat odată ce a fost identificat un anumit subiect al interceptării.

6.3. Responsabilitatea emiterii mandatelor de interceptare în temeiul art. 8 alin. (4) din RIPA îi revine ministrului. Atunci când ministrul emite un mandat de acest tip, trebuie să fie însoțit de un certificat. Certificatul asigură aplicarea unui proces de selecție materialelor interceptate, astfel încât numai materialele descrise în certificat să fie puse la dispoziție spre examinare umană. Dacă materialele interceptate nu pot fi selectate pentru a fi citite, analizate sau ascultate cu respectarea proporționalității și a condițiilor certificatului, nu pot fi citite, examinate sau ascultate de nicio persoană.

Interceptarea în temeiul art. 8 alin. (4) în practică

6.4. Art. 8 alin. (4) garantează autorizarea interceptării comunicațiilor externe. În cazul în care un mandat emis în temeiul art. 8 alin. (4) conduce la obținerea unor volume mari de comunicații, agenția de interceptare va aplica în mod normal un proces de filtrare pentru a elimina automat comunicațiile despre care este puțin probabil să aibă valoare informațională. Persoanele autorizate din cadrul agenției de interceptare pot aplica apoi criterii de căutare pentru a selecta comunicațiile care pot avea valoare informațională, în conformitate cu termenii certificatului emis de ministru. Înainte ca o anumită comunicație să poată fi accesată de o persoană autorizată din cadrul agenției de interceptare, persoana trebuie să explice de ce este necesară pentru unul dintre motivele menționate în certificatul care însoțește mandatul emis de ministru și de ce este proporțională în circumstanțele specifice. Acest proces face obiectul auditului intern și al controlului extern efectuat de Comisarul pentru Interceptarea Comunicațiilor. În cazul în care ministrul constată că acest lucru este necesar, poate autoriza selectarea comunicațiilor unei persoane despre care se știe că se află în Insulele Britanice. În lipsa unei astfel de autorizații, o persoană autorizată nu poate să selecteze astfel de comunicații.

Definirea comunicațiilor externe

6.5. Comunicațiile externe sunt definite de RIPA ca fiind cele trimise sau primite în afara Insulelor Britanice. Printre acestea se numără cele care sunt trimise și primite în afara Insulelor Britanice, indiferent dacă trec sau nu prin Insulele Britanice în cursul transmiterii lor. Acestea nu includ comunicațiile trimise și primite în Insulele Britanice, chiar dacă tranzitează în afara Insulelor Britanice. De exemplu, un e-mail de la o persoană din Londra către o persoană din Birmingham va fi o comunicație internă, iar nu externă, în sensul art. 20 din RIPA, indiferent dacă este direcționată sau nu prin intermediul adreselor IP din afara Insulelor Britanice, întrucât expeditorul și destinatarul preconizat se află în interiorul Insulelor Britanice.

Interceptarea comunicațiilor non-externe pe baza unui mandat emis în temeiul art. 8 alin. (4)

6.6. Art. 5 alin. (6) lit. a) din RIPA menționează cu claritate că activitatea autorizată de un mandat emis în temeiul art. 8 alin. (4) poate include, în principiu, interceptarea comunicațiilor care nu sunt comunicații externe, în măsura în care acest lucru este necesar pentru interceptarea comunicațiilor externe la care se referă mandatul.

6.7. Atunci când efectuează interceptarea pe baza unui mandat emis în temeiul art. 8 alin. (4), o agenție de interceptare trebuie să utilizeze cunoștințele sale cu privire la modul în care sunt dirijate comunicațiile internaționale, în coroborare cu sondaje periodice ale legăturilor de comunicații relevante, pentru a identifica canalele de transmisie individuale care sunt cele mai susceptibile să conțină comunicațiile externe care vor respecta descrierile certificatului emis de ministru în temeiul art. 8 alin. (4). De asemenea, trebuie să efectueze interceptarea într-un mod care să limiteze colectarea comunicațiilor externe la un nivel minim compatibil cu obiectivul interceptării comunicațiilor externe dorite.

Cerere de emitere a unui mandat în temeiul art. 8 alin. (4)

6.8. Ministrul este sesizat cu o cerere de emitere de mandat. Atunci când sunt emise, mandatele de interceptare se adresează persoanei care a depus cererea. Scopul unui astfel de mandat va reflecta, de regulă, una sau mai multe dintre prioritățile în materie de informații stabilite de Consiliul Național de Securitate (*National Security Council* – NSC).

6.9. Înainte de a fi transmisă, fiecare cerere face obiectul unei examinări în cadrul agenției care o întocmește. Acest lucru implică verificarea de către mai mulți funcționari, care vor analiza dacă cererea se încadrează într-un scop care intră sub incidența art. 5 alin. (3) din RIPA și dacă interceptarea propusă este atât necesară, cât și proporțională.

6.10. Fiecare cerere, a cărei copie trebuie păstrată de solicitant, trebuie să conțină următoarele informații:

- contextul operațiunii în cauză:
 - descrierea comunicațiilor care urmează să fie interceptate, detalii privind FSC și o evaluare a fezabilității operațiunii, în cazul în care este relevant; și
 - descrierea activității care urmează să fie autorizată, care trebuie să se limiteze la interceptarea comunicațiilor externe, sau a activității [inclusiv interceptarea altor comunicații care nu sunt identificate în mod specific în mandat, astfel cum prevede art. 5 alin. (6) lit. a) din RIPA], necesară pentru a realiza activitatea autorizată sau impusă de mandat, și pentru a obține datele de comunicații aferente.
- certificatul care va reglementa examinarea materialului interceptat;

- o explicație privind motivul pentru care este considerată necesară interceptarea, pentru unul sau mai multe dintre scopurile prevăzute la art. 5 alin. (3);
- o expunere a motivelor pentru care activitatea care urmează să fie autorizată prin mandat este proporțională cu ceea ce se intenționează a fi atins prin activitatea respectivă;
- în cazul în care o cerere este urgentă, justificarea aferentă;
- o asigurare că materialele interceptate vor fi citite, examinate sau ascultate numai în măsura în care au fost certificate și îndeplinesc condițiile prevăzute la art. 16 alin. (2)-(6) din RIPA; și
- o asigurare că toate materialele interceptate vor fi tratate în conformitate cu garanțiile prevăzute la art. 15 și 16 din RIPA (a se vedea pct. 7.2, respectiv 7.10).

Emiterea unui mandat emis în temeiul art. 8 alin. (4)

6.11. Înainte de a emite un mandat în temeiul art. 8 alin. (4), ministrul trebuie să considere că mandatul este necesar:

- în interesul securității naționale;
- în scopul prevenirii sau depistării unor infracțiuni grave; sau
- în scopul protejării bunăstării economice a Regatului Unit, în măsura în care aceste interese sunt, de asemenea, relevante și pentru interesele securității naționale.

6.12. Competența de a emite un mandat de interceptare în scopul protejării bunăstării economice a Regatului Unit [astfel cum este prevăzută la art. 5 alin. (3) lit. c) din RIPA] poate fi exercitată numai în cazul în care ministrul consideră că circumstanțele sunt relevante pentru interesele securității naționale. Ministrul nu va emite un mandat în temeiul art. 5 alin. (3) lit. c) în cazul în care nu se stabilește o legătură directă între bunăstarea economică a Regatului Unit și securitatea națională. Orice cerere de emitere a unui mandat în temeiul art. 5 alin. (3) lit. c) trebuie, prin urmare, să identifice circumstanțele care sunt relevante pentru interesele securității naționale.

6.13. Ministrul trebuie, de asemenea, să considere că activitatea autorizată prin mandat este proporțională cu ceea ce urmărește să realizeze [art. 5 alin. (2) lit. b)]. Atunci când examinează necesitatea și proporționalitatea, ministrul trebuie să ia în considerare dacă informațiile solicitate ar putea fi obținute în mod rezonabil prin alte mijloace [art. 5 alin. (4)].

6.14. Atunci când ministrul emite un mandat de acest tip, acesta trebuie să fie însoțit de un certificat în care ministrul certifică faptul că consideră că examinarea materialelor interceptate este necesară pentru unul sau mai multe dintre scopurile prevăzute la art. 5 alin. (3). Scopul certificatului prevăzut de lege este de a se asigura că se aplică un proces de selecție a materialelor interceptate, astfel încât numai materialele descrise în certificat să fie puse la dispoziție spre examinare umană. Orice certificat trebuie să reflecte în linii mari „Prioritățile pentru colectarea de informații” stabilite de NSC spre ghidarea serviciilor de informații. De exemplu, un certificat poate să prevadă examinarea materialelor care furnizează informații privind terorismul (astfel cum sunt definite în Legea privind terorismul din 2000) sau privind drogurile controlate (astfel cum sunt definite în Legea privind abuzul de droguri din 1971). Comisarul pentru

interceptarea comunicațiilor trebuie să examineze orice modificare a descrierilor materialelor specificate într-un certificat.

6.15. Ministrul are obligația de a se asigura că sunt în vigoare măsuri care să garanteze că numai acele materiale care au fost certificate ca fiind necesare pentru examinare în sensul art. 5 alin. (3) și care îndeplinesc condițiile prevăzute la art. 16 alin. (2)–(6) sunt, în fapt, citite, analizate sau ascultate. Comisarul pentru Interceptarea Comunicațiilor are obligația de a examina caracterul adecvat al acestor proceduri.

Emiterea urgentă a unui mandat în temeiul art. 8 alin. (4)

6.16. RIPA prevede [art. 7 alin. (1) lit. b)] cazurile în care este necesar un mandat de interceptare de urgență, însă ministrul nu este disponibil pentru a semna mandatul. În aceste cazuri, ministrul va autoriza personal interceptarea, dar mandatul este semnat de un înalt funcționar, în urma discutării cazului între funcționari și ministru. RIPA restricționează emiterea de mandate în acest mod la cazurile urgente în care ministrul a autorizat personal și în mod expres emiterea mandatului [art. 7 alin. (2) lit. a)] și impune ca mandatul să conțină o declarație în acest sens [art. 7 alin. (4) lit. a)].

6.17. Un mandat emis în cadrul procedurii de urgență este valabil cinci zile lucrătoare de la data emiterii, cu excepția cazului în care este reînnoit de către ministru, caz în care încetează după trei luni în cazul infracțiunilor grave sau șase luni în cazul securității naționale sau al bunăstării economice, în același mod ca în cazul altor dispoziții prevăzute la art. 8 alin. (4).

Formatul unui mandat emis în temeiul art. 8 alin. (4)

6.18. Fiecare mandat este transmis persoanei care a depus cererea. Ulterior, o copie poate fi comunicată furnizorilor de servicii de comunicații care vor putea contribui fiecare cum consideră necesar pentru a acorda asistență la punerea în aplicare a interceptării. În mod normal, FSC nu vor primi o copie a certificatului. Mandatul trebuie să includă următoarele:

- o descriere a comunicațiilor care urmează să fie interceptate;
- numărul de referință al mandatului; și
- detalii privind persoanele care pot modifica ulterior certificatul aplicabil mandatului, în caz de urgență [dacă este autorizat în conformitate cu art. 10 alin. (7) din RIPA].

Modificarea unui mandat și/sau a unui certificat emis în temeiul art. 8 alin. (4)

6.19. Mandatele și certificatele de interceptare pot fi modificate în conformitate cu dispozițiile art. 10 din RIPA. Un mandat poate fi modificat numai de ministru sau, în caz de urgență, de un înalt funcționar, cu autorizarea expresă a ministrului. În aceste cazuri, o declarație cu privire la acest fapt trebuie să fie confirmată pe actul modificator, iar modificarea încetează să producă efecte după cinci zile lucrătoare de la data emiterii, cu excepția cazului în care este aprobată de ministru.

6.20. Certificatul trebuie modificat de ministru, cu excepția cazului de urgență în care certificatul poate fi modificat de un înalt funcționar, cu condiția ca funcționarul să dețină o funcție în care este autorizat în mod expres prin dispozițiile cuprinse în certificat să modifice certificatul în numele ministrului sau ca ministrul să fi autorizat în mod expres modificarea, iar o declarație privind acest fapt să fie înscrisă pe actul modificator. În acest din urmă caz, modificarea încetează să producă efecte după cinci zile lucrătoare de la data emiterii, cu excepția cazului în care este aprobată de ministru.

6.21. În cazul în care ministrul consideră că este necesar, certificatul poate fi modificat pentru a autoriza selectarea comunicațiilor unei persoane din Insulele Britanice. Locația unei persoane trebuie evaluată pe baza tuturor informațiilor disponibile. În cazul în care nu este posibil să se determine în mod definitiv unde este localizată persoana pe baza acestor informații, trebuie să se efectueze, cu bună-credință, o evaluare în cunoștință de cauză cu privire la locația în care se află persoana respectivă. În cazul în care există suspiciuni clare că o persoană se află în Regatul Unit, se aplică dispozițiile prevăzute la prezentul alineat.

Reînnoirea unui mandat emis în temeiul art. 8 alin. (4)

6.22. Ministrul poate reînnoi un mandat în orice moment înainte de data expirării acestuia. Cererile de reînnoire sunt adresate ministrului și conțin o actualizare a elementelor prezentate la pct. 6.10 de mai sus. În special, solicitantul trebuie să prezinte o evaluare a valorii interceptării la momentul cererii și să explice motivele pentru care se consideră că interceptarea continuă să fie necesară pentru unul sau mai multe dintre scopurile menționate la art. 5 alin. (3) și motivul pentru care se consideră că interceptarea continuă să fie proporțională.

6.23. În cazul în care ministrul consideră că interceptarea continuă să îndeplinească cerințele RIPA, acesta poate reînnoi mandatul. În cazul în care mandatul este emis pentru infracțiuni grave, mandatul reînnoit este valabil pentru o perioadă suplimentară de trei luni. În cazul în care este emis din motive de securitate națională/bunăstare economică, mandatul reînnoit este valabil pentru o perioadă de șase luni. Aceste date sunt valabile de la data semnării actului de reînnoire.

6.24. În circumstanțele în care a fost solicitată asistența FSC, o copie a actului de reînnoire a mandatului va fi transmisă tuturor celor cărora li s-a transmis o copie a mandatului original, cu condiția ca aceștia să continue să ofere o asistență activă. Actul de reînnoire va include numărul de referință al mandatului sau al mandatelor reînnoite în temeiul acestui act unic.

Anularea mandatului

6.25. Ministrul trebuie să anuleze un mandat de interceptare în cazul în care, în orice moment înainte de data expirării acestuia, consideră că mandatul nu mai este necesar pentru motive care intră sub incidența art. 5 alin. (3) din RIPA. Prin urmare, agențiile de interceptare trebuie să își examineze în permanență mandatele și să notifice ministrul în cazul în care consideră că interceptarea nu mai este necesară. În practică, responsabilitatea de a anula un mandat va fi exercitată de un înalt funcționar din departamentul care emite mandatul în numele ministrului.

6.26. Actul de anulare va fi adresat persoanei căreia i-a fost livrat mandatul (agenția de interceptare). O copie a actului de anulare trebuie trimisă acelor FSC, dacă este cazul, care au dat curs mandatului în perioada precedentelor douăsprezece luni.

Registrele

6.27. Regimul de supraveghere permite Comisarului pentru interceptarea comunicațiilor să examineze cererea de emitere de mandat pe care se bazează decizia ministrului, iar agenția de interceptare poate fi obligată să îi justifice conținutul. Fiecare agenție de interceptare trebuie să pună la dispoziție următoarele informații pentru a fi examinate de către Comisar, după cum consideră necesar:

- toate cererile de emitere de mandat în conformitate cu art. 8 alin. (4) și cererile de reînnoire a acestor mandate;

- toate mandatele și certificatele, precum și copii ale actelor de reînnoire și modificare (dacă este cazul);
- în cazul în care o cerere este respinsă, motivele refuzului prezentate de ministru;
- datele la care a început și a încetat interceptarea.

6.28. De asemenea, trebuie păstrate registre ale procedurilor prin care se garantează că numai materialele care au fost certificate pentru examinare în scopul prevăzut la art. 5 alin. (3) și care îndeplinesc condițiile stabilite la art. 16 alin. (2)-(6) din RIPA, în conformitate cu art. 15 din RIPA, sunt, în fapt, citite, examinate sau ascultate. Trebuie păstrate registre privind procedurile prin care sunt îndeplinite cerințele prevăzute la art. 15 alin. (2) (reducerea la minimum a copierii și distribuției materialelor interceptate) și art. 15 alin. (3) (distrugerea materialelor interceptate). Pentru mai multe detalii, a se vedea capitolul „Garanții”.

7. GARANȚII

7.1. Toate materialele interceptate sub autoritatea unui mandat emis în temeiul art. 8 alin. (1) sau alin. (4) din RIPA și orice date de comunicații aferente trebuie să fie prelucrate în conformitate cu garanțiile pe care ministrul le-a aprobat în conformitate cu obligația care i-a fost impusă de RIPA. Aceste garanții sunt puse la dispoziția Comisarului pentru Interceptarea Comunicațiilor și trebuie să îndeplinească cerințele prevăzute la art. 15 din RIPA, care sunt prezentate mai jos. În plus, garanțiile prevăzute la art. 16 din RIPA se aplică mandatelor emise în temeiul art. 8 alin. (4). Orice încălcare a acestor garanții trebuie raportată Comisarului pentru Interceptarea Comunicațiilor. Agențiile de interceptare trebuie să examineze periodic garanțiile interne pentru a se asigura că acestea sunt în continuare actualizate și efective. În cursul acestor examinări periodice, agențiile trebuie să analizeze dacă o parte din procedurile lor interne pot fi făcute publice în mod sigur și util.

Garanțiile prevăzute la art. 15

7.2. Art. 15 din RIPA impune ca divulgarea, copierea și păstrarea materialelor interceptate să se limiteze la minimul necesar pentru scopurile autorizate. Art. 15 alin. (4) din RIPA prevede că un element este necesar în scopurile autorizate dacă materialele interceptate:

- continuă să fie sau este probabil să fie necesare pentru oricare dintre scopurile prevăzute la art. 5 alin. (3) – și anume, în interesul securității naționale, în scopul prevenirii sau al depistării infracțiunilor grave, sau în scopul protejării bunăstării economice a Regatului Unit, în circumstanțe care par a fi relevante ministrului pentru interesele securității naționale;
- sunt necesare pentru a facilita exercitarea funcțiilor ministrului în temeiul Capitolului I Partea I din RIPA;
- sunt necesare pentru a facilita exercitarea oricăror funcții ale Comisarului pentru Interceptarea Comunicațiilor sau ale IPT;
- sunt necesare pentru a se asigura că o persoană care efectuează cercetarea penală deține informațiile necesare pentru a stabili ceea ce i se solicită prin obligația sa de a asigura caracterul echitabil al urmăririi penale;
- sunt necesare pentru îndeplinirea oricărei obligații impuse prin legile privind arhivele publice.

Diseminarea materialelor interceptate

7.3. Numărul persoanelor cărora le sunt divulgate oricare dintre materialele interceptate și amploarea divulgării este limitat la minimumul necesar pentru scopurile autorizate prevăzute la art. 15 alin. (4) din RIPA. Această obligație se aplică, de asemenea, divulgării către alte persoane din cadrul unei agenții, precum și divulgării în afara agenției. Această obligație este pusă în aplicare prin interzicerea divulgării către persoane care nu au fost evaluate în mod corespunzător, precum și prin principiul „necesității de a cunoaște”: materialele interceptate nu trebuie divulgate niciunei persoane, cu excepția cazului în care atribuțiile persoanei respective, care au legătură cu unul dintre scopurile autorizate, sunt de natură încât trebuie să aibă cunoștință despre materialele interceptate pentru îndeplinirea atribuțiilor respective. În mod similar, numai o mare parte din materialele interceptate pot fi divulgate, în funcție de nevoile destinatarului. De exemplu, în cazul în care este suficient un rezumat al materialelor interceptate, acesta nu trebuie să depășească ceea ce ar trebui divulgat.

7.4. Obligațiile se aplică nu numai interceptorului inițial, ci și oricărei persoane căreia i se divulgă ulterior materialele interceptate. În unele cazuri, acest lucru se va realiza prin solicitarea ca persoana din urmă să obțină aprobarea emitentului înainte de a divulga mai departe materialele interceptate. În alte cazuri, destinatarilor secundari li se aplică garanții explicite.

7.5. Atunci când materialele interceptate sunt divulgate autorităților dintr-o țară sau dintr-un teritoriu din afara Regatului Unit, agenția trebuie să ia măsuri rezonabile pentru a se asigura că autoritățile în cauză dispun și vor menține procedurile necesare pentru a proteja materialele interceptate și pentru a se asigura că acestea sunt divulgate, copiate, distribuite și păstrate numai în măsura minimă necesară. În special, materialele interceptate nu trebuie divulgate ulterior autorităților unei țări terțe sau unui teritoriu terț, cu excepția cazului în care s-a convenit în mod explicit cu agenția emitentă și trebuie returnate organismului emitent sau distruse în condiții de securitate atunci când nu mai sunt necesare.

Copierea

7.6. Materialele interceptate pot fi copiate numai în măsura în care acest lucru este necesar în scopurile autorizate prevăzute la art. 15 alin. (4) din RIPA. Copiile includ nu doar copii directe ale întregului material interceptat, ci și extrase și rezumate care se identifică ca fiind produsul unei interceptări, precum și orice înregistrare referitoare la o interceptare care include identitatea persoanelor cărora le-au fost trimise materialele interceptate sau de către care au fost trimise materialele interceptate. Restricțiile sunt puse în aplicare prin impunerea unui tratament special pentru astfel de copii, extrase și rezumate care sunt realizate prin înregistrarea realizării, distribuirii și distrugerii lor.

Depozitarea

7.7. Materialele interceptate și toate copiile, extrasele și rezumatele acestora trebuie tratate și depozitate în siguranță astfel încât să se reducă la minimum riscul pierderii sau furtului. Trebuie păstrate astfel încât să fie inaccesibile persoanelor care nu au nivelul necesar de autorizare. Această cerință de depozitare sigură a produsului interceptat se aplică tuturor celor care sunt responsabili de tratarea acestuia, inclusiv FSC. Detaliile privind semnificația în practică a unei astfel de cerințe pentru FSC vor fi stabilite în discuțiile pe care le au cu Guvernul înainte de notificarea în temeiul art. 12 (a se vedea pct. 3.13).

Distrugerea

7.8. Materialele interceptate și toate copiile, extrasele și rezumatele care pot fi identificate ca fiind produsul unei interceptări trebuie marcate în vederea ștergerii și distruse în mod securizat cât mai curând posibil, de îndată ce nu mai sunt necesare

pentru niciunul dintre scopurile autorizate. În cazul în care astfel de materiale interceptate sunt păstrate, trebuie examinate la intervale corespunzătoare pentru a confirma că justificarea păstrării lor este încă valabilă în temeiul art. 15 alin. (3) din RIPA.

7.9. Atunci când o agenție de interceptare efectuează interceptarea pe baza unui mandat emis în temeiul art. 8 alin. (4) și primește materiale interceptate neanalizate și date de comunicații aferente interceptării în temeiul mandatului respectiv, agenția trebuie să specifice (sau trebuie să stabilească sistem cu sistem) perioadele maxime de păstrare pentru diferite categorii de date care reflectă natura lor și gradul de intruziune. În mod normal, perioadele specificate nu trebuie să depășească doi ani și trebuie convenite cu Comisarul pentru Interceptarea Comunicațiilor. Datele nu pot fi păstrate pentru o perioadă mai lungă decât perioadele maxime de păstrare aplicabile decât în cazul în care se obține o autorizare prealabilă din partea unui înalt funcționar din cadrul respectivei agenții de interceptare, pe baza faptului că păstrarea continuă a datelor a fost evaluată ca fiind necesară și proporțională. În cazul în care se evaluează ulterior că păstrarea în continuare a unor astfel de date nu mai îndeplinește criteriile de necesitate și proporționalitate, acestea trebuie șterse. În măsura posibilului, toate perioadele de păstrare trebuie puse în aplicare printr-un proces de ștergere automată, care se declanșează odată ce perioada maximă de păstrare aplicabilă a fost atinsă pentru datele în cauză.

Autorizarea personalului

7.10. Toate persoanele care pot avea acces la materialele interceptate sau care trebuie să consulte orice raport în legătură cu acestea trebuie să facă obiectul unei evaluări corespunzătoare. În fiecare an, cadrele de conducere trebuie să identifice orice problemă care ar putea duce la reanalizarea evaluării individuale a membrilor personalului. Evaluarea fiecărui membru al personalului trebuie, de asemenea, examinată periodic. În cazul în care este necesar ca un agent al unei agenții să divulge materiale interceptate unei alte agenții, este responsabilitatea acestuia să se asigure că destinatarul deține autorizarea necesară.

Garantiile prevăzute la art. 16

7.11. Art. 16 prevede garanții suplimentare în ceea ce privește materialele interceptate colectate pe baza unui mandat emis în temeiul art. 8 alin. (4) impunând ca garanțiile:

- să asigure că materialele interceptate sunt citite, examinate sau ascultate de orice persoană numai în măsura în care materialele interceptate fac obiectul unui certificat; și
- să reglementeze utilizarea factorilor de selecție care privesc comunicații ale persoanelor despre care se știe că se află în prezent în Insulele Britanice.

7.12. În plus, orice selecție individuală a materialelor interceptate trebuie să fie proporțională în circumstanțele specifice [având în vedere art. 6 alin. (1) din Legea privind drepturile omului din 1998].

7.13. Certificatul garantează că materialelor interceptate li se aplică un proces de selecție pe baza unui mandat emis în temeiul art. 8 alin. (4), astfel încât nu sunt puse la dispoziție spre examinare umană decât materialele descrise în certificat (în sensul că sunt citite, examinate sau ascultate). Niciun funcționar nu este autorizat să aibă acces la date în afara celor prevăzute de certificat.

7.14. În general, sistemele automatizate trebuie utilizate, atunci când este posibil din punct de vedere tehnic, pentru efectuarea selecției în conformitate cu art. 16 alin. (1) din RIPA. În mod excepțional, un certificat poate permite accesul unui număr limitat

de membri ai personalului autorizat în mod expres la materialele interceptate fără a fi fost prelucrate sau filtrate de sistemele automatizate. Un astfel de acces nu poate fi permis decât în măsura în care este necesar pentru a stabili dacă materialele se încadrează în categoriile principale care urmează să fie selectate în temeiul certificatului sau pentru a se asigura că metodologia utilizată este actualizată și efectivă. O astfel de verificare trebuie să fie necesară din motivele specificate la art. 5 alin. (3) din RIPA. Odată îndeplinite aceste funcții, orice copie a materialelor făcută în acest scop trebuie să fie distrusă în conformitate cu art. 15 alin. (3) din RIPA. Verificarea efectuată de funcționari trebuie să fie menținută la nivelul minim absolut; ori de câte ori este posibil, trebuie utilizate tehnici de selecție automată. Verificarea este controlată de Comisarul pentru Interceptarea Comunicațiilor în timpul inspecțiilor sale.

7.15. Materialele colectate pe baza unui mandat emis în temeiul art. 8 alin. (4) trebuie citite, examinate sau ascultate numai de către persoane autorizate care beneficiază în mod regulat de formare obligatorie cu privire la dispozițiile RIPA și, în special, la funcționarea art. 16 și cerințele privind necesitatea și proporționalitatea. Aceste cerințe și proceduri trebuie să fie stabilite în orientările interne furnizate tuturor persoanelor autorizate, iar atenția tuturor persoanelor autorizate trebuie să fie direcționată în mod specific către garanțiile prevăzute de lege. Toate persoanele autorizate trebuie să facă obiectul unei evaluări corespunzătoare (a se vedea pct. 7.10 pentru informații suplimentare).

7.16. Înainte ca o persoană autorizată să poată citi, examina sau asculta materiale, trebuie creat un registru care să precizeze motivul pentru care accesul la materiale este necesar în conformitate și în temeiul art. 16, precum și al certificatului aplicabil, precum și motivul pentru care un astfel de acces este proporțional. Cu excepția cazului în care materialele sau sistemele automatizate sunt verificate în modul descris la pct. 7.14, registrele trebuie să indice, prin trimitere la factori specifici, materialele la care se solicită accesul și sistemele trebuie, în măsura posibilului, să împiedice accesul la materiale, cu excepția cazului în care o astfel de înregistrare a fost creată. Registrul trebuie să includă orice circumstanțe care ar putea conduce la un anumit grad de încălcare a confidențialității, precum și orice măsuri luate pentru a reduce amploarea intruziunii colaterale. Toate registrele trebuie păstrate în scopul unei examinări ulterioare sau al unui audit ulterior.

7.17. Accesul la materialele descrise la pct. 7.15 trebuie limitat la o anumită perioadă de timp, deși accesul poate fi reînnoit. În cazul în care accesul este reînnoit, registrul trebuie actualizat cu motivul reînnoirii. Trebuie să existe sisteme care să garanteze că, în cazul în care nu se depune o cerere de reînnoire în termenul respectiv, nu se va acorda niciun alt acces. În cazul în care accesul la materiale nu mai este solicitat, motivul trebuie, de asemenea, explicat în registru.

7.18. Trebuie efectuate audituri periodice pentru a se asigura că sunt îndeplinite cerințele prevăzute la art. 16 din RIPA și la Capitolul 3 din prezentul cod. Aceste controale trebuie să includă verificări pentru a se asigura că registrele prin care se solicită accesul la materialele care trebuie citite, examinate sau ascultate au fost compilate corect și, în mod specific, că materialele solicitate intra sub incidența aspectelor stabilite în certificatul emis de ministru. Orice erori sau deficiențe procedurale trebuie să fie notificate conducerii și să fie luate măsuri de remediere. Orice deficiențe grave trebuie aduse în atenția conducerii superioare și orice încălcare a garanțiilor (astfel cum se menționează la pct. 7.1) trebuie raportată Comisarului pentru Interceptarea Comunicațiilor. Toate rapoartele de informații generate de persoanele autorizate trebuie să facă obiectul unui audit de control al calității.

7.19. Pentru a răspunde cerințelor RIPA descrise la pct. 6.3 de mai sus, în cazul în care un factor de selecție privește o persoană cunoscută pentru moment ca fiind în Insulele Britanice și are ca scop sau ca unul dintre scopurile sale identificarea materialelor conținute în comunicațiile trimise sau destinate persoanei respective, trebuie transmisă o cerere către ministru sau un înalt funcționar, în caz de urgență, în care se explică motivele pentru care modificarea certificatului emis în temeiul art. 8 alin. (4) în privință cu o astfel de persoană este necesară pentru un scop care intră sub incidența art. 5 alin. (3) din RIPA și este proporțională în relație cu orice activitate autorizată în temeiul art. 8 alin. (4) din RIPA.

7.20. Ministrul trebuie să se asigure că garanțiile sunt în vigoare înainte ca orice interceptare pe baza unui mandat emis în temeiul art. 8 alin. (4) să poată începe. Comisarul pentru Interceptarea Comunicațiilor are obligația de a examina caracterul adecvat al garanțiilor.

[...]

8. DIVULGAREA ÎN SCOPUL ASIGURĂRII CARACTERULUI ECHITABIL ÎN CADRUL PROCESULUI PENAL

[...]

Excluderea anumitor aspecte din procedurile judiciare

8.3. Regula generală este că nici existența eventuală a interceptării, nici materialele interceptate în sine nu joacă vreun rol în procedurile judiciare. Această regulă este prevăzută la art. 17 din RIPA, care exclude probele, interogarea, declarațiile sau divulgarea în cadrul procedurilor judiciare care pot revela existența (sau absența) unui mandat emis în temeiul prezentei legi (sau al Legii privind interceptarea comunicațiilor din 1985). Această regulă înseamnă că materialele interceptate nu pot fi utilizate nici de partea acuzării, nici de partea apărării. Acest fapt păstrează „egalitatea armelor”, care este o cerință impusă în temeiul art. 6 din CEDO.

[...]

10. SUPRAVEGHEREA

10.1. RIPA prevede desemnarea unui Comisar pentru Interceptarea Comunicațiilor, al cărui mandat este de a asigura o supraveghere independentă a utilizării puterilor conferite de regimul de interceptare în temeiul Capitolului I al Părții I din RIPA.

10.2. Comisarul efectuează inspecții biannuale la fiecare dintre cele nouă agenții de interceptare. Obiectivele principale ale inspecțiilor sunt de a se asigura că Comisarul deține informațiile care îi sunt necesare pentru a-și îndeplini funcțiile în temeiul art. 57 din RIPA și pentru a-și prezenta raportul în temeiul art. 58 din RIPA. Acestea pot include inspectarea sau examinarea:

- sistemelor existente pentru interceptarea comunicațiilor;
- registrelor relevante păstrate de agenția de interceptare;
- legalității interceptării realizate; și
- orice erori și sistemele concepute pentru a preveni astfel de erori.

10.3. Orice persoană care exercită puterile conferite de Capitolul I al Părții I din RIPA trebuie să raporteze Comisarului orice acțiune considerată a fi contrară dispozițiilor RIPA sau orice aplicare necorespunzătoare a garanțiilor prevăzute la art. 15. Aceasta trebuie, de asemenea, să dea curs oricărei cereri din partea Comisarului de a furniza orice informații de care are nevoie pentru a-i permite să își exercite atribuțiile.”

5. *Declarația lui Charles Farr*

97. În declarația pregătită pentru procedura *Liberty* (supra, pct. 40), Charles Farr a indicat că, dincolo de detaliile prevăzute în RIPA, în Codul IC din 2010 și în proiectul de Cod IC din 2016 (care, în acest stadiu, fusese publicat spre consultare), toate detaliile referitoare la garanțiile prevăzute la art. 15 și 16 erau confidențiale. El a examinat personal procedurile și a considerat că nu puteau fi făcute publice fără a afecta eficacitatea metodelor de interceptare. Cu toate acestea, procedurile au fost puse la dispoziția Comisarului IC, care, în temeiul RIPA, avea obligația să le examineze. În plus, fiecare agenție de interceptare avea obligația de a ține un registru al procedurilor în cauză, iar orice încălcare trebuia să fie raportată Comisarului IC.

6. *Strategia de securitate națională și analiza privind apărarea strategică și securitatea din 2015: un Regat Unit sigur și prosper*

98. În cadrul acestei analize, Consiliul Național de Securitate (*National Security Council* – „NSC”) afirma că prioritățile sale pentru următorii cinci ani vor fi:

„Combaterea terorismului pe plan intern și extern într-un mod dur și cuprinzător, combaterea extremismului și lupta împotriva ideologiilor primejdioase care o alimentează. Vom rămâne un lider mondial în domeniul securității cibernetice. Vom descuraja amenințările provenite de la actori statali. Vom răspunde rapid și eficace la crize și vom consolida reziliența atât pe plan intern, cât și extern.

Vom contribui la consolidarea unei ordini internaționale bazate pe norme și instituțiile sale, încurajând reforma pentru a permite participarea puterilor emergente. Vom colabora cu partenerii noștri pentru a reduce conflictele și pentru a promova stabilitatea, buna guvernare și drepturile omului.

Ne vom crește prosperitatea, extinzând relația economică cu puteri emergente precum India și China, contribuind la construirea prosperității la nivel mondial, investind în inovare și în competențe, sprijinind exporturile Regatului Unit în materie de apărare și securitate.”

7. *Hotărârea IPT din 29 martie 2015 în cauza Belhadj și alții împotriva Security Service, Secret Intelligence Service, Government Communications Headquarters, Secretary of State for the Home Department și Secretary of State for the Foreign and Commonwealth Office, IPT/13/132-9/H și IPT/14/86/CH*

99. Reclamanții din această cauză s-au plâns de încălcări ale art. 6, 8 și 14 din Convenție rezultate din pretinsa interceptare a comunicațiilor lor, care făceau obiectul secretului profesional al avocatului. În măsura în care Amnesty International, în cursul procedurii *Liberty*, s-a plâns de caracterul adecvat al modalităților de protecție a materialelor acoperite de secretul profesional al avocatului (*legal professional privilege* – „LPP”), aceste

plângeri au fost „transferate” pentru a fi examinate în această cauză, iar Amnesty International s-a alăturat ca parte reclamantă (supra, pct. 52).

100. În cursul procedurii, părțile adverse au admis că, în lipsa unui sistem legal pentru tratarea LPP, începând cu luna ianuarie 2010, regimul de interceptare/obținere, analiză, utilizare, divulgare și distrugere a materialelor acoperite de secretul profesional nu mai era în conformitate cu legea, în sensul art. 8 § 2 din Convenție și, prin urmare, era ilegal. Security Service și GCHQ au confirmat că vor lucra în următoarele săptămâni pentru a-și revizui politicile și procedurile, în lumina proiectului de Cod IC și nu numai.

101. Ulterior, IPT a organizat o audiere cu ușile închise, cu asistența avocatului de pe lângă Tribunal (infra, pct. 132), pentru a examina dacă orice documente sau informații referitoare la orice materiale acoperite de secretul profesional fuseseră interceptate sau obținute de părțile pârâte. În decizia din 29 martie 2015, IPT a constatat că serviciile de informații nu deținuseră decât două documente aparținând uneia dintre părțile reclamante, care conțineau materiale care erau acoperite de LPP, și nici nu divulgau, nici nu făceau trimitere la consultanță juridică. Prin urmare, a constatat că partea reclamantă în cauză nu a suferit vreo pagubă sau vreun prejudiciu și că decizia a oferit o reparație adecvată. Cu toate acestea, a solicitat GCHQ să se angajeze că acele părți ale documentelor care conțineau materiale acoperite de secretul profesional al avocatului vor fi distruse sau șterse, o copie a documentelor să fie transmisă Comisarului IC pentru a fi păstrată o perioadă de cinci ani și în termen de paisprezece zile să fie furnizat un raport confidențial care să confirme distrugerea și ștergerea documentelor.

102. Ulterior, au fost prezentate spre consultare proiecte de modificări atât la Codul IC, cât și la Codul de bune practici privind achiziția și divulgarea datelor de comunicații, iar codurile care au fost adoptate în urma acestor consultări în 2018 cuprindeau secțiuni extinse privind accesul la informații confidențiale.

B. Schimbul de informații

1. Acordul dintre Regatul Unit și SUA privind schimbul de informații în domeniul comunicațiilor

103. Un acord privind schimbul de informații în domeniul comunicațiilor între Regatul Unit și SUA din 5 martie 1946 reglementa schimbul de informații secrete dintre autoritățile britanice și cele americane în ceea ce privește comunicațiile „străine”, definite prin trimitere la alte țări decât Statele Unite ale Americii, Regatul Unit și Commonwealth-ul. În temeiul acordului, părțile se angajau să schimbe rezultatele mai multor operațiuni de interceptare legate de comunicațiile străine.

2. Cadrul legal relevant pentru funcționarea serviciilor de informații

104. În Regatul Unit există trei servicii de informații: Serviciul de Securitate (*Security Service*, „MI5”), Serviciul Secret de Informații (*Secret Intelligence Service*, „MI6”) și GCHQ.

(a) MI5

105. În temeiul art. 2 din Legea din 1989 privind serviciile de securitate (*Security Service Act* – „SSA”), directorul general al MI5, care era numit de ministrul internelor, avea îndatorirea de a se asigura că există proceduri pentru a se asigura că MI5 nu obține alte informații decât în măsura în care acest lucru este necesar pentru îndeplinirea corespunzătoare a funcțiilor sale sau că nu le divulgă decât cu excepția cazului în care acest lucru este necesar în acest scop sau în scopul prevenirii sau depistării infracțiunilor grave sau pentru un proces penal.

106. În temeiul art. 1 din SSA, funcțiile MI5 erau de a proteja securitatea națională și, în special, de a proteja împotriva amenințărilor de spionaj, terorism și sabotaj, împotriva activităților agenților de puteri străine și împotriva acțiunilor destinate răsturnării sau subminării democrației parlamentare prin mijloace politice, industriale sau violente, de a proteja bunăstarea economică a Regatului Unit împotriva amenințărilor reprezentate de acțiunile sau intențiile persoanelor din afara Insulelor Britanice, și de a acționa în sprijinul activităților forțelor de poliție, ale Agenției Naționale pentru Combaterea Criminalității și ale altor agenții de aplicare a legii, pentru prevenirea și depistarea infracțiunilor grave.

(b) MI6

107. Art. 2 din Legea din 1994 privind serviciile de informații (*Intelligence Services Act* – „ISA”) prevedea că îndatoririle șefului Serviciului MI6, care era numit de ministrul afacerilor externe și Commonwealth-ului (astfel cum era la momentul faptelor), includeau asigurarea faptului că existau proceduri că MI6 nu obține alte informații decât în măsura în care acest lucru este necesar pentru îndeplinirea corespunzătoare a funcțiilor sale și că nu divulgă nicio informație decât în măsura în care acest lucru este necesar în acest scop, în interesul securității naționale, în scopul prevenirii sau depistării infracțiunilor grave sau pentru un proces penal.

108. Conform art. 1 din ISA, atribuțiile MI6 erau de a obține și furniza informații referitoare la acțiunile sau intențiile unor persoane din afara Insulelor Britanice și de a îndeplini alte sarcini legate de acțiunile sau intențiile unor astfel de persoane. Aceste atribuții nu puteau fi exercitate decât în interesul securității naționale, în special cu trimitere la politicile de apărare și externe ale statului, în interesul bunăstării economice a Regatului Unit sau în sprijinul prevenirii sau depistării infracțiunilor grave.

(c) GCHQ

109. Art. 4 din ISA prevedea că directorul GCHQ, care era numit de ministrul afacerilor externe și Commonwealth-ului (astfel cum era la momentul faptelor) avea îndatorirea de a se asigura că există proceduri prin care să se asigure că nu se obține nicio informație decât pentru buna exercitare a funcțiilor sale și că nicio informație nu este divulgată decât în măsura în care era necesar.

110. În temeiul art. 3 din ISA, una dintre atribuțiile GCHQ era de a monitoriza sau de a supraveghea emisiile electromagnetice, acustice și de altă natură și orice echipament producător astfel de emisii și de a obține și furniza informații derivate din sau legate de astfel de emisii sau echipamente, precum și de la materiale criptate. Aceste atribuții nu puteau fi exercitate decât în interesul securității naționale, în special cu trimitere la politicile de apărare și externe ale statului, în interesul bunăstării economice a Regatului Unit sau în sprijinul prevenirii sau depistării infracțiunilor grave.

(d) Legea din 2008 privind combaterea terorismului (*Counter Terrorism Act 2008*)

111. Art. 19 din Legea privind lupta privind combaterea terorismului din 2008 permitea divulgarea de informații către oricare dintre serviciile de informații în scopul exercitării atribuțiilor acestora. Informațiile obținute de un serviciu de informații în cadrul exercitării atribuțiilor sale puteau fi utilizate de serviciul respectiv în cadrul exercitării oricăreia dintre celelalte atribuții ale sale.

112. Informațiile obținute de MI5 puteau fi divulgate în scopul îndeplinirii corespunzătoare a atribuțiilor sale, în scopul prevenirii sau depistării infracțiunilor grave sau pentru un proces penal. Informațiile obținute de MI6 puteau fi divulgate în scopul îndeplinirii corespunzătoare a atribuțiilor sale, în interesul securității naționale, în scopul prevenirii sau depistării infracțiunilor grave sau pentru un proces penal. Informațiile obținute de GCHQ puteau fi divulgate în scopul îndeplinirii corespunzătoare a atribuțiilor sale sau pentru un proces penal.

(e) Legea din 1998 privind protecția datelor (*Data Protection Act – „DPA”*)

113. DPA reprezenta legislația de transpunere în legislația Regatului Unit a Directivei 95/46/CE privind protecția datelor cu caracter personal. Fiecare dintre serviciile de informații era „operator de date” în sensul DPA și, ca atare, era obligat să respecte – sub rezerva exceptării prin certificat ministerial – principiile de protecție a datelor din Partea 1 a Anexei 1, inclusiv:

„(5) Datele cu caracter personal prelucrate în orice scop sau în orice scopuri nu sunt păstrate mai mult decât este necesar în scopul respectiv sau scopurile respective [...]”

și

„(7) Sunt luate măsuri tehnice și organizatorice adecvate împotriva prelucrării neautorizate sau ilegale a datelor cu caracter personal și împotriva pierderii accidentale, a distrugerii sau a deteriorării datelor cu caracter personal.”

(f) Legea din 1989 privind secretul de stat (*Official Secrets Act* - „OSA”)

114. Un membru al serviciilor de informații săvârșește o infracțiune în temeiul art. 1 alin. (1) din OSA în cazul în care divulgă, fără autoritate legală, orice informație, document sau alt articol legat de securitate sau informații care se afla în posesia sa în virtutea calității sale de membru al serviciilor respective.

(g) Legea din 1998 privind drepturile omului (*Human Rights Act* – „HRA”)

115. În temeiul art. 6 din HRA, era ilegal ca o autoritate publică să acționeze într-un mod incompatibil cu un drept conferit de Convenție.

3. Codul de bune practici privind interceptarea comunicațiilor

116. În urma procedurii *Liberty*, informațiile conținute în nota de divulgare din 9 octombrie (supra, pct. 33 și 36) au fost încorporate în Codul IC:

„12. REGULI PRIVIND SOLICITAREA ȘI TRATAREA COMUNICAȚIILOR INTERCEPTATE NEANALIZATE DE LA UN GUVERN STRĂIN

Domeniul de aplicare al prezentului capitol

12.1. Prezentul capitol se aplică agențiilor de interceptare care efectuează interceptări pe baza unui mandat emis în temeiul art. 8 alin. (4).

Cereri de asistență, altele decât cele în conformitate cu un acord internațional de asistență reciprocă

12.2. O agenție de interceptare nu poate depune o cerere către guvernul unei țări sau teritoriu din afara Regatului Unit pentru comunicații interceptate neanalizate (și date de comunicații aferente) altfel decât în conformitate cu un acord internațional de asistență reciprocă, dacă:

- un mandat de interceptare relevant [în temeiul RIPA] a fost deja emis de ministru, asistența guvernului străin este necesară pentru obținerea comunicărilor în cauză deoarece nu pot fi obținute în temeiul mandatului de interceptare relevant al RIPA și este necesar și proporțional ca serviciile de informații să obțină aceste comunicații; sau
- solicitarea de comunicații specifice în lipsa unui mandat de interceptare în temeiul RIPA relevant nu echivalează cu o eludare deliberată a RIPA și nici nu afectează în alt mod obiectivele RIPA (de exemplu, deoarece nu este fezabil din punct de vedere tehnic să se obțină comunicațiile prin interceptarea în temeiul RIPA) și este necesar și proporțional ca agenția de interceptare să obțină aceste comunicații.

12.3. O cerere care intră sub incidența celei de-a doua liniuțe a pct. 12.2 nu poate fi formulată decât în circumstanțe excepționale și trebuie examinată și decisă personal de către ministru.

12.4. În acest scop, un «mandat de interceptare relevant emis în temeiul RIPA» înseamnă: (i) un mandat emis în temeiul art. 8 alin. (1) în legătură cu subiectul în cauză; (ii) un mandat emis în temeiul art. 8 alin. (4) și un certificat atașat, care include una sau mai multe «descrieri ale materialelor interceptate» [în sensul art. 8 alin. (4) lit. b) din RIPA] și care acoperă comunicațiile subiectului, precum și o modificare adecvată a art. 16 alin. (3) (pentru persoanele despre care se cunoaște că se află în Insulele Britanice) sau (iii) un mandat emis în temeiul art. 8 alin. (4) și un certificat atașat, care include una sau mai multe «descrieri ale materialelor interceptate» care acoperă comunicațiile subiectului (către alte persoane).

Garanții aplicabile tratării comunicațiilor interceptate neanalizate de la un guvern străin

12.5. În cazul în care o cerere care intră sub incidența celei de-a doua liniuțe a pct. 12.2 este aprobată de ministru fără să fie legată de selectorii specifici, orice comunicație obținută nu poate fi examinată de agenția de interceptare în conformitate cu factorii menționați la art. 16 alin. (2) lit. a) și b) din RIPA, cu excepția cazului în care ministrul a examinat și a aprobat personal examinarea acestor comunicații în funcție de factorii respectivi.¹

12.6. În cazul în care conținutul comunicațiilor interceptate sau datele de comunicații sunt obținute de agențiile de interceptare astfel cum se prevede la pct. 12.2 sau sunt altfel obținute de la guvernul unei țări sau teritoriu din afara Regatului Unit, în circumstanțe în care materialul se identifică ca fiind produsul unei interceptări (cu excepția cazului în care se face în conformitate cu un acord internațional de asistență reciprocă), conținutul comunicațiilor și datele de comunicații trebuie să facă obiectul acelorași reguli și garanții interne care se aplică acelorași categorii de conținut sau de date atunci când sunt obținute direct de agențiile de interceptare ca urmare a unei interceptări în temeiul RIPA.

12.7. Toate cererile adresate în lipsa unui mandat de interceptare relevant emis în temeiul RIPA guvernului unei țări sau teritoriu din afara Regatului Unit pentru comunicații interceptate neanalizate (și datele de comunicații aferente) sunt notificate Comisarului pentru Interceptarea Comunicațiilor.”

C. Obținerea de date de comunicații

117. Capitolul II al Părții 1 din RIPA stabilește cadrul în care autoritățile publice pot obține date de comunicații de la furnizorii de servicii de comunicații („FSC”).

118. În temeiul art. 22, autorizația pentru obținerea datelor de comunicații de la FSC era acordată de o „persoană desemnată”, care deținea astfel de funcție, grad sau poziție în cadrul autorităților publice relevante, astfel cum se prevedea într-un ordin emis de ministru. Persoana desemnată putea fie să acorde autorizația persoanelor din cadrul aceleiași „autorități publice competente”, similară ei, „să realizeze activitatea căreia i se aplică prezentul

¹ Toate celelalte cereri menționate la pct. 12.2 (cu sau fără un mandat de interceptare relevant emis în temeiul RIPA) se vor face pentru materiale către, dinspre sau cu privire la anumiți selectori (care au, prin urmare, legătură cu o anumită persoană sau anumite persoane). În aceste circumstanțe, ministrul va fi aprobat deja cererea pentru persoana sau persoanele specifice, astfel cum se prevede la punctul [sic.] 12.2.

capitol” [autorizație în temeiul art. 22 alin. (3)], fie putea, prin notificarea FSC, să solicite să divulge datele aflate deja în posesia sa ori să obțină și să divulge date [notificare în temeiul art. 22 alin. (4)]. În sensul art. 22 alin. (3), „autoritățile publice competente” includeau forțele de poliție, Agenția Națională pentru Combaterea Criminalității, Administrația Fiscală și Vamală a Majestății Sale, oricare dintre serviciile de informații, precum și orice autoritate publică care putea fi specificată printr-un ordin emis de ministru.

119. Art. 22 alin. (2) prevedea, de asemenea, că persoana desemnată putea doar să acorde o autorizație în temeiul art. 22 alin. (3) sau putea transmite o notificare în temeiul art. 22 alin. (4), în cazul în care considera că acest lucru era necesar pentru unul dintre următoarele motive:

- „a) în interesul securității naționale;
- b) în scopul prevenirii sau depistării infracțiunilor sau al prevenirii tulburărilor;
- c) în interesul bunăstării economice a Regatului Unit;
- d) în interesul siguranței publice;
- e) în scopul protejării sănătății publice;
- f) în scopul calculării sau colectării oricăror impozite, taxe, taxe fiscale sau alte impuneri, contribuții sau taxe plătibile unui departament guvernamental;
- g) în scopul de a preveni, în caz de urgență, decesul, vătămarea sau o atingere adusă sănătății fizice sau mentale a unei persoane sau de a atenua o vătămare sau atingere adusă sănătății fizice sau mentale a unei persoane;
- h) în orice scop [care nu intră sub incidența lit. a)–g)] care este specificat în sensul prezentului articol printr-un ordin emis de ministru.”

120. De asemenea, persoana desemnată trebuia să considere că obținerea datelor era proporțională cu scopul urmărit.

121. Capitolul II din RIPA a fost completat de Codul de bune practici privind obținerea și divulgarea datelor de comunicații, emis în conformitate cu art. 71 din RIPA.

D. Practica și procedura IPT

1. RIPA

122. IPT a fost înființat în temeiul art. 65 alin. (1) din RIPA pentru a examina acuzațiile formulate de cetățeni cu privire la o ingerință ilicită în comunicațiile lor ca urmare a unei activități care intra sub incidența respectivei legi. Are competența de a investiga orice plângere privind interceptarea comunicațiilor unei persoane și, în cazul în care interceptarea s-a produs, de a examina autoritatea unei astfel de interceptări.

123. Nimirile în IPT sunt în esență de natură judiciară, dar diferă în funcție de faptul dacă candidatul propus este magistrat la instanțe superioare din

Anglia și Țara Galilor, Scoția sau Irlanda de Nord (denumit în continuare „membru judiciar”) sau este „membru nejudiciar”. Membru nejudiciar poate fi un magistrat experimentat cu o vechime de cel puțin zece ani și care nu mai lucrează cu normă întreagă. Procesul de selecție al magistraților din sistemul judiciar din Anglia și Țara Galilor este condus de *Judicial Office*, în numele *Lord Chief Justice*. *Judicial Office* invita judecătorii de la *High Court* din Anglia și Țara Galilor să transmită scrisori de interes, aceștia fiind audiați de un comitet format din președintele IPT, un membru nejudiciar al IPT și un comisar care nu este magistrat și nici jurist din cadrul Comisiei pentru numiri judiciare. Comitetul prezintă apoi un raport către *Lord Chief Justice*, care se adresează în scris ministrului internelor, formulând recomandări oficiale pentru numirile în funcție. În continuare, ministrul se adresează în scris prim-ministrului, solicitându-i să ceară permisiunea Majestății Sale de a acorda patente (*Letters Patent*) pentru numirile recomandate. Prim-ministrul recomandă candidatul sau candidații aleși Majestății Sale Regina, care oficializează numirea prin patentă. Membrii nejudiciari sunt recrutați prin concurs general. IPT publică anunțuri pentru recrutarea de membri nejudiciari într-o serie de ziare naționale și site-uri de recrutare, solicitând transmiterea de scrisori de intenție persoanelor care au calificarea corespunzătoare. Procesul este diferit față de cel al membrilor judiciari prin faptul că nu este implicat *Lord Chief Justice*, dar similar în toate celelalte privințe. În prezent, există cinci membri judiciari [doi membri ai *Court of Appeal* din Anglia (dintre care unul este președintele), un membru al *High Court* din Anglia și doi membri ai *Outer House of the Court of Session* din Scoția (dintre care unul este vicepreședinte)] și cinci membri nejudiciari (dintre care unul este un judecător pensionat al *High Court* din Irlanda de Nord).

124. În temeiul art. 67 alin. (2) și (3) lit. c), IPT trebuie să aplice aceleași principii precum o instanță care se pronunță asupra unei cereri de control judecătoresc. Cu toate acestea, nu are competența de a pronunța o declarație de incompatibilitate în cazul în care constată că legislația primară este incompatibilă cu Convenția europeană a drepturilor omului, întrucât nu este o „instanță” în sensul art. 4 din Legea privind drepturile omului din 1998.

125. Art. 68 alin. (6) și (7) impune celor implicați în autorizarea și executarea unui mandat de interceptare să divulge sau să furnizeze IPT toate documentele și informațiile pe care le solicita.

126. Art. 68 alin. (4) prevede că, în cazul în care IPT examinează o plângere, are competența de a acorda despăgubiri și de a dispune orice alte măsuri pe care le considera adecvate, inclusiv pronunțarea anulării sau încetării oricărui mandat și distrugerea înregistrărilor obținute în temeiul mandatului [art. 67 alin. (7)]. În cazul în care o plângere formulată în fața IPT are câștig de cauză, IPT este obligat, în general, să îl informeze pe prim-ministru [art. 68 alin. (5)].

127. Art. 68 alin. (1) permite IPT să își stabilească propriul regulament de procedură, cu toate că art. 69 alin. (1) prevede că ministrul poate, de asemenea, să adopte norme de procedură.

2. *Regulamentul Tribunalului cu Competențe de Investigare din 2000 („Regulamentul”)*

128. Regulamentul de procedură a fost adoptat de ministru pentru a reglementa diferite aspecte ale procedurii în fața IPT.

129. Art. 9 permite IPT să organizeze, în orice stadiu al examinării, audieri în cadrul cărora reclamantul să poată formula observații, să depună mărturie și să citeze martori. Cu toate că art. 9 prevedea că procedurile IPT, inclusiv audierile, urmau să se desfășoare cu ușile închise, în cauzele IPT/01/62 și IPT/01/77, chiar IPT a decis că, sub rezerva obligației generale impuse de art. 6 alin. (1) de a împiedica divulgarea de informații sensibile, își poate exercita puterea discreționară în favoarea organizării unei audieri publice. Ca urmare a acestui angajament de a organiza audieri publice atunci când era posibil, IPT publică, de asemenea, hotărârile sale cele mai importante pe site-ul său Internet, cu condiția să nu existe niciun risc de divulgare a unor informații cu caracter prejudiciabil.

130. Art. 11 permite IPT să admită probe indiferent de forma lor, chiar și în cazul celor inadmisibile în fața unei instanțe.

131. Conform art. 6, IPT trebuie să se asigure, în exercitarea atribuțiilor sale, că nu sunt divulgate informațiile contrare interesului public sau care aduc atingere securității naționale, prevenirii sau depistării infracțiunilor grave, bunăstării economice a Regatului Unit sau continuării exercitării atribuțiilor oricăruia dintre serviciile de informații.

3. *Avocatul de pe lângă Tribunal*

132. IPT poate numi un avocat de pe lângă Tribunal pentru a prezenta observații în numele reclamantilor în cadrul unor audieri la care aceștia nu pot fi reprezentați. În cauza *Liberty*, avocatul de pe lângă Tribunal a descris rolul său după cum urmează:

„Avocatul de pe lângă Tribunal îndeplinește o funcție diferită [de avocații speciali în procedurile cu ușile închise desfășurate în fața anumitor instanțe], similară celei de *amicus curiae*. Funcția sa este de a asista Tribunalul în orice mod în care îl solicită. Uneori (de exemplu, în legătură cu aspecte în care sunt reprezentate toate părțile), Tribunalul nu specifică din ce perspectivă trebuie prezentate observațiile. În aceste condiții, avocatul va prezenta observații în conformitate cu propria analiză a aspectelor de drept sau de fapt relevante, încercând să acorde o atenție deosebită aspectelor care nu au fost dezvoltate pe deplin de către părți. În alte situații (în special în cazul în care unul sau mai multe interese nu sunt reprezentate), Tribunalul îl poate invita pe avocat să prezinte observații dintr-o anumită perspectivă (în mod normal, punctul de vedere al părții sau părților ale căror interese nu sunt altfel reprezentate).”

133. Această descriere a fost acceptată și aprobată de IPT.

4. R (privind cererea Privacy International) împotriva Investigatory Powers Tribunal și alții [2019] UKSC 22

134. În această hotărâre, care a fost pronunțată la 15 mai 2019, Curtea Supremă a hotărât că art. 67 alin. (8) din RIPA nu exclude controlul judecătoresc al unei decizii a IPT.

E. Controlul

135. Partea IV din RIPA prevede numirea de către prim-ministru a unui Comisar pentru Interceptarea Comunicațiilor (denumit în continuare „Comisarul IC”) și a unui Comisar pentru Serviciile de Informații, însărcinat cu supravegherea activităților serviciilor de informații.

136. Comisarul IC este responsabil cu controlul interceptării comunicațiilor și obținerii și divulgării datelor de comunicații de către serviciile de informații, forțele de poliție și alte autorități publice. În îndeplinirea rolului de a controla practicile de supraveghere, Comisarul IC și inspectorii săi au acces la toate documentele relevante, inclusiv la materialele confidențiale, iar toți cei implicați în activitățile de interceptare au obligația de a-i divulga orice material solicitat. Obligația agențiilor de interceptare de a ține registre asigură accesul efectiv al Comisarului IC la detaliile activităților de supraveghere desfășurate. După fiecare inspecție, este trimis un raport șefului autorității publice, care conține recomandări formale și care solicită autorității publice să răspundă printr-un raport, în termen de două luni, pentru a confirma dacă au fost puse în aplicare recomandările sau ce progrese au fost realizate. Comisarul transmite un raport semestrial prim-ministrului cu privire la îndeplinirea funcțiilor sale și pregătește un raport anual. Respectivul raport este un document public (sub rezerva nedivulgării anexelor confidențiale) care este prezentat în fața Parlamentului.

137. Comisarul pentru Servicii de Informații asigură controlul extern independent suplimentar al utilizării puterilor intruzive ale serviciilor de informații și ale unor părți ale Ministerului Apărării. Acesta transmite, de asemenea, rapoarte anuale prim-ministrului, care sunt prezentate în fața Parlamentului.

138. Legea din 2016 privind competențele de investigare din 2016 (infra, pct. 183-190) a abrogat aceste dispoziții, în măsura în care făceau trimitere la Anglia, Scoția și Țara Galilor, iar în septembrie 2017, Biroul Comisarului pentru Competențe de Investigare (*Investigatory Powers Commissioner's Office* – „IPCO”) a preluat responsabilitatea în ceea ce privește controlul competențelor de investigare. IPCO este format din aproximativ cincisprezece comisari judiciari, judecători în funcție sau recent pensionați de la *High Court*, *Court of Appeal* și Curtea Supremă; un complet consultativ tehnic compus din experți științifici; aproximativ cincizeci de membri ai personalului oficial, inclusiv inspectori, avocați și experți în comunicații.

F. Controlul operațiunilor de interceptare efectuate de serviciile de informații

1. *Comisia pentru Informații și Securitate a Parlamentului (Intelligence and Security Committee of Parliament – „ISC”): Declarația din iulie 2013 privind acuzațiile de interceptare de către GCHQ a comunicațiilor în cadrul programului PRISM al SUA*

139. ISC a fost înființat inițial de ISA pentru a examina politicile, administrarea și cheltuielile MI5, MI6 și GCHQ. Cu toate acestea, odată cu adoptarea Legii privind justiția și securitatea din 2013, ISC a primit în mod explicit statutul de comisie a Parlamentului, i s-au conferit puteri mai mari, iar mandatul său a fost sporit pentru a include controlul activității operaționale și activitățile ample de informații și securitate ale Guvernului. În conformitate cu art. 1-4 din Legea din 2013 privind justiția și securitatea, este alcătuită din nouă membri provenind din ambele camere ale Parlamentului și, în exercitarea funcțiilor lor, acești membri beneficiază în mod regulat de acces la materiale cu un grad ridicat de confidențialitate.

140. În urma dezvăluirilor lui Edward Snowden, ISC a efectuat o anchetă privind accesul GCHQ la conținutul comunicațiilor interceptate în cadrul programului PRISM al Statelor Unite ale Americii, cadrul juridic care reglementa accesul și procedurile pe care GCHQ le-a stabilit cu serviciul omolog din străinătate pentru schimbul de informații. În cursul anchetei, ISC a colectat probe detaliate de la GCHQ și a discutat programul cu NSA.

141. ISC a concluzionat că acuzațiile potrivit cărora GCHQ a eludat dreptul Regatului Unit prin utilizarea programului PRISM pentru a accesa conținutul comunicațiilor private erau nefondate, întrucât GCHQ și-a respectat obligațiile legale cuprinse în ISA. În plus, a constatat că, în fiecare caz în care GCHQ a solicitat informații de la Statele Unite ale Americii, era deja în vigoare un mandat de interceptare semnat de un ministru.

2. *Raportul „Viața privată și securitatea: un cadru juridic modern și transparent” (Privacy and security: a modern and transparent legal framework)*

142. În urma declarației sale din iulie 2013, ISC a efectuat o anchetă mai aprofundată cu privire la întreaga gamă de capacități ale serviciilor de informații. Raportul său, care conținea o cantitate fără precedent de informații cu privire la capacitățile intruzive ale serviciilor de informații, a fost publicat la 12 martie 2015.

143. ISC a considerat că serviciile de informații și de securitate din Regatul Unit nu au încercat să eludeze legea, inclusiv cerințele Legii privind drepturile omului din 1998, care reglementa toate activitățile acestora. Cu toate acestea, comisia a considerat că, întrucât cadrul juridic a evoluat în mod fragmentat, era complicat în mod inutil. Prin urmare, ISC a exprimat

preocupări serioase cu privire la lipsa de transparență rezultată, care nu era în interesul public. Prin urmare, recomandarea-cheie a fost ca actualul cadru juridic să fie înlocuit cu o nouă lege a Parlamentului care să stabilească în mod clar puterile intruzive de care dispun serviciile de informații, scopurile pentru care ar putea să le utilizeze acestea, precum și autorizația necesară înainte să poată face acest lucru.

144. În ceea ce privește capacitatea de interceptare în masă a GCHQ, ancheta a arătat că serviciile de informații nu aveau autoritatea juridică, resursele, capacitatea tehnică sau dorința de a intercepta orice comunicare a cetățenilor britanici sau a Internetului în ansamblu. Prin urmare, GCHQ nu citea e-mailurile tuturor persoanelor din Regatul Unit. Dimpotrivă, sistemele de interceptare în masă ale GCHQ funcționau pe un procent foarte mic de canale de transmisie care constituiau Internetul și ISC avea convingerea că GCHQ aplica niveluri de filtrare și de selecție astfel încât numai o anumită parte a materialelor provenite de la aceste canale de transmisie era colectată. Căutările specifice suplimentare au asigurat faptul că numai acele elemente considerate a fi cu cea mai mare valoare de informații au fost prezentate vreodată analiștilor pentru a le examina, ceea ce a avut drept consecință faptul că doar o mică parte dintre cele colectate au fost consultate vreodată de o ființă umană.

145. În ceea ce privește comunicațiile prin Internet, ISC a considerat că distincția dintre comunicațiile „interne” și cele „externe” era una confuză și lipsită de transparență. Prin urmare, a sugerat Guvernului să publice o explicație precizând care comunicații prin Internet se încadrează în această categorie. Cu toate acestea, ancheta a stabilit că interceptarea în masă nu putea fi utilizată pentru a ținti comunicațiile unei persoane în Regatul Unit fără o autorizație specifică, semnată de un ministru, care să numească respectiva persoană.

146. ISC a observat că mandatul emis în temeiul art. 8 alin. (4) era foarte succint. În măsura în care certificatul atașat stabilea categoriile de comunicații care puteau fi examinate, aceste categorii erau exprimate în termeni foarte generali [de exemplu, „materiale care furnizează informații privind terorismul [astfel cum sunt definite în Legea privind terorismul din 2000 (astfel cum a fost modificată)], inclusiv, dar fără a se limita la acestea, organizații teroriste, teroriști, simpatizanți activi, planificare de atacuri, colectare de fonduri”). Având în vedere că certificatul era atât de generic, ISC și-a pus întrebarea dacă acesta trebuia să fie secret sau dacă, din motive de transparență, putea fi publicat.

147. Cu toate că certificatul emis în temeiul art. 8 alin. (4) stabilea categoriile generale de informații care puteau fi examinate, ISC a constatat că, în practică, selecția canalelor de transmisie și aplicarea unor selectori simpli și a unor criterii de căutare determinau care comunicații erau examinate. Prin urmare, ISC a solicitat asigurări că acestea fac obiectul controlului și verificării miniștrilor și/sau comisarilor. Cu toate acestea,

probele prezentate în fața ISC indicau faptul că nici miniștrii, nici comisarii nu aveau o vizibilitate semnificativă în ceea ce privește aspectele respective. Prin urmare, ISC a recomandat să i se atribuie Comisarului IC responsabilitatea legală de a examina diferitele criterii de selecție utilizate în interceptarea în masă, pentru a se asigura că acestea decurg direct din certificat și din cerințele naționale de securitate valabile.

148. ISC a observat că datele de comunicații erau esențiale pentru investigațiile celor mai multe servicii de informații: acestea puteau fi analizate pentru a găsi modele care să reflecte comportamente on-line specifice asociate activităților, precum planificarea atacurilor, pentru a stabili legături, pentru a se concentra asupra indivizilor pasibili să reprezinte o amenințare, pentru a se asigura că interceptarea este ținută în mod adecvat și pentru a repera relativ rapid rețelele și asocierile. Acestea date erau deosebit de utile în etapele inițiale ale unei anchete, când era necesar ca serviciile de informații să fie în măsură să stabilească dacă persoanele asociate cu o țintă aveau legătură cu complotul (și, prin urmare era necesară o cercetare suplimentară) sau dacă erau spectatori nevinovați. Potrivit ministrului internelor, aceste date „au jucat un rol semnificativ în fiecare operațiune împotriva terorismului din cadrul serviciului de securitate, în ultimul deceniu”. Cu toate acestea, ISC și-a exprimat îngrijorarea față de definiția „datelor de comunicații”. Cu toate că a admis că exista o categorie de date de comunicații mai puțin intruzive decât conținutul și, prin urmare, nu se impunea același grad de protecție, a considerat că existau anumite categorii de date de comunicații care aveau potențialul de a revela detalii mai intruzive cu privire la viața privată a unei persoane și, prin urmare, impuneau existența unor garanții mai ridicate.

149. În sfârșit, în ceea ce privește IPT, ISC a recunoscut în mod expres importanța unui drept la o cale de atac internă.

3. *„O problemă de încredere”: raport privind examinarea competențelor de investigare întocmit de evaluatorul independent al legislației privind terorismul (A Question of Trust, „Raportul Anderson”)*

150. Evaluatorul independent al legislației privind terorismul este o persoană complet independentă de Guvern, numită de ministrul internelor și ministrul Trezoreriei pentru un mandat de trei ani, care poate fi reînnoit. Are sarcina de a raporta ministrului internelor și Parlamentului cu privire la aplicarea legislației privind lupta împotriva terorismului în Regatul Unit. Aceste rapoarte sunt prezentate în fața Parlamentului pentru a informa publicul și pentru dezbateră politică.

151. Scopul raportului Anderson, care a fost prezentat în fața Parlamentului și publicat la 11 iunie 2015 și care purta numele lui David Anderson Q.C., evaluatorul independent al legislației privind terorismul în perioada respectivă, a fost acela de a informa publicul și de a permite

dezbateră politică cu privire la amenințările la adresa Regatului Unit, la capacitățile necesare pentru a lupta împotriva acestor amenințări, la garanțiile existente pentru a proteja viața privată, la provocările legate de evoluția tehnologiei, la aspectele legate de transparență și supraveghere, precum și la necesitatea unei legislații noi sau modificate. Pentru a face acest raport, evaluatorul independent a avut acces nerestricționat, la cel mai înalt nivel de autorizare de securitate, la departamentele guvernamentale responsabile și la autoritățile publice. De asemenea, a colaborat cu furnizori de servicii, experți tehnici independenți, organizații neguvernamentale, cadre universitare, avocați, judecători și autorități de reglementare.

152. Evaluatorul independent a observat, în privința cadrului legal care reglementa competențele de investigare, că se dezvoltase „în mod fragmentat”, ceea ce a avut drept consecință faptul că „puține [legi] erau mai impenetrabile decât RIPA și sateliții săi”.

153. În ceea ce privește importanța datelor de comunicații, a observat că acestea permiteau serviciilor de informații să creeze o imagine a activităților unui subiect de interes și că erau extrem de importante pentru furnizarea de informații cu privire la activitățile infracționale și teroriste. Datele identificau ținte pentru operațiuni ulterioare și contribuiau, de asemenea, la a stabili dacă cineva era complet nevinovat. De importanță majoră era capacitatea de a utiliza datele de comunicații (sub rezerva necesității și proporționalității) pentru:

- (a) a face legătura între o persoană și un cont sau o acțiune (de exemplu, vizitarea unui site Internet sau trimiterea unui e-mail) prin intermediul adresei IP;
- (b) a stabili locul în care se afla o persoană, de regulă prin intermediul locației celulare sau al datelor GPRS;
- (c) a stabili modul în care comunicau suspectii sau victimele (și anume, prin intermediul căror aplicații sau servicii);
- (d) a observa infracționalitatea on-line (de exemplu, care erau site-urile web vizitate în scopuri teroriste, pentru exploatarea sexuală a copiilor sau pentru achiziționarea de arme de foc sau droguri ilegale);
- (e) a exploata datele [de exemplu, pentru a identifica unde, când și cu cine sau cu ce comunica o persoană, cum a fost executat programul malware sau atacuri de tipul „blocarea serviciului” (*denial of service attack*), precum și pentru a corobora alte dovezi].

154. În plus, analiza datelor de comunicații putea fi efectuată imediat, făcându-le extrem de utile în operațiunile cu evoluție rapidă, iar utilizarea datelor de comunicații putea fie să constituie un argument pentru utilizarea unei măsuri mai intruzive, fie să furnizeze informații care să facă alte măsuri să devină inutile.

155. Propunerile de reformă ale evaluatorului independent pot fi rezumate după cum urmează:

- (a) elaborarea unei noi legi cuprinzătoare și ușor de înțeles, care să înlocuiască „multitudinea de competențe existente” și care să prevadă limite și garanții clare cu privire la orice putere intruzivă care ar putea fi necesar să fie utilizată de autoritățile publice;
- (b) revizuirea și clarificarea definițiilor termenilor „conținut” și „date de comunicații”;
- (c) menținerea capacității serviciilor de securitate și de informații de a practica colectarea în masă a materialelor interceptate și a datelor de comunicații asociate, însă numai sub rezerva unor garanții suplimentare stricte, inclusiv autorizarea tuturor mandatelor de către un comisar judiciar în cadrul unei noi comisii independente de supraveghere și de informații (*Independent Surveillance and Intelligence Commission* – „ISIC”);
- (d) precizarea, în certificatul însoțitor, a scopurilor pentru care au fost căutate materiale sau date prin referire la operațiuni sau misiuni specifice (de exemplu, „planificarea atacurilor ISIL în Irak/Siria împotriva Regatului Unit”);
- (e) crearea unei noi forme de mandat de interceptare în masă limitat la obținerea de date de comunicații, care ar putea fi o opțiune proporțională în anumite cazuri;
- (f) ISIC trebuie să preia funcții de supraveghere a serviciilor de informații și trebuie să fie îndreptată spre public, transparentă și accesibilă mass-mediei;
- (g) IPT trebuie să aibă capacitatea de a pronunța declarații de incompatibilitate, iar hotărârile sale trebuie să poată face obiectul unor căi de atac limitate la probleme de drept.

4. „*Un permis pentru a interveni în mod democratic*” (*A Democratic Licence to Operate*): raportul evaluării independente a activităților de supraveghere (*Independent Surveillance Review* – „ISR”)

156. Evaluarea ISR a fost realizată de *Royal United Services Institute*, un grup de reflecție independent, la cererea viceprim-ministrului de atunci, parțial ca răspuns la dezvăluirile lui Edward Snowden. Mandatul institutului era acela de a examina legalitatea programelor de supraveghere ale Regatului Unit și eficacitatea regimurilor care le reglementau, precum și de a sugera reformele care ar putea fi necesare pentru a proteja atât viața privată individuală, cât și capacitățile necesare ale poliției și ale serviciilor de securitate și de informații.

157. După finalizarea evaluării, ISR nu a descoperit nicio dovadă că guvernul britanic a acționat ilegal cu bună știință în interceptarea comunicațiilor private sau că Guvernul a utilizat capacitatea de a colecta date în masă pentru a dispune de o fereastră permanent deschisă în ceea ce privește viața privată a resortisanților britanici. Pe de altă parte, a descoperit dovezi că actualul cadru juridic care autoriza interceptarea comunicațiilor era neclar, nu

a ținut pasul cu evoluțiile din domeniul tehnologiei comunicațiilor și nu era de folos nici Guvernului, nici publicului într-un mod satisfăcător. Prin urmare, a concluzionat că era necesar un cadru juridic nou, cuprinzător și mai clar.

158. În special, a sprijinit opinia exprimată atât în raportul ISC, cât și în Raportul Anderson potrivit căreia, deși actualele competențe de supraveghere erau necesare, se impuneau atât un nou cadru legislativ, cât și un nou regim de supraveghere. De asemenea, a considerat că definițiile termenilor „conținut” și „date de comunicații” trebuie revizuite în cadrul elaborării noii legislații astfel încât acestea să poată fi clar definite prin lege.

159. În ceea ce privește datele de comunicații, raportul observa că despre o persoană erau disponibile volume mai mari față de conținut, întrucât fiecare element de conținut era acompaniat de mai multe date de comunicații. În plus, agregarea seturilor de date putea crea o imagine extrem de precisă a vieții unei persoane, întrucât, existând suficiente date brute, algoritmii și calculatoarele puternice puteau genera o imagine substanțială a persoanei și a modelelor sale de comportament fără a accede vreodată la conținut. În plus, utilizarea unor metode de criptare din ce în ce mai sofisticate făcea ca accesul la conținut să fie din ce în ce mai dificil.

160. Raportul considera, de asemenea, că trebuie menținută capacitatea serviciilor de securitate și de informații de a colecta și analiza materialele interceptate în masă, dar cu garanțiile mai solide recomandate în raportul Anderson. În special, raportul admitea că mandatele de interceptare în masă ar trebui să includă mult mai multe detalii și ar trebui să facă obiectul unui proces de autorizare judiciară, cu excepția cazurilor în care există o cerință urgentă.

161. În plus, experții erau de acord atât cu opiniile ISC, cât și ale Raportului Anderson potrivit cărora era necesar să existe diferite tipuri de mandat pentru interceptarea și obținerea comunicațiilor și a datelor aferente. Se propunea ca mandatele pentru un scop legat de depistarea sau prevenirea infracționalității grave și organizate să fie întotdeauna autorizate de un comisar judiciar, în timp ce mandatele în scopuri legate de securitatea națională să fie autorizate de ministru, sub rezerva controlului jurisdicțional efectuat de un comisar judiciar.

162. În ceea ce privește IPT, ISR recomanda organizarea de audieri publice cu ușile deschise, cu excepția cazului în care audierile private sau cu ușile închise erau necesare în interesul justiției sau al altor interese publice identificabile. În plus, IPT ar trebui să aibă capacitatea de a verifica probele cu caracter secret care îi erau prezentate, eventual prin numirea unui consilier special. În cele din urmă, ISR subscria la opiniile Raportului ISC și ale Raportului Anderson, potrivit cărora dreptul la o cale de atac internă era important și că trebuia luat în considerare în legislația care urma să fie introdusă.

5. *Raport privind controlul competențelor de supraveghere în masă*

163. Raportul privind controlul competențelor de supraveghere în masă a fost realizat în mai 2016 pentru a evalua cadrul operațional al celor patru competențe de supraveghere în masă conținute în ceea ce a devenit apoi proiectul de lege privind competențele de investigare (în prezent, Legea din 2016 privind competențele de investigare din 2016: infra, pct. 183-190). Aceste competențe se refereau la interceptarea în masă și la obținerea de date de comunicații în masă, ingerința în masă asupra sistemelor de comunicații și obținerea de seturi de date cu caracter personal în masă.

164. Controlul a fost efectuat din nou de evaluatorul independent al legislației privind terorismul. Pentru a efectua controlul, aceasta a recrutat o echipă formată din trei membri, toți având autorizația de securitate necesară pentru a accesa materiale cu caracter secret extrem de ridicat, inclusiv o persoană cu cunoștințele tehnice necesare pentru a înțelege sistemele și tehnicile utilizate de GCHQ, precum și utilizările pe care acestea le puteau avea, un anchetator cu experiență în utilizarea informațiilor secrete, inclusiv a informațiilor generate de GCHQ, și un înalt consilier independent cu abilitățile și experiența de a verifica din punct de vedere medico-legal probele și studiile de caz prezentate de serviciile de securitate și cele de informații.

165. Pentru a efectua controlul, echipa a avut contacte semnificative și detaliate cu serviciile de informații de la toate nivelurile ierarhice, precum și cu organele de supraveghere relevante (inclusiv IPT și avocatul de pe lângă Tribunal), cu ONG-uri și cu experți tehnici independenți.

166. Deși controlul privea Legea privind competențele de investigare, o serie de constatări în ceea ce privește interceptarea în masă au fost relevante pentru cauza de față. În special, după examinarea unui mare număr de materiale cu caracter confidențial, analiza a concluzionat că interceptarea în masă constituie o capacitate esențială: în primul rând, întrucât teroristii, infractorii, serviciile de informații străine și ostile s-au sofisticat în a evita depistarea prin mijloace tradiționale și, în al doilea rând, întrucât natura Internetului global făcea ca ruta luată de o comunicație specială să fi devenit extrem de imprevizibilă. Echipa de control a analizat alternative la interceptarea în masă (inclusiv interceptarea țintită, utilizarea surselor umane și a produselor comerciale de apărare cibernetică), dar a concluzionat că nicio alternativă sau combinație de alternative nu era suficientă pentru a înlocui competența de interceptare în masă ca metodă de obținere a informațiilor necesare.

6. *Atentatele în Londra și Manchester din martie-iunie 2017: evaluarea independentă a MI5 și controalele interne ale poliției*

167. În urma unei serii de patru atacuri teroriste comise într-un interval scurt de timp în perioada martie – iunie 2017, în cursul cărora aproximativ treizeci și șase de persoane nevinovate au fost ucise și alte aproape 200 au

fost rănite, ministrul internelor a solicitat evaluatorului independent al legislației privind terorismul, David Anderson Q.C., care se pensionase recent, să verifice controalele interne cu caracter clasificat ale poliției și ale serviciilor de informații implicate. Plasând atacurile în context, raportul a inclus următoarele observații:

„1.4. În primul rând, **nivelul de amenințare** din Regatul Unit generat de așa-numitul «terorism internațional» (în practică, terorismul islamist, indiferent dacă este generat în țară sau în străinătate) a fost evaluat de către Centrul Comun de Analiză a Terorismului (*Joint Terrorism Analysis Centre* – JTAC) ca fiind SEVER încă din august 2014, indicând faptul că atacurile teroriste islamiste în Regatul Unit sunt «foarte probabile». Comentatorii care au avut acces la informațiile relevante au afirmat întotdeauna cu claritate că această evaluare este realistă. Au subliniat, de asemenea, amenințarea mai mică, dar încă mortală, reprezentată de terorismul de extremă dreapta (XRW), exemplificat de asasinarea deputatului Jo Cox în iunie 2016 și de interzicerea grupului neo-nazist *National Action*, în decembrie 2016.

1.5. În al doilea rând, **amplizarea tot mai crescută** a amenințării reprezentate de terorismul islamist este frapantă. Directorul general al MI5, Andrew Parker, a vorbit, în octombrie 2017, despre «o schimbare dramatică a amenințării în acest an» la «cel mai înalt punct pe care l-am văzut în cariera mea de 34 de ani». Deși decesele cauzate de terorismul islamist au loc într-o proporție covârșitoare în Africa, Orientul Mijlociu și Asia de Sud, amenințarea a crescut recent în lumea occidentală și a fost descrisă ca fiind «deosebit de difuză și diversă în Regatul Unit». Rămâne de văzut modul în care această tendință va fi afectată, de bine sau de rău, de prăbușirea fizică a așa-numitului Stat Islamic în Siria și Irak.

1.6. În al treilea rând, profilurile **atacatorilor** [...] prezintă numeroase caracteristici cunoscute. [...]

1.7. În al patrulea rând, deși **țintele** primelor trei atacuri nu s-au extins la întreaga gamă actuală, au avut similități puternice cu obiectivele altor atacuri recente din Occident: centre politice (de exemplu, Oslo 2011, Ottawa 2014, Bruxelles 2016), concerte, adunări festive și mulțimi (de exemplu, Orlando 2016, Paris 2016, Barcelona 2017) și ofițeri de poliție (de exemplu, Melbourne 2014, Berlin 2015, Charleroi 2016). Există precedente și pentru atacurile asupra musulmanilor practicanți care au trecut granița de la infracțiuni motivate de ură la terorism, inclusiv uciderea lui Mohammed Saleem în West Midlands în 2013.

1.8. În al cincilea rând, **modus operandi** (MO) al atacurilor teroriste s-a diversificat și s-a simplificat de-a lungul anilor, Daesh depunând eforturi extraordinare de propagandă pentru a inspira mai degrabă decât pentru a dirija acte de terorism în Vest. Atacurile analizate au fost tipice ca stil pentru momentul și locul lor:

a) Spre deosebire de comploturile islamiste la scară largă, țintite, caracteristice ultimului deceniu, toate cele patru atacuri au fost comise de **persoane care au acționat singure** sau de **grupuri mici**, cu puține probe privind o planificare detaliată sau o țintă precisă.

b) Controlul strict al armelor de foc în Regatul Unit face ca **armele albe** să fie utilizate mai frecvent decât armele de foc în infracțiunile comise în bandă și cele de terorism.

c) De la momentul în care un camion a ucis 86 de persoane nevinovate în Nisa (iulie 2016), **vehiculele** – care figurau în trei dintre cele patru atacuri care sunt analizate – au fost utilizate din ce în ce mai mult ca arme.

d) **Combinația** dintre un vehicul și armele albe, folosită la Westminster și la London Bridge, fusese utilizată anterior pentru a-l ucide pe soldatul Lee Rigby (Woolwich, 2013).

e) **Explozivii**, utilizați în Manchester, au reprezentat cea mai populară armă pentru teroriștii islamiști care au ținut Europa între 2014 și 2017. Explozivul TATP s-a dovedit a fi capabil de produs (cu ajutorul achizițiilor on-line și al instrucțiuni de realizare) mai ușor decât se credea anterior.”

7. *Raportul anual al Comisarului pentru Interceptarea Comunicațiilor din 2016*

168. Comisarul IC a observat că, atunci când efectua o interceptare pe baza unui mandat emis în temeiul art. 8 alin. (4), agenția de interceptare trebuia să își utilizeze cunoștințele cu privire la modul în care erau direcționate comunicațiile internaționale, coroborat cu verificări periodice ale legăturilor de comunicații relevante, pentru a identifica canale de transmisie de comunicații cele mai susceptibile să conțină comunicații externe care să corespundă descrierii materialelor conținute în certificatul emis de ministrul internelor în temeiul art. 8 alin. (4). De asemenea, agenția trebuia să efectueze interceptarea într-un mod care să limiteze colectarea de comunicații externe la un nivel minim compatibil cu obiectivul interceptării comunicațiilor externe dorite.

169. În plus, a observat că, înainte ca analiștii să poată citi, examina sau asculta materiale, aveau obligația să prezinte o justificare care să includă motivele pentru care accesul la materiale era necesar, în temeiul art. 16 și al certificatului aplicabil, și motivul pentru care un astfel de acces era proporțional. Inspecțiile și auditurile au arătat că, deși procedura de selecție era efectuată cu atenție și cu conștiinciozitate, se baza pe judecata profesională a analiștilor, pe formarea acestora și pe supravegherea superiorilor.

170. Potrivit raportului, au fost emise 3007 mandate de interceptare în 2016 și 5 cereri au fost respinse de un ministru. În opinia Comisarului IC, aceste cifre nu surprindeau funcția critică de asigurare a calității desfășurată inițial de personal și de avocații din cadrul agenției de interceptare sau al departamentului care emitea mandatele [departamentele care emiteau mandatele reprezentau o sursă de consiliere independentă pentru ministru și efectuau un control prealabil al autorizării cererilor de emitere de mandat și al reînnoirilor, pentru a se asigura că acestea erau (și rămâneau) necesare și proporționale]. Pe baza inspecțiilor, evaluatorul a considerat că numărul redus de respingeri reflecta atenția acordată utilizării acestor competențe.

171. Inspecția tipică a unei agenții de interceptare includea următoarele:

- o examinare a punctelor de acțiune sau a recomandărilor din cadrul inspecției anterioare și a punerii în aplicare a acestora;

- o evaluare a sistemelor aplicate pentru interceptarea comunicațiilor pentru a se asigura că sunt suficiente în sensul Capitolului 1 al Părții 1 din RIPA și că toate înregistrările relevante au fost păstrate;
- examinarea cererilor de interceptare selectate pentru a evalua dacă erau necesare în primă instanță și dacă cererile îndeplineau cerințele privind necesitatea și proporționalitatea;
- discuții cu responsabili de caz, analiști și/sau lingviști din cadrul investigațiilor sau operațiunilor selectate pentru a evalua dacă interceptarea și justificările pentru obținerea tuturor materialelor au fost proporționale;
- examinarea oricăror aprobări verbale urgente pentru a verifica dacă procesul a fost justificat și utilizat în mod corespunzător;
- examinarea cazurilor în care comunicările care făceau obiectul privilegiului juridic sau al informațiilor confidentiale au fost interceptate și păstrate, precum și a cazurilor în care un avocat a făcut obiectul unei anchete;
- examinarea caracterului adecvat al garanțiilor și al mecanismelor prevăzute la art. 15 și 16 din RIPA;
- investigarea procedurilor în vigoare pentru păstrarea, stocarea și distrugerea materialelor interceptate și a datelor de comunicații aferente;
- examinarea erorilor raportate, inclusiv verificarea faptului că măsurile instituite pentru a preveni repetarea sunt suficiente.

172. După fiecare inspecție, inspectorii întocmesc un raport care include:

- o evaluare a măsurii în care recomandările formulate în urma inspecției anterioare au fost îndeplinite;
- un rezumat al numărului și tipului documentelor interceptate selectate pentru inspecție, inclusiv o listă detaliată a acestor mandate;
- observații detaliate cu privire la toate mandatele selectate pentru examinare și discuțiile purtate în timpul inspecției;
- o evaluare a erorilor raportate Biroului Comisarului CI în timpul perioadei de inspecție;
- o prezentare a examinării procedurilor de păstrare, depozitare și distrugere a materialelor;
- o prezentare a altor aspecte operaționale sau legate de politici pe care agenția sau departamentele care emiteau mandatele le-au semnalat în timpul inspecției;
- o evaluare a modului în care au fost tratate toate materialele care făceau obiectul secretului profesional al avocaților (sau al altor materiale confidențiale); și
- o serie de recomandări care vizează îmbunătățirea conformității și a performanței.

173. În cursul anului 2016, Biroul Comisarului IC a inspectat de două ori toate cele nouă agenții de interceptare și cele patru departamente principale care emit mandatele. Alături de vizitele suplimentare la GCHQ, au fost efectuate în total douăzeci și două de vizite de inspecție. În plus, Comisarul și inspectorii săi au organizat și alte vizite *ad-hoc* la agenții.

174. Inspecția sistemelor existente pentru solicitarea și autorizarea mandatelor de interceptare implică, de regulă, un proces în trei etape. În primul rând, pentru a obține un eșantion reprezentativ de mandate, inspectorii le selectează pentru diferite tipuri de infracțiuni și amenințări la adresa securității naționale. În plus, inspectorii se concentrează asupra celor care prezintă un interes sau grad de sensibilitate deosebit (cum ar fi cele care generează un grad neobișnuit de intruziune colaterală, cele care au fost extinse pentru o perioadă considerabilă, cele aprobate oral, cele care au condus la interceptarea de comunicații protejate de secretul profesional al avocaților sau de altă natură confidențială și așa-numitele mandate „tematice”). În al doilea rând, inspectorii verifică în detaliu mandatele selectate și documentația aferentă în timpul zilelor de lectură care precedă inspecțiile. În această etapă, inspectorii sunt în măsură să examineze declarațiile de necesitate și proporționalitate formulate de analiști atunci când adaugă un selector la sistemul de colectare în vederea examinării. Fiecare declarație trebuia să fie de sine stătătoare și să răspundă cerinței generale privind prioritățile pentru colectarea de informații. În al treilea rând, identifică acele garanții, operațiuni sau zone ale procesului care necesită informații sau clarificări suplimentare și organizează discuții cu personalul operațional,

juridic sau tehnic relevant. În cazul în care e necesar, examinează și alte documente sau sisteme privind respectivele mandate.

175. În cursul celor 22 de inspecții realizate în 2016, au fost examinate 970 de mandate (61% din numărul de mandate în vigoare la sfârșitul anului și 32% din totalul noilor mandate emise în 2016).

176. Perioada de păstrare a datelor nu este prevăzută de lege, însă agențiile trebuie să ia în considerare art. 15 alin. (3) din RIPA, care prevede că materialele sau datele să fie distruse de îndată ce păstrarea lor nu mai este necesară pentru niciunul dintre scopurile autorizate prevăzute la art. 15 alin. (4). Potrivit raportului, fiecare agenție de interceptare are o opinie diferită cu privire la ceea ce constituie perioada adecvată de păstrare a materialelor interceptate și a datelor de comunicații aferente. Prin urmare, perioada de păstrare este diferită în cadrul agențiilor de interceptare; pentru conținut, variază între 30 de zile și un an, iar pentru datele de comunicații aferente variază între 6 luni și un an. Cu toate acestea, în practică, marea majoritate a conținutului este reexaminată și eliminată automat după o perioadă foarte scurtă de timp, cu excepția cazului în care sunt luate măsuri specifice pentru a păstra conținutul pentru o perioadă mai lungă întrucât acest lucru e necesar.

177. Comisarul CI a menționat în mod expres că „a fost impresionat de calitatea” declarațiilor de necesitate și proporționalitate făcute de analiști atunci când adaugă un selector la sistemul de colectare pentru examinare.

178. Inspectorii au formulat în total 28 de recomandări în rapoartele lor de inspecție, 18 dintre acestea fiind formulate în legătură cu procesul de depunere a cererilor. Majoritatea recomandărilor din această categorie se refereau la justificările privind necesitatea, proporționalitatea și/sau intruziunea colaterală din cereri, sau la tratarea materialelor care făceau obiectul secretului profesional al avocaților sau de altă natură confidențială, referitoare la profesii cu caracter sensibil.

179. Numărul total de erori de interceptare raportate Comisarului CI în cursul anului 2016 a fost de 108. Principalele cauze ale erorilor de interceptare au fost colectarea excesivă (în general, erori tehnice de software sau hardware care au cauzat colectarea excesivă a materialelor interceptate și a datelor de comunicații aferente), selectarea/examinarea neautorizată, diseminarea incorectă, neanularea interceptării și interceptarea fie a unei adrese de comunicații incorecte, fie a unei persoane greșite.

180. În cele din urmă, în ceea ce privește schimbul de informații, Comisarul CI observa că:

„GCHQ a furnizat detalii cuprinzătoare cu privire la acordurile de schimb de informații prin care partenerii rețelei Five Eyes puteau accesa elemente ale produsului mandatelor de interceptare ale GCHQ în propriile sisteme. Inspectorii noștri s-au întâlnit, de asemenea, cu reprezentanți ai comunității Five Eyes și au asistat la o demonstrație despre modul în care alți membri ai Five Eyes pot solicita acces la datele GCHQ. Accesul la sistemele GCHQ este strict controlat și trebuie justificat în conformitate cu legislația țării-gazdă și cu instrucțiunile de tratare a datelor enunțate la

garanțiile prevăzute de art. 15/16. Înainte de a obține acces la datele GCHQ, analiștii Five Eyes trebuie să urmeze aceleași cursuri de formare juridică precum personalul GCHQ.”

8. Raportul anual pe 2016 al Comisarului pentru Serviciile de Informații

181. Comisarul pentru Serviciile de Informații, în raportul său privind modul în care sunt respectate „Orientările consolidate pentru agenții serviciilor de informații și personalul militar privind detenția și interogarea deținuților în străinătate, precum și privind transmiterea și primirea informațiilor referitoare la deținuți” (*Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees*), a observat că

„În cursul activității, fiecare agenție colaborează îndeaproape cu parteneri de legătură străini. Aceasta implică schimbul de informații ca rutină și uneori operațiuni în colaborare. Avem convingerea că agențiile sunt atente la implicațiile colaborării cu parteneri care acționează în cadrul unor sisteme juridice diferite și observăm că [comunitatea serviciilor de informații din Regatul Unit] care își desfășoară activitatea în străinătate face toate eforturile să aplice pe cât posibil principiile dreptului Regatului Unit.

[...]

GCHQ colaborează îndeaproape cu partenerii de legătură și este implicată în schimbul periodic de informații și, uneori, în activități în colaborare. Acesta este un domeniu complex atât pentru GCHQ, cât și pentru SIS, personalul agenției lucrând cu parteneri care aplică cadre juridice diferite și uneori incompatibile. Am fost impresionați de eforturile personalului GCHQ de a obține asigurări din partea partenerilor, în special în ceea ce privește orientările consolidate. Am recomandat GCHQ să ia în considerare posibilitatea de a face trimitere, în observațiile relevante, la faptul că legislația locală va afecta activitatea partenerului.

Suntem convinși că GCHQ aplică cu atenție principiile orientărilor consolidate și ne bucurăm că modificările aduse pentru a forma personalul 24/7 sporesc nivelul deja ridicat al procesului de sesizare. Am luat act de faptul că, ocazional, ofițerii GCHQ actualizează jurnalul consolidat al orientărilor după ce au clarificat hotărârile sau detaliile. Deși este important să se înregistreze toate datele disponibile, am recomandat ca GCHQ să prezinte clarificări suplimentare față de înregistrările inițiale, nu modificările aduse acestora. GCHQ a confirmat ulterior că acest lucru a fost pus în aplicare.

[...]

Ministrul afacerilor externe este, de asemenea, responsabil de asigurarea supravegherii ministeriale în cazurile în care sunt implicate orientările consolidate și agențiile intenționează să acționeze, fie prin schimb de informații, fie printr-o intervenție directă. Am recomandat ca [Ministerul Afacerilor Externe și Commonwealth-ului] să obțină o copie a tuturor asigurărilor pe care SIS le-a obținut de la un partener de legătură. Recomandăm ca aceste copii să fie puse la dispoziția ministrului afacerilor externe pentru a le examina luând în considerare orice observații consolidate legate de orientări.”

182. Controlul respectării Orientărilor consolidate intră acum în sfera de competență a noului Comisar pentru Competențe de Investigare. Orientările sunt în prezent în curs de revizuire, întrucât Comisarul pentru Servicii de Informații a indicat, în raportul său din 2015, că, deși „nu a considerat că orientările consolidate erau în mod fundamental imperfecte sau inadecvate scopului”, acesta și-a exprimat totuși opinia că acestea erau „în forma actuală de câțiva ani și că se puteau aduce îmbunătățiri”.

G. Legea privind competențele de investigare din 2016

183. Legea privind competențele de investigare din 2016 a primit avizul regal la 29 noiembrie 2016. Noul regim pe care l-a introdus este în mare măsură operațional, majoritatea competențelor prevăzute de lege intrând în vigoare în cursul anului 2018.

184. Conform dispozițiilor legii din 2016, un mandat de interceptare în masă – care poate acoperi atât „conținutul” comunicațiilor, cât și „datele secundare” – trebuie să fie necesar cel puțin în interesul securității naționale (dar poate fi, de asemenea, în scopul prevenirii sau al depistării infracțiunilor grave sau în interesul bunăstării economice a Regatului Unit, în măsura în care aceste interese sunt relevante și pentru securitatea națională). Mandatul trebuie să specifice „scopurile operaționale” pentru care poate fi selectat pentru examinare orice material obținut în temeiul respectivului mandat. Există dispoziții detaliate privind întocmirea listei de „scopuri operaționale” de către șefii serviciilor de informații. Un scop operațional poate fi specificat în lista respectivă numai cu aprobarea ministrului. Lista scopurilor operaționale trebuie furnizată ISC o dată la 3 luni și trebuie revizuită de prim-ministru cel puțin o dată pe an.

185. Cererea pentru emiterea unui mandat colectiv trebuie să fie formulată de șeful unui serviciu de informații sau în numele acestuia. Competența de a emite un mandat trebuie să fie exercitată personal de ministru și pentru a decide dacă emite un mandat colectiv, acesta trebuie să aplice principiile necesității și proporționalității. Emiterea mandatului face obiectul unei aprobări prealabile din partea unui comisar judiciar, care trebuie să aplice principiile controlului jurisdicțional (așa-numitul „sistem cu protecție dublă”. Prin urmare, comisarul judiciar trebuie să examineze aspecte cum ar fi dacă o ingerință este justificată ca fiind proporțională în temeiul art. 8 § 2 din Convenție.

186. Mandatul este valabil 6 luni, cu excepția cazului în care a fost deja anulat sau reînnoit. Reînnoirea este condiționată de aprobarea de către un comisar judiciar.

187. „Scopul principal” al mandatului trebuie să fie obținerea de „comunicații legate de teritoriile din străinătate, și anume comunicații trimise sau primite de persoane fizice în afara Insulelor Britanice. Selecția pentru examinarea conținutului interceptat sau a „materialelor protejate” face

obiectul „garanției aplicabile Insulelor Britanice”, ceea ce înseamnă că materialele nu pot fi selectate în niciun moment pentru examinare în cazul în care criteriile utilizate pentru selectarea conținutului interceptat pentru examinare au legătură cu o persoană despre care se știe că se află în Insulele Britanice la acel moment, iar scopul utilizării criteriilor respective este de a identifica conținutul comunicațiilor trimise de persoana respectivă sau destinate acesteia.

188. Legea din 2016 a instituit, de asemenea, dreptul la o cale de atac împotriva IPT și a înlocuit Comisarul pentru Interceptarea Comunicațiilor cu un nou Comisar pentru Competențe de Investigare (supra, pct. 138).

189. O serie de noi coduri de bune practici, inclusiv un nou Cod de bune practici privind interceptarea comunicațiilor au intrat în vigoare la 8 martie 2018 (supra, pct. 102).

190. Partea 4 din Legea din 2016, care a intrat în vigoare la 30 decembrie 2016, include competența de a emite un „act de păstrare” operatorilor de telecomunicații, impunându-le păstrarea datelor. În urma acțiunii în justiție formulate de Liberty, Guvernul a admis că Partea a 4-a din Legea din 2016 era, în forma sa existentă, incompatibilă cu cerințele dreptului Uniunii. Partea a 4-a nu a fost modificată și, la 27 aprilie 2018, *High Court* a constatat că Partea a 4-a era incompatibilă cu drepturile fundamentale din dreptul Uniunii, întrucât, în domeniul justiției penale, accesul la datele păstrate nu era limitat la scopul combaterii „infrafracțiunilor grave”, iar accesul la datele păstrate nu a făcut obiectul unei examinări prealabile din partea unei instanțe sau a unui organ administrativ independent.

II. DREPTUL INTERNAȚIONAL RELEVANT

A. Organizația Națiunilor Unite

191. Rezoluția nr. 68/167, adoptată de Adunarea Generală la 18 decembrie 2013, are următorul conținut:

„Adunarea Generală,

[...]

4. *Solicită* tuturor statelor:

[...]

c) Să își revizuiască procedurile, practicile și legislația referitoare la supravegherea și interceptarea comunicațiilor și colectarea de date cu caracter personal, în special cele în masă, interceptarea și colectarea, în vederea protejării dreptului la viață privată, asigurând respectarea deplină a tuturor obligațiilor care le revin în temeiul dreptului internațional al drepturilor omului;

d) Să instituie mecanisme naționale de control independente și eficiente care să poată asigura transparența supravegherii și interceptării comunicațiilor și a colectării de date cu caracter personal pe care le efectuează, după caz, și să asigure răspunderea statului pentru acestea sau să mențină mecanismele deja existente [...].”

B. Consiliul Europei

1. Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, 1981

192. Convenția, care a intrat în vigoare în ceea ce privește Regatul Unit la 1 decembrie 1987, stabilește normele de protecție a datelor în domeniul prelucrării automatizate a datelor cu caracter personal în sectoarele public și privat. În măsura relevanței, prevede:

Preambul

„Statele membre ale Consiliului Europei, semnatare ale prezentei convenții,

considerând că scopul Consiliului Europei este de a realiza o uniune mai strânsă între membrii săi, cu respectarea în special a supremației dreptului și a drepturilor omului și a libertăților fundamentale,

apreciind că este de dorit să se extindă protecția drepturilor și libertăților fundamentale pentru fiecare, în special dreptul la respectarea vieții private, față de intensificarea circulației peste frontiere a datelor cu caracter personal care fac obiectul prelucrării automatizate,

reafirmând în același timp angajamentul lor în favoarea libertății de informare, fără a ține seama de frontiere,

recunoscând necesitatea concilierii valorilor fundamentale de respectare a vieții particulare și de liberă circulație a informațiilor între popoare,

au convenit asupra celor ce urmează:”

Articolul 1 – Obiect și scop

„Scopul prezentei convenții este de a garanta pe teritoriul fiecărui stat parte, fiecărei persoane fizice, oricare ar fi cetățenia sa sau reședința sa, respectarea drepturilor și libertăților sale fundamentale și, în special, dreptul la viața privată, față de prelucrarea automatizată a datelor cu caracter personal care îl privesc (protecția datelor).

[...]”

Articolul 8 – Garanții complementare pentru persoana în cauză

„Orice persoană trebuie:

a. să aibă cunoștința de existența unui fișier automatizat de date cu caracter personal, de scopurile sale principale, precum și de identitatea și de locul de reședință obișnuit sau de sediul principal de care aparține proprietarul fișierului;

b. să obțină la intervale rezonabile și fără întârziere sau cu cheltuieli excesive confirmarea existenței sau inexistenței în fișierul automatizat de date cu caracter personal care o privesc, precum și comunicarea acestor date sub o formă inteligibilă;

c. să obțină, dacă este cazul, modificarea acestor date sau ștergerea lor, dacă acestea au fost prelucrate fără a se respecta dispozițiile din dreptul intern care aplică principiile de bază enunțate la art. 5 și 6;

d. să dispună de o cale de atac, dacă nu s-a dat curs la o cerere de confirmare, sau, dacă este cazul, de comunicare, de modificare ori de ștergere, prevăzute la lit. b) și c).”

Articolul 9 – Excepții și restricții

„1. Nici o excepție la dispozițiile cuprinse la art. 5, 6 și 8 nu este admisă decât în limitele definite în prezentul articol.

2. Este posibilă derogarea de la dispozițiile prevăzute la art. 5, 6 și 8 când o astfel de derogare, prevăzută prin legea părții, constituie o măsură necesară într-o societate democratică pentru:

a. protejarea securității statului, siguranței publice, intereselor monetare ale statului sau reprimarea infracțiunilor penale;

b. a proteja persoanele în cauză sau drepturile și libertățile celorlalți.

[...]”

Articolul 10 – Sancțiuni și căi de atac

„Fiecare parte se angajează să stabilească sancțiuni și căi de atac adecvate în cazul violării dispozițiilor de drept intern care dau efect principiilor de bază pentru protecția datelor, enunțate în prezentul capitol.”

193. Raportul explicativ la convenția menționată expune următoarele:

Articolul 9 – Excepții și restricții

„55. Excepțiile de la principiile de bază privind protecția datelor se limitează la cele necesare pentru protecția valorilor fundamentale într-o societate democratică. Textul paragrafului 2 al acestui articol a fost inspirat din cel al paragrafelor 2 ale art. 6, 8, 10 și 11 din Convenția europeană a drepturilor omului. Din deciziile Comisiei și ale Curții Europene a Drepturilor Omului referitoare la noțiunea «măsuri necesare», rezultă că pentru acest concept criteriile nu pot fi stabilite pentru toate țările și în orice moment, ci trebuie să fie luate în considerare în funcție de situația dată din fiecare țară.

56. Lit. a) a paragrafului 2 enumeră interesele majore ale statului care pot impune excepții. Aceste excepții sunt foarte specifice pentru a se evita ca, în ceea ce privește aplicarea generală a convenției, statele să dispună de o marjă de manevră nejustificat de largă.

Statele își rezervă, în temeiul art. 16, posibilitatea de a refuza aplicarea convenției în cazuri individuale, din motive importante, printre care se numără cele enumerate la art. 9.

Noțiunea de «securitate a statului» trebuie înțeleasă în sensul tradițional al protejării suveranității naționale împotriva amenințărilor interne sau externe, inclusiv protecția relațiilor internaționale ale statului.”

2. *Protocolul adițional 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 de date, adoptat la 18 noiembrie 2001 (CETS nr. 181)*

194. Protocolul, care nu a fost ratificat de Regatul Unit, prevede, în măsura în care este relevant:

Articolul 1 – Autoritățile de control

„1. Fiecare parte contractantă va conferi uneia sau mai multor autorități responsabilitatea pentru asigurarea conformității cu măsurile prevăzute prin legislația

sa internă, care pun în vigoare principiile stabilite în cap. II și III al Convenției, precum și în acest protocol.

2.

a. În acest scop autoritățile mai sus menționate vor avea, în special, dreptul de a investiga și de a interveni, precum și dreptul de a se angaja în procedurile legale sau de a aduce în atenția autorităților juridice competente încălcarea prevederilor din legislația internă care pun în aplicare principiile menționate la paragraful 1 al art. 1 din acest protocol.

b. Fiecare autoritate de control va da curs reclamațiilor depuse de orice persoană în legătură cu protecția drepturilor și libertăților sale fundamentale, cu privire la procesarea datelor personale care sunt în competența acesteia.

3. Autoritățile de control își vor exercita atribuțiile în completă independență.

4. Deciziile autorităților de control, care fac obiectul unei plângeri, pot fi atacate în fața unui tribunal.

[...]”

Articolul 2 – Fluxurile transfrontaliere de date personale trimise către un receptor care nu constituie subiect al jurisdicției unei părți a Convenției

„1. Fiecare parte va asigura transferul datelor personale către un receptor care se află sub jurisdicția Statului sau a organizației care nu este parte la Convenție, numai dacă acel stat sau organizație asigură un nivel adecvat de protecție pentru acel transfer de date.

2. Prin derogare de la paragraful 1 al art. 2 din acest protocol, fiecare parte va permite transferul datelor personale:

a. dacă legislația internă prevede acest lucru, datorită:

– intereselor specifice ale subiectului datelor; sau

– intereselor justificate care prevalează, în special intereselor publice importante; sau

b. dacă măsuri de protecție care pot rezulta, în special, din clauze contractuale sunt asigurate de către autoritatea de control responsabilă pentru transferul datelor și sunt considerate adecvate de către autoritățile competente, în conformitate cu legislația internă.”

3. *Recomandarea Comitetului de Miniștri privind protecția datelor cu caracter personal în domeniul serviciilor de telecomunicații*

195. Recomandarea [nr. R (95) 4 a Comitetului de Miniștri], adoptată la 7 februarie 1995, prevede, în măsura în care este relevant, următoarele:

„2.4. Ingerința autorităților publice în conținutul unei comunicații, inclusiv utilizarea unor dispozitive de ascultare sau captare sau a altor mijloace de supraveghere sau interceptare a comunicațiilor, trebuie să se producă numai atunci când acest lucru este prevăzut de lege și constituie o măsură necesară într-o societate democratică pentru:

a. protejarea securității statului, siguranței publice, intereselor monetare ale statului sau reprimarea infracțiunilor penale;

b. a proteja persoanele în cauză sau drepturile și libertățile celorlalți.

2.5. În cazul ingerinței autorităților publice în conținutul unei comunicații, dreptul intern trebuie să reglementeze:

- a. exercitarea drepturilor de acces și de rectificare ale persoanei vizate;
- b. care sunt circumstanțele în care autoritățile publice responsabile au dreptul de a refuza să furnizeze informații persoanei în cauză sau de a întârzia furnizarea acestora;
- c. stocarea sau distrugerea unor astfel de date.

În cazul în care un operator de rețea sau un furnizor de servicii este instruit de o autoritate publică să efectueze o ingerință, datele astfel colectate nu trebuie comunicate decât organului desemnat în autorizație pentru acea ingerință.”

4. *Raportul din 2015 al Comisiei Europene pentru Democrație prin Drept („Comisia de la Veneția”) privind controlul democratic al serviciilor care culeg informații de origine electromagnetică*

196. Comisia de la Veneția a observat, încă de la început, valoarea pe care o poate avea interceptarea în masă pentru operațiunile de securitate, întrucât permite serviciilor de securitate să adopte o abordare proactivă, căutând pericole necunoscute până acum, în loc să le investigheze pe cele cunoscute. Cu toate acestea, a remarcat, de asemenea, că interceptarea datelor în masă în cursul transmisiei sau solicitarea ca societățile de telecomunicații să stocheze și apoi să furnizeze date sau metadate de telecomunicații agențiilor de aplicare a legii sau de securitate implică o ingerință în viața privată și în alte drepturi ale omului pentru o mare parte a populației lumii. În această privință, Comisia de la Veneția a considerat că principala ingerință în viața privată se produce atunci când datele cu caracter personal stocate sunt accesate și/sau prelucrate de agenții. Din acest motiv, analiza computerizată (de regulă cu ajutorul selectorilor) reprezintă una dintre etapele importante pentru păstrarea unui echilibru între preocupările legate de integritatea personală și celelalte interese.

197. Potrivit raportului, cele mai importante două garanții sunt autorizarea (colectării și accesului) și supravegherea procesului. Din jurisprudența Curții rezultă în mod clar că aceasta din urmă trebuia să fie efectuată de un organ extern independent. Deși Curtea preferă autorizarea judiciară, nu consideră că este o cerință necesară. Mai degrabă sistemul trebuie să fie evaluat în ansamblu și, în cazul în care în etapa de autorizare lipsesc controalele independente, este necesar să existe garanții deosebit de solide în etapa de supraveghere. În această privință, Comisia de la Veneția a examinat exemplul sistemului din Statele Unite ale Americii, unde autorizația era acordată de FISC. Cu toate acestea, în pofida existenței unei autorizații judiciare, lipsa unei supravegheri independente a condițiilor și limitărilor stabilite de instanță era problematică.

198. În mod similar, Comisia a observat că notificarea subiectului supravegherii nu era o cerință absolută a art. 8 din Convenție, întrucât o

procedură generală de soluționare a plângerilor adresată unui organ de supraveghere independent putea compensa lipsa notificării.

199. Raportul considera, de asemenea, că o „garanție principală” o constituie controalele interne. Recrutarea și formarea reprezentau aspecte esențiale; în plus, era important ca agențiile să consolideze respectul pentru viața privată și alte drepturi ale omului în momentul promulgării regulilor interne.

200. Raportul recunoștea faptul că jurnaliștii sunt un grup care are nevoie de protecție specială, întrucât căutarea contactelor acestora le-ar putea dezvălui sursele (iar riscul de descoperire ar putea fi un puternic factor de descurajare a avertizorilor). Cu toate acestea, Comisia considera că nu exista o interdicție absolută de a căuta contactele jurnaliștilor, cu condiția să existe motive foarte solide în acest sens. Potrivit raportului, profesia de jurnalist nu era ușor de definit, întrucât ONG-urile erau, de asemenea, implicate în construirea opiniei publice, și chiar și bloggerii puteau pretinde că au dreptul la o protecție echivalentă.

201. În cele din urmă, raportul analiza pe scurt aspectul schimbului de informații și, în special, riscul ca statele să eludeze astfel procedurile naționale de supraveghere mai stricte și/sau orice limite legale la care agențiile lor puteau fi supuse în ceea ce privește operațiunile de culegere de informații interne. Comisia considera că o garanție adecvată era aceea să se prevadă că datele transferate în masă puteau fi examinate numai dacă toate cerințele materiale ale unei căutări naționale erau îndeplinite și acest lucru era autorizat în mod corespunzător în același mod ca o căutare a datelor în masă obținute de serviciile care culeg informații de origine electromagnetică prin utilizarea propriilor tehnici.

III. DREPTUL UNIUNII EUROPENE

A. Carta drepturilor fundamentale a Uniunii Europene

202. Art. 7, 8 și 11 din Cartă prevăd următoarele:

Articolul 7 – Respectarea vieții private și de familie

„Orice persoană are dreptul la respectarea vieții private și de familie, a domiciliului și a secretului comunicațiilor.”

Articolul 8 – Protecția datelor cu caracter personal

„1. Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc.

2. Asemenea date trebuie tratate în mod corect, în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege. Orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora.

3. Respectarea acestor norme se supune controlului unei autorități independente.”

Articolul 11 – Libertatea de exprimare și de informare

„1. Orice persoană are dreptul la libertatea de exprimare. Acest drept cuprinde libertatea de opinie și libertatea de a primi sau de a transmite informații sau idei fără amestecul autorităților publice și fără a ține seama de frontiere.

2. Libertatea și pluralismul mijloacelor de informare în masă sunt respectate.”

B. Directive și regulamente ale Uniunii Europene referitoare la protecția și prelucrarea datelor cu caracter personal

203. Directiva privind protecția datelor (Directiva 95/46/CE privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date), adoptată la 24 octombrie 1995, a reglementat pentru mulți ani protecția și prelucrarea datelor cu caracter personal în cadrul Uniunii Europene. Întrucât activitățile statelor membre în materie de siguranță publică, apărare și securitate a statului nu intrau în domeniul de aplicare al dreptului comunitar, directiva nu se aplica acestor activități [articolul 3 alineatul (2)].

204. Regulamentul general privind protecția datelor, adoptat în aprilie 2016, a înlocuit Directiva privind protecția datelor și a devenit aplicabil la 25 mai 2018. Regulamentul, care este aplicabil în mod direct în statele membre², conține dispoziții și cerințe referitoare la prelucrarea informațiilor personale identificabile ale persoanelor vizate în cadrul Uniunii Europene și se aplică tuturor întreprinderilor, indiferent de locație, care desfășoară activități în Spațiul Economic European. Procesele operaționale care tratează datele cu caracter personal trebuie să fie realizate cu protecția datelor începând cu momentul conceperii și în mod implicit, ceea ce înseamnă că datele cu caracter personal trebuie să fie stocate prin pseudonimizare sau anonimizare deplină și să se utilizeze în mod implicit cele mai bune setări de confidențialitate posibile, astfel încât datele să nu fie disponibile public fără consimțământul explicit și să nu poată fi utilizate pentru a identifica un subiect fără informații suplimentare stocate separat. Datele cu caracter personal nu pot fi prelucrate decât dacă sunt efectuate cu o bază legală specificată în regulament sau dacă operatorul sau persoana împuternicită de către operator a primit consimțământul explicit și voluntar din partea proprietarului datelor. Proprietarul datelor are dreptul de a revoca această permisiune în orice moment.

205. Operatorul de date cu caracter personal trebuie să divulge în mod clar orice colectare de date, să declare temeiul legal și scopul prelucrării datelor, durata păstrării datelor și dacă acestea sunt comunicate altor părți terțe sau în afara Uniunii Europene. Utilizatorii au dreptul de a solicita o copie portabilă a datelor colectate de operator într-un format comun, precum și dreptul ca datele lor să fie șterse în anumite circumstanțe. Autoritățile publice și

² Înainte ca Regatul Unit să părăsească Uniunea Europeană, a fost acordat, la 23 mai 2018, avizul regal pentru Legea din 2018 privind protecția datelor, care conține reglementări și măsuri de protecție echivalente.

întreprinderile ale căror activități de bază se axează pe prelucrarea regulată sau sistematică a datelor cu caracter personal au obligația de a angaja un responsabil cu protecția datelor (*data protection officer* – DPO), care este responsabil de gestionarea respectării GDPR. Întreprinderile trebuie să raporteze orice încălcare a securității datelor în termen de 72 de ore, în cazul în care acestea au un efect negativ asupra vieții private a utilizatorilor.

206. Directiva asupra confidențialității și comunicațiilor electronice (Directiva 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice), adoptată la 12 iulie 2002, afirmă, la considerentele (2) și (11):

„(2) Prezenta directivă dorește respectarea drepturilor fundamentale și a principiilor recunoscute în special de Carta drepturilor fundamentale a Uniunii Europene. Directiva caută să asigure în special respectarea deplină a drepturilor menționate la articolele 7 și 8 ale Cartei.

[...] [...] [...]

(11) La fel ca Directiva 95/46/CE, prezenta directivă nu se referă la chestiuni de protecție a drepturilor și libertăților fundamentale legate de activități care nu sunt reglementate de legile comunitare. Prin urmare, aceasta nu aduce atingere echilibrului existent între dreptul indivizilor la confidențialitate și posibilitatea ca statele membre să ia măsurile stipulate la articolul 15 alineatul (1) al prezentei directive, posibilitate necesară în vederea protejării siguranței publice, apărării și siguranței statului (inclusiv bunăstării economice a acestuia, în cazul în care activitățile respective sunt legate de chestiuni de siguranța statului) și întăririi legii penale. În consecință, prezenta directivă nu interzice statelor membre să efectueze interceptări legale ale comunicațiilor electronice sau să ia alte măsuri pentru atingerea scopurilor menționate anterior, dacă acest lucru este necesar și în conformitate cu Convenția Europeană pentru Protecția Drepturilor Omului și a Libertăților Fundamentale, așa cum este aceasta interpretată de Curtea Europeană a Drepturilor Omului. Aceste măsuri trebuie să fie corespunzătoare, strict proporționale cu scopul urmărit și necesare în cadrul unei societăți democratice și trebuie însoțite de precauțiile corespunzătoare în conformitate cu Convenția Europeană pentru Protecția Drepturilor Omului și a Libertăților Fundamentale.”

207. Directiva prevede, în continuare, în măsura relevanței:

Articolul 1 – Sfera de aplicare și scopul

„1. Prezenta directivă armonizează dispozițiile statelor membre, lucru necesar în vederea asigurării unui nivel echivalent de protecție a drepturilor și libertăților fundamentale, mai ales a dreptului la confidențialitatea datelor personale, în domeniul prelucrării de date personale în sectorul comunicațiilor electronice și a liberei circulații a acestor date și a serviciilor și echipamentelor de comunicații electronice în interiorul Comunității.

2. Prevederile prezentei directive precizează și completează Directiva 95/46/CE în scopurile menționate la alineatul (1). Mai mult, acestea sunt menite a asigura protecția intereselor legitime ale abonaților persoane juridice.

3. Prezenta directivă nu se aplică activităților care nu sunt cuprinse în domeniul de aplicare al Tratatului de instituire a Comunității Europene, cum sunt cele menționate la titlurile V și VI al Tratatului privind Uniunea Europeană, și în orice caz activităților legate de siguranța publică, de apărare, de siguranța statului (inclusiv de bunăstarea

economică a acestuia, dacă activitățile respective sunt legate de chestiuni de siguranța statului) și activităților statului în domeniul legii penale.”

Articolul 15 – Aplicarea anumitor dispoziții ale Directivei 95/46/CE

„1. Statele membre pot adopta măsuri legislative pentru a restrânge sfera de aplicare a drepturilor și obligațiilor prevăzute la articolul 5, articolul 6, articolul 8 alineatele (1), (2), (3) și (4) și articolul 9 ale prezentei directive, în cazul în care restrângerea lor constituie o măsură necesară, corespunzătoare și proporțională în cadrul unei societăți democratice pentru a proteja securitatea națională (de exemplu siguranța statului), apărarea, siguranța publică sau pentru prevenirea, investigarea, detectarea și urmărirea penală a unor fapte penale sau a folosirii neautorizate a sistemelor de comunicații electronice, în conformitate cu articolul 13 alineatul (1) al Directivei 95/46/CE. În acest scop, statele membre pot adopta, *inter alia*, măsuri legislative care să permită reținerea de date, pe perioadă limitată, pentru motivele arătate anterior în acest alineat. Toate măsurile menționate în acest alineat trebuie să fie conforme cu principiile generale ale legislației comunitare, inclusiv cu cele menționate la articolul 6 alineatele (1) și (2) al Tratatului privind Uniunea Europeană.”

208. La 15 martie 2006 a fost adoptată Directiva privind păstrarea datelor (Directiva privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei 2002/58/CE). Înainte ca hotărârea din 2014 să o declare nevalidă (infra, pct. 209), directiva prevedea, în măsura relevanței:

Articolul 1 – Obiectul și domeniul de aplicare

„1. Prezenta directivă urmărește să armonizeze dispozițiile statelor membre privind obligațiile furnizorilor de servicii de comunicații electronice accesibile publicului sau de rețele de comunicații publice cu privire la păstrarea anumitor date generate sau prelucrate de către aceștia, pentru a se asigura că datele sunt disponibile în vederea cercetării, depistării și urmăririi penale a infracțiunilor grave, astfel cum sunt definite de fiecare stat membru în dreptul său intern.

2. Prezenta directivă se aplică datelor de trafic și localizare, atât pentru entități juridice, cât și pentru persoane fizice, precum și datelor necesare pentru identificarea abonatului sau a utilizatorului înregistrat. Nu se aplică pentru conținutul comunicațiilor electronice, inclusiv informațiile consultate prin utilizarea unei rețele de comunicații electronice.”

Articolul 3 – Obligația de păstrare a datelor

„1. Prin derogare de la articolele 5, 6 și 9 din Directiva 2002/58/CE, statele membre adoptă măsuri pentru a se asigura că datele menționate la articolul 5 din prezenta directivă sunt păstrate în conformitate cu dispozițiile acesteia, în măsura în care acele date sunt generate sau prelucrate de către furnizorii de comunicații electronice accesibile publicului sau de rețele publice de comunicații, de competența acestora, în procesul de furnizare a serviciilor de comunicații respectiv.”

C. Jurisprudența relevantă a Curții de Justiție a Uniunii Europene („CJUE”)

1. *Digital Rights Ireland Ltd împotriva Minister for Communications, Marine and Natural Resources și alții și Kärntner Landesregierung și alții* (cauzele C-293/12 și C-594/12; ECLI:EU:C:2014:238)

209. Într-o hotărâre din 8 aprilie 2014, CJUE a declarat nevalidă Directiva 2006/24/CE privind păstrarea datelor, care prevedea obligația furnizorilor de servicii de comunicații electronice accesibile publicului sau de rețele de comunicații publice de a păstra toate datele de trafic și localizare pentru perioade cuprinse între șase luni și doi ani, pentru a se asigura că datele sunt disponibile pentru cercetarea, depistarea și urmărirea penală a infracțiunilor grave, astfel cum sunt definite de fiecare stat membru în dreptul său național. CJUE observa că, deși directiva nu permite păstrarea conținutului comunicării, datele de transfer și localizare care fac obiectul acesteia ar putea permite să se tragă concluzii foarte precise cu privire la viața privată a persoanelor ale căror date au fost păstrate. În consecință, obligația de păstrare a datelor constituia în sine o ingerință în dreptul la respectarea vieții private și a comunicațiilor, garantat de art. 7 din Carta drepturilor fundamentale a Uniunii Europene, și în dreptul la protecția datelor cu caracter personal, în temeiul art. 8 din Cartă.

210. Accesul autorităților naționale competente la date a constituit o nouă ingerință în drepturile fundamentale, pe care CJUE a considerat-o „deosebit de gravă”. Potrivit CJUE, faptul că datele erau păstrate și utilizate ulterior fără ca abonatul sau utilizatorul înregistrat să fie informat era de natură să genereze în mintea persoanelor în cauză sentimentul că viața lor privată a făcut obiectul unei supravegheri constante. Ingerința a îndeplinit un obiectiv de interes general, și anume acela de a contribui la combaterea criminalității grave și a terorismului și, prin urmare, la securitatea publică. Cu toate acestea, nu a respectat cerința proporționalității.

211. În primul rând, directiva acoperea, în mod generalizat, toate persoanele și toate mijloacele de comunicare electronică, precum și toate datele de trafic, fără nicio diferențiere, limitare sau excepție în raport cu obiectivul combaterii infracțiunilor grave. Prin urmare, implica o ingerință în drepturile fundamentale ale practic întregii populații europene, potrivit CJUE. Se aplica chiar și acelor persoane pentru care nu exista niciun element de natură să sugereze că comportamentul lor putea avea o legătură, chiar indirectă sau îndepărtată, cu o infracțiune gravă.

212. În al doilea rând, directiva nu conținea condiții materiale și procedurale referitoare la accesul autorităților naționale competente la date și la utilizarea lor ulterioară. Limitându-se la a face trimitere, în general, la infracțiuni grave, astfel cum sunt definite de fiecare stat membru în dreptul său național, directiva nu stabilea niciun criteriu obiectiv prin care să se determine care infracțiuni ar putea fi considerate suficient de grave pentru a

justifica o ingerință atât de extinsă în drepturile fundamentale consacrate la art. 7 și 8 din Cartă. Mai presus de toate, accesul autorităților naționale competente la datele păstrate nu era condiționat de un control prealabil efectuat de o instanță sau de un organ administrativ independent a cărui decizie urmărea să limiteze accesul la date și utilizarea acestora la ceea ce era strict necesar pentru atingerea obiectivului urmărit.

213. În al treilea rând, directiva impunea ca toate datele să fie păstrate pentru o perioadă de cel puțin 6 luni, fără a se face vreo distincție între categoriile de date în funcție de eventuala lor utilitate pentru obiectivul urmărit sau în funcție de persoanele vizate. CJUE a concluzionat că directiva implica o ingerință de amploare și deosebit de gravă în drepturile fundamentale consacrate la art. 7 și 8 din Cartă, fără ca o astfel de ingerință să fie încadrată în mod precis de dispoziții care să garanteze că aceasta era limitată efectiv la strictul necesar. CJUE a remarcat, de asemenea, că directiva nu prevedea garanții suficiente, prin intermediul unor măsuri tehnice și organizatorice, pentru a asigura o protecție eficientă a datelor păstrate împotriva riscurilor de abuz și împotriva oricărui acces și utilizare ilegală a acestor date.

2. *Tele2 Sverige AB împotriva Post- och telestyrelsen și Secretary of State for the Home Department împotriva Tom Watson și alții* (cauzele C-203/15 și C-698/15; ECLI:EU:C:2016:970)

214. În *Secretary of State for the Home Department împotriva Watson și alții*, reclamanții au solicitat controlul de către o instanță al legalității art. 1 din Legea din 2014 privind păstrarea datelor și competențele de investigare (*Data Retention and Investigatory Powers Act 2014* – „DRIPA”), conform căreia ministrul internelor putea solicita unui operator de telecomunicații publice să păstreze datele de comunicații relevante în cazul în care considera că acest lucru era necesar și proporțional în raport cu unul sau mai multe dintre scopurile prevăzute la art. 22 alin. (2) lit. a)–h) din RIPA. Reclamanții au susținut, printre altele, că art. 1 era incompatibil cu art. 7 și 8 din Cartă și cu art. 8 din Convenție.

215. La 17 iulie 2015, *High Court* a stabilit că hotărârea *Digital Rights* stabilea „cerințele obligatorii ale dreptului Uniunii Europene” aplicabile legislației statelor membre privind păstrarea datelor de comunicații și accesul la astfel de date. Întrucât, în această hotărâre, CJUE a hotărât că Directiva 2006/24 era incompatibilă cu principiul proporționalității, o reglementare națională care conținea aceleași dispoziții ca directiva menționată putea, de asemenea, să nu fie compatibilă cu acest principiu. În fapt, din logica care a stat la baza hotărârii *Digital Rights* reieșea că o reglementare care institua un ansamblu general de norme pentru păstrarea datelor de comunicații încălca drepturile garantate de art. 7 și 8 din Cartă, cu excepția cazului în care legislația respectivă era completată cu un ansamblu de norme privind accesul la date, ansamblu definit de dreptul național, care să ofere garanții suficiente

pentru a proteja aceste drepturi. Prin urmare, art. 1 din DRIPA nu era compatibil cu art. 7 și 8 din Cartă, întrucât nu prevedea norme clare și precise care să prevadă accesul la datele păstrate și utilizarea acestora, iar accesul la datele respective nu era condiționat de un control prealabil efectuat de o instanță sau de un organ administrativ independent.

216. În urma apelului formulat de ministrul internelor, *Court of Appeal* a solicitat CJUE pronunțarea unei decizii preliminare.

217. În fața CJUE, cauza a fost conexată cu cererea pentru pronunțarea unei hotărâri preliminare formulată de Kammarrätten i Stockholm în cauza C-203/15 *Tele2 Sverige AB* împotriva *Post- och telestyrelsen*. În urma unei audieri în care au intervenit aproximativ 15 state membre ale Uniunii Europene, CJUE s-a pronunțat la 21 decembrie 2016. CJUE a hotărât că art. 15 alin. (1) din Directiva 2002/58, citit în lumina art. 7, 8 și 11, precum și a art. 52 alin. (1) din Cartă, trebuie interpretat în sensul că se opune unei reglementări naționale care reglementează protecția și securitatea datelor de transfer și a datelor de localizare și în special accesul autorităților naționale competente la datele păstrate, fără a limita acest acces, în cadrul combaterii infracționalității, numai la combaterea infracționalității grave, fără a supune respectivul acces unui control prealabil din partea unei instanțe sau a unei autorități administrative independente și fără a impune ca datele în cauză să fie păstrate pe teritoriul Uniunii Europene.

218. CJUE a declarat inadmisibilă întrebarea *Court of Appeal* dacă protecția conferită la art. 7 și 8 din Cartă o depășește pe cea garantată la art. 8 din Convenție.

219. În urma pronunțării hotărârii CJUE, cauza a fost reintrodusă pe rolul *Court of Appeal*. La 31 ianuarie 2018, aceasta a pronunțat o hotărâre declarativă în următorii termeni: art. 1 din DRIPA era incompatibil cu dreptul Uniunii Europene în măsura în care permitea accesul la datele păstrate atunci când obiectul urmărit prin acces nu era limitat numai la combaterea infracțiunilor grave sau atunci când accesul nu făcea obiectul unei examinări prealabile din partea unei instanțe sau a unei autorități administrative independente.

3. *Ministerio Fiscal* (cauza C-207/16; ECLI:EU:C:2018:788)

220. Această cerere pentru pronunțarea unei hotărâri preliminare a fost formulată după ce poliția spaniolă, în cadrul anchetei furtului unui portofel și a unui telefon mobil, a solicitat judecătorului de instrucție să i se acorde accesul la datele de identificare a utilizatorilor de numere de telefon activate cu telefonul furat în cursul unei perioade de douăsprezece zile înaintea furtului. Judecătorul de instrucție a respins cererea pe motiv că, *inter alia*, faptele care făceau obiectul anchetei penale nu constituiau o infracțiune „gravă”. Ulterior, instanța de trimitere a solicitat CJUE orientări pentru a stabili pragul de gravitate a infracțiunilor dincolo de care o ingerință în drepturile fundamentale, precum accesul autorităților naționale competente la

datele cu caracter personal păstrate de furnizorii de servicii de comunicații electronice, poate fi justificată.

221. La 2 octombrie 2018, Marea Cameră a CJUE a hotărât că art. 15 alin. (1) din Directiva 2002/58/CE, citit în lumina art. 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene, trebuie interpretat în sensul că accesul unor autorități publice la date în scopul identificării titularilor cartelelor SIM activate cu un telefon mobil furat, cum ar fi numele de familie, prenumele și, dacă era cazul, adresele titularilor, implica o ingerință în drepturile fundamentale ale acestora care nu era suficient de gravă pentru ca acest acces să fie limitat, în materia prevenirii, urmăririi penale și trimiterii în judecată a infracțiunilor, la combaterea infracțiunilor grave. În special, indica faptul că:

„[În conformitate cu principiul proporționalității, o ingerință gravă nu poate fi justificată, în materie de prevenire, de investigare, de detectare și de trimitere în judecată 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 trimiterea în judecată a unor «infracțiuni» în general.”

222. Instanța nu a considerat că accesul la datele care fac obiectul cererii constituia o ingerință deosebit de gravă, întrucât:

„permit doar să se pună în legătură, pe o perioadă determinată, cartela sau cartelele SIM activate cu telefonul mobil furat cu identitatea civilă a titularilor acestor cartele SIM. Fără o verificare încrucișată a datelor aferente comunicațiilor efectuate cu respectivele cartele SIM și a datelor de localizare, aceste date nu permit 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 permit să se tragă concluzii precise cu privire la viața privată a persoanelor ale căror date sunt vizate.”

4. *Maximillian Schrems împotriva Data Protection Commissioner* (cauza C-362/14; ECLI:EU:C:2015:650)

223. Cererea pentru pronunțarea unei hotărâri preliminare a fost formulată ca urmare a unei plângeri împotriva Facebook Ireland Ltd, care a fost adresată Comisarului irlandez pentru Protecția Datelor de către domnul Schrems, un avocat austriac ce milita pentru protecția vieții private. Domnul Schrems a contestat transferul datelor sale de către Facebook Ireland către Statele Unite și păstrarea lor pe serverele situate în această țară. Comisarul pentru Protecția Datelor a respins plângerea întrucât, într-o decizie din 26 iulie 2000, Comisia Europeană considerase că Statele Unite asigură un nivel adecvat de protecție a datelor cu caracter personal transferate („decizia privind sfera de siguranță”).

224. În hotărârea sa din 6 octombrie 2015, CJUE a declarat că existența unei decizii a Comisiei prin care se constata că o țară terță asigura un nivel

adecvat de protecție a datelor cu caracter personal transferate nu poate anula sau chiar reduce competențele de care dispun autoritățile naționale de supraveghere în temeiul Cartei sau al Directivei privind protecția datelor. Prin urmare, chiar dacă Comisia ar fi pronunțat o decizie, trebuia ca autoritățile naționale de supraveghere să fie în măsură să examineze, în deplină independență, dacă transferul datelor unei persoane către o țară terță respecta cerințele prevăzute de directivă.

225. Cu toate acestea, numai CJUE putea anula o decizie a Comisiei. În această privință, a observat că sistemul sferei de siguranță era aplicabil numai întreprinderilor din Statele Unite care aderaseră la acesta, iar autoritățile publice americane nu erau supuse regimului respectiv. Pe de altă parte, cerințele Statelor Unite în materie de securitate națională, de interes public și de aplicare a legii prevalau asupra sistemului sferei de siguranță, astfel încât întreprinderile americane erau obligate să nu respecte, fără nicio limitare, normele de protecție prevăzute de sistem atunci când se aflau în contradicție cu astfel de cerințe. Prin urmare, sistemul sferei de siguranță permitea ingerința autorităților publice americane în drepturile fundamentale ale persoanelor, iar Comisia nu a făcut referire, în decizia privind sfera de siguranță, nici la existența, în Statele Unite, a unor norme destinate să limiteze orice astfel de ingerință, nici la existența unei protecții juridice efective împotriva ingerinței.

226. În ceea ce privește aspectul dacă nivelul de protecție din Statele Unite era în esență echivalent cu drepturile și libertățile fundamentale garantate în cadrul Uniunii Europene, CJUE a constatat că legislația nu se limita la ceea ce era strict necesar atunci când autoriza, în mod generalizat, stocarea integralității datelor cu caracter personal ale tuturor persoanelor ale căror date au fost transferate din Uniune către Statele Unite fără a se face vreo diferențiere, limitare sau excepție în raport cu obiectivul urmărit și fără a prevedea un criteriu obiectiv pentru delimitarea accesului autorităților publice la date și utilizarea lor ulterioară. Prin urmare, în temeiul dreptului Uniunii, o legislație care permitea autorităților publice accesul generalizat la conținutul comunicațiilor electronice trebuie să fie considerată ca aducând atingere substanței dreptului fundamental la respectarea vieții private. De asemenea, o reglementare care nu prevede nicio posibilitate a unui justițiabil de a exercita căi de atac legale pentru a avea acces la datele sale cu caracter personal sau pentru a obține rectificarea sau ștergerea unor astfel de date ar compromite esența dreptului fundamental la o protecție juridică efectivă.

227. În sfârșit, Curtea a constatat că decizia privind sfera de siguranță priva autoritățile naționale de supraveghere de competențele lor în cazul în care o persoană pune în discuție compatibilitatea deciziei cu protecția vieții private și a drepturilor și libertăților fundamentale ale persoanelor. Comisia nu avea competența de a restricționa competențele autorităților naționale de supraveghere în acest mod și, în consecință, CJUE a hotărât că decizia privind sfera de siguranță era nevalidă.

5. *Cauza Data Protection Commissioner împotriva Facebook Ireland și Maximillian Schrems* (C-311/18; ECLI:EU:C:2020:559)

228. În urma hotărârii CJUE din 6 octombrie 2015, instanța de trimitere a anulat respingerea plângerii formulate de domnul Schrems și a retrimis această decizie în fața Comisarului. În cursul investigației Comisarului, Facebook Ireland a explicat că o mare parte din datele cu caracter personal au fost transferate către Facebook Inc. în temeiul clauzelor standard de protecție a datelor prevăzute în anexa la Decizia 2010/87/UE a Comisiei, astfel cum a fost modificată.

229. Domnul Schrems și-a reformulat plângerea susținând, *inter alia*, că legislația Statelor Unite impunea Facebook Inc. să pună la dispoziția anumitor autorități americane, precum NSA și Biroul Federal de Investigații, datele cu caracter personal care i-au fost transferate. Întrucât aceste date au fost utilizate în cadrul diferitor programe de supraveghere într-un mod incompatibil cu art. 7, 8 și 47 din Cartă, Decizia 2010/87/UE nu putea justifica transferul acestor date către Statele Unite. Pe această bază, a solicitat Comisarului să interzică sau să suspende transferul datelor sale cu caracter personal către Facebook Inc.

230. Într-un proiect de decizie publicat la 24 mai 2016, Comisarul considera în mod provizoriu că datele cu caracter personal ale cetățenilor Uniunii transferate către Statele Unite riscau să fie consultate și prelucrate de autoritățile americane într-un mod incompatibil cu art. 7 și 8 din Cartă și că dreptul Statelor Unite nu le oferea acestora căi de atac compatibile cu art. 47 din Cartă. Comisarul aprecia că clauzele standard de protecție a datelor din anexa la Decizia 2010/87/UE nu erau de natură să remedieze această deficiență, întrucât nu creau obligații pentru autoritățile americane.

231. După ce a examinat activitățile serviciilor de informații din Statele Unite în temeiul art. 702 din FISA și al Decretului nr. 12333, *High Court* a concluzionat că Statele Unite au efectuat operațiuni de prelucrare în masă a datelor cu caracter personal fără a asigura un nivel de protecție echivalent în esență cu cel garantat la art. 7 și 8 din Cartă și că cetățenii Uniunii nu dispuneau de aceleași căi de atac ca cetățenii Statelor Unite, astfel încât dreptul Statelor Unite nu le acorda cetățenilor Uniunii un nivel de protecție echivalent în esență cu cel garantat la art. 47 din Cartă. Instanța a suspendat judecarea cauzei și a adresat CJUE o serie de întrebări preliminare. A întrebat, *inter alia*, dacă dreptul Uniunii se aplică transferului de date de la o societate privată din Uniune la o societate privată dintr-un stat terț; în caz afirmativ, cum trebuie evaluat nivelul de protecție din statul terț și dacă nivelul de protecție acordat de Statele Unite respectă esența drepturilor garantate la art. 47 din Cartă.

232. În hotărârea din 16 iulie 2020, CJUE a declarat că Regulamentul General privind Protecția Datelor („RGPD”) se aplica transferului de date cu caracter personal în scopuri comerciale de un operator economic stabilit într-un stat membru către un alt operator economic stabilit într-o țară terță, în

pofta faptului că, în cursul sau în urma transferului, datele respective puteau 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 efective impuse de RGPD trebuiau să garanteze că persoanele vizate ale căror date cu caracter personal au fost transferate către o țară terță în temeiul clauzelor standard de protecție a datelor beneficiau de un nivel de protecție în esență echivalent cu cel garantat în cadrul Uniunii Europene. În acest scop, aprecierea nivelului de protecție acordat în cadrul unui astfel de transfer trebuia să ia în considerare atât prevederile contractuale convenite între operator sau persoana împuternicită de operator stabilită în Uniune și destinatarul transferului stabilit în țara terță în cauză, cât și, în ceea ce privește orice acces al autorităților publice ale acestei țări terțe la datele cu caracter personal transferate, elementele relevante ale sistemului juridic al respectivei țări terțe.

233. În plus, cu excepția cazului în care a existat o decizie validă a Comisiei privind caracterul adecvat al nivelului de protecție, autoritatea de supraveghere competentă era obligată să suspende sau să interzică transferul de date către o țară terță dacă, în opinia acestei autorități de supraveghere și având în vedere toate circumstanțele transferului respectiv, clauzele standard de protecție a datelor adoptate de Comisie nu erau sau nu puteau fi respectate în țara terță respectivă, iar protecția datelor transferate (astfel cum prevedea dreptul Uniunii) nu putea fi asigurată prin alte mijloace.

234. Pentru a adopta o decizie privind caracterul adecvat al nivelului de protecție, Comisia trebuia să constate, printr-o motivare adecvată, că țara terță în cauză asigură, în temeiul dreptului său intern sau al angajamentelor sale internaționale, un nivel de protecție a drepturilor fundamentale în esență echivalent cu cel garantat în ordinea juridică a Uniunii Europene. În opinia CJUE, decizia privind sfera de siguranță era nelegală. Art. 702 din Legea supravegherea activităților străine de spionaj (*Foreign Intelligence Security Act* – „FISA”) nu indica nicio limitare a competenței pe care o conferea în aplicarea programelor de supraveghere în scopul activităților de informații externe sau existența unor garanții pentru persoanele din afara SUA potențial vizate de programele respective. În aceste condiții, nu putea asigura un nivel de protecție în esență echivalent cu cel garantat de Cartă. În plus, în ceea ce privește programele de supraveghere întemeiate pe Decretul prezidențial nr. 12333, era clar că acest decret nu conferea drepturi opozabile autorităților americane în fața instanțelor.

6. *Privacy International împotriva Secretary of State for Foreign and Commonwealth Affairs și alții* (cauza C-623/17; ECLI:EU:C:2020:790) și *La Quadrature du Net și alții, French Data Network și alții și Ordre des barreaux francophones et germanophone și alții* (cauzele C-511/18, C-512/18 și C-520/18; ECLI:EU:C:2020:791)

235. La 8 septembrie 2017, IPT a pronunțat o hotărâre în cauza *Privacy International*, care privea obținerea de către serviciile de informații de date de comunicații în masă, în temeiul art. 94 din Legea privind telecomunicațiile din 1984, precum și de date cu caracter personal în masă. IPT a constatat că, întrucât existența lor era recunoscută, regimurile erau conforme cu art. 8 din Convenție. Cu toate acestea, a identificat următoarele patru cerințe care păreau să decurgă din hotărârea *Watson și alții* a CJUE și care păreau să fie dincolo de cerințele art. 8 din Convenție: o restricție privind accesul la date în masă neștimate, necesitatea unei autorizații prealabile (cu excepția cazurilor de urgență confirmată) înainte de a putea fi accesate datele, prevederea unei notificări ulterioare a persoanelor afectate și păstrarea tuturor datelor în cadrul Uniunii Europene.

236. La 30 octombrie 2017, IPT a adresat CJUE o cerere pentru pronunțarea unei hotărâri preliminare care să clarifice măsura în care cerințele *Watson* se puteau aplica în cazul în care tehnicile de obținere de date în masă și de prelucrare automată erau necesare pentru protejarea securității naționale. Procedând astfel, își exprima profunda îngrijorare cu privire la faptul că, în cazul în care cerințele *Watson* s-ar aplica măsurilor luate pentru a proteja securitatea națională, ar împiedica luarea unor astfel de măsuri și ar pune în pericol securitatea națională a statelor membre. În special, observa avantajele obținerii de date în masă în contextul securității naționale, riscul ca necesitatea unei autorizații prealabile să afecteze capacitatea serviciilor de informații de a combate amenințarea la adresa securității naționale, pericolul și caracterul impracticabil al punerii în aplicare a unei cerințe de notificare cu privire la obținerea sau utilizarea unei baze de date în masă, în special în ceea ce privește securitatea națională, și impactul pe care o interdicție absolută de a transfera de date în afara Uniunii Europene l-ar putea avea asupra obligațiilor statelor membre în temeiul Convenției.

237. Ședința publică a avut loc la 9 septembrie 2019. Cauza *Privacy International* a fost conexată la cauzele C-511/18 și C-512/18, *La Quadrature du Net și alții*, și C-520/18, *Ordre des barreaux francophones et germanophone și alții*, care priveau, de asemenea, modul de aplicare a Directivei 2002/58 în cazul activităților legate de securitatea națională și de combaterea terorismului. 13 state au intervenit în sprijinul statelor în cauză.

238. La 6 octombrie 2020 au fost pronunțate două hotărâri separate. În *Privacy International*, CJUE a constatat că legislația națională care permitea unei autorități a statului să solicite furnizorilor de servicii de comunicații electronice să transmită datele de transfer și datele de localizare către

serviciile de securitate și de informații în scopul protejării securității naționale intra în domeniul de aplicare al Directivei asupra confidențialității și comunicațiilor electronice. Interpretarea acestei directive trebuia să țină seama de dreptul la viață privată, garantat la art. 7 din Cartă, de dreptul la protecția datelor cu caracter personal, garantat la art. 8, precum și de dreptul la libertatea de exprimare, garantat la art. 11. Limitările aduse exercitării acestor drepturi trebuie să fie prevăzute de lege, să respecte esența drepturilor și să fie proporționale, necesare și să răspundă efectiv obiectivelor de interes general recunoscute de Uniunea Europeană sau necesității de a proteja drepturile și libertățile celorlalți. În plus, limitările aduse protecției datelor cu caracter personal trebuie să se aplice numai în măsura în care este strict necesar și pentru a îndeplini cerința proporționalității, legislația trebuie să stabilească norme clare și precise care să reglementeze domeniul de aplicare și aplicarea măsurii în cauză și să impună garanții minime, astfel încât persoanele ale căror date cu caracter personal sunt afectate să aibă suficiente garanții că datele vor fi protejate în mod eficient împotriva riscului de abuzuri.

239. În opinia CJUE, o legislație națională care impune furnizorilor de servicii de comunicații electronice să facă publice datele de trafic și datele de localizare serviciilor de securitate și informații prin intermediul unei transmisii generalizate și nediferențiate – care afectează toate persoanele care utilizează servicii de comunicații electronice – depășește limitele a ceea ce este strict necesar și nu poate fi considerată în mod justificat conformă cu Directiva asupra confidențialității și comunicațiilor electronice, citită în lumina Cartei.

240. Cu toate acestea, în *La Quadrature du Net și alții*, CJUE a confirmat că, deși Directiva asupra confidențialității și comunicațiilor electronice, interpretată în lumina Cartei, se opunea adoptării unor măsuri legislative care prevedea păstrarea generalizată și nediferențiată a datelor de trafic și localizare, atunci când un stat membru se confrunta cu o amenințare gravă la adresa securității naționale care se dovedea a fi autentică și prezentă sau previzibilă, acest fapt nu excludea măsuri legislative care să impună păstrarea, în mod generalizat și nediferențiat, a datelor de trafic și localizare, pe o perioadă limitată la ceea ce era strict necesar, dar care putea fi prelungită dacă pericolul persista. În scopuri legate de combaterea infracționalității grave și de prevenirea amenințărilor grave la adresa siguranței publice, un stat membru putea, de asemenea, să prevadă, dacă se limita în timp la strictul necesar, păstrarea țintită a datelor de trafic și de localizare, pe baza unor factori obiectivi și nediscriminatorii, în funcție de categoriile de persoane vizate sau utilizând un criteriu geografic, sau a adreselor IP atribuite sursei unei conexiuni la Internet. De asemenea, un stat membru avea posibilitatea de a proceda la păstrarea generalizată și nediferențiată a datelor referitoare la identitatea civilă a utilizatorilor mijloacelor de comunicare electronică, fără ca păstrarea acestora să facă obiectul unei limite de timp specifice.

241. În plus, Directiva asupra confidențialității și comunicațiilor electronice, citită în lumina Cartei, nu se opunea unor reglementări naționale care impuneau furnizorilor de servicii de comunicații electronice să recurgă, în primul rând, la analiza automată și colectarea în timp real a datelor de trafic și de localizare și, în al doilea rând, la colectarea în timp real a datelor tehnice referitoare la localizarea echipamentului terminal utilizat, în cazul în care se limita la situațiile în care un stat membru se confrunta cu o amenințare gravă la adresa securității naționale care era autentică, prezentă sau previzibilă și în care recursul la o astfel de analiză putea face obiectul unui control efectiv efectuat de o instanță sau un organ administrativ independent, a cărui decizie avea caracter obligatoriu; și în cazul în care recursul la colectarea în timp real a datelor de trafic și localizare se limita la persoanele pentru care exista un motiv întemeiat de a suspecta că erau implicate în activități teroriste și această măsură făcea obiectul unui control prealabil efectuat fie de o instanță, fie de un organ administrativ independent a cărui decizie avea caracter obligatoriu.

IV. DREPT ȘI PRACTICĂ COMPARATE RELEVANTE

A. Statele contractante

242. Cel puțin șapte state contractante (Elveția, Finlanda, Franța, Germania, Suedia, Țările de Jos și Regatul Unit) aplică în mod oficial regimuri de interceptare în masă prin cabluri și/sau căi aeriene.

243. Într-un alt stat (Norvegia) este dezbătut un proiect de lege: dacă va fi adoptat, acesta va autoriza, de asemenea, interceptarea în masă.

244. Detalii privind sistemul suedez pot fi regăsite în hotărârea din cauza *Centrum för rättvisa împotriva Suediei* (cererea nr. 35252/08); detaliile sistemului german sunt prezentate în continuare la punctele 247-252.

245. În ceea ce privește acordurile privind schimbul de informații, cel puțin 39 de state contractante fie au încheiat acorduri privind schimbul de informații cu alte state, fie au posibilitatea de a încheia astfel de acorduri. Două interzic în mod expres, iar două permit în mod expres statului să solicite unei puteri străine interceptarea de materiale în numele său. În celelalte state, poziția cu privire la acest aspect nu este clară.

246. În cele din urmă, în majoritatea statelor, garanțiile aplicabile sunt, în linii mari, aceleași ca pentru operațiunile interne, cu diferite restricții în ceea ce privește utilizarea datelor primite și, în unele cazuri, cu obligația de a le distruge dacă devin nerelevante.

B. Hotărârea Curții Constituționale Federale a Germaniei din 19 mai 2020 (1 BvR 2835/17)

247. În această hotărâre, Curtea Constituțională a luat în considerare dacă competențele Serviciului Federal de Informații de a desfășura activități de

culegere de informații strategice (sau „semnale”) privind telecomunicațiile străine au încălcat drepturile fundamentale prevăzute în Legea fundamentală (*Grundgesetz*).

248. Regimul în cauză implica interceptarea atât a conținutului, cât și a datelor de comunicații aferente și urmărea doar să monitorizeze telecomunicațiile străine în afara teritoriului german. O astfel de supraveghere putea fi efectuată în scopul obținerii de informații cu privire la subiecte pentru care mandatul guvernului federal era semnificativ pentru politica externă și de securitate a statului. Cu toate acestea, putea fi utilizată și pentru a ținti anumite persoane. Admisibilitatea și necesitatea ordinelor de a efectua o astfel de supraveghere erau controlate de o comisie independentă. Potrivit hotărârii Curții Constituționale, interceptarea era urmată de un proces de filtrare și evaluare în mai multe etape, complet automatizat. În acest scop, Serviciul Federal de Informații utiliza un număr de șase sute de mii de termeni de căutare care erau controlați de o subunitate internă cu responsabilitatea de se asigura că legătura dintre termenii de căutare utilizați și scopul solicitării de date era explicată într-un mod rezonabil și cuprinzător. După aplicarea procesului automat de filtrare, materialul interceptat era fie eliminat, fie stocat și trimis spre evaluare de către un analist.

249. Schimbul de materiale interceptate cu serviciile de informații străine era însoțit de un acord de cooperare care trebuia să includă restricții privind utilizarea și garanții prin care să se asigure că datele sunt prelucrate și șterse în conformitate cu statul de drept.

250. Curtea Constituțională a hotărât că regimul în cauză nu era conform cu Legea fundamentală. Deși a recunoscut interesul public imperativ al colectării efective de informații externe, a considerat totuși, *inter alia*, că regimul nu se limita la scopuri suficient de specifice, că nu era structurat într-un mod care să permită o supraveghere și un control adecvat și că anumite garanții lipseau, în special în ceea ce privește protecția jurnaliștilor, avocaților și altor persoane ale căror comunicații impuneau o protecție specială a confidențialității.

251. În ceea ce privește schimbul de informații obținute prin supraveghere externă, instanța a constatat din nou lipsa garanțiilor. În special, nu se specifica suficient de clar momentul în care interesele importante puteau justifica transferurile de date. În plus, deși Curtea Constituțională nu a considerat necesar ca un stat destinat să aibă norme comparabile privind prelucrarea datelor cu caracter personal, a considerat totuși că datele puteau fi transferate în străinătate numai dacă exista un nivel adecvat de protecție a datelor și dacă nu exista nicio temere că informațiile ar fi utilizate pentru a încălca principiile fundamentale ale statului de drept. La un nivel mai general, în contextul schimbului de informații, instanța a considerat că cooperarea cu statele străine nu ar trebui să fie utilizată pentru a aduce atingere garanțiilor interne și, în cazul în care Serviciul Federal de Informații dorea să utilizeze termenii de căutare care îi fuseseră furnizați de un serviciu de informații

străin, trebuia mai întâi să confirme existența legăturii necesare între termenii de căutare și scopul solicitării de date și că datele rezultate nu necesitau existența unui anumit grad de confidențialitate (de exemplu, întrucât priveau avertizori sau dizidenți). Deși instanța nu excludea posibilitatea transferului masiv de date către servicii de informații străine, a constatat că acesta nu putea reprezenta un proces continuu, bazat pe un singur scop.

252. În cele din urmă, Curtea Constituțională a constatat că competențele de supraveghere analizate nu făceau, de asemenea, obiectul unei supravegheri independente și continue extinse, care să asigure respectarea legii și să compenseze absența virtuală a garanțiilor garantate în mod obișnuit în temeiul statului de drept. Legiuitorul avea obligația să prevadă două tipuri diferite de supraveghere, care, de asemenea, să se reflecte în cadrul organizațional: în primul rând, un organ asemănător unei instanțe, însărcinat cu supravegherea și luarea unei decizii în cadrul unei proceduri formale de protecție juridică *ex ante* sau *ex post* și, în al doilea rând, o supraveghere de natură administrativă și care să poată, din proprie inițiativă, să examineze în mod aleatoriu întregul proces de supraveghere strategică în ceea ce privește legalitatea acestuia. În opinia Curții Constituționale, anumite măsuri procedurale esențiale impuneau, în principiu, autorizarea *ex ante* din partea unui organ asemănător unei instanțe, și anume: stabilirea formală a diverselor măsuri de supraveghere (nu erau excluse excepțiile în cazuri de urgență), utilizarea unor termeni de căutare, în măsura în care aceste persoane direct vizate, care puteau reprezenta un pericol și, prin urmare, prezentau un interes direct pentru Serviciul Federal de Informații, utilizarea unor termeni de căutare care vizau direct persoane ale căror comunicații necesitau protecție specială, și schimbul de date privind jurnaliștii, avocații și alte profesii care necesitau o protecție specială a confidențialității, în raportul cu serviciile de informații străine.

C. Hotărârea Curții de Apel de la Haga din 14 martie 2017

253. O serie de persoane și asociații s-au plâns că serviciile de informații și de securitate olandeze acționau în mod ilegal întrucât primeau date de la servicii de informații și de securitate străine, în special NSA și GCHQ, care, în opinia lor, fie obținuseră, fie era posibil să fi obținut datele într-un mod „neautorizat” sau „ilegal”. Reclamanții nu au susținut că activitățile NSA și GCHQ erau „ilicite” sau „ilegale” în temeiul dreptului intern, ci mai degrabă că NSA încălcăse Pactul internațional cu privire la drepturile civile și politice (denumit în continuare „PIDCP”), iar GCHQ acționase încălcând Convenția. Reclamanții s-au întemeiat, *inter alia*, pe „dezvăluirile Snowden” (supra, pct. 12).

254. Acțiunile reclamanților au fost respinse de Tribunalul de la Haga la 23 iulie 2014 (ECLI:NL:RBDHA:2014:8966). Apelul formulat împotriva

acestei hotărâri a fost respins de Curtea de Apel Haga la 14 martie 2017 (ECLI:NL:GHDHA:2017:535).

255. Curtea de apel a considerat că, în principiu, trebuie avută încredere că Statele Unite și Regatul Unit își respectă obligațiile care le revin în temeiul acestor tratate. Această încredere trebuia să fie infirmată numai în cazul în care ar fi apărut circumstanțe suficient de concrete pentru a se considera că nu era justificată.

256. În ceea ce privește colectarea datelor de telecomunicații de către NSA, nu existau indicii clare că NSA a acționat încălcând PIDCP. În măsura în care reclamanții au încercat să susțină că competențele legale conferite autorităților interne de legislația națională în materia colectării de date erau mai extinse decât cele permise în temeiul PIDCP, curtea de apel a considerat că reclamanții nu au explicat suficient în ce privință erau inadecvate legile și reglementările relevante.

257. În ceea ce privește colectarea datelor de către GCHQ, reclamanții nu și-au justificat afirmația potrivit căreia GCHQ a acționat încălcând Convenția.

258. Prin urmare, reclamanții nu au demonstrat că modul în care au acționat NSA și GCHQ era, cel puțin în principiu, în conflict cu PIDCP și cu Convenția. Deși nu putea fi exclus faptul că, într-un caz specific, NSA sau GCHQ sau orice alt serviciu de informații străin ar fi putut să fi colectat date într-un mod care să încalce PIDCP sau Convenția, principiul încrederii nu permitea ca această simplă posibilitate să implice faptul că serviciile de informații olandeze nu puteau primi date de la serviciile de informații străine fără a verifica, în fiecare caz în parte, că aceste date fuseseră obținute fără a încălca obligațiile relevante prevăzute în Convenție.

259. În sfârșit, curtea de apel a admis că, chiar dacă serviciile de informații străine acționau în limitele competențelor lor legale și ale obligațiilor lor statutare, faptul că aceste competențe statutare puteau fi mai extinse decât cele ale serviciilor de informații olandeze putea, în anumite circumstanțe, să ridice probleme. De exemplu, era posibil ca serviciile de informații olandeze să acționeze contrar Legii privind serviciile de informații și securitate din 2002 (sau spiritului acesteia) dacă ar fi primit în mod sistematic sau cu bună știință date de la serviciile de informații străine cu privire la rezidenții olandezi, deși nu ar fi putut colecta aceste date în virtutea propriilor competențe. În acest caz, restricțiile impuse serviciilor de informații de Legea din 2002 ar deveni literă moartă. Cu toate acestea, reclamanții nu au justificat și nici nu au prezentat probe că serviciile de informații olandeze au exploatat în mod sistematic sau conștient o astfel de discrepanță între dreptul olandez și dreptul străin.

260. Prin hotărârea din 7 septembrie 2018 (ECLI:NL:HR:2018:1434), Curtea Supremă (*Hoge Raad*) a respins recursul reclamanților, în care aceștia au denunțat, în principal, erorile curții de apel la interpretarea pretențiilor lor și întinderea sarcinii probei care le-a fost impusă.

D. Statele Unite ale Americii

261. Serviciile de informații din Statelor Unite operează programul Upstream în conformitate cu art. 702 din FISA.

262. Procurorul general și directorul serviciului de informații național emit certificări anuale care autorizează supravegherea persoanelor care nu sunt resortisanți americani despre care se crede în mod rezonabil că se află în afara Statelor Unite ale Americii. Aceștia nu trebuie să precizeze FISC persoanele specifice care nu sunt resortisanți americani care urmează să fie vizate și nu există nicio cerință de a demonstra că există motive probabile pentru a crede că persoana vizată este un agent al unei puteri străine. În schimb, certificatele emise în temeiul art. 702 identifică categoriile de informații care trebuie colectate, care trebuie să corespundă definiției legale a informațiilor operative străine. Certificatele care au obținut autorizare includ informații privind terorismul internațional și achiziționarea de arme de distrugere în masă.

263. În temeiul autorizației, NSA, cu asistența obligatorie a furnizorilor de servicii, copiază și caută fluxuri de trafic pe Internet pe măsură ce datele circulă pe Internet. Sunt colectate atât apelurile telefonice, cât și comunicațiile prin Internet. Înainte de luna aprilie 2017, NSA a obținut comunicații prin Internet care erau „către”, „de la” sau „despre” un selector țintit. O comunicație „către” sau „de la” reprezintă o comunicație pentru care expeditorul sau destinatarul era utilizator al unui selector țintit în temeiul art. 702. O comunicare „despre” reprezintă o comunicație în care selectorul țintit figurează în cadrul comunicației pe Internet obținute, dar ținta nu era în mod necesar un participant la comunicație. Prin urmare, colectarea de comunicații „despre” implică căutarea conținutului comunicațiilor care circulă pe Internet. Cu toate acestea, începând din aprilie 2017, NSA nu mai achiziționează sau nu mai colectează comunicații care sunt doar „despre” un obiectiv. În plus, NSA a declarat că, în cadrul acestei restricții, va elimina, cât mai curând posibil, marea majoritate a comunicațiilor prin Internet obținute anterior în cadrul Upstream.

264. Art. 702 impune guvernului să elaboreze proceduri de țintire și de minimizare care fac obiectul unui control al FISC.

265. Decretul nr. 12333, care a fost semnat în 1981, autorizează colectarea, păstrarea și difuzarea de informații obținute în cursul unei anchete legale de obținere de informații externe, contrainformații, privind traficul internațional de stupefiante sau în cursul unei anchete internaționale privind terorismul. Supravegherea resortisanților străini în temeiul Decretului nr. 12333 nu face obiectul reglementărilor naționale în temeiul FISA. Nu se cunoaște cantitatea de date colectate în temeiul Decretului nr. 12333 în raport cu cele colectate în temeiul art. 702.

ÎN DREPT

266. Părțile reclamante din cele trei cauze conexate s-au plâns de compatibilitatea cu art. 8 și art. 10 a trei regimuri distincte: regimul de interceptare în masă a comunicațiilor în temeiul art. 8 alin. (4) din Legea din 2000 privind competențele de investigare (*Regulation of Investigatory Powers Act* – „RIPA”), regimul de primire a informațiilor de la servicii de informații străine și regimul de obținere a datelor de comunicații de la furnizorii de servicii de comunicații („FSC”).

267. Înainte de a examina succesiv fiecare dintre aceste regimuri, Marea Cameră va examina mai întâi o chestiune preliminară.

I. ASPECTE PRELIMINARE ÎN FAȚA MARII CAMERE

268. În conformitate cu jurisprudența constantă a Curții, „cauza” trimisă în fața Marii Camere cuprinde în mod necesar toate aspectele cererii examinate anterior de Cameră în hotărârea sa. „Cauza” trimisă în fața Marii Camere este cererea, astfel cum a fost declarată admisibilă, precum și capetele de cerere care nu au fost declarate inadmisibile [*S.M. împotriva Croației* (MC), nr. 60561/14, pct. 216, 25 iunie 2020, și trimerile citate].

269. Părțile reclamante din prezenta cauză au introdus cererile în 2013, 2014 și, respectiv, în 2015. Plângerile respective priveau, în principal, activitățile de supraveghere ale statului în temeiul RIPA și al codurilor de bune practici aferente. Codurile de bune practici au fost modificate ulterior. Mai mult, Legea din 2016 privind competențele de investigare (*Investigatory Powers Act* – „IPA”) a primit avizul regal la 29 noiembrie 2016, iar dispozițiile sale au început să intre în vigoare din decembrie 2016. Noile regimuri de supraveghere prevăzute în IPA au fost în cea mai mare parte operaționale până în vara anului 2018. Dispozițiile Capitolului I al Părții I din RIPA au fost abrogate în cursul anului 2018.

270. Camera a examinat conformitatea cu Convenția a legii în vigoare la data la care a examinat admisibilitatea plângerilor părților reclamante, și anume a luat în considerare legea care era în vigoare la 7 noiembrie 2017. Întrucât aceasta este „cererea, astfel cum a fost declarată admisibilă”, Marea Cameră trebuie, de asemenea, să își limiteze examinarea la cadrul legislativ care era în vigoare la 7 noiembrie 2017. Această abordare se impune întrucât regimurile juridice introduse treptat ca urmare a intrării în vigoare a IPA sunt în prezent contestate în fața instanțelor interne și nu ar fi posibil ca Marea Cameră să examineze noua legislație înainte ca respectivele instanțe să fi avut mai întâi posibilitatea de a o face.

271. Părțile reclamante nu au contestat concluzia Camerei potrivit căreia Tribunalul cu competențe de investigare (*Investigatory Powers Tribunal* – „IPT”) oferă în prezent o cale de atac efectivă atât pentru plângerile individuale, cât și pentru cele generale în ceea ce privește conformitatea cu

Convenția a unui regim de supraveghere, iar Guvernul nu a contestat concluzia acesteia potrivit căreia, în circumstanțele cauzei, părțile reclamante au epuizat căile de atac interne în sensul art. 35 § 1 din Convenție. Prin urmare, niciunul dintre aceste aspecte nu trebuie examinat de Marea Cameră.

II. INTERCEPTAREA ÎN MASĂ A COMUNICAȚIILOR

A. Cu privire la competența teritorială

272. În ceea ce privește regimul prevăzut la art. 8 alin. (4), Guvernul nu a invocat nicio excepție în temeiul art. 1 din Convenție și nici nu a sugerat că interceptarea comunicațiilor a avut loc în afara competenței teritoriale a statului. În plus, în cursul ședinței în fața Marii Camere, Guvernul a confirmat în mod expres că nu a invocat nicio excepție pe acest motiv, întrucât cel puțin unele dintre părțile reclamante se aflau în mod clar sub competența teritorială a statului. Prin urmare, în scopul prezentei cauze, Curtea va pleca de la premisa că, în măsura în care părțile reclamante se plâng de regimul prevăzut la art. 8 alin. (4), faptele denunțate intră sub jurisdicția Regatului Unit.

B. Cu privire la pretinsa încălcare a art. 8 din Convenție

273. Părțile reclamante din toate cele trei cauze conexate s-au plâns de incompatibilitatea regimului de interceptare în masă a comunicațiilor cu art. 8 din Convenție, care prevede:

„1. Orice persoană are dreptul la respectarea vieții sale private și de familie, a domiciliului său și a corespondenței sale.

2. Nu este admis amestecul unei autorități publice în exercitarea acestui drept decât în măsura în care acest amestec este prevăzut de lege și dacă constituie o măsură care, într-o societate democratică, este necesară pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protejarea sănătății sau a moralei, ori protejarea drepturilor și libertăților altora.”

1. Hotărârea Camerei

274. Camera a recunoscut în mod expres ca statele se bucură de o marjă largă de apreciere pentru a decide ce tip de regim de interceptare este necesar pentru a proteja securitatea națională, dar a considerat că marja de apreciere conferită acestora în utilizarea unui regim de interceptare trebuie în mod necesar să fie mai restrânsă. În această privință, Curtea a amintit că a identificat șase „garanții minime” care ar trebui stabilite prin lege pentru a evita abuzurile de putere: natura infracțiunilor care pot da naștere unui mandat de interceptare, definirea categoriilor de persoane susceptibile de a le fi interceptate comunicațiile, limitarea duratei interceptării, procedura care trebuie urmată pentru examinarea, utilizarea și stocarea datelor obținute, măsurile de precauție care trebuie luate atunci când comunică datele altor părți și circumstanțele în care pot fi șterse sau distruse datele interceptate.

Aceste garanții, care au fost stabilite pentru prima dată în *Huvig împotriva Franței*, 24 aprilie 1990, pct. 34, seria A nr. 176 B, și în *Kruslin împotriva Franței*, 24 aprilie 1990, seria A nr. 176-A, au fost aplicate în mod curent de Curte în jurisprudența sa privind interceptarea comunicațiilor și în două cauze privind în mod specific interceptarea în masă a comunicațiilor [*Weber și Saravia împotriva Germaniei* (dec.), nr. 54934/00, CEDO 2006-XI; *Liberty și alții împotriva Regatului Unit*, nr. 58243/00, 1 iulie 2008].

275. În opinia Camerei, decizia de a utiliza un regim de interceptare în masă se încadrează în marja de apreciere acordată statelor contractante. Camera a evaluat funcționarea regimului de interceptare în masă din Regatul Unit în raport cu cele șase garanții minime prevăzute la punctul anterior. Întrucât primele două garanții nu se aplică direct interceptării în masă, Camera a reamintit aceste garanții, ținând seama, în primul rând, de caracterul suficient de clar al motivelor pentru emiterea unui mandat; în al doilea rând, dacă dreptul intern oferă cetățenilor indicații adecvate privind circumstanțele în care comunicațiile lor ar putea fi interceptate; și, în al treilea rând, dacă dreptul intern oferă cetățenilor indicații adecvate privind circumstanțele în care comunicațiile lor ar putea fi selectate spre examinare. În plus, în lumina jurisprudenței recente (inclusiv *Roman Zakharov împotriva Rusiei*, nr. 47143/06, CEDO 2015), Camera a ținut seama, de asemenea, de modalitățile de control al punerii în aplicare a măsurilor de supraveghere secretă, existența unor mecanisme de notificare și orice căi de atac prevăzute de dreptul intern.

276. A identificat următoarele două domenii de interes în cadrul regimului prevăzut la art. 8 alin. (4): în primul rând, lipsa supravegherii în ceea ce privește selecția canalelor de transmisie vizate de interceptare, selectorii utilizați pentru filtrarea comunicațiilor interceptate și procesul prin care analiștii selectează comunicațiile interceptate spre examinare și, în al doilea rând, lipsa oricăror garanții reale aplicabile căutării și selectării datelor de comunicații aferente. Având în vedere controlul independent asigurat de Comisarul pentru interceptarea comunicațiilor („Comisarul IC”) și de IPT, precum și anchetele independente ample care au urmat dezvăluirilor lui Edward Snowden, Camera a considerat că Regatul Unit nu a abuzat de competențele sale de interceptare în masă. Cu toate acestea, în lumina deficiențelor sus-menționate, a hotărât, cu majoritate de voturi, că regimul de interceptare în masă nu îndeplinea cerința privind „calitatea legii” și nu era capabil să mențină „ingerința” la ceea ce era „necesar într-o societate democratică”.

2. Argumentele părților

(a) Părțile reclamante

277. Părțile reclamante au susținut că interceptarea în masă nu era, în principiu, nici necesară, nici proporțională în sensul art. 8 din Convenție și,

ca atare, nu se încadra în marja de apreciere a statului. Hotărârea pronunțată în cauza *Szabó și Vissy împotriva Ungariei*, nr. 37138/14, 12 ianuarie 2016, sugera că o măsură de supraveghere secretă trebuie să fie „strict necesară” pentru protejarea instituțiilor democratice și obținerea de informații esențiale și nu s-a demonstrat că interceptarea în masă îndeplinește acest criteriu. Deși era, fără îndoială, o capacitate utilă, din jurisprudența Curții reiese în mod clar că nu toate elementele utile serviciilor de informații sunt permise într-o societate democratică [*S. și Marper împotriva Regatului Unit* (MC) nr. 30562/04 și 30566/04, CEDO 2008].

278. Potrivit părților reclamante, au existat ingerințe separate în dreptul la respectarea vieții private și a corespondenței, prevăzut la art. 8, prin interceptarea unei comunicații (datele legate de conținut și/sau datele de comunicații aferente), stocarea, prelucrarea automatizată și examinarea acesteia. Deși admit că a existat o ingerință „substanțială” atunci când au fost examinate comunicațiile interceptate, consideră că este greșit să se sugereze că nu a existat nicio ingerință „semnificativă” înainte de acel moment. Dimpotrivă, jurisprudența Curții a arătat că și stocarea informațiilor cu caracter personal de către stat constituie o ingerință gravă în drepturile unei persoane în temeiul art. 8 din Convenție [a se vedea, de exemplu, *Rotaru împotriva României* (MC), nr. 28341/95, CEDO 2000 V, și *S. și Marper*, citată anterior]. Această situație se produce, în special, atunci când datele fac obiectul prelucrării automate. De fapt, în măsura în care puterea de prelucrare și învățarea automată au avansat rapid, stocarea și prelucrarea electronică a datelor ar putea fi, în sine, extrem de intruzivă, fără să fie necesar ca vreun conținut subiacent sau date de comunicații aferente să fie vizualizate de o persoană. În această privință, părțile reclamante au susținut că, contrar „supei amorfe” invocate de Guvern (infra, pct. 288), datele colectate erau mai degrabă asemănătoare unei „biblioteci bine organizate și indexate în care se poate găsi rapid orice se dorește”. Disponibilitatea prelucrării automate ridică probleme deosebit de grave în ceea ce privește protecția vieții private și nu minimizează, astfel cum susținea Guvernul, riscurile de intruziune.

279. În cazul în care Marea Cameră ar considera că funcționarea unui regim de interceptare în masă se încadrează în marja de apreciere a statului, părțile reclamante au susținut că regimul prevăzut la art. 8 alin. (4) nu era prevăzut de lege. În primul rând, RIPA era inutil de complexă, fapt recunoscut de toți evaluatorii independenți, astfel încât, în realitate, natura reală și amploarea supravegherii efectuate au devenit clare doar în urma dezvăluirilor lui Edward Snowden. În plus, procedurile „nepublice” fuseseră stabilite chiar de GCHQ, nu erau accesibile și nici aprobate de Parlament, făceau, în cadrul politicii interne, obiectul unor schimbări după voia executivului și nu aveau caracter obligatoriu. Prin urmare, părțile reclamante au susținut că nu ar trebui să intre în discuție în analiza Curții.

280. În ceea ce privește evaluarea previzibilității, părțile reclamante au susținut că schimbările survenite atât în societate, cât și în tehnologie au

condus la necesitatea ca Curtea să își actualizeze abordarea existentă – și să consolideze garanțiile necesare – pentru a se asigura că drepturile conferite de Convenție rămân concrete și efective. Jurisprudența existentă a Curții privind interceptarea în masă a derivat din decizia pronunțată în *Weber și Saravia* (citată anterior), dar această decizie datează din 2006, când lumea era diferită. Telefoanele inteligente erau rudimentare și aveau o funcționalitate limitată, aplicația Facebook era utilizată în principal de studenți și Twitter abia apăruse. Astăzi oamenii își trăiesc o mare parte a vieții lor on-line, utilizând Internetul să comunice, să transmită idei, să facă cercetare, să stabilească relații, să caute sfaturi medicale, să țină jurnale, să organizeze călătorii, să asculte muzică, să se orienteze și să facă tranzacții financiare. În plus, tehnologia modernă a generat o cantitate enormă de date de comunicații, care sunt foarte revelatoare, chiar dacă conținutul aferent nu a fost examinat, și care sunt structurate astfel încât calculatoarele să le poată prelucra și să poată căuta modele mai rapid și mai eficient decât căutările similare asupra conținutului. De exemplu, telefoanele mobile generează în mod constant date de comunicații, întrucât contactează rețeaua mobilă, realizând o înregistrare a locației telefonului, permițând urmărirea mișcărilor utilizatorului și dezvăluind modul în care acesta utilizează Internetul.

281. În opinia părților reclamante, era necesar ca garanțiile actualizate și consolidate să includă autorizarea judiciară prealabilă independentă a mandatelor, alegerea selectorilor și selectarea materialului interceptat spre examinare. În plus, în cazul în care selectorii sau termenii de căutare făceau trimitere la o anumită persoană, e necesar să existe probe obiective ale unei bănuieli întemeiate în privința persoanei respective. În cele din urmă, ar trebui să existe, de asemenea, o notificare ulterioară cu privire la orice obiectiv de supraveghere clar definit, în cazul în care acest lucru nu ar aduce prejudicii substanțiale interesului public.

282. Părțile reclamante au identificat o serie de elemente ale regimului de interceptare în masă din Regatul Unit pe care le consideră inadecvate. În primul rând, supravegherea nu este autorizată de un organ independent, cu atât mai puțin judiciar. Faptul că autorizarea judiciară poate să nu constituie în sine o protecție suficientă împotriva abuzurilor nu susține concluzia că nu este necesară. În plus, părțile reclamante au considerat că ar trebui să existe și o aprobare independentă, dacă nu judiciară, a selectorilor și a termenilor de căutare utilizați de GCHQ. Cu toate acestea, nici canalele de transmisie care urmau să fie interceptate, nici selectorii puternici nu sunt menționați în mandat.

283. În al doilea rând, distincția dintre comunicațiile interne și cele externe nu doar că este insuficient definită, ci și lipsită de sens, majoritatea comunicațiilor fiind susceptibile de a intra în categoria „externe”. În opinia părților reclamante, ar fi fost posibil să se asigure o protecție mai semnificativă a comunicațiilor interne. De exemplu, în Suedia, toate

comunicațiile interne trebuie să fie distruse imediat în cazul în care sunt descoperite.

284. În al treilea rând, garanțiile sunt limitate pentru conținutul comunicațiilor persoanelor cunoscute ca fiind în Insulele Britanice și practic nu există garanții pentru datele de comunicații aferente acestora. GCHQ este în măsură să păstreze toate datele de comunicații aferente obținute în cadrul regimului de interceptare în masă, sub rezerva limitării capacității sale de stocare și a perioadei maxime de păstrare. Aceste date – extrem de intruzive – pot fi căutate în funcție de un factor atribuit unei persoane cunoscute ca fiind în Insulele Britanice, fără a fi necesar ca ministrul să certifice mai întâi că căutarea era necesară și proporțională.

285. În al patrulea rând, regimul nu specifică, în drept și în detaliu, scopul în care pot fi examinate materialele și, potrivit Comisiei pentru Informații și Securitate a Parlamentului (*Intelligence and Security Committee of Parliament* – „ISC”), descrierea materialelor din certificatul ministerial este „generică”.

286. În sfârșit, părțile reclamante au susținut că Comisarul IC asigură supravegherea doar cu normă parțială și, cu resurse limitate, nu este suficient pentru a garanta o supraveghere semnificativă și solidă. Eficacitatea IPT este, de asemenea, limitată, întrucât nu poate oferi o cale de atac pentru lipsa unei autorizări judiciare prealabile și, în orice caz, trebuie ca persoanele să aibă un anumit temei pentru a crede că au făcut obiectul unei supravegheri secrete înainte ca IPT să admită plângerea lor.

(b) Guvernul

287. Guvernul susține că informațiile obținute în cadrul regimului de interceptare în masă erau esențiale pentru protecția Regatului Unit împotriva amenințărilor la adresa securității naționale. Nu numai că informațiile i-au permis să descopere amenințări necunoscute până la acel moment, ci i-au permis, de asemenea, să supravegheze ținte cunoscute în afara competenței sale teritoriale. Caracterul imprevizibil al rutelor comunicațiilor electronice (și faptul că aceste comunicații erau defalcate în pachete care puteau fi transmise prin diferite rute) însemna că, pentru a obține chiar și o mică parte din comunicațiile unor ținte cunoscute din străinătate, era necesar să fie interceptate toate comunicațiile care circulau printr-o selecție de canale de transmisie. Competența de a intercepta date în masă a făcut obiectul unei analize detaliate și repetate de către o serie de organe independente în ultimii ani și a existat o opinie unanimă potrivit căreia nu exista „nici o alternativă” [...] sau o combinație de alternative suficiente care să se substituie competenței de a intercepta date în masă”. Potrivit Guvernului, statelor ar trebui să li se acorde de drept o marjă largă de apreciere atunci când apreciază ce sisteme ar fi necesare pentru a proteja comunitatea generală împotriva unor astfel de amenințări, iar prin supunerea acestor sisteme unui control, Curtea ar trebui să se asigure că nu aduce atingere eficacității unui mijloc de obținere

a unor informații care să salveze vieți, și care nu ar putea fi colectate în niciun alt mod.

288. Guvernul susține că interceptarea comunicațiilor în cadrul sistemului de interceptare în masă nu ar conduce la o ingerință semnificativă în drepturile unei persoane în temeiul art. 8 decât în cazul în care comunicațiile acesteia fie ar fi selectate spre examinare (și anume incluse într-un index de comunicații din care un analist poate alege elemente care să fie inspectate), fie ar fi examinate efectiv de un analist. Nu se poate afirma că drepturile unei persoane au fost încălcate în cel mai mic grad în cazul în care o copie a unei comunicații fie a fost eliminată aproape instantaneu, fie a fost păstrată cel mult câteva zile într-o „supă amorfă” generală de date; cu alte cuvinte, dacă a făcut obiectul unei căutări folosind selectori și întrebări, dar nu a fost examinată sau utilizată. Majoritatea covârșitoare a comunicațiilor care circulă prin fiecare cablu interceptat nu ar putea fi „selectate spre examinare” și, prin urmare, ar trebui să fie eliminate.

289. În ceea ce privește garanțiile necesare, Guvernul este de acord cu poziția Camerei potrivit căreia e oportun ca un regim de interceptare în masă să fie evaluat pe baza aceluiași norme care au fost elaborate de Curte în cauzele referitoare la interceptarea ținută a comunicațiilor. De asemenea, Guvernul este de acord în mare măsură cu opinia Camerei cu privire la regimul prevăzut la art. 8 alin. (4) în raport cu aceste norme. Guvernul a reamintit că nu exista posibilitatea ca o comunicație să fie examinată de un analist decât în cazul în care a fost selectată spre examinare, în urma procesului de filtrare automată; selectarea și orice examinare ulterioară sunt supuse unui control foarte minuțios; nu poate fi întocmit niciun raport de informații cu privire la date de comunicații sau comunicații decât în cazul în care acestea au fost examinate de un analist; art. 16 alin. (2) din RIPA impune ca ministrul să certifice necesitatea și proporționalitatea căutării conținutului de comunicații, potrivit unui factor legat de o persoană despre care se cunoaște că se află în Insulele Britanice; este necesar ca funcțiile de supraveghere combinate ale ISC, Comisarului IC și ale IPT să îndeplinească cerințele Convenției. În toate etapele procesului de interceptare în masă, garanțiile aplicabile sunt construite în jurul conceptelor de necesitate și proporționalitate consacrate de Convenție. Aceste principii fundamentale guvernează, în primul rând, obținerea materialelor, examinarea, tratarea, stocarea, divulgarea, păstrarea și ștergerea acestora.

290. În ceea ce privește acele aspecte ale regimului care, potrivit Camerei, nu oferă garanții adecvate împotriva abuzurilor, Guvernul a furnizat clarificări suplimentare. În primul rând, deși recunoaște că mandatul nu precizează canalele de transmisie care urmează să fie vizate, întrucât există obstacole și dificultăți considerabile în includerea acestor informații în mandat, acesta cuprinde totuși o descriere a ceea ce urmează să implice interceptarea și o descriere a tipurilor de canale de transmisie care urmează să fie interceptate. Comisarul IC este informat periodic de către GCHQ cu

privire la baza prin care au fost selectate canalele de transmisie spre interceptare.

291. În al doilea rând, Guvernul clarifică faptul că alegerea selectorilor este în fapt controlată cu atenție. Ori de câte ori este adăugat în sistem un nou selector, analistul care îl adăugă trebuie să completeze un registru scris, explicând de ce este necesară și proporțională aplicarea selectorului în scopurile menționate în certificatul emis de ministrul internelor. Acest lucru se realizează prin selectarea textului dintr-un meniu vertical, urmat de adăugarea, de către analist, a unui text liber, explicând motivul pentru care este necesar și proporțional să se efectueze căutarea. În cazul unui „selector puternic”, trebuie ca analistul să explice, de exemplu, justificarea pentru solicitarea de a examina comunicațiile unei anumite ținte, modul în care selectorul are legătură cu metoda de comunicare a țintei și motivul pentru care selectarea comunicațiilor relevante nu implică un grad inacceptabil de intruziune colaterală în viața privată. În cazul unei noi „interogări complexe”, analistul trebuie să elaboreze criteriile de selecție cele mai în măsură să identifice comunicațiile cu informații utile și, în mod similar, să explice motivele pentru care sunt justificate criteriile și motivul pentru care utilizarea lor este necesară și proporțională în scopurile indicate în certificatul emis de ministru. Selectorii utilizați pentru a specifica sau pentru a descoperi ținta pot fi utilizați maxim 3 luni înainte de a se impune controlul acestora.

292. Orice selector trebuie să fie proporțional și cât mai precis posibil pentru a selecta materialele minime necesare în scopul colectării de informații. În cazul în care, prin analiză, se stabilește că selectorii nu sunt utilizați de ținta vizată, trebuie să fie luate măsuri prompte pentru a-i elimina din sistemele relevante. Utilizarea selectorilor trebuie să fie înregistrată într-o locație aprobată care permite să fie auditate; este creat un registru al selectorilor în uz care să poată fi verificat, astfel încât Comisarul IC să îl poată controla. Controlul independent ferm asupra selectorilor și criteriilor de căutare constituie așadar una din competențele Comisarului IC: până la momentul raportului său din 2014, acesta pusese în aplicare sisteme și procese pentru a se asigura că totul funcționa bine în realitate și, în urma hotărârii Camerei, Guvernul a colaborat cu Biroul Comisarului IC pentru a asigura o supraveghere sporită a selectorilor și a criteriilor de căutare, în temeiul IPA. Cu toate acestea, Guvernul afirmă că nu este posibil ca fiecare selector să aibă o autorizație judiciară prealabilă fără a modifica în mod fundamental capacitatea sistemului de a descoperi și de a respinge amenințările. Sistemele GCHQ tratează în mod necesar mii de selectori care, uneori, trebuie să fie modificați prompt pentru a ține pasul cu investigațiile în desfășurare și cu descoperirea amenințărilor.

293. Comunicațiile cărora li se aplică doar procesul „selectorului puternic” sunt imediat eliminate în cazul în care nu corespund selectorului puternic. Comunicațiile pentru care se aplică și procesul de „interogare complexă” sunt păstrate câteva zile, pentru a permite desfășurarea procesului, fiind apoi șterse

automat în cazul în care nu sunt selectate spre examinare. Comunicațiile selectate spre examinare pot fi păstrate numai în cazul în care măsura e necesară și proporțională. Poziția implicită era aceea că perioada de păstrare a comunicațiilor selectate nu depășește câteva luni, după care sunt șterse automat (deși materialele sunt citate în raportarea informațiilor, rapoartele sunt păstrate). În circumstanțe excepționale, se poate lua în considerare păstrarea comunicațiilor selectate pentru o perioadă mai îndelungată, astfel cum prevede Codul de bune practici privind interceptarea comunicațiilor („Codul IC”).

294. Guvernul reamintește că e necesar ca toți analiștii care examinează materialele selectate să fie autorizați în mod special în acest sens și să beneficieze de formare periodică obligatorie, inclusiv formare privind cerințele de necesitate și proporționalitate. De asemenea, sunt evaluați. Înainte de a examina materialul, aceștia creează un registru în care indică motivele pentru care e necesar accesul la materiale, motivul pentru care accesul este conform cu certificatul ministerial și cu cerințele RIPA și motivul pentru care este proporțional (inclusiv considerații privind orice circumstanțe susceptibile să conducă la un anumit grad de încălcare a vieții private). În cazul în care nu este creat un astfel de registru, sistemele GCHQ nu permit accesul la materiale.

295. În ceea ce privește garanțiile aplicabile datelor de comunicații aferente, Guvernul susține că examinarea conținutului celor mai sensibile și private comunicații implică întotdeauna un grad mai mare de intruziune decât examinarea datelor de comunicații aferente, indiferent dacă aceste date sunt agregate pentru a oferi o imagine detaliată a locului în care se află o persoană, a site-urilor Internet pe care le-a vizitat sau cu cine a ales să comunice. Pe această bază, normele care reglementează conținutul trebuie să fie mai exigente decât cele care reglementează datele de comunicații aferente. Cu toate acestea, Guvernul admite că ministrul trebuie să fie obligat să certifice necesitatea examinării datelor de comunicații aferente în temeiul unui mandat colectiv, potrivit unui regim analog (chiar dacă nu identic) cu regimul de certificare în vigoare pentru conținutul comunicațiilor, în temeiul art. 16 din RIPA. Noul cod de bune practici urmează să fie modificat în acest sens.

296. Cu toate acestea, până la acel moment, datele de comunicații sunt supuse aceluiași proces inițial de filtrare precum conținutul, prin care sistemele de prelucrare ale GCHQ elimină automat anumite tipuri de comunicații în timp cvasi-real. Ulterior, acestea sunt supuse, prin mijloace automatizate, unor interogări simple sau complexe. Cu toate acestea, există două diferențe principale între tratamentul conținutului și tratamentul datelor de comunicații aferente. În primul rând, garanțiile prevăzute la art. 16, care prevede că, pentru a fi examinate, trebuie ca materialele să intre în domeniul de aplicare al certificatului ministrului și nu pot fi selectate în funcție de un factor legat de o persoană despre care se știe că se află pentru moment în Insulele Britanice pentru a-i identifica comunicațiile – se aplică doar

conținutului. Potrivit Guvernului, nu este posibil să se aplice această garanție datelor de comunicații aferente. Sunt făcute mult mai multe interogări ale datelor de comunicații (până la câteva mii dintr-o săptămână), iar într-un număr mare de cazuri, identitatea persoanei la care se referă datele nu este cunoscută. În plus, datele de comunicații aferente nu au adeseori decât o calitate temporală, iar obligația de a amâna efectuarea căutărilor unor astfel de date până la obținerea unei mandat individual riscă să afecteze în mod grav utilitatea acestora din punct de vedere al informației. Nu ar fi posibil să se solicite ministrului să certifice necesitatea și proporționalitatea în fiecare caz în parte, înainte de efectuarea căutărilor.

297. În al doilea rând, datele de comunicații aferente care nu sunt selectate spre examinare nu sunt imediat eliminate. Principalul motiv este acela că datele de comunicații sunt utilizate în mare măsură pentru a descoperi amenințări sau ținte despre care GCHQ ar fi putut să nu fi avut cunoștință anterior. Prin urmare, e necesară o activitate analitică mai intensă, pe o perioadă lungă de timp, pentru a descoperi „necunoscutele necunoscute”. O astfel de descoperire poate implica un exercițiu de fragmentare a unor mici elemente disparate de date de comunicații pentru a forma un „puzzle” care să reveleze o amenințare și poate include posibila examinare a unor elemente care, inițial, nu par a fi de interes pentru serviciile de informații. Eliminarea datelor de comunicații neselectate imediat sau numai după câteva zile ar face ca acest exercițiu să fie imposibil de realizat.

298. Cu toate acestea, Guvernul confirmă că, înainte ca un analist să poată examina toate datele de comunicații, acesta trebuie să completeze un registru în care să explice motivul pentru care este necesar și proporțional să facă acest lucru, în exercitarea funcțiilor statutare ale GCHQ. Prin urmare, este întocmit un registru verificabil care stabilește justificarea examinării datelor, iar aceste registre sunt disponibile pentru inspecție. În plus, nu este posibilă raportarea informațiilor pe baza datelor de comunicații decât în momentul și în măsura în care datele au fost examinate. În cele din urmă, comunicațiile aferente pot fi păstrate numai în cazul în care acest lucru este necesar și proporțional, pe o perioadă maximă de câteva luni, cu excepția cazului în care există o circumstanță excepțională pentru a le menține pe o perioadă mai lungă de timp. În caz contrar, datele de comunicații aferente sunt șterse automat după expirarea perioadei maxime de timp.

299. În sfârșit, având în vedere hotărârea Camerei, Guvernul a confirmat că este gata să ia măsuri pentru a se asigura că, în cazul în care datele fără conținut urmează să fie selectate spre examinare în legătură cu o persoană despre care se crede că se află în Insulele Britanice, selecția trebuie să fie certificată de ministru ca fiind necesară și proporțională, pe o bază tematică specifică. În așteptarea introducerii unui regim de certificare „tematic”, prin intermediul unor modificări aduse codului care reglementează interceptarea comunicațiilor în temeiul IPA, GCHQ colaborează cu Biroul Comisarului IC pentru a genera un instrument de gestionare a informațiilor care să fie utilizat

de Comisarul IC pentru a consolida supravegherea ulterioară efectivă a datelor de comunicații aferente. În special, GCHQ a adus modificări sistemelor sale astfel încât, în orice caz, în situația în care un analist intenționează să selecteze date secundare spre examinare referitoare la o persoană despre care se crede că se află în Insulele Britanice prin trimitere la un factor legat de persoana respectivă, această situație este semnalată împreună cu motivarea care justifică selectarea datelor relevante.

3. *Observațiile terților intervenienți*

(a) **Guvernul francez**

300. Guvernul francez a susținut că, în fața unor amenințări precum infracționalitatea internațională și transfrontalieră și având în vedere complexitatea tot mai mare a tehnologiilor comunicațiilor, supravegherea strategică în masă a comunicațiilor este de o importanță vitală pentru state în protejarea societății democratice. În plus, este greșit să se presupună că interceptarea în masă constituie o intruziune mai gravă în viața privată a unei persoane decât o interceptare țintită, care, prin natura sa, este mai probabil să conducă la obținerea și la examinarea unui volum mare de comunicații ale subiectului. În opinia sa, nu există niciun motiv pentru care criteriile stabilite de Curte în *Weber și Saravia* (citată anterior) să nu poată fi considerate la fel de relevante pentru supravegherea eficientă a interceptării și prelucrării datelor în cadrul unui regim de interceptare în masă. Cu toate acestea, criteriile respective ar trebui aplicate în contextul unei evaluări globale, evaluând eventualele deficiențe în raport cu garanțiile existente și cu eficiența garanțiilor împotriva abuzurilor.

301. Nu există nicio justificare pentru a adăuga la aceste criterii necesitatea de a avea o „bănuială întemeiată”. În general, autoritățile nu sunt în măsură să știe anterior persoanele ale căror comunicații electronice ar putea fi utile pentru a le monitoriza în interesul ordinii publice sau al securității naționale, iar o astfel de cerință privează măsura de supraveghere de orice interes operațional. În plus, în opinia guvernului francez, nu este necesar ca o autoritate judiciară să fie implicată în autorizarea unor astfel de operațiuni de informații sau să efectueze un control *a posteriori*, cu condiția ca autoritatea de autorizare să fie independentă de executiv, organul de supraveghere să fie investit cu suficiente puteri și competențe pentru a exercita un control efectiv și continuu, iar cele două organe să fie independente unul față de celălalt.

302. În sfârșit, guvernul intervenient a susținut că metadatele sunt, prin natura lor, mai puțin intruzive decât conținuturile, întrucât conțineau în mod clar informații mai puțin sensibile despre comportamentul și viața privată a persoanei în cauză. Această opinie a fost susținută de raportul Comisiei de la Veneția (supra, pct. 196-201) și de CJEU în *Digital Rights Ireland* (supra, pct. 209-213).

(b) Guvernul Regatului Țărilor de Jos

303. Guvernul Regatului Țărilor de Jos a susținut, de asemenea, că interceptarea în masă este necesară pentru a identifica amenințări necunoscute la adresa securității naționale. Pentru a proteja securitatea națională, serviciile de informații au nevoie de instrumente pentru a investiga amenințările emergente în timp util și în mod eficient. În acest scop, au nevoie de competențe necesare care să le permită să detecteze și/sau să prevină nu numai activități teroriste (cum ar fi planificarea atacurilor, recrutarea, propaganda și finanțarea), ci și activități cibernetice intruzive ale actorilor statali sau nestatali care ar viza destabilizarea democrației (de exemplu, prin influențarea alegerilor naționale sau obstrucționarea investigațiilor organizațiilor naționale și internaționale. Un exemplu în acest sens a fost tentativa de piratare a anchetei privind utilizarea armelor chimice în Siria de către Organizația pentru Interzicerea Armelor Chimice de la Haga). În plus, dependența tot mai mare a sectoarelor vitale de infrastructurile digitale înseamnă că astfel de sectoare, inclusiv managementul apei, energia, telecomunicațiile, transporturile, logistica, porturile și aeroporturile sunt din ce în ce mai vulnerabile la atacurile cibernetice. Consecințele perturbărilor din aceste sectoare ar avea un impact profund asupra societății, dincolo de daunele monetare substanțiale.

304. Un factor care complică toate aceste aspecte îl constituie dezvoltarea de noi mijloace de comunicare digitală și creșterea exponențială a datelor transmise și stocate la nivel mondial. În multe cazuri, natura și originea unei anumite amenințări nu sunt cunoscute, iar utilizarea interceptării țintite nu este fezabilă. Cu toate acestea, deși interceptarea în masă nu este definită la fel de strict ca interceptarea țintită, nu a fost niciodată complet nețintită. Dimpotrivă, a fost aplicată în scopuri specifice.

305. În opinia guvernului intervenient, nu este necesar să se impună garanții minime suplimentare sau actualizate; cele identificate anterior de Curte sunt suficient de robuste și „rezistente la proba timpului”. Cerințele suplimentare propuse de părțile reclamante în fața Camerei – în special cerința de a demonstra „bănuiala întemeiată” – ar reduce în mod inacceptabil eficiența serviciilor de informații, fără a oferi o protecție suplimentară semnificativă drepturilor fundamentale ale persoanelor.

306. În plus, potrivit guvernului intervenient, este relevant în continuare să se facă distincția între conținut și datele de comunicații, întrucât conținutul comunicațiilor este susceptibil să fie mai sensibil decât datele de comunicații. Guvernul intervenient este de acord, de asemenea, cu opinia Camerei potrivit căreia este greșit să se presupună în mod automat că interceptarea în masă constituie o intruziune mai mare în viața privată a unei persoane decât interceptarea țintită, întrucât, în cazul unei interceptări țintite, este probabil ca toate sau aproape toate comunicațiile interceptate să fie analizate. Acest lucru nu este valabil în cazul interceptării în masă, caz în care restricțiile

privind examinarea și utilizarea datelor determină caracterul intruziv al interceptării asupra drepturilor fundamentale ale persoanelor.

307. În sfârșit, guvernul intervenient a susținut că orice cerință de explicare sau de justificare a selectorilor sau a criteriilor de căutare în autorizație restrânge în mod grav eficiența interceptării în masă, având în vedere gradul ridicat de incertitudine cu privire la sursa unei amenințări. Supravegherea *a posteriori* oferă garanții suficiente.

(c) Guvernul Regatului Norvegiei

308. Guvernul norvegian susține că, în ceea ce privește decizia statelor de a introduce și de a opera o formă de regim de interceptare în masă în scopuri de securitate națională, marja de apreciere trebuie să fie largă. Acest lucru se datorează faptului că este necesar ca serviciile de informații să țină pasul cu evoluțiile rapide din domeniul tehnologiei informației și comunicațiilor. Actorii ostili și-au schimbat dispozitivele și identitățile digitale într-un ritm care îngreunează urmărirea lor în timp. De asemenea, este dificil să se descopere și să se contracareze operațiunile cibernetice ostile în timp util, fără instrumente capabile să identifice anomalii și semnături relevante. Prin urmare, este, fără îndoială, clar că sunt necesare capacități moderne, cum ar fi interceptarea în masă, pentru a identifica amenințări necunoscute care operează în domeniul digital și pentru a permite serviciilor să descopere și să urmărească amenințările relevante în materie de informații.

309. În opinia guvernului norvegian, supravegherea Curții trebuie să se bazeze pe o evaluare globală a caracterului adecvat și suficient al garanțiilor procedurale împotriva abuzurilor. Trebuie să fie evitate cerințele absolute. De asemenea, nu trebuie să fie aplicate criterii care să submineze indirect marja largă de apreciere acordată statelor atunci când decid aplicarea unui regim de interceptare în masă din motive de securitate națională. Cerință de a avea o „bănuială întemeiată” sau de a transmite o „notificare ulterioară” ar avea acest efect.

310. În cele din urmă, guvernul intervenient a încurajat Curtea să se abțină de la a importa concepte și criterii de la CJUE. În primul rând, la momentul faptelor, 19 state contractante ale Consiliului Europei nu erau membre ale Uniunii Europene. În al doilea rând, deși Convenția și Carta drepturilor fundamentale au multe trăsături comune, există, de asemenea, diferențe, în special art. 8 din Cartă, care consacră dreptul la protecția datelor cu caracter personal. De asemenea, CJUE a formulat „proportionalitatea” în mod diferit, utilizând metoda „strictei necesități” care nu se compară cu cea utilizată de Curte.

(d) Raportorul special al Organizației Națiunilor Unite pentru promovarea dreptului la libertatea de opinie și de exprimare

311. Raportorul special susține că supravegherea aruncă o umbră asupra comunicațiilor, astfel încât persoanele fizice ar putea să se abțină de la a se

implica în activități protejate în temeiul dreptului internațional al drepturilor omului. Aceasta nu înseamnă că toate operațiunile de supraveghere constituie o încălcare a legii drepturilor omului, unele putând fi tolerabile atunci când sunt îndeplinite condițiile de legalitate, necesitate și legitimitate. Cu toate acestea, toate tipurile de supraveghere necesită o evaluare riguroasă a conformității acestora cu normele de drept internațional în materie de drepturile omului.

312. În opinia Raportorului special, dreptul la viață privată trebuie să fie protejat nu numai ca drept fundamental, independent de toate celelalte, ci și pentru a proteja alte drepturi, cum ar fi libertatea de opinie și de exprimare, care depind de o sferă privată pentru a beneficia de acestea. Astfel cum a indicat Raportorul special în raportul său din 2015, sistemele de supraveghere riscă să submineze dreptul de a formula o opinie, întrucât teama de divulgare nedorită a activităților on-line poate descuraja persoanele fizice să acceseze informații.

313. Raportul Înaltului Comisar al ONU s-a opus ca metadatele să fie diferențiate de conținut atunci când este examinată gravitatea ingerinței în drepturile protejate în temeiul Pactului Internațional cu privire la Drepturile Civile și Politice („PIDCP”). Raportul din 2014 a indicat faptul că agregarea metadatelor prin intermediul supravegherii guvernamentale poate dezvălui mai multe detalii private despre o persoană decât poate chiar o comunicație privată. Raportorul special a indicat, de asemenea, că distincția dintre comunicațiile interne și cele externe poate fi contrară PIDCP. PIDCP impune statelor obligația de a respecta și de a asigura toate drepturile aferente tuturor persoanelor aflate sub jurisdicția lor, iar în ultimul său comentariu general, Comitetul pentru drepturile omului a interpretat acest standard ca incluzând activitățile statului care au un impact direct asupra drepturilor în afara propriului său teritoriu.

314. În sfârșit, Raportorul special a subliniat importanța garanțiilor pentru protecția împotriva abuzurilor, în special necesitatea ca o instanță, un tribunal sau un alt organ decizional să supravegheze aplicarea măsurii ingerinței, notificarea ulterioară a subiecților supravegherii, publicarea informațiilor privind domeniul de aplicare al tehnicilor și competențelor de supraveghere și dreptul la căi de atac efective în cazul apariției abuzurilor.

(e) Acces Now

315. Access Now a susținut că supravegherea în masă în discuție în prezenta cauză nu respectă PIDCP și Principiile internaționale privind aplicarea drepturilor omului în cazul supravegherii comunicațiilor, întrucât Regatul Unit nu a demonstrat că o astfel de supraveghere este strict necesară sau proporțională. A susținut, de asemenea, că programele de supraveghere nu trebuie să fie luate în considerare în mod independent, ci trebuie privite în raport cu ansamblul activităților de supraveghere ale unei națiuni ca învățare automată, prin care algoritmi matematici ar putea trage concluzii din

colecțiile de date, măbind caracterul invaziv al seturilor de volume mari de date și al extragerii de date.

(f) Articolul 19

316. Articolul 19 a susținut că o colectare, o analiză și o păstrare fără discernământ și fără suspiciuni a comunicațiilor persoanelor fizice este, prin natura sa, disproporționată. Numai supravegherea specifică bazată pe o bănuială întemeiată și autorizată de o instanță ar constitui o restricție legitimă adusă drepturilor la viață privată.

(g) European Digital Rights („EDRi”) și alte organizații active în domeniul drepturilor omului în societatea informațională

317. EDRi și alte asociații au susținut că prezenta cauză oferă Curții o ocazie esențială de a-și revizui cadrul de protecție a metadatelor. Guvernele și-au construit programele de supraveghere pe baza distincției stabilite între conținut și metadata în *Malone împotriva Regatului Unit*, 2 august 1984, Seria A nr. 82, dar, la momentul pronunțării în cauza respectivă, nu existau nici Internetul, nici telefoanele mobile. La momentul actual, metadatale ar putea zugrăvi o imagine detaliată și intimă a unei persoane: acestea permit navigarea în rețelele sociale, urmărirea locației, urmărirea istoricului de navigare pe Internet, maparea modelelor de comunicații, și informații despre persoana cu care a interacționat. În plus, nivelul de detaliere care ar putea fi clarificat crește atunci când este analizat pe scară largă. Într-adevăr, Stewart Baker, consilier general al NSA, a indicat faptul că metadatale ar putea dezvălui totul despre viața unei persoane și că, dacă există suficiente metadata, nu mai este nevoie de conținut. Prin urmare, nu ar trebui să se acorde grade diferite de protecție datelor cu caracter personal bazate pe distincția arbitrară și irelevantă dintre conținut și metadata, ci mai degrabă pe consecințele care ar putea fi deduse din date.

(h) Fundația pentru o Societate Deschisă (*Open Society Justice Initiative* – OSJI)

318. OSJI a susținut că atât volumul actual de date disponibile pentru interceptare, cât și apetitul guvernelor pentru date depășește cu mult ceea ce era posibil în trecut. În consecință, interceptarea în masă reprezintă o ingerință deosebit de gravă în viața privată, care poate, prin „efectul descurajator” al acesteia, să aducă atingere altor drepturi precum libertatea de exprimare și libertatea de asociere. Pentru a fi legală, interceptarea în masă trebuie, așadar, să îndeplinească mai multe condiții: cadrul juridic să fie suficient de precis, domeniul de aplicare al informațiilor colectate să fie limitat în timp și geografic, iar informațiile să fie colectate doar pe baza unei „bănuieli întemeiate”.

(i) Fundația Helsinki pentru Drepturile Omului (*Helsinki Foundation for Human Rights* – „HFHR”)

319. HFHR a descris experiența sa atunci când a contestat supravegherea comunicațiilor de către autoritățile publice din Polonia, care a culminat cu constatarea de către Tribunalul Constituțional a anumitor aspecte ale legislației relevante ca fiind neconstituționale. Ulterior, legislația a fost modificată.

(j) Comisia Internațională a Juriștilor (*International Commission of Jurists* – „ICJ”)

320. ICJ a susținut că, având în vedere scara și amploarea ingerinței în viața privată pe care o implică supravegherea în masă, distincția dintre metadata și conținut a devenit o noțiune depășită. Pe de altă parte, faptul că, în cadrul unei operațiuni de supraveghere în masă, anumite elemente ale ingerinței în drepturi pot avea loc în afara competenței teritoriale a unui stat nu se opune angajării răspunderii acestui stat, întrucât controlul său asupra informațiilor este suficient pentru stabilirea competenței.

(k) Law Society of England and Wales

321. Law Society și-a exprimat profunda îngrijorare cu privire la implicațiile regimului prevăzut la art. 8 alin. (4) pentru principiul secretului profesional al avocaților. În opinia sa, regimul permite interceptarea comunicațiilor confidențiale și care fac obiectul secretului profesional între avocați și clienți, chiar și atunci când ambele părți se aflau în Regatul Unit. De asemenea, permite colectarea sistematică a metadatelor aferente unor astfel de comunicații. În plus, odată interceptate, aceste comunicații confidențiale și care fac obiectul secretului profesional al avocaților ar putea fi utilizate, cu condiția ca scopul și obiectul principal al mandatului să fie colectarea de comunicații externe. Acest acord – și lipsa unor constrângeri adecvate în privința utilizării unor astfel de materiale – poate avea un potențial efect descurajator major asupra sincerității și deschiderii comunicațiilor între avocați și clienți.

4. Motivarea Curții

(a) Observații preliminare

322. Prezenta plângere privește interceptarea în masă a comunicațiilor transfrontaliere de către serviciile de informații. Deși nu este prima dată când Curtea a examinat acest tip de supraveghere (*Weber și Saravia* și *Liberty și alții*, ambele citate anterior), în cursul procedurii a devenit evident că evaluarea unui astfel de regim prezintă dificultăți specifice. În această perioadă din ce în ce mai digitalizată, marea majoritate a comunicațiilor iau formă digitală și sunt transportate prin rețele globale de telecomunicații utilizând o combinație a celor mai rapide și mai ieftine căi fără niciun raport

semnificativ cu frontierele naționale. Prin urmare, supravegherea care nu țintește direct persoanele fizice are capacitatea de a avea într-adevăr o rază de acțiune foarte largă, atât pe teritoriul statului care efectuează supravegherea, cât și în afara acestuia. Prin urmare, garanțiile sunt esențiale și, totodată, evazive. Spre deosebire de interceptarea țintită, care a făcut obiectul unei mari părți a jurisprudenței Curții și care este utilizată în principal pentru investigarea infracțiunilor, interceptarea în masă este, de asemenea, – poate chiar în mod predominant – utilizată pentru a colecta informații externe și pentru a identifica noi amenințări atât din partea actorilor cunoscuți, cât și a celor necunoscuți. Atunci când își desfășoară activitatea în acest domeniu, statele contractante au o nevoie legitimă de confidențialitate, ceea ce înseamnă că puține informații cu privire la funcționarea sistemului vor fi făcute publice, iar informațiile disponibile pot fi formulate într-o terminologie obscură și care poate varia semnificativ de la un stat la altul.

323. Deși capacitățile tehnologice au crescut considerabil volumul comunicațiilor care traversează Internetul la nivel mondial, amenințările cu care se confruntă statele contractante și cetățenii acestora s-au înmulțit deopotrivă. Printre acestea se numără terorismul mondial, traficul de droguri, traficul de ființe umane și exploatarea sexuală a copiilor, fără a se limita la acestea. Multe dintre aceste amenințări provin din partea unor rețele internaționale de actori ostili care au acces la tehnologii din ce în ce mai sofisticate, care le permit să comunice nedetectați. Accesul la astfel de tehnologii permite, de asemenea, actorilor statali și nestatali ostili să perturbe infrastructura digitală și chiar buna funcționare a proceselor democratice prin utilizarea atacurilor cibernetice, o amenințare gravă la adresa securității naționale care, prin definiție, există doar în domeniul digital și, ca atare, nu poate fi detectată și investigată decât în acest domeniu. În consecință, Curtea este obligată să evalueze modul în care respectă Convenția regimurile de interceptare în masă ale statelor contractante, o capacitate tehnologică prețioasă de a identifica noi amenințări în domeniul digital, prin trimitere la existența unor garanții împotriva arbitrarului și abuzurilor, pe baza unor informații limitate cu privire la modul în care funcționează regimurile respective.

(b) Cu privire la existența unei ingerințe

324. Guvernul nu contestă faptul că a existat o ingerință în drepturile părților reclamante consacrate de art. 8, deși susține că, în sensul acestui articol, singura ingerință semnificativă ar fi putut avea loc atunci când au fost selectate comunicațiile spre examinare.

325. Curtea consideră interceptarea în masă ca fiind un proces gradual în care gradul de ingerință în drepturile persoanelor fizice în temeiul art. 8 crește pe măsură ce procesul avansează. Este posibil ca regimurile de interceptare în masă să nu urmeze toate exact același model, iar diferitele etape ale procesului nu vor fi neapărat discrete sau urmate în ordine cronologică strictă.

Cu toate acestea, sub rezerva restricțiilor menționate mai sus, Curtea consideră că etapele procesului de interceptare în masă care trebuie luate în considerare pot fi descrise după cum urmează:

(a) interceptarea și păstrarea inițială a comunicațiilor și a datelor de comunicații aferente (și anume, datele de trafic care aparțin comunicațiilor interceptate);

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

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

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

326. În ceea ce Curtea a considerat a fi prima etapă, comunicațiile electronice (sau „pachetele” de comunicații electronice) vor fi interceptate în masă de serviciile de informații. Aceste comunicații vor aparține unui număr mare de persoane, dintre care multe nu vor prezenta niciun interes pentru serviciile de informații. Unele comunicații care e puțin probabil să fie de interes pentru serviciile de informații pot fi filtrate în această etapă.

327. Căutarea inițială, care este în cea mai mare parte automată, are loc în ceea ce Curtea a considerat a fi a doua etapă, atunci când diferite tipuri de selectori, inclusiv „selectori puternici” (cum ar fi o adresă de e-mail) și/sau interogări complexe, sunt aplicați pachetelor de comunicații și datelor de comunicații aferente păstrate. Aceasta poate fi etapa în care procesul începe să vizeze persoanele prin utilizarea de selectori puternici.

328. În cursul a ceea ce Curtea a considerat a fi a treia etapă, materialele interceptate sunt examinate pentru prima dată de un analist.

329. Ceea ce Curtea a considerat a fi etapa finală este momentul în care materialele interceptate sunt utilizate efectiv de serviciile de informații. Această etapă poate implica crearea unui raport informativ, difuzarea materialului către alte servicii de informații din cadrul statului interceptor sau chiar transmiterea de materiale către servicii de informații străine.

330. Curtea consideră că art. 8 se aplică în fiecare din etapele de mai sus. Deși interceptarea inițială, urmată de eliminarea imediată a unor părți ale comunicațiilor, nu constituie o ingerință deosebit de semnificativă, gradul de ingerință în drepturile persoanelor consacrate de art. 8 va crește, pe măsură ce procesul de interceptare în masă avansează. În această privință, Curtea a precizat în mod clar că și simpla stocare a datelor referitoare la viața privată a unei persoane constituie o ingerință în sensul art. 8 (*Leander împotriva Suediei*, 26 martie 1987, pct. 48, Seria A nr. 116) și că necesitatea unor garanții va fi cu atât mai mare în ceea ce privește protecția datelor cu caracter personal care fac obiectul prelucrării automate (*S. și Harper*, citată anterior, pct. 103). Faptul că materialele stocate au o formă codificată, inteligibilă numai prin utilizarea tehnologiei informatice și care poate fi interpretată numai de un număr limitat de persoane, nu poate avea nicio influență asupra

acestei constatări [*Amann împotriva Elveției* (MC), nr. 27798/95, pct. 69, CEDO 2000-II, și *S. și Marper*, citată anterior, pct. 67 și 75]. În sfârșit, la finalul procesului, atunci când informațiile referitoare la o anumită persoană vor fi analizate sau conținutul comunicațiilor este examinat de un analist, nevoia de garanții va fi la cel mai înalt nivel. Această abordare a Curții este conformă cu constatarea Comisiei de la Veneția, care, în raportul său privind Supravegherea democratică a agențiilor care colectează informații de origine electromagnetică, a considerat că, în cazul interceptării în masă, ingerința principală în viața privată are loc atunci când datele cu caracter personal stocate sunt prelucrate și/sau accesate de agenții (supra, pct. 196).

331. Astfel, gradul de ingerință în dreptul la viața privată va crește pe măsură ce procesul trece de-a lungul diferitelor etape. Atunci când va examina dacă această ingerință din ce în ce mai mare a fost justificată, Curtea va realiza propria evaluare a regimului prevăzut la art. 8 alin. (4) pe baza acestei înțelegeri a naturii ingerinței.

(c) Cu privire la întrebarea dacă ingerința a fost justificată

(i) *Principii generale referitoare la măsurile secrete de supraveghere, inclusiv interceptarea comunicațiilor*

332. Orice ingerință în drepturile unei persoane consacrate de art. 8 nu poate fi justificată în temeiul art. 8 § 2 decât dacă este prevăzută de lege, urmărește unul sau mai multe dintre scopurile legitime la care se referă alineatul respectiv și este necesară într-o societate democratică pentru atingerea unui astfel de obiectiv (*Roman Zakharov*, citată anterior, pct. 227; *Kennedy împotriva Regatului Unit*, pct. 130, 18 mai 2010). Formularea „prevăzută de lege” impune ca măsura contestată să aibă un anumit temei în dreptul intern (spre deosebire de o practică care nu are un temei juridic specific – *Heglas împotriva Republicii Cehe*, nr. 5935/02, pct. 74, 1 martie 2007). De asemenea, aceasta trebuie să fie compatibilă cu statul de drept, care este menționat în mod expres în preambulul Convenției și inerent obiectului și scopului art. 8. Prin urmare, legea trebuie să fie accesibilă persoanei în cauză și previzibilă în ceea ce privește efectele sale (*Roman Zakharov*, citată anterior, pct. 228; a se vedea, de asemenea, printre multe altele, *Rotaru*, citată anterior, pct. 52, *S. și Marper*, citată anterior, pct. 95, precum și *Kennedy*, citată anterior, pct. 151).

333. Sensul expresiei „previzibilitate” în contextul supravegherii secrete nu este același ca în multe alte domenii. În special, în contextul măsurilor de supraveghere secretă precum interceptarea comunicațiilor, „previzibilitatea” nu poate însemna că o persoană ar trebui să poată prevedea situațiile în care autoritățile i-ar putea intercepta comunicațiile, astfel încât să își poată adapta comportamentul în consecință. Totuși, atunci când o putere investită de executiv este exercitată în secret, există evidente riscuri de apariție a arbitrarului. Este așadar esențial să existe norme clare și detaliate privind

măsurile de supraveghere secretă, în special având în vedere că tehnologia disponibilă pentru utilizare este în permanență din ce în ce mai sofisticată. Legea internă 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 asemenea măsuri (*Roman Zakharov*, citată anterior, pct. 229; *Malone*, citată anterior, pct. 67; *Leander*, citată anterior, pct. 51; *Huvig*, citată anterior, pct. 29; *Kruslin*, citată anterior, pct. 30; *Valenzuela Contreras împotriva Spaniei*, 30 iulie 1998, pct. 46, *Culegere de rapoarte și decizii 1998-V*; *Rotaru*, citată anterior, pct. 55; *Weber și Saravia*, citată anterior, pct. 93; și *Asociația pentru integrare europeană și drepturile omului și Ekimdzhiev împotriva Bulgariei*, nr. 62540/00, pct. 75, 28 iunie 2007). În plus, legea trebuie să indice domeniul de aplicare al oricărei marje de apreciere conferite autorităților competente și modul de exercitare a acesteia cu suficientă claritate pentru a oferi protecție adecvată individuală împotriva ingerințelor arbitrare (*Roman Zakharov*, citată anterior, pct. 230; a se vedea, printre altele, *Malone*, citată anterior, pct. 68; *Leander*, citată anterior, pct. 51; *Huvig*, citată anterior, pct. 29; *Kruslin*, citată anterior, pct. 30; și *Weber și Saravia*, citată anterior, pct. 94).

334. În cazurile în care legislația care permite supravegherea secretă este contestată în fața Curții, caracterul legal al ingerinței este strâns legat de întrebarea dacă a fost respectat criteriul „necesității” și, prin urmare, este oportun pentru Curte să abordeze în comun cerințele ca ingerința să fie „prevăzută de lege” și „necesitatea” sa. În acest sens, „calitatea legislației” implică faptul că dreptul intern nu trebuie să fie accesibil și previzibil în aplicarea sa, ci trebuie, de asemenea, să asigure că măsurile de supraveghere secretă se aplică numai atunci când sunt „necesare într-o societate democratică”, în special prin prevederea unor garanții adecvate și eficiente și prin existența unor garanții împotriva abuzurilor (*Roman Zakharov*, citată anterior, pct. 236; *Kennedy*, citată anterior, pct. 155).

335. În această privință trebuie reamintit că, în jurisprudența sa privind interceptarea comunicațiilor în cadrul anchetelor penale, Curtea a elaborat următoarele cerințe minime care ar trebui stabilite prin lege pentru a evita abuzurile de putere: (i) natura infracțiunilor care pot da naștere unui mandat de interceptare; (ii) definirea categoriilor de persoane susceptibile de a fi interceptate; (iii) limitarea duratei interceptării; (iv) procedura care trebuie urmată pentru examinarea, utilizarea și stocarea datelor obținute; (v) măsurile de precauție care trebuie luate atunci când comunică datele celorlalte părți; și (vi) circumstanțele în care datele interceptate pot sau trebuie să fie șterse sau distruse (*Huvig*, citată anterior, pct. 35; *Kruslin*, citată anterior, pct. 35; *Valenzuela Contreras*, citată anterior, pct. 46; *Weber și Saravia*, citată anterior, pct. 95; și *Asociația pentru integrare europeană și drepturile omului și Ekimdzhiev*, citată anterior, pct. 76). În *Roman Zakharov* (citată anterior, pct. 231), Curtea a confirmat că aceleași șase garanții minime au fost, de

asemenea, aplicate în cauzele în care interceptarea a avut loc din motive de securitate națională; cu toate acestea, pentru a stabili dacă legislația incriminată încălca prevederile art. 8, a avut în vedere și modalitățile de control al aplicării măsurilor secrete de supraveghere, orice mecanisme de notificare și căile de atac prevăzute de dreptul intern (*Roman Zakharov*, citată anterior, pct. 238).

336. Controlul și supravegherea măsurilor secrete de supraveghere pot avea loc în trei etape: atunci când supravegherea este dispusă prima dată, când este efectuată sau după încheierea acesteia. În ceea ce privește primele două etape, natura și logica supravegherii secrete impun ca nu doar supravegherea în sine, ci și controlul acesteia să se efectueze fără cunoștința persoanei. În consecință, întrucât persoana în cauză va fi în mod necesar împiedicată să apeleze la o cale de atac efectivă din proprie inițiativă sau să participe direct la orice procedură de control, este esențial ca procedurile instituite să ofere ele însele garanții adecvate și echivalente care să îi protejeze drepturile. Într-un domeniu în care abuzurile în cazuri individuale pot apărea atât de ușor și ar putea avea consecințe atât de nocive pentru societatea democratică în ansamblul său, Curtea a hotărât că, în principiu, este de dorit să se încredințeze unui judecător controlul supravegherii, controlul judiciar oferind cele mai bune garanții de independență, imparțialitate și o procedură adecvată (*Roman Zakharov*, citată anterior, pct. 233; *Klass și alții împotriva Germaniei*, 6 septembrie 1978, pct. 55 și 56, Seria A nr. 28).

337. În ceea ce privește cea de-a treia etapă, după încheierea supravegherii, chestiunea notificării ulterioare a măsurilor de supraveghere constituie un factor relevant pentru evaluarea caracterului efectiv al căilor de atac în fața instanțelor și, prin urmare, pentru existența unor garanții efective împotriva abuzurilor puterii de supraveghere. În principiu, există puține posibilități de a formula căi de atac în fața instanțelor de judecată de către persoana în cauză, cu excepția cazului în care aceasta din urmă este informată cu privire la măsurile luate fără știrea sa și astfel să aibă posibilitatea să le conteste retroactiv legalitatea (*Roman Zakharov*, citată anterior, pct. 234; *Klass și alții*, citată anterior, pct. 167); sau, ca alternativă, cu excepția cazului în care orice persoană care suspectează că a făcut obiectul unei supravegheri se poate adresa instanțelor, a căror competență nu depinde de notificarea subiectului supravegherii cu privire la măsurile luate (*Roman Zakharov*, citată anterior, pct. 234; *Kennedy*, citată anterior, pct. 167).

338. În ceea ce privește întrebarea dacă o ingerință a fost „necesară într-o societate democratică” în vederea atingerii unui obiectiv legitim, Curtea a recunoscut că autoritățile naționale beneficiază de o marjă largă de apreciere atunci când aleg cea mai bună modalitate de a atinge obiectivul legitim de a proteja securitatea națională (*Weber și Saravia*, citată anterior, pct. 106).

339. Cu toate acestea, marja de apreciere face obiectul unui control european care cuprinde atât legislația, cât și deciziile prin care se aplică. Având în vedere riscul ca un sistem de supraveghere secretă instituit pentru a

proteja securitatea națională (și alte interese naționale esențiale) să afecteze sau chiar să distrugă buna funcționare a proceselor democratice sub masca apărării lor, Curtea trebuie să se asigure că există garanții adecvate și efective împotriva abuzurilor. Evaluarea depinde de toate circumstanțele cauzei, precum natura, domeniul de aplicare și durata eventualelor măsuri, motivele pentru care sunt dispuse, autoritățile care au competența de a autoriza, de a desfășura și de a supraveghea aceste măsuri, precum și tipul de măsuri reparatorii prevăzute de dreptul intern. Curtea trebuie să stabilească dacă procedurile de supervizare a deciziei și de aplicare a măsurilor restrictive sunt de natură să mențină „îngerința” la ceea ce este „necesar într-o societate democratică” (*Roman Zakharov*, citată anterior, pct. 232; *Klass și alții*, citată anterior, pct. 49, 50 și 59, *Weber și Saravia*, citată anterior, pct. 106 și *Kennedy*, citată anterior, pct. 153 și 154).

(ii) *Cu privire la necesitatea dezvoltării jurisprudenței*

340. În *Weber și Saravia* și *Liberty și alții* (citate anterior), Curtea a admis că regimurile de interceptare în masă nu se află *per se* în afara marjei de apreciere a statelor. Având în vedere proliferarea amenințărilor cu care se confruntă în prezent statele din partea rețelelor de actori internaționali, utilizând Internetul atât pentru comunicare, cât și ca instrument, precum și existența unei tehnologii sofisticate care ar permite acestor actori să evite detectarea (supra, pct. 323), Curtea consideră că decizia de a aplica un regim de interceptare în masă pentru a identifica amenințările la adresa securității naționale sau a intereselor naționale esențiale este o decizie care continuă să se încadreze în această marjă.

341. Atât în *Weber și Saravia*, cât și în *Liberty și alții* (citate anterior), Curtea a aplicat cele șase garanții minime sus-menționate, dezvoltate în jurisprudența sa privind interceptarea ținută (supra, pct. 335). Cu toate acestea, deși regimurile de interceptare în masă luate în considerare în aceste cauze erau similare cu cele în discuție în prezenta cauză, cele două cauze au în prezent o vechime de peste zece ani, iar în anii care au trecut evoluțiile tehnologice au schimbat în mod semnificativ modul în care oamenii comunică. Viața este din ce în ce mai răspândită în mediul on-line, generând atât un volum semnificativ mai mare de comunicații electronice, cât și comunicații de o natură și o calitate semnificativ diferite față de cele care ar fi putut fi generate cu un deceniu în urmă (supra, pct. 322). Prin urmare, domeniul de aplicare al activității de supraveghere avute în vedere în aceste cauze ar fi fost mult mai restrâns.

342. Același lucru este valabil și în cazul datelor de comunicații aferente. Astfel cum a observat ISR în raportul său, în prezent sunt disponibile volume mai mari de date de comunicații despre un anumit conținut, întrucât fiecare element de conținut este acompaniat de multiple date de comunicații (supra, pct. 159). Deși conținutul ar putea fi criptat și, în orice caz, nu poate dezvălui nimic despre expeditor sau destinatar, datele de comunicații aferente pot

dezvăluie un număr mare de informații cu caracter personal, cum ar fi identitățile și localizările geografice ale expeditorului și destinatarului, precum și echipamentul prin intermediul căruia a fost transmisă comunicația. Pe de altă parte, orice intruziune cauzată de obținerea datelor de comunicații aferente va fi amplificată atunci când sunt obținute în masă, întrucât în prezent pot fi analizate și interogate astfel încât să ofere o imagine intimă a unei persoane prin cartografierea rețelelor de socializare, urmărirea locațiilor, urmărirea navigației pe Internet, cartografierea modelelor de comunicare și cunoașterea persoanelor cu care a interacționat (supra, pct. 317).

343. Un alt element este mai important: în *Weber și Saravia și Liberty și alții*, Curtea nu a luat în considerare, în mod special, faptul că supravegherea era de altă natură și de o amploare diferită față de cea examinată în cauzele anterioare. Cu toate acestea, interceptarea ținută și interceptarea în masă sunt diferite sub mai multe aspecte importante.

344. În primul rând, interceptarea în masă vizează, în general, comunicațiile internaționale (și anume comunicațiile care traversează fizic frontierele statale) și, în timp ce interceptarea și chiar examinarea comunicațiilor persoanelor din statul care efectuează supravegherea ar putea să nu fie excluse, în multe cazuri scopul declarat al interceptării în masă este cel de a monitoriza comunicațiile persoanelor aflate în afara jurisdicției teritoriale a statului, care nu ar putea fi monitorizate prin alte forme de supraveghere. De exemplu, sistemul german are ca scop doar să monitorizeze telecomunicațiile străine în afara teritoriului german (supra, pct. 248). În Suedia, materialele interceptate nu pot privi semnale în cazul în care atât expeditorul, cât și destinatarul se află în Suedia [a se vedea hotărârea pronunțată astăzi în cauza *Centrum för rättvisa împotriva Suediei* (cererea nr. 35252/08)].

345. În plus, astfel cum s-a observat deja, scopurile pentru care poate fi utilizată interceptarea în masă par a fi diferite. În măsura în care Curtea a luat în considerare interceptarea ținută, aceasta a fost, în cea mai mare parte, utilizată de statele pârâte în scopul investigării infracțiunilor. Cu toate acestea, deși interceptarea în masă poate fi utilizată pentru investigarea anumitor infracțiuni grave, statele membre ale Consiliului Europei care aplică un regim de interceptare în masă par să îl utilizeze în scopuri legate de colectarea de informații externe, detectarea timpurie și investigarea atacurilor cibernetice, contraspionajul și combaterea terorismului (supra, pct. 303, 308 și 323).

346. Deși interceptarea în masă nu este utilizată neapărat pentru a viza anumite persoane, evident poate fi – și este – utilizată în acest scop. Atunci când este cazul totuși, dispozitivele persoanelor vizate nu sunt monitorizate. Mai degrabă, persoanele sunt „vizate” prin aplicarea unor selectori puternici (cum ar fi adresele lor de e-mail) la comunicațiile interceptate în masă de către serviciile de informații. Doar acele „pachete” de comunicații ale persoanelor vizate care trec prin canalele de transmisie selectate de serviciile

de informații vor fi interceptate în acest mod și doar acele comunicații interceptate care corespund fie unui selector puternic, fie unei interogări complexe pot fi examinate de un analist.

347. La fel ca în cazul oricărui regim de interceptare, există, desigur, un potențial considerabil ca interceptarea în masă să fie utilizată în mod abuziv într-un mod care să afecteze negativ dreptul persoanelor la respectarea vieții private. Deși art. 8 din Convenție nu interzice utilizarea interceptării în masă pentru a proteja securitatea națională și alte interese naționale esențiale împotriva amenințărilor externe grave, și statele se bucură de o marjă largă de apreciere atunci când decid ce tip de regim de interceptare este necesar, în acest scop, pentru operarea unui astfel de sistem, marja de apreciere care le este acordată trebuie să fie mai restrânsă și va trebui să existe o serie de garanții. Curtea a identificat deja acele garanții care ar trebui să facă parte dintr-un regim de interceptare specific conform cu Convenția. Deși aceste principii oferă un cadru util pentru acest exercițiu, va trebui să fie adaptate pentru a reflecta caracteristicile specifice ale unui regim de interceptare în masă și, în special, gradului tot mai mare de intruziune în drepturile persoanelor fizice în temeiul art. 8, pe măsură ce operațiunea trece prin etapele identificate supra la pct. 325.

(iii) *Abordarea care trebuie urmată în cazurile de interceptare în masă*

348. Este clar că primele două din cele șase „garanții minime” pe care Curtea le-a constatat, în cadrul interceptării selective, trebuie definite în mod clar în dreptul intern pentru a evita abuzurile de putere (și anume, natura infracțiunilor care pot da naștere la un mandat de interceptare și categoriile de persoane susceptibile de a le fi interceptate comunicațiile: supra, pct. 335), nu sunt aplicabile cu promptitudine unui regim de interceptare în masă. În mod similar, cerința de a exista o „bănuială întemeiată”, care poate fi găsită în jurisprudența Curții privind interceptarea țintită în contextul anchetelor penale, este mai puțin relevantă în contextul interceptării în masă, al cărei scop este în principiu mai degrabă preventiv decât de a investiga o țintă specifică și/sau o infracțiune identificabilă. Cu toate acestea, Curtea consideră că este imperativ ca, atunci când un stat aplică un astfel de regim, dreptul intern să conțină norme detaliate cu privire la momentul în care autoritățile pot recurge la astfel de măsuri. În special, dreptul intern trebuie să stabilească cu suficientă claritate motivele pentru care interceptarea în masă poate fi autorizată și circumstanțele în care comunicațiile unei persoane pot fi interceptate. Celelalte patru garanții minime definite de Curte în hotărârile sale anterioare – și anume, că dreptul intern trebuie să stabilească o limită privind durata interceptării, procedura care trebuie urmată pentru examinarea, utilizarea și stocarea datelor obținute, precauțiile care trebuie luate la comunicarea datelor către alte părți și circumstanțele în care datele interceptate pot sau trebuie să fie șterse sau distruse – sunt la fel de relevante pentru interceptarea în masă.

349. În jurisprudența sa privind interceptarea ținută, Curtea a avut în vedere modalitățile de supraveghere și control al regimului de interceptare (*Roman Zakharov*, citată anterior, pct. 233-234). În contextul interceptării în masă, importanța supravegherii și a controlului va fi amplificată, având în vedere riscul inerent de abuz și faptul că nevoia legitimă de confidențialitate va însemna în mod inevitabil că, din motive de securitate națională, statele nu vor avea adesea libertatea de a divulga informații privind funcționarea regimului incriminat.

350. Prin urmare, pentru a reduce la minimum riscul abuzului de putere de interceptare în masă, Curtea consideră că procesul trebuie să facă obiectul unor „garanții de la un capăt la altul”, ceea ce înseamnă că, la nivel intern, trebuie efectuată o evaluare în fiecare etapă a procesului necesității și proporționalității măsurilor luate, iar interceptarea în masă ar trebui să facă obiectul unei autorizări independente la început, atunci când sunt definite obiectul și amploarea operațiunii; și că operațiunea trebuie să facă obiectul supravegherii și al unui control *a posteriori*. În opinia Curții, acestea sunt garanții fundamentale care vor constitui piatra de temelie a oricărui regim de interceptare în masă conform cu art. 8 (a se vedea, de asemenea, raportul Comisiei de la Veneția, supra, pct. 197, care a considerat în mod similar că două dintre cele mai importante garanții într-un regim de interceptare în masă sunt autorizarea și controlul procesului).

351. Revenind la autorizare, Marea Cameră este de acord cu opinia Camerei potrivit căreia, deși autorizația judiciară reprezintă o „garanție importantă împotriva arbitrariului”, nu constituie o „cerință necesară” (pct. 318-320 din hotărârea Camerei). Cu toate acestea, interceptarea în masă trebuie autorizată de un organ independent, adică de un organ independent de executiv.

352. În plus, pentru a oferi o protecție eficientă împotriva abuzurilor, organul de autorizare independent trebuie să fie informat atât cu privire la scopul interceptării, cât și cu privire la canalele de transmisie sau rutele de comunicații posibil să fie interceptate. Acest lucru ar permite organului de autorizare independent să evalueze necesitatea și proporționalitatea operațiunii de interceptare în masă și, de asemenea, să evalueze dacă selecția canalelor este necesară și proporțională cu scopurile în care are loc interceptarea.

353. Utilizarea selectorilor – în special a unor selectori puternici – reprezintă una din cele mai importante etape ale procesului de interceptare în masă, întrucât acesta este momentul în care comunicațiile unei anumite persoane pot fi vizate de serviciile de informații. Cu toate acestea, deși anumite sisteme permit autorizarea prealabilă a unor categorii de selectori [a se vedea, de exemplu, sistemul suedez descris în detaliu în *Centrum för rättvisa împotriva Suediei* (cererea nr. 35252/08)], Curtea observă că atât Guvernul Regatului Unit, cât și Guvernul Țărilor de Jos au susținut că orice obligație de a explica sau de a justifica selectorii sau criteriile de căutare din

autorizație ar restrânge în mod grav eficacitatea interceptării în masă (supra, pct. 292 și 307). Acest argument a fost acceptat de IPT, care a constatat că includerea selectorilor în autorizație „ar fi afectat și ar fi limitat în mod inutil executarea mandatului și ar fi putut să fie un lucru total nerealist” (supra, pct. 49).

354. Luând în considerare caracteristicile interceptării în masă (supra, pct. 344-345), numărul mare de selectori utilizați și nevoia inerentă de flexibilitate în alegerea selectorilor, care, în practică, poate fi exprimată drept combinații tehnice de numere sau litere, Curtea admite că includerea tuturor selectorilor în autorizație ar putea să nu fie posibilă în practică. Cu toate acestea, având în vedere că alegerea selectorilor și a termenilor de căutare determină comunicațiile care vor fi eligibile spre examinare de către un analist, autorizația ar trebui să identifice cel puțin tipurile sau categoriile de selectori care urmează să fie utilizați.

355. În plus, ar trebui să existe garanții sporite atunci când serviciile de informații utilizează selectori puternici legați de persoane identificabile. Utilizarea fiecărui astfel de selector trebuie să fie justificată – în ceea ce privește principiile necesității și proporționalității – de serviciile de informații și justificarea trebuie să fie înregistrată cu rigurozitate și să facă obiectul unui proces de autorizare internă prealabilă care să prevadă verificarea separată și obiectivă a conformității justificării cu principiile menționate anterior.

356. Fiecare etapă a procesului de interceptare în masă – inclusiv autorizarea inițială și orice reînnoire ulterioară, selectarea purtătorilor, alegerea și aplicarea selectorilor și a termenilor de căutare, precum și utilizarea, stocarea, transmiterea și ștergerea ulterioară a materialelor interceptate – trebuie, de asemenea, să facă obiectul supravegherii unei autorități independente și supravegherea trebuie să fie suficient de robustă pentru a menține „ingerința” la ceea ce este „necesar într-o societate democratică” (*Roman Zakharov*, citată anterior, pct. 232; *Klass și alții*, citată anterior, pct. 49, 50 și 59; *Weber și Saravia*, citată anterior, pct. 106; *Kennedy*, citată anterior, pct. 153 și 154). În special, organul de supraveghere trebuie să fie în măsură să evalueze necesitatea și proporționalitatea acțiunii întreprinse, ținând seama în mod corespunzător de nivelul corespunzător de intruziune în drepturile consacrate de Convenție ale persoanelor susceptibile de a fi afectate. Pentru a facilita această supraveghere, serviciile de informații trebuie să țină registre detaliate în fiecare etapă a procesului.

357. În sfârșit, orice persoană care suspectează interceptarea comunicațiilor sale de către serviciile de informații trebuie să dispună de o cale de atac efectivă, fie pentru a contesta legalitatea interceptării suspectate, fie pentru a contesta conformitatea cu Convenția a regimului de interceptare. În contextul interceptării țintite, Curtea a considerat în mod repetat că notificarea ulterioară a măsurilor de supraveghere reprezintă un factor relevant în evaluarea caracterului efectiv al căilor de atac în fața instanțelor și, prin urmare, a existenței unor garanții eficiente împotriva abuzului de

puterea de supraveghere. Cu toate acestea, a recunoscut că notificarea nu este necesară în cazul în care sistemul de căi de atac interne permite oricărei persoane suspectate că comunicațiile sale sunt sau au fost interceptate să se adreseze instanțelor; cu alte cuvinte, atunci când competența instanțelor nu depinde de notificarea către subiectul interceptării a faptului că a existat o interceptare a comunicațiilor sale (*Roman Zakharov*, citată anterior, pct. 234, și *Kennedy*, citată anterior, pct. 167).

358. Curtea consideră că o cale de atac care nu depinde de notificarea subiectului interceptării poate constitui, de asemenea, o cale de atac efectivă în contextul interceptării în masă; de fapt, în funcție de circumstanțe, o asemenea cale de atac poate oferi garanții mai bune ale unei proceduri adecvate decât un sistem bazat pe notificare. Indiferent dacă materialele au fost dobândite prin interceptare țintită sau în masă, existența unei excepții legate de securitatea națională ar putea priva o cerință de notificare de orice efect practic real. Probabilitatea ca o cerință de notificare să aibă un efect practic redus sau inexistent va fi mai acută în contextul interceptării în masă, întrucât o astfel de supraveghere poate fi utilizată în scopul colectării de informații externe și va viza, în cea mai mare parte, comunicațiile persoanelor aflate în afara jurisdicției teritoriale a statului. Prin urmare, chiar dacă identitatea unei ținte este cunoscută, este posibil ca autoritățile să nu aibă cunoștință de locul în care se află.

359. Competențele și garanțiile procedurale pe care le deține o autoritate sunt relevante pentru a stabili dacă o cale de atac este efectivă. Prin urmare, în lipsa unei obligații de notificare, este imperativă formularea căii de atac în fața unui organ care, deși nu este neapărat judiciar, este independent de executiv și asigură caracterul echitabil al procedurii, oferind, în măsura posibilului, o procedură contradictorie. Deciziile unei astfel de autorități vor fi motivate și obligatorii din punct de vedere legal în ceea ce privește, printre altele, încetarea interceptării ilegale și distrugerea materialelor interceptate și/sau stocate ilegal (a se vedea, *mutatis mutandis*, *Segerstedt-Wiberg și alții împotriva Suediei*, nr. 62332/00, pct. 120, CEDO 22006-VII, și, de asemenea, *Leander*, citată anterior, pct. 81-83, în care lipsa de competență pentru pronunțarea unei decizii obligatorii din punct de vedere juridic a constituit o deficiență majoră a controlului oferit).

360. În lumina celor de mai sus, Curtea urmează să stabilească dacă un regim de interceptare în masă este conform cu Convenția, efectuând o evaluare globală a funcționării acestuia. O astfel de evaluare se va concentra, în principal, asupra întrebării dacă cadrul juridic intern conține suficiente garanții împotriva abuzurilor și dacă procesul este supus unor „garanții de la un capăt la altul” (supra, pct. 350). În acest sens, va ține seama de funcționarea efectivă a sistemului de interceptare, inclusiv de verificările și echilibrul exercitării puterii, precum și de existența sau lipsa oricărei dovezi de abuz real (*Asociația pentru integrare europeană și drepturile omului și Ekimdzhiev*, citată anterior, pct. 92).

361. Pentru a aprecia dacă statul pârât a acționat în limitele marjei sale de apreciere (supra, pct. 347), Curtea trebuie să țină seama de o gamă mai largă de criterii decât cele șase garanții *Weber*. Mai precis, examinând coroborat criteriile conform cărora măsura trebuie să fie „prevăzută de lege” și „necesară”, aceasta fiind abordarea consacrată în acest domeniu (*Roman Zakharov*, citată anterior, pct. 236 și *Kennedy*, citată anterior, pct. 155), Curtea va examina dacă cadrul juridic intern a definit în mod clar:

1. motivele pentru care poate fi autorizată interceptarea în masă;
2. care sunt „circumstanțele” în care comunicațiile unei persoane pot fi interceptate;
3. procedura care trebuie urmată pentru acordarea autorizației;
4. procedurile care trebuie urmate pentru selectarea, examinarea și utilizarea materialelor interceptate;
5. măsurile de precauție care trebuie luate la comunicarea datelor către alte părți;
6. limitele privind durata interceptării, stocarea materialelor interceptate și circumstanțele în care aceste materiale trebuie șterse și distruse;
7. procedurile și modalitățile de supraveghere de către o autoritate independentă a respectării garanțiilor de mai sus și puterile acesteia de a soluționa cazurile de neconformitate;
8. procedurile pentru controlul *a posteriori* independent al unei astfel de conformități și puterile conferite organului competent în abordarea cazurilor de neconformitate.

362. Deși este unul dintre cele șase criterii *Weber*, până în prezent Curtea nu a furnizat orientări specifice cu privire la măsurile de precauție care trebuie luate pentru comunicarea către alte părți a materialelor interceptate. Cu toate acestea, în prezent este clar că unele state fac schimb periodic de materiale cu serviciile de informații partenere și chiar, în unele cazuri, permit acestor parteneri de informații să aibă acces direct la propriile lor sisteme. În consecință, Curtea consideră că transmiterea de către un stat contractant către state străine sau către organizații internaționale a materialelor obținute prin interceptare în masă trebuie să se limiteze la materialele colectate și stocate în conformitate cu Convenția și trebuie să facă obiectul anumitor garanții specifice suplimentare referitoare la transferul în sine. În primul rând, 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 statul destinatar, în cadrul prelucrării datelor, dispune de garanții de natură să prevină abuzurile și ingerințele disproporționate. În special, statul destinatar trebuie să garanteze stocarea sigură 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 atunci când este clar că sunt transferate

materiale care necesită o confidențialitate specială – precum materialele jurnalistice confidențiale. În sfârșit, Curtea consideră că transferul de materiale către servicii de informații partenere străine trebuie, de asemenea, să facă obiectul unui control independent.

363. Pentru motivele identificate supra la pct. 342, Curtea nu este convinsă că obținerea datelor de comunicații aferente prin interceptarea în masă este în mod necesar mai puțin intruzivă decât achiziția de conținut. Prin urmare, consideră că interceptarea, păstrarea și căutarea datelor de comunicații aferente trebuie analizată în raport cu aceleași garanții precum cele aplicabile conținutului.

364. Acestea fiind spuse, deși interceptarea datelor de comunicații aferente va fi în mod normal autorizată în același timp cu autorizarea interceptării conținutului, odată obținute, acestea pot fi tratate diferit de serviciile de informații (de exemplu, supra, pct. 153-154). Având în vedere caracterul diferit al datelor de comunicații aferente și diferitele moduri în care sunt utilizate de serviciile de informații, atât timp cât garanțiile menționate mai sus sunt în vigoare, Curtea consideră că este posibil ca dispozițiile legale care le reglementează tratamentul să nu fie neapărat identice în toate privințele cu cele care reglementează tratamentul conținutului.

(iv) *Motivarea Curții în speță*

(1) *Observații preliminare*

365. La momentul faptelor, interceptarea în masă avea ca temei juridic Capitolul I din RIPA. În plus, Curtea este convinsă că regimul menționat urmărea obiectivele legitime de a proteja securitatea națională, de a preveni tulburările de ordine și infracțiunile și de a proteja drepturile și libertățile altora. Prin urmare, urmând abordarea descrisă supra la pct. 334, a rămas de stabilit dacă dreptul intern era accesibil și conținea dispoziitive și garanții adecvate și efective pentru a îndeplini cerințele de „previzibilitate” și „necesitate într-o societate democratică”.

366. Prevederile legislative relevante care reglementau funcționarea regimului de interceptare în masă erau, fără îndoială, complexe; într-adevăr, majoritatea rapoartelor privind regimurile de supraveghere secretă ale Regatului Unit criticau lipsa lor de claritate (supra, pct. 143, 152 și 157). Aceste prevederi au fost însă elucidate în Codul de bune practici privind interceptarea comunicațiilor („Codul IC” – supra, pct. 96). Pct. 6.4 din Codul IC recunoștea în mod clar existența interceptării în masă și furniza detalii suplimentare cu privire la modul în care acest regim special de supraveghere funcționa în practică (supra, pct. 96). Codul IC este un document public aprobat de ambele Camere ale Parlamentului, care este publicat de Guvern on-line și în versiune tipărită și care trebuie luat în considerare atât de persoanele care exercită atribuții de interceptare, cât și de instanțe (supra, pct. 93-94). În consecință, Curtea a admis că dispozițiile sale puteau fi luate

în considerare pentru a evalua previzibilitatea RIPA (*Kennedy*, citată anterior, pct. 157). În consecință, Curtea a admis că dreptul intern era „accesibil” în mod adecvat.

367. În continuare, îndreptându-se asupra întrebării dacă dreptul intern conținea dispoziție și garanții adecvate și efective pentru a îndeplini cerințele de „previzibilitate” și „necesitate într-o societate democratică”, Curtea va aborda la subsecțiunea (β) fiecare dintre cele opt cerințe prezentate anterior la pct. 361, în ceea ce privește interceptarea conținutului comunicațiilor electronice. La subsecțiunea (γ), va examina, în special, interceptarea datelor de comunicații aferente.

(2) Interceptarea conținutului comunicațiilor

– 1. *Motivele pentru care poate fi autorizată interceptarea în masă*

368. În temeiul art. 5 alin. (3) din RIPA și al pct. 6.11 din Codul IC (supra, pct. 62 și 96), ministrul nu putea emite un mandat de interceptare în masă decât dacă era convins că era necesar în interesul securității naționale, pentru prevenirea sau detectarea infracțiunilor grave sau în scopul protejării bunăstării economice a Regatului Unit, în măsura în care aceste interese erau, de asemenea, relevante pentru interesele securității naționale.

369. Aceste motive erau supuse următoarelor limitări. În primul rând, Comisarul IC clarificase faptul că, în practică, „securitatea națională” permitea supravegherea activităților care amenințau siguranța sau bunăstarea statului și a activităților care urmăreau subminarea sau distrugerea democrației parlamentare prin mijloace politice, industriale sau violente (*Kennedy*, citată anterior, pct. 333). În al doilea rând infracțiunea gravă era definită la art. 81 alin (2) lit. b) ca fiind o infracțiune pentru care se putea aștepta în mod rezonabil ca făptuitorul (presupunând că a împlinit douăzeci și unu de ani și nu avea condamnări anterioare) să fie condamnat la pedeapsa cu închisoarea de cel puțin trei ani; sau în cazul în care comportamentul a implicat recursul la violență, a avut ca rezultat un câștig financiar substanțial sau a fost săvârșit de un număr mare de persoane în urmărirea unui scop comun (supra, pct. 63). În al treilea rând, art. 17 din RIPA și punctul 8.3 din Codul IC prevedeau că, în general, nici posibilitatea de interceptare, nici materialele interceptate nu puteau, în sine, juca un rol în acțiunile judiciare (supra, pct. 83 și 96). Prin urmare, deși interceptarea putea fi utilizată în scopul prevenirii sau detectării infracțiunilor grave, materialele interceptate nu puteau fi utilizate în cadrul procesului penal. În plus, punctul 6.8 din Codul IC prevedea că scopul mandatului emis în temeiul art. 8 alin. (4) va „reflecta, de regulă, una sau mai multe dintre prioritățile în materie de informații stabilite de Consiliul Național de Securitate” (supra, pct. 96 și 98).

370. În principiu, cu cât motivele sunt mai ample, cu atât este mai mare potențialul apariției de abuzuri. Cu toate acestea, motive mai restrânse și/sau mai bine definite ar oferi o garanție efectivă împotriva abuzurilor numai dacă

ar exista suficiente alte garanții pentru a se asigura că interceptarea în masă este autorizată numai pentru un motiv permis și că aceasta este necesară și proporțională în acest scop. Întrebarea strâns legată de existența unor garanții suficiente pentru a se asigura că interceptarea a fost necesară sau justificată este, prin urmare, la fel de importantă ca gradul de precizie cu care pot fi definite motivele pentru care se poate acorda autorizația. Prin urmare, în opinia Curții, un regim care permite dispunerea interceptării în masă pentru motive relativ largi poate fi în continuare conform cu art. 8 din Convenție, cu condiția ca, privit în ansamblu, sistemul să includă suficiente garanții împotriva abuzurilor pentru a compensa această deficiență.

371. În Regatul Unit, deși motivele pentru care putea fi autorizată interceptarea în masă erau formulate în termeni relativ generali, acestea se concentrau în continuare asupra securității naționale, precum și asupra infracțiunilor grave și asupra bunăstării economice a țării, în măsura în care aceste interese erau, de asemenea, relevante pentru interesele securității naționale (supra, pct. 368). Prin urmare, Curtea va analiza celelalte garanții integrate în regimul prevăzut la art. 8 alin. (4) pentru a stabili dacă, privite în ansamblu, acestea erau conforme cu art. 8 din Convenție.

– 2. „Circumstanțele” în care comunicațiile unei persoane pot fi interceptate

372. Pct. 6.2 din Codul IC (supra, pct. 96) prevedea în mod clar că „[s]pre deosebire de art. 8 alin. (1), un mandat emis în temeiul art. 8 alin. (4) nu trebuie să numească sau să descrie subiectul interceptării sau un set de spații în legătură cu care urmează să aibă loc interceptarea. De asemenea, art. 8 alin. (4) nu impune o limitare expresă a numărului de comunicații externe care pot fi interceptate”. Cu alte cuvinte, erau vizate mai degrabă canalele de transmisie de comunicații decât dispozitivele de la care erau trimise comunicațiile, sau expeditorii sau destinatarii comunicațiilor. În lipsa unei limite a numărului de comunicații care puteau fi interceptate, se pare că toate pachetele de comunicații transmise prin canalele de transmisie vizate în perioada în care mandatul era în vigoare erau interceptate.

373. Acestea fiind spuse, un mandat emis în temeiul art. 8 alin. (4) era un mandat de interceptare a comunicațiilor externe (supra, pct. 72), iar pct. 6.7 din Codul IC (supra, pct. 96), impunea ca agenția care efectua interceptarea în temeiul unui mandat emis în temeiul art. 8 alin. (4) să se folosească de cunoștințele sale despre modul în care comunicațiile internaționale erau rutate, coroborat cu verificări regulate ale legăturilor de comunicații relevante, pentru a identifica operatorii de comunicații individuali care aveau cele mai multe șanse să conțină comunicații externe care respectau descrierea elementelor menționate în certificatul ministerial. De asemenea, agenția trebuia să efectueze interceptarea într-un mod care să limiteze colectarea de comunicații externe la un nivel minim compatibil cu obiectivul interceptării comunicațiilor externe dorite. Prin urmare, canalele de transmisie nu erau alese aleatoriu. Dimpotrivă, erau selectate, întrucât se considera că sunt cele

mai susceptibile de a purta comunicații externe de interes pentru serviciile de informații.

374. Pct. 6.5 din Codul IC definea „comunicațiile externe” ca fiind comunicații care fie au fost trimise, fie au fost primite în afara Insulelor Britanice (supra, pct. 96). În cazul în care atât expeditorul, cât și destinatarul se aflau în interiorul Insulelor Britanice, comunicațiile erau interne. Prin urmare, aspectul dacă o comunicație era sau nu „externă” depindea de localizarea geografică a expeditorului și a destinatarului, nu de ruta prin care comunicația a ajuns la destinație. Comunicațiile care depășeau frontierele Regatului Unit (comunicații internaționale) puteau fi în continuare „interne”, deoarece o comunicație (sau pachete de comunicații) atât trimise din, cât și primite în Regatul Unit puteau fi, cu toate acestea, rutate prin una sau mai multe țări terțe.

375. Distincția dintre comunicațiile interne și cele externe nu împiedica, așadar, interceptarea comunicațiilor interne care traversau granițele Regatului Unit și, în realitate, „captura accidentală” a unor astfel de comunicații era permisă în mod expres de art. 5 alin. (6) din RIPA, care prevedea că comportamentul autorizat de un mandat de interceptare includea interceptarea comunicațiilor neidentificate de mandat, dacă era necesar, pentru a se realiza ceea ce era autorizat în mod expres de mandat (supra, pct. 68). În plus, definiția termenului „extern” era ea însăși suficient de largă pentru a include stocarea în cloud și activitățile de navigare și de comunicare socială ale unei persoane în Regatul Unit (supra, pct. 75 și 76). Cu toate acestea, astfel cum a admis Camera, garanția acordată „comunicațiilor externe” avusese un rol de jucat la nivelul macro de selectare a canalelor de transmisie pentru interceptare (pct. 337 din hotărârea Camerei), întrucât agenția de interceptare trebuia să se folosească de cunoștințele sale despre modul în care erau rutate comunicațiile internaționale pentru a le identifica pe cele care aveau cele mai mari șanse să conțină comunicații externe de valoare operațiunii, chiar dacă totuși, într-o măsură limitată, garanția restrângea categoriile de persoane susceptibile să le fie interceptate comunicațiile. De asemenea, garanția era relevantă în ceea ce privește proporționalitatea, întrucât statele puteau dispune de măsuri mai puțin intruzive pentru a obține comunicațiile persoanelor aflate sub jurisdicția lor teritorială.

376. În lumina celor de mai sus, Curtea consideră că, în temeiul regimului prevăzut la art. 8 alin. (4), comunicațiile internaționale (și anume, comunicațiile care depășeau granițele statale) puteau fi interceptate; serviciile de informații își utilizau doar competența de a le intercepta pe cele mai susceptibile să transmită comunicații externe de interes pentru serviciile de informații. În contextul interceptării în masă, este dificil *in abstracto* de imaginat cum ar putea fi delimitate și mai mult circumstanțele în care ar putea fi interceptate comunicațiile unei persoane. În orice caz, întrucât nici expeditorul, nici destinatarul unei comunicații electronice nu ar putea

controla ruta pe care a parcurs-o până la destinație, în practică, nicio restricție suplimentară privind alegerea canalelor de transmisie nu făcea ca dreptul intern să fie mai previzibil în ceea ce privește efectele sale. Prin urmare, Curtea admite că circumstanțele în care comunicațiile unei persoane puteau fi interceptate în temeiul regimului prevăzut la art. 8 alin. (4) erau suficiente de „previzibile” în sensul art. 8 din Convenție.

– 3. *Procedura care trebuie urmată pentru acordarea autorizației*

377. Cerere de emitere a mandatului prevăzut la articolul 8 alin. (4) din RIPA era transmisă ministrului, singurul abilitat să emită un astfel de mandat. Înainte de a fi formulată, fiecare cerere făcea obiectul unui control în cadrul agenției care o întocmea. Aceasta presupunea examinarea de către mai mult de un funcționar, care trebuia să analizeze dacă cererea era depusă într-un scop care intra sub incidența art. 5 alin. (3) din RIPA și dacă interceptarea propusă respecta standardele de necesitate și de proporționalitate prevăzute de Convenție (punctul 6.9 din Codul IC, supra, pct. 96). Acest nivel suplimentar de control intern era fără îndoială valoros, dar rămâne problema că, la momentul faptelor, interceptarea în masă efectuată în temeiul regimului prevăzut la art. 8 alin. (4) era autorizată de ministru, nu de un organism independent de executiv. În consecință, regimul prevăzut la art. 8 alin. (4) nu conținea una dintre garanțiile fundamentale, și anume, faptul că interceptarea în masă ar fi trebuit să facă obiectul unei autorizări independente încă de la început (supra, pct. 350).

378. În ceea ce privește nivelul de control exercitat de ministru, pct. 6.10 din Codul IC preciza în detaliu informațiile care trebuia să fie incluse în cerere (supra, pct. 96). Cererea includea următoarele: o descriere a comunicațiilor care urmau să fie interceptate, detalii ale furnizorului (furnizorilor) de servicii de comunicații și o evaluare a fezabilității operațiunii, după caz; o descriere a operațiunii care urma să fie autorizată; certificatul care va reglementa examinarea materialelor interceptate (infra, pct. 378 și 379); o explicație a motivului pentru care interceptarea era considerată necesară pentru unul sau mai multe dintre scopurile prevăzute la art. 5 alin. (3); o prezentare a motivelor pentru care se considera că operațiunea era proporțională cu ceea ce se dorea a fi îndeplinit; o garanție privind faptul că materialele interceptate vor fi citite, consultate sau ascultate doar în măsura în ceea ce se preciza în certificat și că erau îndeplinite condițiile art. 16 alin. (2) din RIPA; o garanție că materialele interceptate vor fi tratate în conformitate cu garanțiile prevăzute la art. 15 și art. 16.

379. Prin urmare, ministrul era informat despre scopul operațiunii [care trebuia să fie unul din scopurile prevăzute la art. 5 alin. (3)] și, înainte de a emite un mandat, trebuia să se asigure că era necesar în acest scop și că era proporțional cu ceea ce se intenționa să se realizeze (pct. 6.11 și 6.13 din Codul IC, supra, pct. 96). În cadrul aprecierii proporționalității, ministrul trebuia să examineze dacă mandatul era excesiv în ansamblul circumstanțelor

cauzei și dacă informațiile solicitate puteau fi obținute în mod rezonabil prin mijloace mai puțin intruzive (pct. 3.6 din Codul IC, supra, pct. 96). În special, trebuia să fie pusă în balanță dimensiunea și amploarea ingerinței în raport cu ceea ce se intenționa să se realizeze; era necesară o explicație privind modul și motivele pentru care metodele ar provoca cea mai mică intruziune posibilă asupra subiectului și a altora; trebuia să se examineze dacă activitatea constituia o modalitate adecvată de a obține rezultatul necesar, având în vedere toate alternativele rezonabile; și, în măsura în care era rezonabil posibil, trebuia să fie oferite dovezi ale altor metode avute în vedere, dar evaluate ca fiind insuficiente pentru îndeplinirea obiectivelor operaționale (pct. 3.7 din Codul IC, supra, pct. 96).

380. Deși cererea de emitere a unui mandat în temeiul art. 8 alin. (4) trebuia să includă „o descriere a comunicațiilor care urmează să fie interceptate” și „detalii privind furnizorul (furnizorii) de servicii de comunicații”, Guvernul a confirmat în ședință că mandatul nu preciza anumite canale de transmisie, deoarece ar exista „dificultăți grave de ordin practic” dacă aceasta ar fi o cerință. Cu toate acestea, era obligatoriu să existe o descriere adecvată a ceea ce ar implica interceptarea și detalii privind „tipurile de canale de transmise” care urmau să fie interceptate. Aceste informații stăteau la baza evaluării efectuate de ministru cu privire la necesitatea și proporționalitatea operațiunii descrise în cerere. În plus, Guvernul a confirmat în observațiile prezentate în fața Marii Camere că GCHQ îl informa pe Comisarul IC în mod regulat cu privire la baza prin care fuseseră selectate canalele de transmisie spre interceptare (supra, pct. 290).

381. De asemenea, cererea de emitere a unui mandat în temeiul art. 8 alin. (4) nu trebuia să includă o mențiune a categoriilor de selectori care trebuie utilizați. În consecință, nu exista nicio posibilitate ca necesitatea și proporționalitatea acestora să fie evaluate în etapa de autorizare, deși alegerea selectorilor făcea ulterior obiectul unei supravegheri independente. În observațiile prezentate în fața Marii Camere, Guvernul a confirmat că, ori de câte ori un nou selector era adăugat în sistem, analistul care îl adăuga trebuia să completeze un registru scris, explicând de ce era necesar și proporțional să fie aplicat selectorul în scopurile menționate în certificatul ministrului. Acest lucru se realiza prin selectarea textului dintr-un meniu vertical, urmat de adăugarea, de către analist, a unui text liber, explicând motivul pentru care era necesar și proporțional să se efectueze căutarea. Utilizarea selectorilor trebuia să fie înregistrată într-o locație aprobată care permitea să fie auditată; era creat un registru al selectorilor în uz care să poată fi verificat, astfel încât Comisarul IC să îl poată controla (supra, pct. 291-292). Alegerea selectorilor era, prin urmare, supusă controlului Comisarului IC, iar în raportul său anual pe 2016 „a fost impresionat de calitatea declarațiilor” întocmite de analiști care explicau necesitatea și proporționalitatea adăugării unui nou selector (supra, pct. 177).

382. Având în vedere că alegerea selectorilor și a termenilor de căutare determinau care erau comunicațiile care puteau fi examinate de un analist, Curtea a indicat că este de o importanță fundamentală ca cel puțin categoriile de selectori să fie identificate în autorizație și ca acești selectori puternici legați de persoane identificabile să facă obiectul unei autorizări interne prealabile, care să prevadă verificarea separată și obiectivă a conformității justificării cu principiile sus-menționate (supra, pct. 353-355).

383. În speță, lipsa oricărei supravegheri a categoriilor de selectori în momentul autorizării constituia o deficiență a regimului prevăzut la art. 8 alin. (4). Controlul ulterior al tuturor selectorilor individuali nu îndeplinea nici cerința unor garanții sporite pentru utilizarea unor selectori puternici legați de persoane identificabile, nici necesitatea de a avea aplicat un proces de autorizare internă prealabilă, care să prevadă verificarea separată și obiectivă a conformității justificării cu principiile sus-menționate (supra, pct. 355). Chiar dacă analiștii aveau obligația să înregistreze și să justifice utilizarea fiecărui selector în ceea ce privește principiile necesității și proporționalității consacrate de Convenție și această justificare făcea obiectul unei supravegheri independente din partea Comisarului IC, selectorii puternici legați de persoane identificabile nu făceau însă obiectul unei autorizări interne prealabile.

– 4. *Procedurile care trebuie urmate pentru selectarea, examinarea și utilizarea materialelor interceptate*

384. Pct. 6.4 din Codul IC prevedea că, în cazul în care un mandat emis în temeiul art. 8 alin. (4) conducea la obținerea unor volume mari de comunicații, persoanele autorizate din cadrul agenției de interceptare puteau aplica selectori puternici și căutări complexe pentru a genera un index (supra, pct. 96). Acest proces de selecție era delimitat de art. 16 alin. (2) din RIPA și de pct. 7.19 din Codul IC, care prevedeau că un selector nu se putea referi la o persoană despre care se cunoaște că se află în Insulele Britanice și să aibă ca scop identificarea materialelor conținute în comunicațiile trimise sau destinate acestuia, cu excepția cazului în care ministrul autorizase personal utilizarea selectorului, după ce se asigurase în prealabil că acest lucru era necesar în interesul securității naționale, în scopul prevenirii sau al detectării unei infracțiuni grave, sau în scopul protejării intereselor economice ale Regatului Unit, precum și că era proporțional (supra, pct. 85 și 96).

385. Doar materialele din index puteau fi examinate de un analist (supra, pct. 96 și 289); nu putea fi emis niciun raport de informații despre niciun fel de comunicații sau date de comunicații decât în cazul în care acestea erau examinate de un analist (supra, pct. 289). În plus, pct. 7.13 din Codul IC prevedea că doar elementele descrise în certificatul emis de ministru erau disponibile spre examinare umană și niciun funcționar nu era autorizat să aibă acces la materiale altele decât cel autorizat de certificat (supra, pct. 96). În plus, punctul 6.4 prevedea că, înainte ca o anumită comunicație să poată fi

accesată de o persoană autorizată din cadrul agenției de interceptare, aceasta trebuia să explice de ce era necesară pentru unul dintre motivele menționate în certificatul însoțitor și de ce era proporțională în împrejurările specifice, ținând seama de aspectul dacă informațiile puteau fi obținute în mod rezonabil prin mijloace mai puțin intruzive (supra, pct. 96).

386. Certificatul ministrului era emis odată cu mandatul și urmărea să asigure aplicarea unui proces de selecție a materialelor interceptate astfel încât numai elementele descrise în certificat să fie puse la dispoziție spre examinare umană (pct. 6.3 și 6.14 din Codul IC, supra, pct. 96). Deși certificatul juca un rol important în reglementarea accesului la materialele interceptate, atât rapoartele ISC, cât și cele ale evaluatorului independent al legislației în materie de combatere a terorismului (*Independent Reviewer of Terrorism Legislation*) au criticat faptul că materialele identificate în aceste certificate erau redactate în termeni foarte generali [de exemplu, „materiale care furnizează informații privind terorismul, astfel cum sunt definite în Legea privind terorismul din 2000 (astfel cum a fost modificată)"] (pct. 342 din hotărârea Camerei și supra, pct. 146 și 155). Curtea este de acord cu opinia Camerei potrivit căreia aceasta constituia o deficiență a sistemului de garanții oferite în temeiul regimului prevăzut la art. 8 alin. (4).

387. Cu toate acestea, potrivit ISC, deși certificatul stabilea categoriile generale de informații care puteau fi examinate, în practică era vorba despre selectarea canalelor de transmisie, aplicarea unor selectori simpli și a unor criterii de căutare inițiale, iar apoi căutări complexe care determinau care erau comunicațiile examinate (supra, pct. 146-147). Cu alte cuvinte, deși certificatele reglementau selectarea de către analist a materialelor dintr-un index generat de calculator, alegerea canalelor de transmisie și a selectorilor/termenilor de căutare era cea care determina în primul rând comunicațiile care figurau în respectivul index (și, prin urmare, erau eligibile spre examinare). Cu toate acestea, Curtea a afirmat deja că atât lipsa identificării categoriilor de selectori în cererea de emitere a unui mandat, cât și lipsa unei autorizări interne prealabile a acestor selectori puternici legați de o persoană identificabilă constituiau deficiențe ale regimului prevăzut la art. 8 alin. (4) (supra, pct. 382). Aceste deficiențe au fost agravate de caracterul general al certificatelor emise de ministru. Nu doar că nu exista o autorizare independentă prealabilă a categoriilor de selectori utilizați pentru a genera indexul și nicio autorizare internă a acestor selectori puternici legați de o persoană identificabilă, ci mai mult, certificatul care reglementa accesul la materialele din index era redactat în termeni insuficient de preciși pentru a stabili vreo restricție semnificativă.

388. Pct. 7.16 din Codul IC impunea, în plus, ca analistul care solicita accesul la materialele din index să indice orice circumstanțe susceptibile să conducă la o anumită încălcare colaterală a vieții private, precum și măsurile luate pentru a reduce amploarea acestei intruziuni (supra, pct. 96). Orice acces ulterior al analistului era limitat la o anumită perioadă de timp și, în

cazul în care această perioadă era reînnoită, registrul trebuia actualizat pentru a justifica reînnoirea (pct. 7.17 din Codul IC, supra, pct. 96). Potrivit pct. 7.18 din Codul IC, erau efectuate audituri regulate care includeau verificări pentru a se asigura că registrele cererilor de acces la materiale erau corect întocmite și că materialele solicitate intrau în domeniile de interes ale certificatului ministerial (supra, pct. 96).

389. În plus, potrivit pct. 7.15, materialele colectate în temeiul unui mandat emis în temeiul art. 8 alin. (4) puteau fi citite, consultate sau ascultate numai de persoane autorizate (analiști) care beneficiau în mod regulat de formare obligatorie în ceea ce privește dispozițiile RIPA și cerințele privind necesitatea și proporționalitatea, și care erau evaluate în mod corespunzător (supra, pct. 96). În temeiul punctului 7.10, evaluarea fiecărui membru al personalului făcea obiectul unei reexaminări periodice (supra, pct. 96).

390. Pct. 7.6 din Codul IC prevedea că materialele interceptate puteau fi copiate numai în măsura în care era necesar pentru scopurile autorizate și sub rezerva unei aplicări stricte a principiului „necesității de a cunoaște”, inclusiv furnizarea de extrase sau rezumate în cazul în care era suficient pentru utilizator de a cunoaște. Art. 15 alin. (5) din RIPA prevedea proceduri care să garanteze că fiecare copie a materialelor sau a datelor care era făcută era stocată, atâta timp cât era păstrată, în siguranță (supra, pct. 81), iar pct. 7.7 impunea, de asemenea, ca înainte de distrugere, materialele interceptate, precum și toate copiile, extrasele și rezumatele acestora să fie stocate în siguranță și să nu poată fi accesibile persoanelor fără nivelul de autorizare de securitate necesar (supra, pct. 96).

391. Sub rezerva deficiențelor menționate anterior referitoare la autorizarea selectorilor (supra, pct. 381 și 382) și a naturii generale a certificatelor ministrului internelor (supra, pct. 386), Curtea consideră că circumstanțele în care materialele interceptate puteau fi selectate, examinate, utilizate și stocate în temeiul art. 8 alin. (4) erau suficient de „previzibile” în sensul art. 8 din Convenție și că furnizau garanții adecvate împotriva abuzurilor.

– 5. *Măsurile de precauție care trebuie luate la comunicarea datelor către alte părți;*

392. Art. 15 alin. (2) din RIPA prevedea ca următoarele să fie limitate la minimum necesar pentru „scopuri autorizate”: numărul de persoane cărora le erau divulgate sau puse la dispoziție materialele sau datele, măsura în care materialele sau datele erau divulgate sau puse la dispoziție, măsura în care materialele sau datele erau copiate, numărul de copii care erau făcute (supra, pct. 78). Conform art. 15 alin. (4) și pct. 7.2 din Codul IC, o acțiune era necesară, în scopurile autorizate, numai dacă măsura continua să fie sau putea deveni necesară în scopurile menționate la art. 5 alin. (3) din RIPA; pentru a facilita îndeplinirea vreuneia dintre funcțiile de interceptare a ministrului; pentru a facilita îndeplinirea oricăror funcții ale Comisarului IC sau ale IPT; pentru a se asigura că o persoană care efectua cercetarea penală deținea

informațiile de care avea nevoie pentru a stabili ce era necesar de făcut menținând caracterul echitabil al procedurii (deși materialele interceptate nu puteau fi ele însele utilizate în cadrul procesului penal – pct. 8.3 din Codul IC, supra, pct. 96); pentru a îndeplini oricare din obligațiile impuse oricărei persoane în temeiul legilor privind arhivele publice (supra, pct. 80 și 96).

393. Pct. 7.3 din Codul IC interzicea divulgarea către persoanele care nu fuseseră verificate în mod corespunzător și, de asemenea, principiul „necesității de a cunoaște”: materialele interceptate nu puteau fi divulgate niciunei persoane decât dacă atribuțiile respectivei persoane, care trebuia să aibă legătură cu unul dintre scopurile autorizate, erau de natură să „aibă nevoie să cunoască” informații despre materialele interceptate pentru îndeplinirea respectivelor atribuții. În mod similar, din materialele interceptate putea fi divulgat numai ceea ce avea nevoie destinatarul (supra, pct. 96). Pct. 7.3 se aplica în mod egal și divulgării de informații altor persoane suplimentare din cadrul unei agenții, precum și divulgării în afara agenției (supra pct. 96). În temeiul pct. 7.4, interdicția nu se aplica doar interceptorului inițial, ci și oricărei persoane căreia îi erau divulgate ulterior materialele interceptate (supra, pct. 96).

394. Astfel cum a observat Camera, întrucât exprimarea „putea deveni necesar” nu a fost definită mai în detaliu în RIPA sau în Codul IC și nici în altă parte, art. 15 alin. (4) și pct. 7.2 ar fi putut, în practică, să confere autorităților puteri extinse de a divulga și de a copia materialele interceptate. Cu toate acestea, materialele nu puteau fi divulgate decât unei persoane care dispunea de un nivel adecvat de autorizare de securitate, care avea „nevoie să cunoască”, iar din materialele interceptate putea fi divulgat numai ceea ce persoana avea nevoie să cunoască. Prin urmare, Curtea este de acord cu opinia Camerei potrivit căreia includerea expresiei „putea deveni necesar” nu reducea în mod semnificativ garanțiile care protejau datele obținute prin interceptarea în masă (pct. 368 și 369 din hotărârea Camerei).

395. Examinând, în continuare, transferul materialelor interceptate în afara Regatului Unit, la momentul interceptării materialelor în conformitate cu dreptul intern, Curtea consideră că transferul acestor materiale către un serviciu partener de informații străin sau către o organizație internațională nu ar ridica o problemă în temeiul art. 8 din Convenție decât dacă statul care a efectuat interceptarea nu s-ar asigura în prealabil că serviciul partener de informații, în momentul tratării materialelor, dispune de garanții de natură să prevină abuzurile și ingerințele disproporționate și, în special, poate garanta stocarea în siguranță a materialelor și restricționează divulgarea ulterioară a acestora (supra, pct. 362).

396. În Regatul Unit, se pare că partenerii Five Eyes puteau accesa elemente ale produsului mandatelor de interceptare ale GCHQ în propriile sisteme (supra, pct. 180). În astfel de cazuri, interceptarea materialului de către serviciile de informații din Regatul Unit a fost efectuată în conformitate cu dreptul intern, inclusiv, în măsura în care este relevant în speță, cu art. 8

alin. (4) din RIPA. Potrivit pct. 7.5 din Codul IC, în cazul în care materialele interceptate erau divulgate autorităților unei țări sau ale unui teritoriu din afara Regatului Unit, trebuia ca serviciile de informații să ia măsuri rezonabile pentru a se asigura că autoritățile în cauză aveau și continuau să mențină procedurile necesare pentru a proteja materialele interceptate și pentru a se asigura că acestea erau divulgate, copiate, distribuite și păstrate numai în măsura strictului minim necesar. Materialele interceptate nu puteau fi dezvăluite ulterior autorităților unei țări terțe sau ale unui teritoriu terț decât cu excepția cazului în care se convenea în mod explicit cu agenția emitentă și era necesar ca materialele să fie returnate agenției emitente sau distruse în condiții de siguranță, atunci când nu mai erau necesare (supra, pct. 96). Art. 15 alin. (7) din RIPA prevedea, de asemenea, că era necesar să fie în vigoare restricții care să împiedice orice acțiune în legătură cu o procedură judiciară desfășurată în afara Regatului Unit care ar divulga conținutul sau datele de comunicații aferente ale unei comunicații interceptate, în cazul în care o astfel de divulgare nu ar fi putut fi efectuată în Regatul Unit (supra, pct. 82).

397. În ceea ce privește materialele confidențiale, pct. 4.30 din Codul IC prevedea că, în cazul în care informațiile confidențiale erau diseminate unui organ extern, trebuia să fie luate măsuri rezonabile pentru a marca informațiile ca fiind confidențiale. În cazul în care existau îndoieli cu privire la legalitatea diseminării preconizate a informațiilor confidențiale, trebuia să se solicite consiliere din partea unui consilier juridic din cadrul agenției de interceptare relevante și înainte ca orice diseminare ulterioară a materialului să se producă (supra, pct. 96).

398. Prin urmare, erau instituite garanții pentru a se asigura că serviciile de informații partenere vor garanta depozitarea în condiții de siguranță a materialelor transferate și vor restricționa divulgarea ulterioară a acestora. O ultimă garanție, căreia Curtea îi acordă o importanță deosebită, este supravegherea asigurată de comisarul IC și de IPT (infra, pct. 411 și 414).

399. Având în vedere cele de mai sus, Curtea consideră că măsurile de precauție care trebuia să fie luate pentru comunicarea materialelor interceptate către alte părți erau suficient de clare și ofereau garanții suficient de solide împotriva abuzurilor.

– 6. *Limitele privind durata interceptării, stocarea materialelor interceptate și circumstanțele în care aceste materiale trebuiau șterse sau distruse*

400. În ceea ce privește durata mandatelor emise în temeiul art. 8 alin. (4) din motive legate de securitatea națională sau bunăstarea economică a Regatului Unit, în măsura în care aceste interese erau relevante și pentru interesele securității naționale, în temeiul art. 9 din RIPA, acestea încetau să mai producă efect după șase luni, cu excepția cazului în care erau reînnoite. Mandatele emise de ministru în temeiul art. 8 alin. (4) în scopul prevenirii infracțiunilor grave încetau să mai producă efect după trei luni, cu excepția

cazului în care erau reînnoite. Aceste mandate puteau fi reînnoite pentru perioade de șase, respectiv de trei luni, și puteau fi reînnoite în orice moment înainte de data expirării lor, printr-o cerere adresată ministrului. Cererea respectivă trebuia să conțină aceleași informații ca cererea inițială, precum și o evaluare a valorii interceptării până la acest punct și o explicație a motivului pentru care reînnoirea era necesară, în sensul art. 5 alin. (3), și proporțională (art. 9 din RIPA, supra, pct. 67, și pct. 6.22-6.24 din Codul IC, supra, pct. 96). Ministrul avea obligația să anuleze un mandat – chiar înainte de data inițială de expirare – în cazul în care considera că nu mai este necesar, din motivele enunțate la art. 5 alin. (3) (art. 9 din RIPA, supra, pct. 67).

401. Având în vedere limitarea clară a duratei mandatelor emise în temeiul art. 8 alin. (4) și cerința ca acestea să facă obiectul unei verificări permanente, Curtea consideră că regulile referitoare la durata interceptării în temeiul regimului prevăzut la art. 8 alin. (4) erau suficient de clare și ofereau garanții adecvate împotriva abuzurilor.

402. Pct. 7.9 din Codul IC prevedea că, în cazul în care un serviciu de informații primea materiale interceptate neanalizate și date de comunicații aferente interceptării în executarea unui mandat emis în temeiul art. 8 alin. (4), acesta trebuia să specifice perioadele maxime de păstrare pentru diferite categorii de materiale, care să reflecte natura și gradul de intruziune al mandatului. În mod normal, perioadele specificate nu puteau depăși doi ani și trebuia ca acestea să fie convenite cu Comisarul IC. În măsura posibilului, trebuia ca toate perioadele de păstrare să fie puse în aplicare printr-un proces de ștergere automată, declanșat odată ce a fost atinsă perioada maximă de păstrare aplicabilă (supra, pct. 96). În conformitate cu pct. 7.8 din Codul IC, materialele interceptate păstrate erau verificate la intervale corespunzătoare pentru a se confirma că justificarea păstrării acestora era încă valabilă în temeiul art. 15 alin. (3) din RIPA (supra, pct. 96).

403. În observațiile prezentate în fața Marii Camere, Guvernul a furnizat informații suplimentare cu privire la perioadele de păstrare. Comunicațiile cărora li se aplica doar procesul „selectorului puternic” erau imediat eliminate în cazul în care nu corespundeau selectorului puternic. Comunicațiile pentru care se aplica și procesul de „căutare complexă” erau păstrate câteva zile, pentru a permite desfășurarea procesului, iar apoi erau șterse în mod automat, cu excepția cazului în care erau selectate spre examinare. Comunicațiile care erau selectate spre examinare puteau fi păstrate numai în cazul în care era necesar și proporțional. Poziția implicită era aceea că perioada de păstrare a comunicațiilor selectate nu depășea câteva luni, după care erau șterse automat (deși materialele erau citate în raportarea informațiilor, rapoartele erau păstrate), dar în circumstanțe excepționale, se poate lua în considerare păstrarea comunicațiilor selectate pentru o perioadă mai îndelungată (supra, pct. 293). Prin urmare, în practică, se pare că perioadele de păstrare erau semnificativ mai scurte decât perioada maximă de păstrare de doi ani.

404. În sfârșit, art. 15 alin. (3) din RIPA și pct. 7.8 din Codul IC impuneau ca fiecare copie a materialelor interceptate (alături de eventualele extrase și rezumate) să fie distruse în siguranță de îndată ce păstrarea nu mai era necesară pentru niciunul dintre scopurile prevăzute la art. 5 alin. (3) (supra, pct. 79 și 96).

405. În cadrul procedurii *Liberty*, IPT a examinat procedurile care reglementau păstrarea materialelor și distrugerea acestora și le-a considerat adecvate (supra, pct. 50). Curtea consideră, de asemenea, că măsurile „nepublice” care stabileau circumstanțele în care trebuia ca materialele interceptate să fie șterse sau distruse erau suficient de clare. Cu toate acestea, în opinia sa, ar fi fost de dorit ca perioadele de păstrare mai scurte identificate de Guvern în cursul prezentei proceduri să se fi reflectat în măsuri legislative și/sau în alte măsuri generale adecvate.

– 7. *Supravegherea*

406. Supravegherea regimului prevăzut la art. 8 alin. (4) a fost efectuată în primul rând de către Comisarul CI, deși, potrivit acestuia, „funcția critică de asigurare a calității [era] desfășurată inițial de personal și de avocați din cadrul agenției de interceptare sau al departamentului care emitea mandatele” care ofereau consiliere independentă ministrului și efectuau un control prealabil al autorizării cererilor de emitere de mandat și al reînnoirilor, pentru a se asigura că acestea erau (și rămâneau) necesare și proporționale (supra, pct. 170).

407. Comisarul CI era independent de executiv și de legislativ și deținea o înaltă funcție judiciară. Principala sa misiune era de a examina exercitarea și realizarea, de către miniștri și de către autoritățile publice relevante, a puterilor prevăzute în Partea 1 (și, într-o măsură limitată, Partea 3) din RIPA și de a supraveghea un regim de inspecție care să îi permită să efectueze o supraveghere independentă a modului în care era aplicată legea. Comisarul prezenta prim-ministrului în mod regulat rapoarte semestriale cu privire la activitățile sale și redacta un raport anual care era prezentat ambelor Camere ale Parlamentului. În plus, după fiecare inspecție, șefului agenției inspectate îi era trimis un raport care conținea recomandări formale și care solicita ca agenția să răspundă tot printr-un raport, în termen de două luni, pentru a confirma dacă au fost puse în aplicare recomandările sau ce progrese au fost realizate. Rapoartele sale periodice au fost publicate începând cu 2002, iar din 2013 au fost publicate integral, fără anexe cu caracter confidențial. În plus, art. 58 alin. (1) din RIPA impunea tuturor funcționarilor publici dintr-o organizație obligația statutară de a divulga sau de a-i furniza Comisarului IC toate documentele sau informațiile necesare pentru a-și putea îndeplini atribuțiile (supra, pct. 136 și 135).

408. Raportul din 2016 al Comisarului IC furnizează dovezi cu privire la întinderea competențelor sale de supraveghere. Pe scurt, în timpul inspecțiilor, a evaluat sistemele existente pentru interceptarea comunicațiilor

și s-a asigurat că toate registrele relevante fuseseră păstrate; a examinat cererile de interceptare selectate pentru a evalua dacă îndepliniseră cerințele de necesitate și proporționalitate; a intervievat ofițerii de caz și analiștii pentru a evalua dacă interceptările și justificările pentru obținerea tuturor materialelor fuseseră proporționale; a examinat orice aprobări orale urgente pentru a verifica dacă procesul fusese justificat și utilizat în mod corespunzător; a examinat acele cazuri în care comunicațiile care făcuseră obiectul secretului profesional sau alte informații confidențiale fuseseră interceptate și păstrate, și orice cazuri în care un avocat fusese subiectul unei investigații; a examinat caracterul adecvat al măsurilor de protecție și al dispozițiilor prevăzute la art. 15 și 16 din RIPA; a investigat procedurile existente pentru păstrarea, stocarea și distrugerea materialelor interceptate și a datelor de comunicații aferente; a analizat erorile raportate și suficiența oricăror măsuri adoptate pentru a preveni reparația acestora (supra, pct. 171).

409. În cursul anului 2016, Biroul Comisarului IC a inspectat de două ori toate cele nouă agenții de interceptare și cele patru departamente principale care emiteau mandatele. Au fost inspectate 970 de mandate, reprezentând 61% din numărul de mandate în vigoare la sfârșitul anului și 32% din totalul noilor mandate emise în 2016 (supra, pct. 173 și 175).

410. Inspecțiile implicau, de regulă, un proces în trei etape. În primul rând, pentru a obține un eșantion reprezentativ de mandate, inspectorii le selectau pentru diferite tipuri de infracțiuni și amenințări la adresa securității naționale, concentrându-se pe cele de interes sau sensibilitate deosebită. În al doilea rând, inspectorii verificau în detaliu mandatele selectate și documentația aferentă în timpul zilelor de lectură care precedau inspecțiile. În această etapă, inspectorii examinau declarațiile de necesitate și proporționalitate formulate de analiști atunci când adăugau un selector la sistemul de colectare în vederea examinării. Fiecare declarație trebuia să fie de sine stătătoare și să răspundă cerinței generale privind prioritățile pentru colectarea de informații. În al treilea rând, identificau acele garanții, operațiuni sau zone ale procesului care necesitau informații sau clarificări suplimentare și stabileau întâlniri cu personalul operațional, juridic sau tehnic relevant. Atunci când era necesar, examinau și alte documente sau sisteme referitoare la mandatele respective (supra, pct. 174).

411. Comisarul IC a supravegheat, de asemenea, schimbul de materiale interceptate cu serviciile de informații partenere. În raportul său din 2016, a indicat faptul că GCHQ furnizase inspectorilor săi „detalii cuprinzătoare cu privire la acordurile de schimb de informații prin care partenerii rețelei Five Eyes puteau accesa elemente ale produsului mandatelor de interceptare ale GCHQ în propriile sisteme”. Inspectorii s-au întâlnit, de asemenea, cu reprezentanți ai comunității Five Eyes și au asistat la o demonstrație despre modul în care alți membri ai Five Eyes pot solicita acces la datele GCHQ. A observat că „accesul la sistemele GCHQ este strict controlat și trebuie justificat în conformitate cu legislația țării-gazdă și cu instrucțiunile de tratare

a datelor enunțate la garanțiile prevăzute la art. 15/16. A mai observat că, înainte de a avea acces la materialul de interceptare al GCHQ, analiștii Five Eyes urmau aceleași cursuri de formare juridică precum personalul GCHQ (supra, pct. 180).

412. În lumina celor de mai sus, Curtea este convinsă că Comisarul IC a asigurat o supraveghere independentă și eficientă a funcționării regimului prevăzut la art. 8 alin. (4). În special, acesta și inspectorii săi au fost în măsură să evalueze necesitatea și proporționalitatea unui număr semnificativ de cereri de emitere de mandat și alegerea ulterioară a selectorilor, precum și să investigheze procedurile în vigoare pentru păstrarea, stocarea și distrugerea comunicațiilor interceptate și a datelor de comunicații aferente. De asemenea, puteau să adreseze recomandări oficiale conducătorului autorităților publice în cauză, iar aceste autorități erau obligate să raporteze, în termen de două luni, cu privire la progresele realizate în punerea în aplicare a acestor recomandări. În plus, Guvernul a confirmat, în observațiile prezentate în fața Marii Camere, că GCHQ îl informa pe Comisarul IC în mod regulat cu privire la baza prin care fuseseră selectate canalele de transmisie spre interceptare (supra, pct. 290). Serviciile de informații erau obligate să țină registre în fiecare etapă a procesului de interceptare în masă și erau obligate să acorde inspectorilor acces la aceste registre (punctele 6.27 și 6.28 din Codul IC, supra, pct. 96). În sfârșit, Comisarul IC supraveghea, de asemenea, schimbul de materiale interceptate cu serviciile de informații partenere (supra, pct. 180).

– 8. Controlul *a posteriori*

413. Controlul *a posteriori* era efectuat de IPT, care, în prezenta cauză, a fost prezidat în toate momentele relevante de un judecător al *High Court*. Camera a concluzionat – iar părțile reclamante nu au contestat – că IPT oferă o cale de atac efectivă pentru reclamantii care se plâng atât de cazuri specifice de supraveghere, cât și de conformitate generală cu Convenția a regimurilor de supraveghere (pct. 265 din hotărârea Camerei). În această privință, Camera a concluzionat că era relevant faptul că IPT avea o competență extinsă pentru a examina orice plângere privind interceptarea ilegală care nu depindea de notificarea persoanei în privința interceptării (supra, pct. 122). În consecință, orice persoană care considera că a făcut obiectul unei supravegheri secrete putea depune o cerere în acest sens. Membrii IPT erau magistrați experimentați sau avocați calificați cu o vechime de cel puțin zece ani (supra, pct. 123). Persoanele implicate în autorizarea și executarea unui mandat de interceptare erau obligate să divulge IPT toate documentele pe care le putea solicita, inclusiv documentele „nepublice”, care nu puteau fi făcute publice din motive de securitate națională (supra, pct. 125). În plus, putea să organizeze audieri publice, atunci când era posibil (supra, pct. 129); în cadrul procedurilor cu ușile închise, putea solicita avocatului de pe lângă Tribunal să depună observații în numele reclamantilor

care nu puteau fi reprezentați (supra, pct. 132); atunci când se pronunța în privința unui reclamant, IPT avea competența de a acorda despăgubiri și de a dispune orice alte măsuri pe care le considera adecvate, inclusiv pronunțarea anulării sau încetării oricărui mandat și distrugerea înregistrărilor obținute în temeiul mandatului (supra, pct. 126). În sfârșit, hotărârile sale erau publicate pe propriul website dedicat, sporind astfel nivelul de control exercitat asupra activităților de supraveghere secrete în Regatul Unit (*Kennedy*, citată anterior, pct. 167).

414. În plus, IPT avea competență pentru a examina orice plângere cu privire la conformitatea cu Convenția, fie a transferului de materiale interceptate către terți, fie a regimului care reglementa transferul materialelor interceptate. Or, în speță, părțile reclamante din a treia cauză conexată nu au formulat niciun capăt de cerere specific în această privință în cursul procedurilor interne. Mai degrabă, plângerile lor cu privire la schimbul de informații s-au concentrat exclusiv asupra regimului care guverna primirea de informații de la țări terțe (infra, pct. 466-515).

415. Prin urmare, Curtea este convinsă că IPT a oferit o cale de atac solidă oricărei persoane care suspecta că comunicațiile sale au fost interceptate de serviciile de informații.

(3) Date de comunicații aferente

416. Curtea a precizat că, în contextul interceptării în masă, interceptarea, păstrarea și căutarea datelor de comunicații aferente trebuie analizate în raport cu aceleași garanții aplicabile conținutului, dar că dispozițiile legale care reglementează prelucrarea datelor de comunicații aferente nu trebuie să fie în mod necesar identice în toate privințele cu cele care reglementează tratarea conținutului (supra, pct. 363-364). În Regatul Unit, art. 8 alin. (4) impunea autorizarea interceptării atât în cazul conținutului, cât și în cel al datelor de comunicații aferente. Acestea din urmă erau tratate, în majoritatea privințelor, în mod identic în cadrul regimului prevăzut la art. 8 alin. (4). Astfel, deficiențele deja identificate cu privire la regimul care reglementa interceptarea conținutului (supra, pct. 377, 381-382) se aplicau deopotrivă și datelor de comunicații aferente, și anume: lipsa unei autorizații independente (supra, pct. 377); neidentificarea categoriilor de selectori din cererea de emiteră a unui mandat (supra, pct. 381 și 382); faptul că selectorii legați de persoane identificabile nu făceau obiectul unei autorizări interne prealabile; lipsa previzibilității circumstanțelor în care comunicațiile puteau fi examinate (supra, pct. 391), având în vedere atât lipsa identificării categoriilor de selectori în cererea de emiteră a unui mandat (supra, pct. 381 și 382), cât și caracterul general al certificatelor ministrului (supra, pct. 386).

417. Totodată, tratamentul datelor de comunicații beneficia în cea mai mare parte de aceleași garanții ca cele aplicate conținutului. La fel ca acestea din urmă, primele făceau obiectul unui proces de filtrare automată în timp cvasi-real, o mare parte din acestea fiind șterse instantaneu în această fază; de

asemenea, făceau obiectul unor căutări simple sau complexe pentru a stabili materialele cu potențială valoare pentru serviciile de informații. În plus, selectorii utilizați în ceea ce privește datele de comunicații aferente făceau obiectul aceluiași garanții precum conținutul. Mai precis, analiștii completau un registru în care explicau motivul pentru care fiecare nou selector adăugat în sistem era necesar și proporțional, acest registru făcând obiectul unui audit efectuat de Comisarul CI, iar selectorii erau eliminați dacă se stabilea că nu erau utilizați de ținta prevăzută, și exista o perioadă maximă în care selectorii puteau rămâne în uz înainte de a fi necesar un control (supra, pct. 298).

418. Datele legate de conținut și datele de comunicații aferente făceau, de asemenea, obiectul multora dintre aceleași proceduri privind stocarea, accesul, examinarea și utilizarea, aceleași precauții în comunicarea către terți și aceleași proceduri privind ștergerea și distrugerea lor. În această privință, atât datele legate de conținut, cât și datele de comunicații aferente făceau obiectul garanțiilor prevăzute la art. 15 din RIPA, care impuneau ca analiștii care doresc să acceseze datele de comunicații aferente au obligația să completeze un registru auditabil în care să explice motivele pentru care accesul era necesar și proporțional și interzicea întocmirea unui raport de informații pe baza datelor de comunicații aferente atât timp cât acestea nu erau examinate.

419. Cu toate acestea, existau două căi principale prin care regimul interceptării în masă trata datele legate de conținut și datele de comunicații aferente: datele de comunicații aferente erau excluse de la garanția oferită de art. 16 alin. (2), ceea ce înseamnă că, în cazul în care un analist dorea să utilizeze un selector legat de o persoană despre care era cunoscut că se află pentru moment în Insulele Britanice, nu avea obligația de a-i fi certificată utilizarea selecției ca fiind necesară și proporțională de către ministru; datele de comunicații aferente care nu se potriveau nici unui selector puternic, nici unei căutări complexe nu erau distruse imediate, ci erau păstrate o perioadă de câteva luni (supra, pct. 296-298). Prin urmare, Curtea va examina dacă dreptul intern definea în mod clar procedurile care trebuiau să fie urmate pentru selectarea datelor de comunicații aferente spre examinare, precum și limitele privind durata stocării datelor de comunicații aferente.

420. Conform regimului prevăzut la art. 8 alin. (4), art. 16 alin. (2) constituia principala garanție legală care stabilea limitele procesului de selecție a materialelor interceptate spre examinare. Cu toate acestea, nu constituia singura garanție. Astfel cum s-a menționat deja la punctul 417 anterior, trebuia ca toți noii selectori să fie justificați de analiști prin crearea unui registru scris care să explice motivele pentru care alegerea selectorului era atât necesară, cât și proporțională (supra, pct. 291-292 și 298); analiștii care doreau să examineze datele de comunicații aferente trebuiau să completeze un registru suplimentar în care să explice motivele pentru care alegerea selectorului era necesară și proporțională în acest sens, în urmărirea funcțiilor statutare ale GCHQ (pct. 6.4 din Codul IC, supra, pct. 96); aceste

registre făceau obiectul auditului și controlului Comisarului IC (supra, pct. 135-136 și 381). Potrivit Guvernului, nu ar fi fost fezabil să fie extinsă garanția prevăzută la art. 16 alin. (2) la datele de comunicații aferente, întrucât ministrul ar fi trebuit să certifice necesitatea și proporționalitatea țintirii persoanei vizate în fiecare caz. Numărul de căutări cu privire la datele de comunicații era semnificativ mai mare decât numărul de căutări cu privire la conținut (posibil de ordinul miilor săptămânal în legătură cu persoane cunoscute sau despre care se credea că se află în Regatul Unit), iar în multe dintre aceste cazuri identitatea persoanei nu era cunoscută. În plus, Guvernul a subliniat că datele de comunicații aferente aveau o valoare temporară și că obligația de a întârzia efectuarea căutărilor în așteptarea obținerii unei autorizații individuale risca în mod serios să compromită utilizarea acestora din punct de vedere al informațiilor (supra, pct. 296).

421. Curtea acceptă faptul că datele de comunicații aferente reprezintă un instrument esențial pentru serviciile de informații în lupta împotriva terorismului și a infracțiunilor grave și că ar exista circumstanțe în care ar fi atât necesar, cât și proporțional să se caute și să se acceseze datele de comunicații aferente ale persoanelor despre care se știe că se află în Regatul Unit. În plus, deși art. 16 alin. (2) conține o garanție importantă care reglementează procesul de selecție a materialelor interceptate spre examinare, este demn de remarcat faptul că, la evaluarea regimului care reglementează interceptarea în masă a conținutului, Curtea acordă o pondere mult mai mare existenței sau lipsei unui mecanism eficient pentru a se asigura că alegerea selectorilor este supusă atât cerințelor de necesitate, cât și de proporționalitate impuse de Convenție, precum și că făceau obiectul supravegherii, atât interne și cât externe. Prin urmare, deși Curtea ar dori să reamintească preocupările exprimate cu privire la alegerea și controlul selectorilor exprimate supra la pct. 381 și 382, nu consideră că excluderea datelor de comunicații aferente de la garanțiile oferite de art. 16 alin. (2) ar trebui să aibă o pondere decisivă în evaluarea globală.

422. În ceea ce privește durata stocării, Guvernul a susținut că datele de comunicații aferente „necesită o activitate analitică mai intensă, pe o perioadă lungă de timp, pentru a descoperi «necunoscutele necunoscute»”. O astfel de descoperire poate implica un exercițiu de fragmentare a unor mici elemente disperate de date de comunicații pentru a forma un „puzzle” care să reveleze o amenințare și poate include posibila examinare a unor elemente care, inițial, nu par a fi de interes pentru serviciile de informații. Eliminarea datelor de comunicații neselectate imediat sau numai după câteva zile ar face ca acest exercițiu să fie imposibil de realizat (supra, pct. 297).

423. În lumina celor de mai sus și având în vedere că exista o perioadă maximă de păstrare, care nu depășea „câteva luni”, iar diferența de tratament era justificată în mod obiectiv și rezonabil, Curtea acceptă că dispozițiile privind stocarea datelor de comunicații aferente erau suficient de solide, chiar

dacă erau diferite în esență de dispozițiile privind conținutul. Cu toate acestea, perioadele de păstrare au fost divulgate numai în cadrul procedurii în fața Curții. În consecință, perioadele mai scurte de reținere nu erau evidente pentru cititorii Codului IC și nici nu exista niciun indiciu în Codul IC că perioadele de păstrare pentru datele de comunicații aferente erau diferite de datele privind conținutul. În opinia Curții, pentru a îndeplini cerința de „previzibilitate” impusă de art. 8, perioadele de păstrare divulgate în cadrul procedurii desfășurate în fața sa trebuie să fie incluse în măsuri legislative și/sau în alte măsuri generale adecvate.

(4) Concluzie

424. Curtea admite că interceptarea în masă este de o importanță vitală pentru statele contractante în identificarea amenințărilor la adresa securității lor naționale. Acest lucru a fost recunoscut de Comisia de la Veneția (supra, pct. 196) și a fost poziția adoptată de guvernul pârât, precum și de Guvernele Franței și al Țărilor de Jos în intervențiile acestora (supra, pct. 300 și 303). A fost, de asemenea, concluzia evaluatorului independent al legislației în materie de combatere a terorismului, care, după examinarea unui volum mare de materiale cu caracter confidențial, a concluzionat că interceptarea în masă constituie o capacitate esențială: în primul rând, întrucât teroriștii, infractorii, serviciile de informații străine și ostile s-au sofisticat în a evita depistarea prin mijloace tradiționale și, în al doilea rând, întrucât natura Internetului global făcea ca ruta luată de o comunicație specială să fi devenit extrem de imprevizibilă. Deși el și echipa sa au avut în vedere alternative la interceptarea în masă (inclusiv interceptarea țintită, utilizarea surselor umane și a produselor comerciale de apărare cibernetică), au concluzionat că nicio alternativă sau combinație de alternative nu ar fi suficientă pentru a înlocui competența de interceptare în masă (supra, pct. 166).

La fel ca în cazul oricărui regim de interceptare, există, desigur, un potențial considerabil ca interceptarea în masă să fie utilizată în mod abuziv într-un mod care să afecteze negativ dreptul persoanelor la respectarea vieții private. Prin urmare, într-un stat guvernat de statul de drept, menționat în mod expres în preambulul Convenției și inerent obiectului și scopului art. 8 (*Roman Zakharov*, citată anterior, pct. 228), Curtea consideră că, atunci când este privit în ansamblu său, regimul prevăzut la art. 8 alin. (4), în pofida garanțiilor sale, inclusiv a unora solide, astfel cum sunt menționate mai sus (a se vedea, de exemplu, supra, pct. 412 și 415), nu conțineau suficiente garanții „de la un capăt la altul” pentru a oferi garanții adecvate și eficiente împotriva arbitrarului. În special, Curtea 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 (supra, pct. 377-382). Aceste deficiențe priveau nu numai interceptarea conținutului comunicațiilor, ci și interceptarea datelor de comunicații aferente (supra, pct. 416). Deși

Comisarul IC asigura o supraveghere independentă și eficientă a regimului, iar IPT oferea o cale de atac solidă oricărei persoane care suspecta interceptarea comunicațiilor sale de către serviciile de informații, aceste garanții importante nu erau suficiente pentru a contrabalansa deficiențele evidențiate anterior, la pct. 377-382.

425. Cu toate acestea, în lumina deficiențelor sus-menționate, a hotărât, cu majoritate de voturi, că regimul de interceptare în masă nu îndeplinea cerința privind „calitatea legii” și nu era capabil să mențină „ingerința” la ceea ce era „necesar într-o societate democratică”.

426. Prin urmare, a fost încălcat art. 8 din Convenție.

C. Cu privire la pretinsa încălcare a art. 10 din Convenție

427. Părțile reclamante atât din cea de-a doua, cât și din cea de-a treia din cauzele conexe s-au plâns, în temeiul art. 10 din Convenție, de regimul prevăzut la art. 8 alin. (4), susținând că protecția acordată de art. 10 comunicațiilor confidențiale avea o importanță crucială pentru acestea, în calitate de jurnaliști și, respectiv, de ONG-uri. Cu toate acestea, întrucât Camera a declarat inadmisibil capătul de cerere formulat de părțile reclamante în cea de-a treia din cauzele conexe pentru neepuizarea căilor de atac interne, doar capătul de cerere în temeiul art. 10 privind jurnaliștii intră în obiectul cauzei trimise în fața Marii Camere.

428. Art. 10 din Convenție prevede:

„1. Orice persoană are dreptul la libertatea de exprimare. Acest drept include libertatea de opinie și libertatea de a primi sau de a comunica informații ori idei fără amestecul autorităților publice și fără a ține seama de frontiere. Prezentul articol nu împiedică statele să supună societățile de radiodifuziune, de cinematografie sau de televiziune unui regim de autorizare.

2. Exercițarea acestor libertăți ce comportă îndatoriri și responsabilități poate fi supusă unor formalități, condiții, restrângeri sau sancțiuni prevăzute de lege, care constituie măsuri necesare, într-o societate democratică, pentru securitatea națională, integritatea teritorială sau siguranța publică, apărarea ordinii și prevenirea infracțiunilor, protecția sănătății sau a moralei, protecția reputației sau a drepturilor altora, pentru a împiedica divulgarea de informații confidențiale sau pentru a garanta autoritatea și imparțialitatea puterii judecătorești.”

1. Hotărârea Camerei

429. Camera a constatat că, întrucât măsurile de supraveghere luate în cadrul regimului prevăzut la art. 8 alin. (4) nu vizau monitorizarea jurnaliștilor sau dezvăluirea surselor jurnalistice, interceptarea unor astfel de comunicații nu poate fi calificată, în sine, drept o ingerință deosebit de gravă în libertatea de exprimare. Cu toate acestea, a considerat că ingerința ar fi fost mai mare dacă aceste comunicații erau selectate spre examinare. Dacă aceasta ar fi fost situația, ingerința putea fi „justificată de o cerință imperativă de interes public” doar dacă era însoțită de garanții suficiente. În special,

circumstanțele în care astfel de comunicații ar putea fi selectate în mod intenționat spre examinare trebuie să fi fost stabilite suficient de clar în dreptul intern și trebuie să existe măsuri adecvate pentru a asigura protecția confidențialității, în cazul în care astfel de comunicații au fost selectate, în mod intenționat sau în alt mod, spre examinare. În lipsa unor proceduri accesibile publicului care să limiteze capacitatea serviciilor de informații de a căuta și de a examina alte materiale jurnalistice confidențiale dacă acest lucru nu era justificat de o cerință imperativă de interes public, Camera a constatat că a fost, de asemenea, încălcat art. 10 din Convenție.

2. *Argumentele părților*

(a) *Părțile reclamante*

430. Părțile reclamante din cea de-a doua din cauzele conexate au susținut că regimul interceptării în masă încălca art. 10, întrucât interceptarea la scară largă și păstrarea unor baze largi de date cu informații au avut un efect descurajator asupra libertății de comunicare a jurnaliștilor.

431. Având în vedere importanța fundamentală a libertății presei, părțile reclamante au susținut că orice ingerință în libertatea jurnalistică, în special în dreptul de a păstra confidențialitatea surselor, trebuia să fie însoțită de garanții procedurale legale proporționale cu importanța principiului în cauză. În special, noțiunea „prevăzută de lege” prevedea că, în cazul în care o măsură permitea să se identifice surse jurnalistice sau să se dezvăluie materiale jurnalistice, aceasta trebuia să fie autorizată de un judecător sau de un alt organ decizional independent și imparțial, evaluarea trebuia să fie *ex ante*, iar organul de autorizare trebuia să fie investit cu competența de a stabili dacă era „justificată de o cerință imperativă de interes public” și, în special, dacă o măsură mai puțin intruzivă ar fi putut fi suficientă pentru a servi interesului public imperativ [*Sanoma Uitgevers B.V. împotriva Țărilor de Jos* (MC), nr. 38224/03, 14 septembrie 2010]. Niciuna dintre aceste garanții nu era prezentă în regimul prevăzut la art. 8 alin. (4).

(b) *Guvernul*

432. Guvernul a susținut, în primul rând, că în jurisprudența Curții nu exista nicio decizie pentru a susține că era necesară o autorizație judiciară (sau independentă) prealabilă pentru funcționarea unui regim de supraveghere strategică, pe motiv că anumite elemente jurnalistice ar putea fi interceptate în cursul funcționării acestui regim. Dimpotrivă, Curtea a făcut o distincție clară între monitorizarea strategică a comunicațiilor și/sau a datelor de comunicații, care ar putea „prinde” accidental anumite materiale jurnalistice, și măsurile care vizau materiale jurnalistice (*Weber și Saravia*, citată anterior, pct. 151, și, *a contrario*, *Sanoma Uitgevers B.V.*, citată anterior, și *Telegraaf Media Nederland Landelijke Media B.V. și alții împotriva Țărilor de Jos*, nr. 39315/06, 22 noiembrie 2012). Cerința unei

autorizări judiciare prealabile nu ar avea sens în contextul interceptării în masă, întrucât judecătorul ar putea fi informat doar că există posibilitatea ca executarea mandatului să conducă la interceptarea unor materiale jurnalistice confidențiale.

433. Astfel, Guvernul a acceptat concluzia Camerei potrivit căreia era necesară o protecție suplimentară la momentul selecției spre examinare. Prin urmare, a confirmat că Codul IC a fost modificat, iar pasajul relevant era astfel redactat: „[t]rebuie să se acorde o atenție deosebită interceptării comunicațiilor sau selecției spre examinare a conținutului care cuprinde informații despre care persoanele ar putea în mod rezonabil să considere că au un grad ridicat de confidențialitate. Aceasta include cazurile în care comunicațiile conțin informații acoperite de secretul profesional al avocaților, materialele jurnalistice confidențiale sau cazurile în care comunicațiile identifică sursa unui jurnalist”.

(c) Terții intervenienți

(i) Guvernul francez

434. Guvernul francez a susținut că supravegherea jurnaliștilor era permisă în temeiul art. 10 din Convenție dacă urmarea un scop legitim și era necesară și dacă măsura nu viza jurnaliștii și nu viza identificarea surselor acestora. Nu se putea face nicio paralelă între situația în care comunicațiile jurnaliștilor erau interceptate din întâmplare și situația în care o decizie a autorităților naționale impunea unui jurnalist să își dezvăluie sursele.

(ii) Guvernul Regatului Norvegiei

435. Guvernul norvegian a susținut că marja largă de apreciere oferită în temeiul art. 8 în ceea ce privește decizia de a introduce un regim de interceptare în masă se aplica în mod logic și atunci când decizia era examinată din perspectiva art. 10. Ar fi contrar naturii și scopului unui regim de interceptare în masă ca instanța să condiționeze decizia de instituire a acestuia de criteriul „justificat de o cerință imperativă de interes public” pentru simplul motiv că unele dintre comunicațiile interceptate ar putea implica contactul cu jurnaliștii.

(iii) Raportorul special al Organizației Națiunilor Unite pentru promovarea și protecția dreptului la libertatea de opinie și de exprimare

436. Raportorul special a susținut că măsurile de supraveghere au adus atingere dreptului la libertatea de exprimare și, prin urmare, era necesar ca măsurile respective să fie în conformitate cu art. 19 alin. (3) din PIDCP, care impunea restricții privind exprimarea „numai în măsura în care sunt prevăzute de lege și sunt necesare” pentru protejarea drepturilor și reputației altora, a securității naționale, a ordinii publice, a sănătății publice sau a moralei. Programele de supraveghere în masă generează dificultăți semnificative în

ceea ce privește cerința unei legislații accesibile, din cauza complexității modului în care funcționează tehnologiile de supraveghere, a unor standarde juridice vagi pentru interceptarea comunicațiilor și a unor cadre administrative complicate și adesea cu caracter clasificat. În plus, exista o preocupare serioasă legată de proporționalitate în ceea ce privește ingerința în activitatea jurnaliștilor și protecția surselor acestora. Întrucât legislația privind drepturile omului conferea confidențialității un standard ridicat de protecție, trebuia ca restricțiile să fie excepționale și puse în aplicare numai de autoritățile judiciare, iar recurgera la sisteme de eludare pentru a submina confidențialitatea sursei ar trebui interzisă, cu excepția cazului în care a fost autorizată judiciar pe bază de norme clare și stricte. În această privință, domeniul de aplicare al protecției comunicațiilor confidențiale trebuia să țină seama de înțelegerea largă a termenului „jurnalist”, în temeiul PIDCP.

(iv) *Articolul 19*

437. Articolul 19 a solicitat Curții să extindă pentru ONG-uri aceeași protecție pe care o extinde în mod normal pentru jurnaliști.

(v) *Fundația Helsinki pentru Drepturile Omului (The Helsinki Foundation for Human Rights – „HFHR”)*

438. Fundația Helsinki a susținut că protecția surselor jurnalistice era subminată nu numai de supravegherea conținutului comunicațiilor jurnaliștilor, ci și de supravegherea metadatelor aferente, care putea permite, în sine, identificarea surselor și a informatorilor. Era deosebit de problematic faptul că informațiile confidențiale puteau fi obținute fără cunoștința sau controlul jurnaliștilor, privându-i astfel de dreptul de a invoca confidențialitatea, iar sursele lor să se bazeze pe garanțiile privind confidențialitatea.

(vi) *Media Lawyers' Association („MLA”)*

439. MLA și-a exprimat îngrijorarea cu privire la faptul că regimurile de supraveghere în masă erau capabile să intercepteze comunicațiile jurnalistice și datele de comunicații care puteau identifica sursele. În opinia asociației, simpla interceptare de materiale jurnalistice putea aduce atingere art. 10 din Convenție, chiar dacă materialul nu fusese analizat efectiv. Prin urmare, era imperativ să existe garanții adecvate pentru a proteja confidențialitatea surselor jurnalistice, indiferent de scopul pentru care erau colectate informațiile. În plus, un regim care permitea statelor să intercepteze comunicațiile jurnaliștilor fără o autorizație judiciară prealabilă era mai susceptibil să afecteze jurnalismul de interes public, întrucât natura unor astfel de relatări însemna că statul ar fi avut un interes deosebit în a identifica sursele. Riscul ar fi deosebit de grav în cazul în care sursa ar fi un avertizor funcționar guvernamental. Efectul descurajator al simplei posibilități de a

identifica astfel de surse era unul semnificativ. În consecință, MLA a susținut că art. 10 impunea cel puțin o supraveghere judiciară independentă prealabilă a oricărei încercări de a obține materiale jurnalistice sau de a identifica surse jurnalistice, și că procesul judiciar era unul *inter partes*.

(vii) *Sindicatul Național al Jurnaliștilor (The National Union of Journalists – „NUJ”) și Federația Internațională a Jurnaliștilor (International Federation of Journalists – „IFJ”)*

440. NUJ și IFJ au susținut că confidențialitatea surselor este indispensabilă pentru libertatea presei. Și-au exprimat, de asemenea, îngrijorarea cu privire la posibilul schimb de date păstrate de Regatul Unit cu alte țări. Dacă materialele jurnalistice cu caracter confidențial au fost partajate cu o țară care nu putea să le trateze în condiții de siguranță, acesta ar putea ajunge în mâinile unor persoane care ar putea să îi facă rău jurnalistului sau sursei sale. În opinia intervenientelor, garanțiile din Codul IC actualizat și din Codul de bune practici privind obținerea datelor de comunicații nu erau adecvate, în special în cazul în care jurnalistul sau identificarea sursei sale nu făcea obiectul măsurii de supraveghere.

3. Motivarea Curții

(a) Principii generale privind protecția surselor jurnaliștilor

441. Întrucât libertatea de exprimare constituie unul dintre fundamentele esențiale ale unei societăți democratice, Curtea a supus întotdeauna garanțiile privind respectarea libertății de exprimare în cauzele examinate în temeiul art. 10 din Convenție unui control special. Garanțiile care trebuie acordate presei au o importanță deosebită, iar protecția surselor jurnalistice este una dintre pietrele de temelie ale libertății presei. Fără această protecție, sursele ar putea fi descurajate să ajute presa să informeze publicul despre chestiuni de interes public. În consecință, rolul vital de gardian public al presei ar putea fi subminat, iar capacitatea presei de a prezenta informații corecte și demne de încredere ar putea fi afectată negativ (a se vedea, *inter alia*, *Goodwin împotriva Regatului Unit*, nr. 17488/90, pct. 39, 27 martie 1996; *Sanoma Uitgevers B. V.*, citată anterior, pct. 50; și *Weber și Saravia*, citată anterior, pct. 143).

442. Ordinul de a divulga sursa ar avea un impact negativ nu doar asupra sursei, a cărei identitate ar putea fi dezvăluită, ci și asupra ziarului sau altor publicații împotriva cărora este îndreptat ordinul, a căror reputație ar putea fi afectată negativ în ochii viitoarelor surse potențiale, prin divulgare, precum și asupra publicului interesat să primească informații prin intermediul unor surse anonime. Cu toate acestea, există o „diferență fundamentală” între autoritățile care dispun ca un jurnalist să dezvăluie identitatea surselor sale și autoritățile care fac percheziții la domiciliul și la locul de muncă al unui jurnalist în vederea descoperirii surselor sale (a se compara *Goodwin*, citată

anterior, pct. 39, cu *Roemen și Schmit împotriva Luxemburgului*, nr. 51772/99, pct. 57, CEDO 2003-IV). Acțiunea din urmă, chiar dacă nu produce rezultate, constituie o măsură mai drastică decât un ordin de divulgare a identității unei surse, întrucât anchetatorii care fac cercetări la locul de muncă al unui jurnalist au acces la toate documentele deținute de acesta (*Roemen și Schmit*, citată anterior, pct. 57).

443. Ingerința în protecția surselor jurnalistice nu poate fi compatibilă cu art. 10 din Convenție decât dacă este justificată de o cerință imperativă de interes public general (*Sanoma Uitgevers B. V.*, citată anterior, pct. 51; *Goodwin*, citată anterior, pct. 39; *Roemen și Schmit*, citată anterior, pct. 46; *Voskuil împotriva Țărilor de Jos*, nr. 64752/01, pct. 65, 22 noiembrie 2007). În plus, orice ingerință în dreptul la protecția surselor jurnalistice trebuie să fie însoțită de garanții procedurale legale proporționale cu importanța principiului în discuție (*Sanoma Uitgevers B.V.*, citată anterior, pct. 88-89). Printre aceste garanții se numără în primul rând garantarea controlului exercitat de o instanță sau de un alt organ decizional independent și imparțial care are competența de a stabili dacă există o cerință de interes general care prevalează asupra principiului protecției surselor jurnalistice înainte de preluarea unor astfel de materiale și de a preveni accesul inutil la informații care pot divulga identitatea surselor, în cazul în care nu există (*Sanoma Uitgevers B.V.*, citată anterior, pct. 88-90).

444. Având în vedere caracterul preventiv al unui astfel de control, instanța sau alt organ independent și imparțial trebuie să fie în măsură să efectueze această punere în balanță a riscurilor potențiale și a intereselor respective înainte de orice divulgare și cu referire la materialele a căror divulgare se solicită astfel încât argumentele autorităților care solicită divulgarea să poată fi evaluate în mod corespunzător. Decizia care urmează să fie luată trebuie să fie guvernată de criterii clare, inclusiv dacă o măsură mai puțin intruzivă poate fi suficientă pentru a servi intereselor publice imperative stabilite. Instanța sau altă autoritate trebuie să aibă posibilitatea de a refuza emiterea unui ordin de divulgare sau de a emite un ordin limitat sau calificat pentru a proteja sursele împotriva divulgării, indiferent dacă acestea sunt sau nu menționate în mod specific în materialele reținute, pe motiv că a comunica astfel de informații creează un risc serios de compromitere a identității surselor jurnalistului [*Sanoma Uitgevers B.V.*, citată anterior, pct. 92, și *Nordisk Film & TV A/S împotriva Danemarcei*, nr. 40485/02, CEDO 2005-XIII]. În situații de urgență, trebuie să existe o procedură de identificare și izolare, înainte de exploatarea materialelor de către autorități, a informațiilor care ar putea conduce la identificarea surselor de informații care nu prezintă un astfel de risc (*mutatis mutandis*, *Wieser and Bicos Beteiligungen GmbH împotriva Austriei*, nr. 74336/01, pct. 62-66, CEDO 2007-XI).

(b) Art. 10 în contextul interceptării în masă

445. În *Weber și Saravia*, Curtea a recunoscut că regimul de „monitorizare strategică” a adus atingere libertății de exprimare a primei reclamante, ca jurnalistă. Cu toate acestea, a considerat decisiv faptul că măsurile de supraveghere nu vizau monitorizarea jurnaliștilor sau dezvoltarea surselor jurnalistice. Ca atare, a considerat că ingerința în libertatea de exprimare a primei reclamante nu putea fi calificată ca fiind deosebit de gravă și, având în vedere garanțiile aferente, a declarat inadmisibile capetele sale de cerere ca vădit nefondate (*Weber și Saravia*, citată anterior, pct. 143-145 și 151).

(c) Abordarea care trebuie adoptată în prezenta cauză

446. În temeiul regimului prevăzut la art. 8 alin. (4), serviciile de informații ar fi putut accesa materiale jurnalistice confidențiale fie în mod intenționat, prin utilizarea deliberată a selectorilor sau a termenilor de căutare legați de un jurnalist sau de o organizație de știri, fie în mod neintenționat, ca „captură accidentală” în cadrul operațiunii de interceptare în masă.

447. În cazul în care intenția serviciilor de informații este de a accesa materiale jurnalistice confidențiale, de exemplu prin utilizarea deliberată a unui selector puternic legat de un jurnalist sau în cazul în care, în urma alegerii unor astfel de selectori puternici, există o probabilitate mare ca aceste materiale să fie selectate spre examinare, Curtea consideră că ingerința va fi proporțională cu cea ocazionată de percheziția domiciliului sau a locului de muncă al unui jurnalist; indiferent dacă serviciile de informații au sau nu intenția de a identifica o sursă, utilizarea selectorilor sau a termenilor de căutare legați de un jurnalist ar conduce foarte probabil la obținerea unor cantități semnificative de materiale jurnalistice confidențiale care ar putea submina protecția surselor într-o măsură și mai mare decât ordinul de divulgare a unei surse (*Roemen și Schmit*, citată anterior, pct. 57) Prin urmare, Curtea consideră că, înainte ca serviciile de informații să utilizeze selectori sau termeni de căutare cunoscuți ca fiind legați de un jurnalist sau care ar face foarte probabilă selectarea de materiale jurnalistice confidențiale spre examinare, selectorii sau termenii de căutare trebuie să fi fost autorizați de o instanță sau de un alt organ decizional independent și imparțial investit 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 putut servi interesului public imperativ (*Sanoma Uitgevers B.V.*, citată anterior, pct. 90).

448. Chiar și în cazul în care nu există intenția de a accesa materiale jurnalistice confidențiale, iar selectorii și termenii de căutare utilizați nu sunt de natură să facă foarte probabilă selectarea de materiale jurnalistice confidențiale spre examinare, va exista totuși riscul ca astfel de materiale să fie interceptate, chiar examinate, ca o „captură accidentală” în cadrul unei operațiuni de interceptare în masă. În opinia Curții, această situație este

semnificativ diferită de supravegherea ținută a unui jurnalist prin intermediul regimurilor prevăzute la art. 8 alin. (1) sau art. 8 alin. (4). Întrucât interceptarea oricărei comunicații jurnalistice ar fi inadvertentă, gradul de ingerință în comunicațiile și/sau sursele jurnalistice nu ar putea fi prevăzut de la 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 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.

449. În *Weber și Saravia*, Curtea a reținut că ingerința în libertatea de exprimare cauzată de monitorizarea strategică nu putea fi calificată ca fiind deosebit de gravă, întrucât nu urmărea să controleze jurnaliștii, iar autoritățile nu puteau cunoaște decât în momentul examinării telecomunicațiilor interceptate, dacă era cazul, că au fost monitorizate comunicațiile unui jurnalist (*Weber și Saravia*, citată anterior, pct. 151). Prin urmare, a admis că interceptarea inițială, fără examinarea materialelor interceptate, nu a constituit o ingerință gravă în dreptul consacrat de art. 10 din Convenție. Cu toate acestea, astfel cum a observat deja Curtea, capacitățile tehnologice actuale, într-o perioadă din ce în ce mai digitalizată, au crescut considerabil volumul comunicațiilor care traversează internetul la nivel mondial și, în consecință, supravegherea care nu țintește în mod direct persoanele are capacitatea de a avea un domeniu de aplicare foarte larg, atât pe teritoriul statului care efectuează supravegherea, cât și în afara acestuia (supra, pct. 322-323). Întrucât examinarea de către un analist a comunicațiilor unui jurnalist sau a datelor de comunicații aferente ar putea conduce la identificarea unei surse, Curtea consideră că este imperativ ca dreptul intern să conțină garanții solide în ceea ce privește stocarea, examinarea, utilizarea, transmiterea și distrugerea ulterioară a unor astfel de informații confidențiale. În plus, chiar și în cazul în care comunicațiile jurnalistice sau datele de comunicații aferente nu au fost selectate spre examinare prin utilizarea deliberată a unui selector sau a unui termen de căutare despre care se știe că are legătură cu un jurnalist, dacă și când devine evident că comunicațiile sau datele de comunicații aferente conțin materiale jurnalistice confidențiale, stocarea și examinarea lor continuă 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 investit cu competența de a stabili dacă stocarea și examinarea continuă sunt „justificate de o cerință imperativă de interes public”.

(d) Aplicarea criteriilor sus-menționate la faptele prezentei cauze

450. În *Weber și Saravia*, Curtea a recunoscut în mod expres că regimul de supraveghere incriminat a adus atingere dreptului primei reclamante la libertatea de exprimare, ca jurnalistă (*Weber și Saravia*, citată anterior, pct. 143-145). În speță, Curtea a admis că funcționarea regimului prevăzut la

art. 8 alin. (4) a adus atingere tuturor drepturilor părților reclamante în temeiul art. 8 din Convenție (supra, pct. 324-331). Întrucât părțile reclamante din cea de-a doua cauză conexată erau o organizație care colecta știri, respectiv un jurnalist, Curtea a concluzionat că regimul prevăzut la art. 8 alin. (4) aducea, de asemenea, atingere și dreptului lor la libertatea de exprimare ca jurnaliști, drept prevăzut de art. 10 din Convenție.

451. Astfel cum s-a indicat deja, regimul prevăzut la art. 8 alin. (4) avea un temei clar în dreptul intern (supra, pct. 365 și 366). Cu toate acestea, evaluând previzibilitatea și necesitatea în temeiul art. 8 din Convenție, Curtea a identificat următoarele deficiențe ale regimului și garanțiile sale aferente: lipsa unei autorizații independente (supra, pct. 377), lipsa identificării categoriilor de selectori din cererea de emitere de mandat (supra, pct. 381-382) și lipsa unei autorizații interne prealabile pentru selectorii legați de o persoană identificabilă (supra, pct. 382).

452. Cu toate acestea, la punctele 4.1-4.3 și 4.26-4.31 din Codul IC erau prevăzute anumite garanții suplimentare cu privire la materialele jurnalistice confidențiale (supra, pct. 96). Potrivit pct. 4.1, orice cerere de emitere a unui mandat trebuia să precizeze dacă interceptarea era susceptibilă să conducă la o ingerință colaterală în viața privată, inclusiv în cazul în care era vorba despre comunicații jurnalistice și, dacă este posibil, trebuia să precizeze măsurile care trebuie luate pentru a reduce amploarea ingerinței colaterale. Cu toate acestea, pct. 4.1 nu îi impunea ministrului decât să ia în considerare aceste circumstanțe și măsuri atunci când examina o cerere de emitere a unui mandat în temeiul art. 8 alin. (1), și anume un mandat de autorizare a unei interceptări țintite. Pct. 4.2 prevedea, de asemenea, că „trebuie să se acorde o atenție deosebită” în cazurile în care ar fi putut fi implicate materiale jurnalistice confidențiale, iar pct. 4.26 prevedea că trebuie să se acorde „o atenție deosebită” interceptării comunicațiilor care implica materiale jurnalistice confidențiale.

453. Potrivit Guvernului, punctul 4.28 se aplica, de asemenea, și materialelor jurnalistice confidențiale. Atunci când intenția era de a obține informații cu caracter personal confidențiale, pct. 4.28 indica faptul că trebuia ca motivele, precum și necesitatea specifică și proporționalitatea unei astfel de intenții să fie documentate în mod clar. În cazul în care obținerea unor astfel de materiale era probabilă, dar neintenționată, trebuia să fie avute în vedere eventuale măsuri de atenuare și, în cazul în care nu erau disponibile, trebuia să se analizeze dacă erau necesare modalități speciale de tratare a datelor în cadrul agenției de interceptare (supra, pct. 96). Cu toate acestea, Curtea observă că, la punctul 4.26 din Codul IC, „informațiile cu caracter personal confidențiale” păreau a se diferenția de „materialele jurnalistice confidențiale” (supra, pct. 96).

454. În ceea ce privește stocarea materialelor confidențiale, pct. 4.29 din Codul IC prevedea că acestea puteau fi păstrate numai atunci când erau necesare și proporționale pentru unul dintre scopurile autorizate prevăzute la

art. 15 alin. (4) din RIPA și trebuia să fie distruse în condiții de siguranță atunci când nu mai erau necesare pentru unul dintre aceste scopuri (supra, pct. 96). În plus, potrivit pct. 4.30, în cazul în care erau păstrate sau transmise unui organ extern, trebuia să fie luate măsuri rezonabile pentru a marca caracterul confidențial al informațiilor. În cazul în care existau îndoieli cu privire la legalitatea transmiterii propuse a informațiilor confidențiale, trebuia să se solicite consiliere din partea unui consilier juridic din cadrul agenției de interceptare relevante și înainte ca orice transmitere ulterioară a materialului să poată avea loc (supra, pct. 96). În sfârșit, conform pct. 4.31, Comisarul IC era informat cu privire la păstrarea unor astfel de materiale cât mai curând posibil și astfel de materiale îi erau puse la dispoziție la cerere (supra, pct. 96).

455. Având în vedere cele de mai sus, Curtea admite că garanțiile din Codul IC referitoare la stocarea, transmiterea ulterioară și distrugerea materialelor jurnalistice confidențiale erau adecvate. Cu toate acestea, garanțiile suplimentare din Codul IC nu soluționau deficiențele identificate de Curte în analiza sa privind regimul în temeiul art. 8 din Convenție și nici nu îndeplineau cerințele identificate anterior de Curte la pct. 447-449. În special, nu exista nicio cerință ca utilizarea selectorilor sau a termenilor de căutare cunoscuți ca fiind legați de un jurnalist să fie autorizată de o instanță sau de un alt organ decizional independent și imparțial investit cu competența de a stabili dacă acesta era „justificată de o cerință imperativă de interes public” și dacă o măsură mai puțin intruzivă ar fi putut fi suficientă pentru a servi interesul public imperativ. Dimpotrivă, în cazul în care intenția era de a avea acces la materiale jurnalistice confidențiale sau acest lucru era foarte probabil având în vedere utilizarea unor selectori legați de un jurnalist, era necesar numai ca motivele care au stat la baza acestui acces, precum și necesitatea și proporționalitatea acesteia să fie documentate în mod clar.

456. În plus, nu existau garanții suficiente pentru a se asigura 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 știe că are legătură cu un jurnalist conținea totuși materiale jurnalistice confidențiale, aceasta putea fi păstrată și examinată în continuare de către un analist numai dacă era autorizată de o instanță sau de un alt organ decizional independent și imparțial investit cu competența de a stabili dacă stocarea și examinarea erau „justificate de o cerință imperativă de interes public”. În schimb, singurul lucru care era prevăzut la pct. 4.2 din Codul IC era să se acorde „o atenție deosebită” oricărei interceptări care ar fi putut implica interceptarea de materiale jurnalistice confidențiale, inclusiv luarea în considerare a eventualelor măsuri de atenuare a acestui risc (supra, pct. 96).

457. Având în vedere atât aceste deficiențe, cât și cele identificate de Curte în examinarea plângerii în temeiul art. 8 din Convenție, Curtea constată, de asemenea, că a fost încălcat art. 10 din Convenție ca urmare a aplicării regimului prevăzut la art. 8 alin. (4).

III. CU PRIVIRE LA PRIMIREA DE INFORMAȚII DE LA SERVICII DE INFORMAȚII STRĂINE

A. Art. 8 din Convenție

458. Părțile reclamante din prima din cauzele conexate s-au plâns de primirea de către autoritățile Regatului Unit a unor materiale de la servicii de informații străine. Părțile reclamante din cea de-a treia din cauzele conexate au reproșat, în special, faptul că primirea de către statul pârât a unor materiale interceptate de NSA în cadrul PRISM și Upstream le-a încălcat drepturile care le reveneau în temeiul art. 8 din Convenție.

1. Domeniul de aplicare al capătului de cerere formulat în fața Marii Camere

459. În cadrul procedurii *Liberty*, IPT a identificat trei categorii de materiale care puteau fi primite de la serviciile de informații partenere străine: materiale de interceptare nesolicitate, materiale de interceptare solicitate și materiale neinterceptate. În măsura în care Guvernul a informat Camera că era „puțin plauzibil și rar” ca materialele interceptate să fie comunicate autorităților britanice fără ca acestea să le fi „solicitat”, Camera nu a examinat materialele care se încadrau în această categorie (pct. 417 din hotărârea Camerei). De asemenea, Camera a refuzat să examineze primirea de materiale neinterceptate, întrucât părțile reclamante nu au specificat tipul de materiale pe care serviciile de informații străine le-ar putea obține prin alte metode decât interceptare și, ca atare, nu a considerat că acestea au demonstrat în mod suficient că obținerea de informații în acest mod aducea atingere drepturilor lor în temeiul art. 8 (pct. 449 din hotărârea Camerei). Părțile reclamante nu au contestat niciuna dintre aceste constatări.

460. În plus, întrucât procedura *Liberty* fusese introdusă de părțile reclamante din cea de-a treia din cauzele conexate, IPT a luat în considerare numai primirea de informații de la NSA. În observațiile prezentate în fața Camerei și a Marii Camere, părțile s-au concentrat, de asemenea, pe primirea de materiale de la NSA.

461. Prin urmare, Marea Cameră își va limita examinarea la capătul de cerere legat de primirea materialelor interceptate solicitate de la NSA.

2. Cu privire la excepția preliminară a Guvernului

462. Guvernul a susținut că părțile reclamante din prima și cea de-a treia din cauzele conexate nu puteau pretinde că sunt victime ale pretensei încălcări, întrucât niciuna dintre cele două condiții din *Roman Zakharov* (citată anterior, pct. 171) nu era îndeplinită (și anume, nu era posibil ca părțile reclamante să fi fost afectate de legislația care permitea măsuri de supraveghere secrete și erau disponibile căi de atac la nivel național). În special, a susținut că părțile reclamante nu au prezentat niciun motiv pentru

care erau expuse unui risc real să le fie interceptate comunicațiile în cadrul PRISM sau Upstream, nici să le fie solicitate comunicațiile de către serviciile de informații din Regatul Unit. În plus, părțile reclamante dispuneau de o cale de atac efectivă la nivel național pentru a descoperi dacă făcuseră obiectul unui schimb ilegal de informații.

(a) Hotărârea Camerei

463. Întrucât Camera a admis că IPT le oferise părților reclamante o cale de atac efectivă pentru plângerea formulată în temeiul Convenției, a considerat că acestea puteau pretinde că sunt „victime” numai ca urmare a simplei existențe a regimului schimbului de informații dacă ar fi fost în măsură să demonstreze că erau potențial expuse riscului de a le fi obținute comunicațiile lor de către autoritățile din Regatul Unit prin intermediul unei cereri adresate unui serviciu de informații străin (pct. 392-393 din hotărârea Camerei, cu trimitere la *Roman Zakharov*, citată anterior, pct. 171).

464. Pe baza informațiilor care i-au fost prezentate, Camera a constatat că părțile reclamante erau potențial expuse atât riscului de a le fi obținute comunicațiile de către un serviciu de informații străin, cât de a le fi solicitate de la un serviciu de informații străin de către autoritățile din Regatul Unit (pct. 395 din hotărârea Camerei). Deși ar fi putut să le fie solicitate comunicațiile doar dacă exista un mandat emis în temeiul art. 8 alin. (1) sau al art. 8 alin. (4) care să acopere comunicațiile, din procedura Liberty reieșea în mod clar că, în cazul a cel puțin două din părțile reclamante din a treia din cauzele conexate, comunicațiile le fuseseră interceptate în mod legal și fuseseră selecționate spre examinare de către serviciile de informații din Regatul Unit în temeiul regimului prevăzut la art. 8 alin. (4). În pofida faptului că Camera nu a identificat niciun motiv pentru a considera că respectivele părți reclamante erau de interes pentru serviciile de informații, a observat că comunicațiile lor ar fi putut fi obținute în mod legal în temeiul regimului prevăzut la art. 8 alin. (4) dacă, astfel cum susțineau, ar fi fost în contact cu persoane care erau de interes pentru servicii. În mod similar, comunicațiile lor ar fi putut fi solicitate în mod legal unei țări terțe în temeiul regimului schimbului de informații, dacă ar fi fost în contact cu o persoană care făcuse obiectul unei astfel de cereri.

465. Întrucât Upstream funcționa în mod similar cu regimul prevăzut la art. 8 alin. (4), Camera a admis, de asemenea, că comunicațiile părților reclamante ar fi putut fi eventual obținute de către NSA.

(b) Motivarea Curții

466. Părțile reclamante nu au contestat constatarea Camerei potrivit căreia IPT le oferise o cale de atac efectivă internă pentru capetele de cerere formulate în temeiul Convenției referitoare la funcționarea unui regim de supraveghere și, pentru motivele expuse supra, la pct. 413-415, Marea

Camera este de acord cu această constatare. Prin urmare, astfel cum a observat Camera, părțile reclamante puteau pretinde că au fost „victime” numai ca urmare a simplei existențe a regimului schimbului de informații dacă ar fi putut să demonstreze că erau potențial expuse riscului de a le fi obținute comunicațiile de către autoritățile din Regatul Unit prin intermediul unei cereri adresate unui serviciu de informații străin (*Roman Zakharov*, citată anterior, pct. 171). Aceasta ar fi fost situația numai dacă ar fi fost potențial expuse riscului ca atât comunicațiile să le fie interceptate de către un serviciu de informații străin, cât și ca aceste comunicații să fie solicitate de GCHQ.

467. Guvernul, concentrându-se pe primirea de informații din Statele Unite, a susținut că părțile reclamante nu erau expuse riscului potențial de a le fi interceptate comunicațiile în cadrul Upstream, întrucât era un regim de interceptare țintit. Cu toate acestea, potrivit NSA, înainte de aprilie 2017, Upstream obținuse comunicații către, dinspre sau către un selector care ținea de art. 702 (cum ar fi o adresă de e-mail) și doar începând din aprilie 2017 obținuse comunicații către sau dinspre un selector care ținea de art. 702 (supra, pct. 263). Având în vedere că selectorii care țineau de art. 702 erau aplicați tuturor comunicațiilor care traversau cablurile specificate, se pare că Upstream nu era atât de diferit de regimul prevăzut la art. 8 alin. (4), care intercepta, de asemenea, toate comunicațiile care circulau printr-un anumit număr de cabluri și le filtra cu ajutorul selectorilor. Singura diferență aparentă dintre cele două regimuri era aceea că, începând din aprilie 2017, NSA nu mai putea căuta decât comunicații către sau de la un selector puternic, în timp ce GCHQ își păstrase capacitatea de a efectua căutări prin intermediul unor interogări complexe.

468. În cursul procedurii Liberty, IPT a confirmat că cel puțin în cazul a două dintre părțile reclamante din cea de-a treia din cauzele conexe nu numai că le fuseseră interceptate o parte din comunicații pe baza unui mandat emis în temeiul part. 8 alin. (4), ci și că respectivele comunicații fuseseră păstrate în mod legal și proporțional în temeiul mandatului (supra, pct. 58-60). Pentru a fi păstrate în mod legal, trebuia ca respectivele comunicații să corespundă fie unui „selector puternic” (aparținând fie părților reclamante, fie unei persoane cu care erau în contact), fie unei „interogări complexe”. Curtea acceptă că, în cazul în care unele comunicații ale părților reclamante ar fi corespuns unui „selector puternic” utilizat de GCHQ, ar fi fost, de asemenea, potențial expuse riscului de a fi interceptate și păstrate de NSA în cadrul Upstream, pe baza faptului că erau „la destinația” sau „la proveniența” unui selector care ținea de art. 702. Chiar dacă nu corespundeau unui selector puternic, anumite comunicații ale părților reclamante trebuie să fi fost totuși de interes pentru serviciile de informații. Înainte de aprilie 2017, comunicațiile ar fi putut fi, de asemenea, interceptate și păstrate în cadrul Upstream dacă erau „despre” un selector care ținea de art. 702. Dacă aceasta ar fi fost situația, la momentul faptelor (și anume, la 7 noiembrie 2017), aceste

comunicații ar fi putut fi încă păstrate de NSA întrucât, în urma modificării politicii, în aprilie 2017, indica doar faptul că va elimina comunicațiile prin Internet obținute anterior în cadrul Upstream „cât mai curând posibil” (supra, pct. 263). Prin urmare, este posibil ca respectivele comunicații obținute înainte de această dată și care erau „despre” un selector puternic să fi fost stocate în continuare de NSA pentru o anumită perioadă de timp după acea dată.

469. În consecință, Curtea admite că, la momentul faptelor (și anume la 7 noiembrie 2017), părțile reclamante din prima și din cea de-a treia din cauzele conexate erau potențial expuse riscului ca cel puțin o parte din comunicațiile lor să fi fost interceptate și păstrate în cadrul Upstream.

470. Cu toate acestea, părțile reclamante nu puteau fi considerate în continuare victime ale regimului schimbului de informații decât dacă ar fi riscat, de asemenea, ca comunicațiile lor să fie solicitate de către GCHQ, iar o astfel de cerere ar fi putut fi formulată numai în cazul în care era deja în vigoare un mandat pentru materialele solicitate. Cu toate acestea, astfel cum a observat deja Curtea, faptul că, cel puțin în cazul a două dintre părțile reclamante din cea de-a treia din cauzele conexate, comunicațiile fuseseră păstrate de GCHQ sugerează că cel puțin o parte din comunicațiile acestora erau acoperite de un mandat emis în temeiul art. 8 alin. (4). În consecință, Curtea admite că părțile reclamante din prima și din cea de-a treia din cauzele conexate erau potențial expuse riscului ca comunicațiile lor să fi fost solicitate și de către GCHQ.

471. Prin urmare, Curtea constată că părțile reclamante din prima și din cea de-a treia din cauzele conexate pot pretinde că sunt victime, în ceea ce privește capetele de cerere referitoare la regimul schimbului de informații. Prin urmare, excepția preliminară ridicată de Guvern este respinsă.

3. *Cu privire la fond*

(a) **Hotărârea Camerei**

472. Pentru a aprecia conformitatea cu art. 8 a regimului care reglementează primirea de materiale interceptate de la servicii de informații străine cum ar fi NSA, Camera a aplicat o versiune modificată a celor șase garanții minime (supra, pct. 275). Întrucât primele două cerințe nu se pot aplica actului de solicitare a unor materiale interceptate de la guverne străine, Camera a verificat în schimb dacă circumstanțele în care putea fi solicitată interceptarea erau delimitate suficient pentru a împiedica statele să se folosească de această competență pentru a eluda dreptul intern sau obligațiile prevăzute de Convenție. Ulterior, a aplicat ultimele patru cerințe în ceea ce privește tratamentul aplicat materialelor interceptate odată ce acestea erau obținute de serviciile de informații din Regatul Unit.

473. Camera a considerat că dreptul intern, împreună cu clarificările aduse prin modificarea Codului IC, indica cu suficientă claritate procedura de

solicitare fie a interceptării, fie a transmiterii de materiale interceptate de la servicii de informații străine. În plus, nu exista nicio dovadă a unor deficiențe semnificative în aplicarea și funcționarea regimului de supraveghere. Prin urmare, a hotărât, cu majoritate de voturi, că nu a fost încălcat art. 8 din Convenție.

(b) Argumentele părților

474. Părțile reclamante au susținut că garanțiile existente în ceea ce privește regimul schimbului de informații erau insuficiente. În special, au susținut că problemele care au determinat Camera să constate o încălcare a art. 8 din Convenție în ceea ce privește regimul de interceptare în masă (și anume, lipsa de supraveghere a utilizării selectorilor și garanțiile inadecvate în ceea ce privește datele de comunicații aferente) se aplicau în egală măsură regimului schimbului de informații.

475. Guvernul, pe de altă parte, a susținut că regimul schimbului de informații avea o bază clară în dreptul intern, fiind stabilit prin lege, completat de Capitolul 12 din Codul IC, precum și că legea în cauză era accesibilă. În ceea ce privește previzibilitatea, Guvernul a susținut că, în loc să aplice o versiune modificată a celor șase garanții minime, Camera ar fi trebuit, în schimb, să aplice criteriul mai general – aplicat în mod obișnuit în cazurile de colectare de informații care nu implicau interceptarea comunicațiilor – dacă legea indica cu suficientă claritate marja de apreciere și modul de exercitare a acestora pentru a oferi persoanei o protecție adecvată împotriva ingerințelor arbitrare. În orice caz, Guvernul a susținut că regimul schimbului de informații îndeplinea cele șase garanții minime. Codul IC descria în mod clar natura infracțiunilor care putea duce la obținerea informațiilor, limitele duratei obținerii unor astfel de informații, procesul de examinare, utilizarea și stocarea informațiilor obținute, precum și circumstanțele în care informațiile urmau să fie șterse sau distruse.

476. În sfârșit, în opinia Guvernului, nu exista niciun motiv întemeiat pentru a izola comunicațiile interceptate și datele de comunicații aferente de alte tipuri de informații care, în principiu, puteau fi obținute de la un serviciu de informații străin, cum ar fi informațiile provenite din surse de informații umane infiltrate sau supravegherea audio/vizuală sub acoperire. Într-adevăr, în multe cazuri, era posibil ca serviciile de informații nici măcar să nu știe dacă comunicațiile care le fuseseră furnizate de un serviciu de informații străin fuseseră obținute ca urmare a unei interceptări.

(c) Observațiile terților intervenienți

(i) Guvernul francez

477. Guvernul francez a observat că schimbul de informații între serviciile partenere – fie ad-hoc, fie în mod regulat – au o importanță vitală, în special în lupta împotriva amenințărilor din ce în ce mai transnaționale și mai difuze

pe care trebuie ca statele să le prevină, în primul rând prin identificarea suspecților înainte ca aceștia să acționeze. O astfel de luptă justifică dezvoltarea unei comunități de informații, fără de care serviciile de informații, cu capacitatea lor limitată de a acționa în străinătate, nu ar fi în măsură să își îndeplinească misiunea care le este încredințată.

478. În plus, guvernul francez a susținut că, în contextul schimbului de informații, ingerința nu a avut loc în contextul interceptării, ci mai degrabă în cel al obținerii de informații, chiar dacă materialul a fost interceptat la cererea statului destinatar. Guvernul francez a observat abordarea adoptată de Camera în analiza regimului schimbului de informații din Regatul Unit și a invitat Marea Cameră să adopte aceeași abordare.

479. În opinia guvernului francez, fiabilitatea serviciului destinatar reprezintă unul dintre principalele criterii pe care statul de origine și-a întemeiat decizia de a face schimb de date și, în consecință, statul destinatar trebuie să garanteze stricta confidențialitate a informațiilor care i-au fost comunicate. Prin urmare, trebuie ca garanțiile necesare pentru gestionarea informațiilor colectate prin intermediul unui schimb de date cu un serviciu partener să fie în conformitate cu „regula părții terțe”, care interzice unei agenții care a primit informații de la un partener străin să le comunice unei părți terțe fără consimțământul emitentului. În lipsa unei astfel de garanții, statele ar putea refuza să transfere informații.

(ii) *Raportorul special al Organizației Națiunilor Unite pentru promovarea și protecția dreptului la libertatea de opinie și de exprimare*

480. Raportorul special a susținut că trebuia să se aplice aceleași standarde pentru obținerea de date de la servicii de informații străine precum cele aplicate atunci când autoritățile naționale au obținut datele. O poziție contrară ar putea determina autoritățile statului să externalizeze *de facto* operațiuni de supraveghere care să eludeze garanțiile oferite de PIDCP.

(iii) *Acces Now*

481. Access Now a susținut că, deși tratatele de asistență judiciară reciprocă (*Mutual Legal Assistance Treaties*, „MLATs”) oferă un proces transparent și formal pentru ca un stat parte să solicite informații de la un altul, funcționarea programelor secrete de colectare de informații de origine electromagnetică (de exemplu, rețeaua de schimb de informații de origine electromagnetică Five Eyes, din care făceau parte Regatul Unit, Statele Unite ale Americii, Australia, Canada și Noua Zeelandă) nu este transparentă și este interzisă de standardele internaționale în materie de drepturile omului. Astfel de programe secrete nu sunt necesare, întrucât informațiile relevante pot fi obținute în cadrul MLAT.

(iv) *Dutch Against Plasterk („Burgers tegen Plasterk”)*

482. Dutch Against Plasterk, o coaliție compusă din cinci persoane fizice și patru asociații, a fost parte reclamantă într-o cauză împotriva Țărilor de Jos, în care a contestat schimbul de date dintre autoritățile olandeze și partenerii lor de informații străini (inclusiv Statele Unite ale Americii și Regatul Unit).

483. În intervenția părții terțe în fața Curții, această coaliție a susținut că schimbul de informații trebuia să fie permis numai dacă era însoțit de garanții suficiente, iar autoritatea străină avea o bază legală solidă pentru interceptarea materialelor. În caz contrar, exista riscul eludării protecției conferite de art. 8 din Convenție. Statelor nu ar trebui să li se permită să obțină de la autorități străine materiale pe care nu le-ar putea intercepta în mod legal.

(v) *Center for Democracy and Technology („CDT”) și Pen American Center („PEN America”)*

484. CDT și PEN America au susținut că circumstanțele cooperării internaționale în ceea ce privește supravegherea în masă a datelor și comunicațiilor impun îndeplinirea a cel puțin trei condiții: statele trebuie să evalueze activ și să fie convinse de caracterul adecvat al cadrului juridic și administrativ al partenerilor lor străini care reglementează interceptarea și să stabilească caracterul adecvat al respectivelor măsuri în dreptul intern; să existe o autorizație acordată independent – de preferință una judiciară – pe baza existenței unei bănuieli întemeiate, pentru utilizarea selectorilor identificabili în funcție de ținte specifice pentru a face căutări pe baza informațiilor obținute de la partenerii străini; să existe o notificare ulterioară a celor care au făcut obiectul supravegherii.

485. CDT și PEN America au susținut că regimurile de interceptare aplicate de NSA – în special, în temeiul art. 702 din FISA și al Decretului 12333 – nu au îndeplinit nici cerința de a fi „prevăzute de lege”, nici pe cea de „proporționalitate” prevăzute la art. 8 din Convenție, iar aceste deficiențe au afectat legalitatea regimului schimbului de informații din Regatul Unit.

(vi) *Rețeaua europeană a instituțiilor naționale din domeniul drepturilor omului (European Network of National Human Rights Institutions – „ENNHRI”)*

486. ENNHRI a prezentat exemple din partea statelor contractante care, în opinia sa, arată că natura schimbului internațional de informații s-a schimbat în mod semnificativ, astfel încât a devenit dificil să se facă distincția între datele „solicitate” și cele „nesolicitate”. Din punct de vedere istoric, schimbul internațional de informații a implicat transferul de date evaluate sau informații finite. Cu toate acestea, apariția noilor tehnologii a condus la intensificarea schimbului de date „brute” neevaluate. Chiar și în cazul în care exista un acord care să reglementeze cooperarea bilaterală sau multilaterală în domeniul serviciilor de informații, apariția automatizării și a volumelor mari de date a făcut mult mai dificilă evaluarea a ceea ce primea o parte de la

cealaltă, inclusiv dacă informațiile rămâneau în parametrii cererii inițiale. În consecință, era necesară o supraveghere independentă solidă a schimbului internațional de informații, fără a se face o distincție între datele solicitate și cele nesolicitate. Organele de supraveghere ar trebui să fie mandatate prin lege să supravegheze toate aspectele activităților de cooperare internațională ale serviciilor lor de informații, să coopereze cu organe independente de supraveghere din statele terțe implicate în schimbul de informații și să angajeze specialiști independenți, cu experiență în tehnologia modernă a informației și comunicațiilor, acolo unde acest lucru ar fi necesar.

(vii) *Human Rights Watch („HRW”)*

487. Deși prezentele cereri s-au axat, în principal, pe primirea de informații externe din Statele Unite ale Americii, HRW a considerat că rețeaua de state cu care comunicațiile în materie de informații au fost partajate era mult mai mare. De exemplu, „Five Eyes Alliance” era formată din Regatul Unit, Statele Unite ale Americii, Australia, Canada și Noua Zeelandă și se credea că există și alte coaliții care făceau schimb de informații, mai restricționate (de exemplu, „Nine Eyes, la care se adăugau Danemarca, Franța, Olanda și Norvegia, „Fourteen Eyes”, la care se adăugau Germania, Belgia, Italia, Spania și Suedia, și „Forty-One Eyes”, la care se adăugau alte țări din coaliția aliată din Afganistan).

(viii) *Fundația pentru o Societate Deschisă (Open Society Justice Initiative – OSJI”)*

488. OSJI a susținut că statele nu ar trebui să primească sau să solicite date de la un terț într-un mod care să eludeze drepturile persoanelor consacrate de art. 8. Pentru a se asigura că acest lucru nu se întâmplă, sunt necesare garanții în momentul în care materialul e colectat pentru prima dată, inclusiv examinarea prealabilă a situației din punct de vedere al drepturilor omului și al legilor și practicilor privind interceptarea din statul străin, precum și o supraveghere independentă, de preferință de natură judiciară, a oricărei modalitate de schimb de informații, pentru a se asigura că au fost instituite și puse în aplicare garanții.

(ix) *The Electronic Privacy Information Center („EPIC”)*

489. EPIC a susținut că legislația din Statele Unite ale Americii autoriza supravegherea în masă, nediferențiată, a persoanelor care nu erau cetățeni americani. Această supraveghere era realizată în temeiul art. 702 din FISA și al Decretului prezidențial nr. 12333. Supravegherea în temeiul art. 702 se realiza în Statele Unite ale Americii cu asistența obligatorie din partea furnizorilor de servicii de comunicații și îi viza pe cei care nu erau cetățeni americani SUA despre care se credea în mod rezonabil că se află în afara Statelor Unite. Nu exista un control judiciar anterior al activității de supraveghere, nu era necesară existența unei bănuieli întemeiate și nu exista

nici o obligație statutară de a notifica subiecții supravegherii. Tot ceea ce era necesar era ca FISC să revizuiască anual procedurile de țintire și de reducere la minimum menite să limiteze obținerea comunicațiilor cetățenilor americani sau ale persoanelor aflate în Statele Unite.

490. Decretul prezidențial nr. 12333 a autorizat NSA să obțină informații externe și contrainformații. Decretul oferea o largă autoritate pentru a efectua supravegherea informațiilor pe baza semnalelor electromagnetice dintr-o gamă largă de surse, inclusiv din rețelele de fibră optică. Colectarea se realiza în afara teritoriului Statelor Unite. Nu existau rapoarte sau divulgări oficiale cu privire la amploarea supravegherii în temeiul decretului, aceasta neputând fi nici controlată judiciar.

491. În opinia EPIC, supravegherea exercitată de către NSA încălca art. 8 din Convenție întrucât domeniul său de aplicare și durata nu erau limitate, nu făcea obiectul unui control adecvat, persoanele țintite nu erau informate, nu asigura o supraveghere adecvată și nici căi de atac efective.

(x) *Comisia Internațională a Juriștilor (The International Commission of Jurists – „ICJ”)*

492. ICJ a adus în atenția Curții art. 15 și 16 din Articolele privind răspunderea statului ale Comisiei de Drept Internațional (denumite în continuare „articolele CDI”). ICJ a susținut că, potrivit art. 15, un stat contractant poate fi răspunzător pentru supravegherea în masă efectuată de un stat necontractant dacă se acționează în forme organizate și structurate de cooperare și că, potrivit art. 16, un stat contractant poate fi răspunzător pentru supravegherea în masă efectuată de un stat necontractant dacă a contribuit la programul de supraveghere și dacă are cunoștință în mod efectiv sau constructiv de încălcările obligațiilor internaționale în materie de drepturi ale omului inerente sistemului. ICJ a susținut, de asemenea, că statele contractante care au participat la un program de supraveghere în masă sau care au contribuit la un astfel de program sunt obligate să instituie un sistem de garanții pentru a proteja drepturile consacrate de art. 8 și au, de asemenea, obligația de a proteja persoanele aflate sub jurisdicția lor împotriva încălcărilor drepturilor prevăzute la art. 8 cauzate de programele de supraveghere în masă.

(xi) *Law Society of England and Wales*

493. Law Society a susținut că regimul prevăzut la art. 8 alin. (4) și codurile conexe nu oferă garanții solide sau transparente pentru materialele acoperite de secretul profesional al avocaților. Întrucât aceleași garanții se aplică materialelor acoperite de secretul profesional al avocaților obținute de state străine și divulgate serviciilor de informații din Regatul Unit, aceleași deficiențe afectează deopotrivă și respectivul regim.

(d) Motivarea Curții**(i) Criteriul aplicabil**

494. În opinia Camerei, interceptarea comunicațiilor de către serviciile de informații străine nu putea angaja răspunderea unui stat destinatar și nici nu putea intra sub jurisdicția statului respectiv în sensul art. 1 din Convenție, chiar dacă interceptarea fusese efectuată la cererea acestui stat (pct. 420 din hotărârea Camerei). În primul rând, în măsura în care unele părți terțe au invocat articolele CDI, Camera a considerat că acestea ar fi relevante numai în următoarele cazuri: serviciile străine de informații ar fi la dispoziția statului destinatar și ar acționa în cadrul unor elemente ale autorității guvernamentale a statului respectiv (art. 6); statul destinatar ar ajuta sau ar asista serviciile străine de informații la interceptarea comunicărilor, aceasta reprezentând un fapt internațional ilicit din partea statului responsabil de serviciile respective, iar statul destinatar ar avea cunoștință de circumstanțele faptului internațional ilicit și interceptarea ar constitui un fapt internațional ilicit dacă ar fi comis de statul destinatar (art. 16); statul destinatar ar da directive sau ar exercita control asupra guvernului străin (art. 17). În al doilea rând, potrivit jurisprudenței Curții, interceptarea comunicațiilor de către un serviciu de informații străin ar putea intra sub incidența competenței statului destinatar numai dacă acest stat și-ar exercita autoritatea sau controlul asupra serviciului străin de informații [a se vedea, de exemplu, *Al-Skeini și alții împotriva Regatului Unit* (MC), nr. 55721/07, pct. 130-139, CEDO 2011, și *Jaloud împotriva Țărilor de Jos* (MC), nr. 47708/08, pct. 139 și 151, CEDO 2014].

495. Marea Cameră admite opinia Camerei potrivit căreia niciunul dintre aceste elemente nu a fost prezent în speță și, de altfel, în observațiile prezentate în fața Marii Camere, părțile reclamante nu au sugerat acest lucru. Prin urmare, o ingerință în drepturile consacrate de art. 8 din Convenție ar putea să se producă numai în cererea inițială și în primirea ulterioară a materialelor interceptate, urmată de stocarea, examinarea și utilizarea ulterioară a acestora de către serviciile de informații ale statului destinatar.

496. Protecția conferită de Convenție ar deveni inoperantă în cazul în care statele ar eluda de la obligațiile Convenției solicitând fie interceptarea comunicărilor de către state necontractante, fie transmiterea comunicațiilor interceptate de către acestea, fie, chiar dacă nu este în discuție în mod direct în spețele de față, prin obținerea unor astfel de comunicații prin accesul direct la bazele de date ale statelor respective. Prin urmare, în opinia Curții, atunci când o cerere de interceptare a unor elemente trebuie să fie 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 (*Roman Zakharov*, citată anterior, pct. 228). De asemenea, va fi necesar să existe norme detaliate suficient care să ofere resortisanților indicații adecvate cu privire la circumstanțele și la condițiile în care autoritățile publice au dreptul de a face o astfel de cerere (*Roman Zakharov*,

citată anterior, pct. 229; *Malone*, citată anterior, pct. 67; *Leander*, citată anterior, pct. 51; *Huvig*, citată anterior, pct. 29; *Kruslin*, citată anterior, pct. 30; *Valenzuela Contreras*, citată anterior, pct. 46; *Rotaru*, citată anterior, pct. 55; *Weber și Saravia*, citată anterior, pct. 93; *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiev*, citată anterior, pct. 75) și care să prevadă garanții efective împotriva folosirii unei astfel de competențe pentru a eluda dreptul intern și/sau obligațiile care le revin statelor în temeiul Convenției.

497. În momentul primirii materialelor interceptate, Curtea consideră că statul destinatar trebuie să dispună de garanții adecvate pentru examinarea, utilizarea și stocarea acestora, pentru transmiterea ulterioară și pentru ștergerea și distrugerea acestora. Aceste garanții, dezvoltate pentru prima dată de Curte în jurisprudența sa privind interceptarea comunicațiilor de către statele contractante, se aplică și în cazul primirii de către un stat contractant a unor materiale interceptate solicitate de la un serviciu de informații străin. În cazul în care, astfel cum susține Guvernul, statele nu au întotdeauna cunoștință dacă materialele primite de la servicii de informații străine sunt rezultatul interceptării, atunci Curtea consideră că aceleași standarde ar trebui să se aplice tuturor materialelor primite de la serviciile de informații străine care ar putea fi rezultatul interceptării.

498. În sfârșit, Curtea consideră că orice regim care permite serviciilor de informații să solicite fie interceptarea, fie transmiterea unor materiale interceptate provenind din state necontractante, fie accesul direct la astfel de materiale, ar trebui să facă obiectul unei supravegheri independente și ar trebui să existe, de asemenea, posibilitatea unui control *a posteriori* independent.

(ii) *Aplicarea acestui criteriu în speța de față*

499. Acordul dintre Regatul Unit și Statele Unite ale Americii privind comunicarea de informații din 5 martie 1946 permitea în mod expres schimbul de informații între Statele Unite ale Americii și Regatul Unit (supra, pct. 103). Cu toate acestea, detaliile privind procedurile interne (sau „nepublice”) ale serviciilor de informații au fost divulgate doar în cursul procedurii Liberty (supra, pct. 33-36). Aceste noi informații au fost integrate ulterior în Capitolul 12 din Codul IC (supra, 116), care, după cum s-a arătat deja, era un document public, sub rezerva aprobării ambelor Camere ale Parlamentului, și care trebuia luat în considerare atât de către cei care îndeplineau funcții de interceptare, cât și de către instanțe (supra, pct. 93-94). Curtea a admis că dispozițiile Codului IC puteau fi luate în considerare pentru a evalua previzibilitatea regimului RIPA (*Kennedy*, citată anterior, pct. 157 și supra, pct. 366) și că același lucru trebuie să fie valabil în mod necesar pentru regimul schimbului de informații.

500. În consecință, Curtea consideră că regimul de solicitare și de primire a informațiilor de la state necontractante avea un temei clar în dreptul intern

și, în urma modificării Codului IC, legea respectivă era suficient de accesibilă. Întrucât urmărea, fără îndoială, obiectivele legitime de protecție a securității naționale, de prevenire a tulburărilor și a infracțiunilor, precum și de protecție a drepturilor și libertăților celorlalți, Curtea va aprecia în continuare – în conformitate cu metodologia sa obișnuită (supra, pct. 334) – caracterul previzibil și necesar al regimului schimbului de informații.

501. Capitolul 12 din Codul IC (supra, pct. 116) urmează aceeași abordare ca cea adoptată de dreptul intern în ceea ce privește interceptarea în masă. Potrivit Capitolului 12, serviciile de informații puteau adresa o cerere unui guvern străin pentru a primi comunicații interceptate neanalizate și/sau date de comunicații aferente numai dacă un mandat de interceptare relevant în temeiul RIPA fusese deja emis de ministru, asistența guvernului străin fiind necesară pentru a obține comunicațiile în cauză întrucât acestea nu puteau fi obținute în temeiul mandatului existent (pct. 12.2 din Codul IC, supra, pct. 116) și era necesar și proporțional ca agenția de interceptare să obțină respectivele comunicații. În acest scop, un mandat de interceptare relevant în temeiul RIPA însemna fie un mandat emis în temeiul art. 8 alin. (1) în legătură cu subiectul în cauză; un mandat emis în temeiul art. 8 alin. (4) și un certificat însoțitor care să conțină una sau mai multe „descrieri ale materialelor interceptate” care să acopere comunicațiile subiectului, fie, în cazul în care se cunoștea că acesta se află în Insulele Britanice, un mandat emis în temeiul art. 8 alin. (4) și un certificat însoțitor care să conțină una sau mai multe „descrieri ale materialelor interceptate” care să acopere comunicațiile acestuia, împreună cu un document modificator emis în temeiul art. 16 alin. (3).

502. În cazul unor circumstanțe excepționale, solicitarea de comunicații specifice în lipsa unui mandat de interceptare în temeiul RIPA relevant nu echivala cu o eludare deliberată a RIPA și nici nu afecta în alt mod obiectivele RIPA (de exemplu, deoarece nu era fezabil din punct de vedere tehnic să se obțină comunicațiile prin interceptarea în temeiul RIPA) și era necesar și proporțional ca agenția de interceptare să obțină aceste comunicații. Într-un astfel de caz, cererea trebuia să fie examinată și aprobată personal de ministru și, în conformitate cu Codul IC revizuit, notificată Comisarului IC. Potrivit informațiilor divulgate în cursul procedurii *Liberty* și confirmate în observațiile Guvernului atât în fața Camerei, cât și în fața Marii Camere, nu a fost formulată niciodată o cerere de interceptare de materiale interceptate în lipsa unui mandat existent emis în temeiul RIPA (supra, pct. 42).

503. În lumina celor de mai sus, Curtea consideră că dreptul intern stabilește norme juridice clare care oferă resortisanților o indicație adecvată cu privire la circumstanțele și condițiile în care autoritățile ar putea solicita materiale interceptate de la un stat străin.

504. În cazul în care fie un mandat relevant emis fie în temeiul art. 8 alin. (1), fie în temeiul art. 8 alin. (4) era deja în vigoare, acest mandat trebuia să fi fost autorizat de ministru. Mai precis, din cuprinsul pct. 12.5 din Codul

IC coroborat cu nota de subsol aferentă reiese că, în cazul în care o cerere se întemeia pe un mandat existent, această cerere era formulată în relație cu sau despre selectori specifici (cu alte cuvinte, referitori la o anumită persoană sau anumite persoane), iar ministrul a aprobat deja cererea de interceptare a comunicațiilor acestor persoane. Cu toate că, în circumstanțe excepționale, o cerere putea fi formulată în lipsa unui mandat relevant, ministrul trebuia să aprobe personal cererea și, în cazul în care era bazată pe selectori specifici, trebuia să examineze și să aprobe personal examinarea respectivelor comunicații în raport cu astfel de factori (supra, pct. 116).

505. Întrucât legislația internă urma, în ceea ce privește astfel de cereri de schimb de informații, aceeași abordare ca în cazul interceptării în masă și în măsura în care dreptul intern prevedea în mod explicit că nu trebuie să existe nicio eludare, nu este necesar ca Curtea să examineze separat procedura de autorizare.

506. În ceea ce privește garanțiile pentru examinarea, utilizarea, stocarea, transmiterea ulterioară, ștergerea și distrugerea materialelor interceptate solicitate, din cuprinsul pct. 12.6 din Codul IC reieșea că trebuia ca conținutul sau datele de comunicații aferente interceptate, obținute de serviciile de informații din Regatul Unit de la un alt stat, date care erau identificate ca fiind rezultatul interceptării, să facă obiectul aceluiași norme interne și garanții care se aplicau aceluiași categorii de conținut sau de date atunci când ar fi fost obținute direct de agențiile de interceptare, ca urmare a unei interceptări în temeiul RIPA. În consecință, garanțiile prevăzute la art. 15 și 16 din RIPA, astfel cum au fost completate de Codul IC, se aplicau deopotrivă și comunicațiilor interceptate și datelor de comunicații obținute de la servicii de informații străine, cu condiția ca materialele „să fi fost identificate ca fiind rezultatul interceptării”.

507. Curtea a examinat garanțiile prevăzute la art. 15 și art. 16 în ceea ce privește regimul de interceptare în masă și este convinsă că procedurile de stocare, de accesare, de examinare și de utilizare a materialelor obținute, de comunicare a materialelor către celelalte părți, precum și de ștergere și distrugere a materialelor obținute erau suficient de clare și ofereau o protecție adecvată împotriva abuzurilor (supra, pct. 384-405). Având în vedere constatările la care a ajuns supra, pct. 497, Curtea observă că pct. 12.6 din Codul IC nu extinde garanțiile prevăzute la art. 15 și 16 din RIPA, astfel cum au fost completate de Codul IC, pentru toate materialele primite de la serviciile de informații străine care ar putea fi rezultatul interceptării, limitând aceste garanții doar la materialele care au fost identificate ca atare; cu toate acestea, Curtea nu consideră că doar acest fapt afectează în mod iremediabil modul în care regimul schimbului de informații respectă prevederile art. 8.

508. În contextul regimului prevăzut la art. 8 alin. (4), Curtea și-a exprimat îngrijorarea cu privire la exceptarea datelor de comunicații aferente de la garanțiile prevăzute la art. 16. Cu toate acestea, în temeiul regimului prevăzut la art. 8 alin. (4), statul era în măsură să intercepteze, să stocheze și să caute

toate pachetele de comunicații care traversau anumite canale de transmisie. Prin urmare, exceptarea generală a datelor de comunicații aferente de la garanția prevăzută de art. 16 însemna că toate datele respective, indiferent dacă erau sau nu de interes în materie de informații, puteau fi examinate de serviciile de informații aparent fără restricții. Pe de altă parte, în temeiul Capitolului 12 din Codul IC, serviciile de informații nu solicitau în masă date privind conținutul și date de comunicații aferente. Pct. 12.5 din Codul IC, împreună cu nota de subsol aferentă, indică faptul că, în cazul în care o cerere se baza pe un mandat existent, cererea trebuia să aibă legătură și să fie despre selectori specifici (și anume, anumite persoane), iar ministrul să fi aprobat deja cererea de interceptare a comunicațiilor persoanelor respective. Deși, în împrejurări excepționale, cererea putea fi formulată în lipsa unui mandat, ministrul trebuia să aprobe personal cererea și, în cazul în care se baza pe selectori specifici, trebuia să ia în considerare și să aprobe personal examinarea respectivelor comunicații în raport cu astfel de factori. În cazul în care cererea nu privea selectori specifici, eventualele comunicații obținute ulterior nu puteau fi examinate în funcție de un factor legat de o persoană cunoscută ca fiind în Insulele Britanice, cu excepția cazului în care ministrul aprobase examinarea respectivelor comunicații (supra, pct. 116). Cu alte cuvinte, serviciile de informații fie solicitaseră informații despre o persoană pentru care ministrul examinase deja necesitatea și proporționalitatea obținerii comunicațiilor sale, fie garanția prevăzută de art. 16 era aplicabilă materialelor obținute. Întrucât nu a fost formulată încă nicio cerere fără mandat, se pare că, până în prezent, toate cererile s-au încadrat în prima categorie.

509. Prin urmare, Curtea consideră că Regatul Unit a instituit garanții adecvate pentru examinarea, utilizarea și stocarea datelor privind conținutul și comunicațiile primite de la partenerii de informații, pentru transmiterea ulterioară a acestor materiale și pentru ștergerea și distrugerea lor.

510. În sfârșit, Curtea arată că un nivel suplimentar de protecție era asigurat de către Comisarul IC și de către IPT (supra, pct. 41). Comisarul IC supraveghea regimul schimbului de informații: pct. 12.7 din Codul IC (supra, pct. 116) impunea ca acesta să fie informat cu privire la toate cererile formulate în lipsa unui mandat și să fi supravegheat deja acordarea de mandate și stocarea de materiale de către serviciile de informații.

511. În plus față de supravegherea asigurată de Comisarul IC, IPT asigura controlul *a posteriori* efectiv al regimului schimbului de informații. Astfel cum reiese din procedura *Liberty*, orice persoană care dorea să depună o plângere specifică sau generală cu privire la regimul schimbului de informații o putea face în fața IPT; în răspuns, IPT era în măsură să examineze atât acordurile „publice”, cât și pe cele „nepublice”, pentru a evalua conformitatea cu Convenția a regimului.

512. În consecință, Curtea consideră că regimul de solicitare și de primire a materialelor interceptate era compatibil cu art. 8 din Convenție. Existau

norme detaliate clare care ofereau resortisanților o indicație adecvată asupra circumstanțelor și condițiilor în care autoritățile erau împuternicite să solicite elemente interceptate unui serviciu de informații străin; dreptul intern conținea garanții eficiente împotriva utilizării unor astfel de cereri pentru a eluda dreptul intern și/sau obligațiile ce îi reveneau Regatului Unit în temeiul 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 *a posteriori* efectuat de IPT.

513. Prin urmare, nu a fost încălcat art. 8 din Convenție.

B. Cu privire la art. 10 din Convenție

514. Părțile reclamante din cea de-a treia din cauzele conexate s-au plâns, de asemenea, de faptul că regimul schimbului de informații le-a încălcat drepturile care le reveneau în temeiul art. 10 din Convenție. În măsura în care acest capăt de cerere privea activitatea lor în calitate de ONG-uri, Camera a declarat-o inadmisibilă pentru neepuizarea căilor de atac interne, întrucât reclamantele l-au invocat tardiv în cadrul procedurii interne pentru ca acesta să poată fi examinat (pct. 473 din hotărârea Camerei). Prin urmare, acest aspect al cererii nu intră în domeniul de aplicare al examinării Marii Camere.

515. Părțile reclamante din cea de-a treia din cauzele conexate s-au plâns, de asemenea, într-un mod mai general, de conformitatea regimului schimbului de informații cu art. 10. Deși acest argument a fost invocat în fața IPT în termen, Curtea este de acord cu opinia Camerei potrivit căreia nu se ridică o problemă separată față de cea care decurge din art. 8 din Convenție (pct. 474 din hotărârea Camerei). Prin urmare, hotărăște că nu a fost încălcat art. 10 din Convenție.

IV. OBȚINEREA DE DATE DE COMUNICAȚII DE LA FURNIZORII DE SERVICII DE COMUNICAȚII

A. Cu privire la art. 8 din Convenție

516. Părțile reclamante din cea de-a doua din cauzele conexate s-au plâns de faptul că regimul obținerii datelor de comunicații prevăzut la Capitolul II din RIPA era incompatibil cu drepturile lor în temeiul art. 8 din Convenție.

1. Hotărârea Camerei

517. La data examinării cauzei de către Cameră, Guvernul Regatului Unit urma să înlocuiască cadrul juridic existent pentru efectuarea supravegherii secrete odată cu noua IPA. Dispozițiile noii legi care reglementa păstrarea datelor de comunicații de către furnizorii de servicii de comunicații („FSC”) au făcut obiectul unei căi de atac interne formulată de Liberty. În cursul

respectivei proceduri, Guvernul a admis că dispozițiile relevante nu erau conforme cu cerințele dreptului Uniunii. În consecință, *High Court* a constatat că Partea 4 era incompatibilă cu drepturile fundamentale din dreptul Uniunii, întrucât, în domeniul justiției penale, accesul la datele păstrate nu era limitat la scopul combaterii „infrațiunilor grave”, iar accesul la datele păstrate nu a făcut obiectul unei examinări prealabile din partea unei instanțe sau a unui organ administrativ independent (supra, pct. 190).

518. Având în vedere atât supremația dreptului Uniunii asupra dreptului Regatului Unit, cât și faptul că Guvernul a recunoscut în cadrul procedurilor interne că dispozițiile din IPA care reglementau păstrarea datelor de comunicații de către FSC erau incompatibile cu dreptul Uniunii, Camera a considerat că era „clar” că dreptul intern impunea ca orice regim care permitea autorităților să acceseze datele păstrate de FSC ar trebui să limiteze accesul la scopul combaterii „infrațiunilor grave”, iar 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, Camera a constatat că acesta nu putea fi prevăzut de lege în sensul art. 8 din Convenție (pct. 465-468 din hotărârea Camerei).

2. *Argumentele părților*

519. Părțile nu au prezentat observații suplimentare în fața Marii Camere cu privire la acest capăt de cerere.

3. *Motivarea Curții*

520. Guvernul nu a contestat concluziile Camerei în fața Marii Camere. În plus, aceasta din urmă nu identifică niciun motiv pentru a nu admite concluziile Camerei.

521. În consecință, Curtea consideră că, în speță, a fost încălcat art. 8 din Convenție ca urmare a faptului că funcționarea regimului prevăzut la Capitolul II din RIPA nu era „prevăzută de lege”.

B. Cu privire la art. 10 din Convenție

522. Părțile reclamante din cea de-a doua din cauzele conexe s-au plâns, de asemenea, în temeiul art. 10 din Convenție, de regimul de obținere a datelor de comunicații de la FSC.

1. *Hotărârea Camerei*

523. Camera a admis că regimul prevăzut la Capitolul II oferea o protecție sporită în cazul în care datele erau solicitate în scopul identificării sursei unui jurnalist. În special, pct. 3.77 din Codul de bune practici privind obținerea datelor de comunicații prevedea că, în cazul în care o cerere urmărea să

identifice sursa de informații jurnalistice, trebuia să existe o cerință imperativă de interes public, iar o astfel de cerere trebuia să se folosească de procedurile prevăzute de Legea din 1984 privind funcționarea Poliției și administrarea probelor penale (*Police and Criminal Evidence Act* – „PACE”) pentru a solicita unei instanțe un ordin de divulgare în vederea obținerii acestor date. În temeiul Anexei 1 la PACE, cererea de emitere a unui ordin de divulgare era adresată unui judecător și, în cazul în care cererea privea materiale care constau în sau includeau materiale jurnalistice, cererea trebuia formulată *inter partes*. Autorizația internă putea fi utilizată numai în cazul în care se considera că există o amenințare imediată de pierdere a vieții umane, iar viața acestei persoane ar fi fost pusă în pericol de întârzierea inerentă a procesului de autorizare judiciară (pct. 498 din hotărârea Camerei).

524. Cu toate acestea, dispozițiile respective nu se aplicau decât în cazul în care scopul cererii era de a identifica o sursă; nu se aplicau în toate cauzele în care exista o cerere care viza datele de comunicații ale unui jurnalist sau în cazul în care o astfel de intruziune colaterală era posibil să se producă. În plus, în cauzele care priveau accesul la datele de comunicații ale unui jurnalist, nu existau dispoziții speciale care să restricționeze accesul la scopul combaterii „infracțiunilor grave”. În consecință, Camera a considerat că regimul nu era „prevăzut de lege” în sensul capătului de cerere formulat în temeiul art. 10 (pct. 496-499 din hotărârea Camerei).

2. Argumentele părților

525. Părțile nu au prezentat observații suplimentare în fața Marii Camere cu privire la acest capăt de cerere.

3. Motivarea Curții

526. Guvernul nu a contestat constatările Camerei în fața Marii Camere. În plus, aceasta din urmă nu găsește niciun motiv pentru a nu fi de acord cu concluziile Camerei.

527. În consecință, Curtea consideră că, în prezenta cauză, a existat, de asemenea, o încălcare a art. 10 din Convenție ca urmare a faptului că funcționarea regimului prevăzut la Capitolul II din RIPA nu era „prevăzută de lege”.

V. CU PRIVIRE LA APLICAREA ART. 41 DIN CONVENȚIE

528. Art. 41 din Convenție prevede:

„Dacă Curtea declară că a avut loc o încălcare a Convenției sau a protocoalelor sale și dacă dreptul intern al înaltei părți contractante nu permite decât o înlăturare incompletă a consecințelor acestei încălcări, Curtea acordă părții lezate, dacă este cazul, o reparație echitabilă.”

A. Prejudiciu

529. Părțile reclamante nu au formulat nicio pretenție cu titlu de prejudiciu material sau moral. În consecință, Curtea consideră că nu este necesar să le acorde vreo sumă în această privință.

B. Cheltuieli de judecată

530. În fața Camerei, părțile reclamante au solicitat în prima dintre cauzele conexate 208 958,55 GBP pentru cheltuielile de judecată, iar părțile reclamante din cea de-a doua din cauzele conexate au solicitat 45 127,89 GBP. Reclamantele din cea de-a treia cauză conexată nu au formulat nicio pretenție cu privire la cheltuielile de judecată.

531. Camera a acordat părților reclamante din prima din cauzele conexate suma de 150 000 EUR pentru procedura în fața sa, iar părților reclamante din cea de-a doua din cauzele conexate suma de 35 000 EUR pentru procedura în fața sa.

532. În fața Marii Camere, părțile reclamante au solicitat, în prima dintre cauzele conexate, o sumă suplimentară în valoare de 138 036,66 GBP, iar părțile reclamante din cea de-a doua din cauzele conexate au solicitat suplimentar 69 200,20 GBP, iar în cea de-a treia din cauzele conexate, 44 993,60 GBP.

533. Guvernul a contestat sumele pretinse.

534. În conformitate cu jurisprudența Curții, un reclamant are dreptul la rambursarea cheltuielilor de judecată numai în măsura în care se stabilește caracterul real, necesar și rezonabil al acestora. În speță, ținând seama de documentele aflate în posesia sa și de criteriile de mai sus, Curtea consideră rezonabil să se acorde următoarele sume care să acopere toate cheltuielile de judecată aferente procedurii în fața Camerei: părților reclamante din prima din cauzele conexate suma de 150 000 EUR, iar părților reclamante din cea de-a doua din cauzele conexate suma de 35 000 EUR. Comisia consideră, de asemenea, că este rezonabil să se acorde părților reclamante următoarele sume care să acopere toate cheltuielile de judecată aferente procedurii în fața Marii Camere: părților reclamante din prima din cauzele conexate suma de 77,500 EUR, părților reclamante din cea de-a doua din cauzele conexate suma de 55 000 EUR, și părților reclamante din cea de-a treia din cauzele conexate suma de 36 000 EUR.

C. Dobânzi moratorii

535. Curtea consideră necesar ca rata dobânzilor moratorii să se întemeieze pe rata dobânzii facilității de împrumut marginal, practică de Banca Centrală Europeană, majorată cu trei puncte procentuale.

PENTRU ACESTE MOTIVE, CURTEA

1. *hotărăște*, în unanimitate, că a fost încălcat art. 8 din Convenție în ceea ce privește regimul prevăzut la art. 8 alin. (4) din RIPA;

2. *hotărăște*, în unanimitate, că a fost încălcat art. 8 din Convenție în ceea ce privește regimul prevăzut la Capitolul II din RIPA;

3. *hotărăște*, cu douăsprezece voturi pentru și cinci împotrivă, că nu a fost încălcat art. 8 din Convenție în ceea ce privește primirea de informații de la servicii de informații străine;

4. *hotărăște*, în unanimitate, că, în măsura în care a fost invocat de părțile reclamante din cea de-a doua din cauzele conexe, a fost încălcat art. 10 din Convenție în ceea ce privește regimul prevăzut la art. 8 alin. (4) și regimul prevăzut la Capitolul II din RIPA;

5. *hotărăște*, cu douăsprezece voturi pentru și cinci împotrivă, că nu a fost încălcat art. 10 din Convenție în ceea ce privește primirea de informații de la servicii de informații străine;

6. *hotărăște*, în unanimitate,

(a) a) că statul pârât trebuie să plătească părților reclamante, în termen de trei luni, următoarele sume, care trebuie convertite în moneda statului pârât la rata de schimb aplicabilă la data plății:

(i) părților reclamante din prima din cauzele conexe: 227 500 EUR (două sute douăzeci și șapte mii cinci sute de euro), plus orice sumă ce poate fi datorată de părțile reclamante cu titlu de impozit, în ceea ce privește cheltuielile de judecată;

(ii) părților reclamante din cea de-a doua din cauzele conexe: 90 000 EUR (nouăzeci de mii de euro), plus orice sumă ce poate fi datorată de părțile reclamante cu titlu de impozit, pentru cheltuielile de judecată;

(iii) părților reclamante din cea de-a treia din cauzele conexe: 36 000 EUR (treizeci și șase de mii de euro), plus orice sumă ce poate fi datorată de părțile reclamante cu titlu de impozit, pentru cheltuielile de judecată;

(b) că, de la expirarea termenului de trei luni menționat și până la efectuarea plății, aceste sume trebuie majorate cu o dobândă simplă, la o rată

anuală egală cu rata dobânzii facilității de împrumut marginal practică de Banca Centrală Europeană, majorată cu trei puncte procentuale;

7. *respinge*, în unanimitate, cererea de acordare a unei reparații echitabile pentru celelalte capete de cerere.

Redactată în limbile engleză și franceză, apoi comunicată în scris, la 25 mai 2021, în temeiul art. 77 § 2 și 3 din Regulamentul Curții.

Søren Prebensen
Grefier-adjunct

Robert Spano
Președinte

În conformitate cu art. 45 § 2 din Convenție și art. 74 § 2 din Regulamentul Curții, la prezenta hotărâre sunt anexate următoarele opinii separate:

- a) Opinia comună parțial concordantă a domnilor judecători Lemmens, Vehabović și Bošnjak;
- b) Opinia parțial concordantă și opinia parțial dizidentă a domnului judecător Pinto de Albuquerque;
- c) Opinia comună parțial dizidentă a domnilor judecători Lemmens, Vehabović și Bošnjak;

R.S.O.
S.C.P.

OPINIA COMUNĂ PARȚIAL CONCORDANTĂ A DOMNILOR JUDECĂTORI LEMMENS, VEHABOVIĆ ȘI BOŠNJAK

1. În prezenta cauză, suntem de acord cu concluziile la care a ajuns majoritatea în dispozitivul hotărârii, cu excepția punctelor nr. 3 (neîncălcarea art. 8 din Convenție în ceea ce privește primirea de informații din partea serviciilor de informații străine) și nr. 5 (neîncălcarea art. 10 din Convenție în ceea ce privește primirea de informații din partea serviciilor de informații străine). Pentru a arăta unde nu suntem de acord cu rezultatul cauzei, prezentăm o opinie separată împreună cu colegul nostru, domnul judecător Ranzoni. În plus, prezentăm această opinie concordantă pentru a sublinia că, deși prezenta hotărâre, în ansamblul său, este elegant structurată și în mare măsură clară în mesajul său, a pierdut, de asemenea, o oportunitate excelentă de a susține pe deplin importanța vieții private și a corespondenței atunci când ne confruntăm cu ingerințe care iau forma supravegherii în masă.

I. OBSERVAȚII PRELIMINARE

2. Prezenta cauză privește un exercițiu de punere în balanță între interesele legitime urmărite de statele contractante și drepturile omului și libertățile fundamentale, în special cu cele protejate de art. 8 din Convenție. La începutul motivării sale (pct. 322 și 323 din hotărâre), Marea Cameră descrie pe larg natura amenințărilor moderne cu care se confruntă statele contractante și recunoaște cât de valoroasă poate fi interceptarea în masă pentru identificarea și prevenirea acestor amenințări. În plus, hotărârea subliniază necesitatea păstrării confidențialității operațiunilor în acest domeniu, pe care le consideră legitime, ceea ce înseamnă că publicului nu i se vor oferi decât foarte puține sau niciun fel de informații cu privire la un sistem dat. Deși am putea subscrie, într-o anumită măsură, la această descriere a interesului legitim de a opera un regim de interceptare în masă, nu se pune un accent similar pe importanța vieții private sau pe orice alt interes privat în aceleași observații preliminare. Cu toate că acest lucru nu are un impact direct asupra evaluării sistemului de interceptare în masă examinat, am fi preferat o introducere mai echilibrată a acestei evaluări.

3. Înainte de a începe să analizăm ceea ce considerăm a fi punctele slabe ale prezentei hotărâri, este util să reamintim că viața privată constituie o condiție fundamentală pentru o varietate de interese individuale fundamentale, dar și pentru existența unei societăți democratice. Este esențială pentru confortul, autonomia, autodezvoltarea și capacitatea unei persoane de a stabili relații semnificative cu alte persoane. Constituie, de asemenea, o condiție prealabilă necesară pentru exercitarea drepturilor civile și, prin urmare, pentru statutul de membru liber și egal al unei societăți

democratice al unei persoane. Atingerile aduse vieții private nu doar reduc autonomia individuală și sănătatea mintală și fizică, ci inhibă, de asemenea, autoguvernarea democratică.

4. În primul rând, viața privată este importantă pentru sănătatea mintală și fizică a unei persoane. Simplul sentiment că o persoană este observată și evaluată constant de ceilalți poate avea efecte grave asupra confortului mental și fizic al unei persoane. Aceasta face ca persoanele să își interiorizeze prea mult comportamentul social, astfel încât se simt vinovate sau rușinate din cauza oricăror sentimente sau gânduri, dorințe sau practici pe care nu ar dori să le exprime public. Astfel de tensiuni între cerințele vieții lor interne și presiunile prezentării de sine pot duce la probleme grave de sănătate.

5. În al doilea rând, observarea externă și presiunile asupra prezentării de sine pot obstrucționa „promovarea libertății, a autonomiei, a individualității, a relațiilor umane și promovarea existenței unei societăți libere”¹. Supravegherea este inhibitivă, întrucât diminuează măsura în care putem relaționa spontan și pe deplin cu alte persoane și ne putem implica în anumite activități. Lipsa vieții private ar avea un efect inhibitor asupra vieții noastre interne, a relațiilor noastre și, în cele din urmă, asupra autonomiei noastre. „Astfel, se va pierde [...] esența personală interioară, care este sursa criticilor la adresa conveniențelor, a creativității, a rebeliunii și a reînnoirii”².

6. În al treilea rând, viața privată este esențială pentru autoguvernarea democratică. Supravegherea în masă exercită presiuni interne și externe pentru conformare, făcând ca persoanele să devină supuse și deferente. Pentru a evita opresiunea directă și pentru a-și conferi poleiala de legitimitate, există pericolul inerent ca statul să recurgă la supraveghere pentru a asigura conformitatea și conformismul. Astfel cum a descris George Orwell în romanul 1984:

„Sigur că nu ai cum ști, în fiecare moment, dacă ești sau nu ascultat. Cât de des, sau după ce criterii intră Poliția Gândirii pe fiecare post individual este ceva ce ține de domeniul presupunerilor. N-ar fi imposibil nici să urmărească tot timpul pe toată lumea. În tot cazul, pot intra pe firul tău când au ei chef. Te obligă să trăiești – și de fapt chiar așa trăiești, dintr-o obișnuință devenită instinct – cu presupunerea că orice sunet pe care-l scoți este ascultat și orice mișcare observată, afară de cazul când, să zicem, stai pe întuneric.”³

7. Prin asigurarea unui domeniu al activităților neobservate, viața privată promovează și încurajează autonomia morală a cetățenilor, o cerință centrală a autoguvernării în democrații⁴. Doar ființele autonome se pot autoguverna

¹ Ruth Gavison (1980), „Privacy and the Limits of Law”, *Yale Law Journal* 89, pag. 347.

² Jeffrey Reiman (1995), „Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Information Technology of the Future”, *Santa Clara High Technology Law Journal* 11:1, pag. 42.

³ George Orwell (2008), *1984* (Londra: Penguin), pag. 4-5.

⁴ Daniel Solove (2008), *Understanding Privacy* (Cambridge, MA: Harvard University Press), pag. 98.

cu adevărat și doar ființele autonome se pot bucura cu adevărat de toate drepturile civile, cum ar fi dreptul de vot, libertatea de asociere și de participare la societatea civilă, libertatea de gândire și de conștiință, libertatea de exprimare și libertatea de religie, care sunt esențiale pentru autoguvernare. Nu se poate spune că ne bucurăm pe deplin de libertățile pe care aceste drepturi ar trebui să ni le permită dacă libertatea noastră internă este compromisă.

8. Însă supravegherea nu exercită doar presiuni interne asupra libertății. În măsura în care cetățenii își păstrează autonomia, exercită, de asemenea, presiuni externe asupra libertății lor de a-și exercita drepturile civile. La fel cum faptul de a trăi sub un control social constant ne face mai puțin înclinați să acționăm în conformitate cu sentimentele și gândurile noastre, de teama ostracizării, faptul de a trăi sub supravegherea constantă a guvernului poate face ca cetățenii să fie ceva mai precauți atunci când se implică în convingerile lor politice, mai puțin probabil să se asocieze liber, mai puțin înclinați să vorbească liber, mai puțin dispuși să candideze pentru funcții publice. Efectul cumulat al unor simple inhibări marginale poate sufoca ceea ce a fost cândva o societate liberă, în special pe măsură ce oamenii cresc într-un mediu cu un grad ridicat de conformism și de lașitate morală. William O. Douglas, judecător de la Curtea Supremă de Justiție a Statelor Unite ale Americii, redactând opinia sa separată în *Osborn împotriva Statelor Unite ale Americii*, descrie în mod impresionant amenințarea pe care supravegherea în masă o reprezintă pentru libertățile noastre democratice:

„[...] Ar putea veni ziua în care nimeni nu va mai putea fi sigur dacă cuvintele sale nu sunt înregistrate pentru a fi folosite la un moment dat; când fiecare dintre noi se va teme că gândurile sale cele mai secrete nu mai sunt ale sale, ci aparțin guvernului; atunci când cele mai confidentiale și intime conversații sunt întotdeauna ascultate de urechi dornice să audă, urechi iscoditoare. Când va veni acea zi, viața privată și, odată cu ea libertatea, vor dispărea. Dacă viața privată a unui om poate fi invadată după bunul plac, cine poate spune că este liber? Dacă fiecare cuvânt este preluat și evaluat, sau dacă îi este teamă pentru fiecare cuvânt, cine poate spune că se bucură de libertatea de exprimare? Dacă fiecare relație este cunoscută și înregistrată, dacă fiecare conversație cu relațiile noastre sunt sustrase, cine poate spune că se bucură de libertatea de asociere? Când vor fi atinse astfel de condiții, cetățenilor noștri le va fi frică să rostească orice altceva decât cele mai sigure și ortodoxe gânduri; se vor teme se asocieze cu oricine, chiar și cu cei mai acceptabili oameni. Libertatea, așa cum o concepe Constituția, va fi dispărut.”⁵

9. Pentru a conchide, dezvoltarea de noi tehnologii care să permită supravegherea în masă și utilizarea mai eficace a informațiilor colectate a crescut amenințările la adresa vieții private, precum și riscul de abuz asupra datelor cu caracter personal. Nu intenționăm să susținem că aceste amenințări și riscuri s-au materializat deja pe scară largă sau că au generat consecințele discutate mai sus. Cu toate acestea, trebuie să fim conștienți în mod

⁵ *Osborn împotriva Statelor Unite ale Americii*, 385 U.S. 323 (1966).

corespunzător de existența acestora atunci când creăm un sistem capabil să prevină, să detecteze și să sancționeze orice abuz care ar putea avea loc.

10. În opinia noastră, aceste considerații ar fi trebuit să determine Curtea să acorde o mai mare importanță vieții private în general și, în special, confidențialității corespondenței atunci când le-a pus în balanță cu interesele legitime ale statului pârât în ceea ce privește operarea sistemului său de interceptare în masă. În consecință, Marea Cameră ar fi trebuit (a) să identifice cu acuratețe și să acorde o pondere adecvată ingerințelor în viața privată și corespondență; (b) să introducă garanții minime clare, capabile să protejeze persoanele împotriva ingerințelor arbitrare sau excesive; în consecință, (c) să evalueze sistemul de interceptare în masă criticat într-un mod mai strict.

II. INGERINȚE ÎN VIAȚA PRIVATĂ ȘI CORESPONDENȚĂ

11. La pct. 325 din hotărâre, majoritatea descrie etapele sistemului de interceptare în masă. Consideră că etapa inițială, descrisă ca interceptarea și păstrarea inițială a comunicațiilor și a datelor aferente comunicațiilor, urmată de eliminarea imediată a unor părți ale comunicațiilor, „nu constituie o ingerință deosebit de semnificativă” (pct. 330 din hotărâre). Cu respect, nu suntem de acord. Suntem convinși că, deja în această etapă, ingerința este semnificativă. În primul rând, prin interceptarea și păstrarea inițială a datelor, toate comunicațiile oricărei persoane care trece prin canalele de transmisie selectate și toate datele de comunicații aferente ajung în mâinile autorităților statului. În al doilea rând, deși este adevărat că, în această etapă, conținutul acestor comunicări nu a fost încă analizat sau adus în atenția factorilor de decizie și, prin urmare, nu poate conduce încă la nicio acțiune împotriva unei persoane particulare, prima etapă constituie o condiție *sine qua non* pentru orice etapă ulterioară. Nu se cunoaște amploarea exactă a comunicațiilor și a datelor aferente astfel colectate de serviciile de informații. Există însă motive pentru a crede că, în mod regulat, o mare parte a comunicațiilor a milioane de persoane este interceptată. Această situație este agravată de faptul că persoanele în cauză nu vor fi, de regulă, conștiente de această ingerință. Într-o asemenea situație, în care oamenii nu pot ști dacă comunicațiile lor sunt vizate, dar sunt conștienți că există o probabilitate puternică ca acest lucru să se întâmple, apare un al treilea element de ingerință: oamenii își pot adapta comportamentul, cu multe consecințe grave, astfel cum se descrie mai sus la pct. 3-8 din prezenta opinie separată.

12. Potrivit pct. 330 din hotărâre, anumite părți ale comunicațiilor interceptate sunt eliminate imediat. Curtea nu deține nicio informație cu privire la modul în care se realizează această „eliminare”. Se poate presupune, în mod rezonabil, că nu se realizează în mod aleatoriu, fără nicio logică internă, și că, în acest exercițiu, serviciile de informații aplică anumite criterii care separă elementele fără valoare de materialele care ar putea fi utile. Însuși

faptul că acest act este realizat în obscuritate și pe o bază necunoscută ar trebui, în opinia noastră, să constituie un motiv serios de îngrijorare. O astfel de lipsă de transparență, cel puțin, nu poate îndeplini decât cu greutate cerința de previzibilitate, aceasta fiind, la rândul său, una dintre condițiile pentru legalitatea oricărei ingerințe în drepturile protejate de art. 8 din Convenție. Cu toate acestea, majoritatea nu abordează în niciun fel această etapă specifică a procesului de interceptare în masă. Considerăm că este o deficiență foarte importantă a hotărârii.

III. GARANȚII MINIME DE PROTECȚIE A PERSOANELOR ÎMPOTRIVA INGERINȚELOR ARBITRARE SAU EXCESIVE

13. La pct. 335, hotărârea subliniază jurisprudența Curții cu privire la șase cerințe minime care ar trebui stabilite în dreptul intern pentru a evita abuzurile de putere în cazurile de interceptare a comunicațiilor în scopul cercetării penale. Curtea explică în continuare că, în *Roman Zakharov împotriva Rusiei* [(MC), nr. 47143/06, CEDO 2015], a hotărât că aceleași șase garanții minime se aplică și în cazurile în care interceptarea a avut loc din motive de securitate națională. În etapa următoare, Marea Cameră identifică necesitatea de a dezvolta și de a adapta aceste cerințe la specificitățile interceptării în masă și, în final, prezintă o listă de opt criterii pe care cadrul juridic intern trebuie să le definească în mod clar pentru a se conforma cu art. 8 din Convenție (pct. 361 din hotărâre).

14. Această listă este foarte bine susținută de argumente și poate cu certitudine să servească drept protecție împotriva arbitrariului și abuzului. Cu toate acestea, criteriile incluse în această listă:

a) nu servesc, în mod clar, drept norme minime de sine stătătoare, deoarece nerespectarea oricăreia dintre normele respective pare a fi „reparabilă” în procesul de evaluare globală;

b) impun o definiție clară a garanțiilor speciale în dreptul intern, dar nu stabilesc ele însele garanții minime;

c) nu oferă nicio protecție materială clară unei persoane împotriva unei ingerințe disproporționate, în special în etapa de aplicare a selectorilor puternici la materialul colectat, iar protecția procedurală oferită de aceste criterii este, de asemenea, insuficientă.

15. În ceea ce privește lit. a), am dori să atragem atenția cititorului asupra pct. 360 din hotărâre, care anunță necesitatea unei evaluări globale a unui anumit regim de interceptare în masă. Deși acest lucru poate fi atractiv, erodează în mod necesar importanța fiecărei garanții. În schimb, considerăm că fiecare garanție etichetată ca fiind minimă nu poate fi compensată niciodată de factori de compensare oferți cu privire la un alt criteriu. Cu alte cuvinte, nerespectarea unei garanții care este considerată a fi minimă ar trebui să conducă automat la constatarea unei încălcări a art. 8 din Convenție, indiferent dacă o evaluare globală ar putea revela o imagine mai pozitivă. Din

păcate, majoritatea nu pare să fi optat pentru o astfel de abordare. Adăugăm că o abordare care stabilește norme minime ca limite absolute, precum linii roșii groase care nu pot fi depășite, ar asigura o protecție mai strictă și mai previzibilă, ceea ce este extrem de important într-un domeniu în care acțiunea autorităților statului se desfășoară cu un nivel ridicat de confidențialitate, astfel încât, în termenii prezentei hotărâri (pct. 322), sunt disponibile puține informații, sau nu există deloc informații cu privire la funcționarea sistemului, iar informațiile disponibile pot fi formulate într-o terminologie obscură.

16. În ceea ce privește lit. b), majoritatea afirmă că cele opt criterii menționate la pct. 361 trebuie să fie definite cu claritate în cadrul juridic intern. Deși aceasta este o cerință care trebuie salută, în special din punctul de vedere al previzibilității legii, aceste criterii nu stabilesc, în sine, cerințe minime în ceea ce privește condițiile de fond sau procedurale care trebuie respectate pentru a aplica regimul de interceptare în masă și pentru a trece de la etapa inițială la unele mai intruzive. Această deficiență este parțial remediată de faptul că anumite (dar nu toate) dintre elementele discutate la pct. 348-360 din hotărâre sunt prezentate nu doar în pasaje descriptive care fac trimitere la jurisprudența existentă, ci și în termeni prescriptivi care stabilesc anumite cerințe, în special în ceea ce privește autorizarea interceptării în masă în etapele sale specifice. Cu toate acestea, susținem că cerințele stabilite de majoritate nu merg suficient de departe în protejarea unei persoane împotriva ingerințelor arbitrare, excesive sau abuzive în viața privată și în corespondența acesteia.

17. Acest fapt ne aduce la lit. c). În contextul interceptării țintite, în principal în scopul detectării și investigării activităților infracționale, Curtea a făcut referire la anumite garanții materiale împotriva abuzurilor. Astfel, Curtea a cerut ca natura infracțiunilor care pot genera un mandat de interceptare să fie definită, alături de categoriile de persoane susceptibile a face obiectul interceptării comunicațiilor. În plus, în numeroase ocazii, Curtea a recurs la cerința existenței unei bănueli întemeiate. Majoritatea consideră pur și simplu că aceste garanții nu sunt ușor de aplicat în cazul interceptării în masă. Deși putem fi de acord că nu pot fi transpuse direct, este în continuare nevoie de o protecție substanțială solidă, prin care garanțiile dezvoltate în cadrul interceptării specifice în scopul combaterii infracționalității să poată servi drept o sursă excelentă de inspirație, astfel cum vom încerca să explicăm mai jos.

18. În primul rând, spre deosebire de interceptarea specifică în cadrul prevenirii infracționalității, interceptarea în masă este utilizată în mare măsură în scopuri de securitate națională. Este dificil de înțeles de ce nu ar trebui să ne așteptăm ca legislația internă să definească în mod clar posibilele amenințări la adresa securității naționale și circumstanțele în care aceste amenințări pot declanșa interceptarea în masă.

19. În ceea ce privește a doua cerință de fond legată de interceptarea țintită, și anume definirea categoriilor de persoane susceptibile să le fie interceptate

comunicațiile, se poate recunoaște că o cerință similară nu ar avea sens în prima etapă a interceptării în masă, atunci când toate comunicațiile care trec prin anumite canale de transmisie sunt interceptate fără discriminare. Cu toate acestea, amploarea ingerinței nu ar trebui să fie o scuză pentru abandonarea unei anumite garanții. În plus, în etapele ulterioare ale interceptării în masă, în special atunci când se aplică selectori puternici în scopul identificării și analizării comunicațiilor unei persoane identificate, situația devine în mare măsură comparabilă cu cea a interceptării țintite. A aștepta cadrul juridic să definească categoriile de persoane care pot fi vizate de aplicarea unor selectori puternici nu ar fi o cerință excesivă, ci mai degrabă o cerință pe deplin adecvată.

20. În al treilea rând, cerința existenței unei bănuieli întemeiate reprezintă o protecție importantă împotriva ingerințelor arbitrare și disproporționate în mai multe drepturi ale Convenției. Se referă la probabilitatea ca o infracțiune care a condus la o ingerință să fi fost comisă sau să fie pe cale de a fi comisă. Deși interceptarea în masă nu ar trebui utilizată în investigarea infracțiunilor, ci mai degrabă limitată la scopuri de securitate națională, considerăm că un standard similar bănuielii întemeiate ar trebui să fie aplicabil motivelor pentru care poate fi autorizată interceptarea în masă. Acest fapt este valabil în special atunci când interceptarea în masă începe să vizeze o persoană identificată prin aplicarea unor selectori puternici. Pentru a fi clar, considerăm că, într-o societate democratică, serviciile de informații nu pot inspecta comunicațiile și datele de comunicare conexe ale unei persoane decât odată ce pot demonstra unui observator obiectiv că persoana respectivă poate fi implicată sau este pe punctul de a se implica în activități care aduc atingere unui interes specific în materie de securitate națională sau este o persoană care este sau poate fi în contact cu persoane implicate sau pe punctul de a se implica în astfel de activități. Nicio astfel de cerință sau o cerință similară nu a fost introdusă de majoritate în prezenta hotărâre.

21. În locul acestor trei garanții, majoritatea a stabilit o cerință de fond excesiv de largă, și anume că motivele pentru care poate fi autorizată interceptarea în masă și circumstanțele în care pot fi interceptate comunicările unei persoane trebuie să fie clar definite în cadrul juridic intern. Din păcate, trimiterea la „motive” și „circumstanțe” este destul de vagă, în special în absența oricărei referiri la care ar putea sau nu ar putea fi astfel de motive și circumstanțe. În plus, potrivit formulării utilizate la pct. 361 din hotărâre, cerința specifică referitoare la motive se aplică numai etapei de autorizare a interceptării în masă, și nu oricărei etape ulterioare, neoferind astfel nicio indicație cu privire la aspectul dacă o cerință de fond este legată, de exemplu, de aplicarea unor selectori puternici care să vizeze comunicațiile unei persoane identificate.

22. Lipsa unei protecții pe fond adecvate are un impact important asupra eficacității protecției procedurale. Principalul element al protecției procedurale este cerința autorizării prealabile, pe care prezenta hotărâre o

introduce atât în prima etapă a interceptării în masă, cât și înainte de aplicarea selectorilor puternici. Aspectul esențial al oricărei autorizări prealabile este acela de a verifica dacă ingerința avută în vedere respectă criteriile pe fond ale unei astfel de ingerințe. Cu toate acestea, în cazul în care criteriile pe fond sunt vagi, excesiv de extinse sau chiar inexistente, cerința autorizării prealabile nu va oferi în mod necesar o protecție suficient de eficientă împotriva arbitrariului și abuzului.

23. În ceea ce privește obligația de autorizare prealabilă, hotărârea impune ca o astfel de autorizație să fie exercitată în etapa inițială de către un organism independent de executiv. Putem fi de acord. Cu toate acestea, respectăm, dar nu suntem deloc de acord că este suficient ca aplicarea unor selectori puternici referitori la persoane identificabile să facă obiectul unei autorizări interne prealabile. În schimb, susținem că, în această etapă, ar fi necesar un control judiciar prealabil. Deși jurisprudența existentă a Curții nu impune neapărat o autorizație judiciară pentru interceptarea ținută a comunicațiilor persoanelor, considerăm că există motive pentru un standard de protecție consolidat în cauzele în care sunt aplicați selectori puternici în interceptarea în masă. Aceste motive sunt următoarele:

a) interceptarea în masă, spre deosebire de interceptarea ținută, nu se limitează la o categorie specifică de persoane și, astfel, poate fi examinată o bază de comunicații mult mai mare decât în cazul comunicațiilor ținute;

b) în plus, un selector puternic aplicabil unei persoane identificate poate, atunci când este aplicat, să deschidă ușa unui număr mult mai mare de comunicații, și anume când se face referire la acea persoană, chiar dacă s-a implicat sau nu în respectivele comunicații (spre deosebire de comunicarea prin intermediul mijloacelor de comunicare pe care aceasta le utilizează personal);

c) interceptările ținute realizate în scopul aplicării legii sunt, în general, supuse unei forme de control judiciar la un anumit moment dat. De exemplu, atunci când probele sunt obținute prin interceptare ținută, acestea vor fi prezentate în cadrul unor proceduri penale ulterioare, astfel încât o instanță sesizată cu procedura respectivă să fie în măsură să verifice dacă interceptarea ținută a respectat cerințele legale în respectiva cauză. În mod normal, nu se va realiza un astfel de control judiciar ulterior în cauzele de interceptare în masă combinate cu aplicarea unor selectori puternici.

24. În complet contrast cu această viziune, majoritatea consideră că autorizarea internă prealabilă este suficientă. În opinia noastră, autorizarea internă nu poate oferi un nivel de protecție împotriva arbitrariului și abuzului comparabil cu protecția oferită de un control independent. Este greu de imaginat modul în care o persoană care are o legătură organizațională și, eventual, colegială cu autoritatea solicitantă ar putea evalua adecvat o cerință, într-un mod echitabil și dezinteresat. Este probabil ca cerințele de autorizare să nu fie pe deplin respectate și, astfel, scopul însuși al acestei garanții nu va fi îndeplinit. Acest lucru este cu atât mai probabil să se întâmple în cazul

înalțelor părți contractante care nu au o tradiție îndelungată de supraveghere democratică a serviciilor de informații.

25. Observăm că guvernele Regatului Unit și Țărilor de Jos au susținut că orice cerință de a explica sau de a motiva selecția sau criteriile de căutare ar restrânge în mod grav eficacitatea interceptării în masă (pct. 353 din hotărâre) și că majoritatea arată o anumită înțelegere pentru acest argument (pct. 354 din hotărâre). Nu putem subscrie la acest argument. Considerăm că, într-o societate democratică, datele privind comunicațiile și comunicațiile aferente ale unei persoane identificate nu pot fi identificate și examinate fără consimțământul persoanei respective, cu excepția cazului în care există motive foarte convingătoare în acest sens. În cazul în care un serviciu de informații sau o altă autoritate nu este în măsură să prezinte astfel de motive și să le demonstreze în fața unei instituții independente, acest lucru ar trebui să însemne pur și simplu că nu ar trebui să aibă acces la astfel de comunicații. Recunoaștem că ocazional poate apărea o situație în care procesul normal de autorizare este prea greu pentru a neutraliza efectiv o amenințare la adresa securității naționale și că ar trebui oferite și alte soluții în acest sens. Cu toate acestea, dacă un sistem solid de autorizare, conceput pentru a proteja în mod corespunzător drepturile omului, este perceput ca un obstacol inutil, societatea democratică ar trebui să fie avertizată.

IV. EVALUAREA REGIMULUI DE INTERCEPTARE ÎN MASĂ ÎN CAUZĂ

26. Suntem de acord cu ceilalți membri ai Marii Camere în concluziile lor de la punctele nr. 1, 2 și 4 din dispozitivul hotărârii. Acestea fiind spuse, considerăm că evaluarea anumitor caracteristici ale regimului contestat nu merge suficient de departe și nu reușește să identifice în mod corespunzător unele dintre deficiențele acestuia.

27. De exemplu, dorim să direcționăm atenția cititorului asupra motivelor pentru care ar putea fi autorizată interceptarea în masă, în temeiul sistemului din Regatul Unit (pct. 368-371 din hotărâre). Un mandat de interceptare în masă poate fi emis dacă acest lucru este necesar: a) în interesul securității naționale; b) în scopul prevenirii sau detectării infracțiunilor grave; sau c) în scopul protejării bunăstării economice a Regatului Unit, în măsura în care aceste interese sunt relevante și pentru interesele securității naționale.

28. Atât scopurile menționate la literele a), cât și c) au făcut referire la interesele securității naționale. Se pare că nici securitatea națională, nici interesele sale nu au fost definite nicăieri. Deși luăm act de trimiterea din hotărâre la clarificarea de către Comisarul IC a modului în care practica percepe termenul „securitate națională” (pct. 369 din hotărâre), susținem că această clarificare a rămas insuficientă din punctul de vedere al cerinței de previzibilitate. În plus, avem îndoieli cu privire la faptul că clarificarea adusă de Comisarul IC poate fi asimilată unei jurisprudențe consacrate, care,

potrivit jurisprudenței Curții, poate compensa caracterul vag al legislației. Drept consecință a lipsei unei definiții clare, o persoană nu poate fi sigură, chiar și cu ajutorul unei consilieri calificate, cu privire la motivele exacte pentru care comunicațiile sale ar putea fi interceptate și analizate de serviciile de informații.

29. Scopul prevăzut la lit. b) nu prezenta deficiențele menționate mai sus în ceea ce privește scopurile menționate la lit. a) și c). Infracțiunea gravă era definită ca fiind o infracțiune pentru care se putea aștepta în mod rezonabil ca autorul (presupunând că a împlinit douăzeci și unu de ani și nu avea condamnări anterioare) să fie condamnat la pedeapsa cu închisoarea de cel puțin trei ani sau în cazul în care actul infracțional a implicat recurgerea la violență, a avut ca rezultat un câștig financiar substanțial sau a fost săvârșit de un număr mare de persoane în urmărirea unui scop comun (pct. 369 din hotărâre). O astfel de definiție acoperă o gamă foarte largă de fapte, ceea ce ridică îndoieli serioase cu privire la proporționalitatea acestui motiv. În plus, într-o societate democratică, serviciile de informații nu ar trebui să aibă nicio competență în combaterea infracționalității, cu excepția cazului în care activitățile infracționale amenință securitatea națională⁶. Explicația guvernului pârlat, și anume că informațiile obținute prin interceptarea în masă nu pot fi utilizate în cadrul unui proces penal, nu este, în opinia noastră, convingătoare. Se pare că, pe baza informațiilor astfel obținute, agențiile de aplicare a legii ar putea acționa, de exemplu, prin adoptarea de măsuri de investigare sau chiar prin arestări, furnizând, la rândul lor, probe în cadrul procesului penal. Este probabil ca, într-un viitor nu atât de îndepărtat, prin explorarea acestui teren specific, investigarea infracțiunilor să treacă de la supravegherea țintită la interceptarea în masă a datelor.

V. CONCLUZIE

30. Sunt rare ocaziile în care Curtea se pronunță asupra unei cauze care modelează viitorul societăților noastre. Prezenta cauză este un astfel de exemplu. Marea Cameră a profitat parțial de această oportunitate și a prezentat un set cuprinzător de principii care vizează protejarea drepturilor omului și a libertăților fundamentale, în special a celor consacrate la art. 8 și 10 din Convenție. Cu toate acestea, din motivele explicate în această opinie separată, în momentul efectuării exercițiului de punere în balanță, majoritatea nu a reușit să acorde importanța cuvenită vieții private și corespondenței, care, în mai multe privințe, rămân insuficient protejate în fața ingerințelor cauzate de interceptarea în masă. Putem spera că, în cauzele viitoare care vor

⁶ A se vedea, de exemplu, Recomandarea 1402 (1999) a Adunării Parlamentare a Consiliului Europei privind controlul serviciilor de securitate internă în statele membre ale Consiliului Europei, în special Orientarea A ii). Această recomandare abordează activitățile serviciilor de securitate internă, dar considerăm că este perfect aplicabilă și în cazul serviciilor de informații străine.

ridica aspecte de ingerință concretă în drepturile persoanelor, Curtea va interpreta și va dezvolta în continuare principiile într-un mod care să susțină în mod corespunzător societatea democratică și valorile pe care le reprezintă.

**OPINIA PARȚIAL CONCORDANTĂ ȘI PARȚIAL
SEPARATĂ A DOMNULUI JUDECĂTOR PINTO DE
ALBUQUERQUE**

- I. Introducere (pct. 1)**
- II. Deconstrucția regimului de interceptare în masă *pro autoritate* al Curții (pct. 2-18)**
 - A. Limbaj vag (pct. 2-3)
 - B. Metodologie părtinitoare (pct. 4-12)
 - C. Un regim al garanțiilor deficient (pct. 13-15)
 - D. Concluzie preliminară (pct. 16-18)
- III. Construcția regimului de interceptare în masă *pro autoritate* (pct. 19-34)**
 - A. Interceptarea în masă a comunicațiilor (pct. 19-29)
 - B. Schimbul de date interceptate cu serviciile de informații străine (pct. 30-31)
 - C. Interceptarea în masă a datelor de comunicații aferente (pct. 32)
 - D. Concluzie preliminară (pct. 33-34)
- IV. Critici aduse regimului de interceptare în masă din Regatul Unit în litigiu în prezenta speță (pct. 35-58)**
 - A. Interceptarea în masă a comunicațiilor în temeiul RIPA (pct. 35-49)
 - B. Schimbul de date interceptate cu serviciile de informații străine (pct. 50-54)
 - C. Interceptarea în masă a datelor de comunicații aferente (pct. 55-57)
 - D. Concluzie preliminară (pct. 58)
- V. Concluzie (pct. 59-60)**

I. INTRODUCERE

1. Am votat cu majoritatea, cu excepția constatării neîncălării art. 8 și 10 în ceea ce privește primirea de materiale interceptate de la serviciile de informații străine, și anume a materialelor interceptate în masă de Agenția Națională de Securitate a Statelor Unite ale Americii (NSA) în cadrul programelor PRISM și Upstream. În plus, nu suntem de acord cu esența motivării majorității în ceea ce privește constatarea unei încălcări a art. 8 și 10. Scopul acestei opinii este de a prezenta motivele care stau la baza dezacordului nostru¹.

¹ Este a doua oară când formulăm o opinie separată cu privire la interceptarea în masă. În *Szábo și Vissy împotriva Ungariei*, nr. 37138/14, 12 ianuarie 2016, am avut ocazia să ne exprimăm opiniile cu privire la panta alunecoasă pe care a alunecat regimul maghiar de

II. DECONSTRUCȚIA REGIMULUI DE INTERCEPTARE ÎN MASĂ PRO AUTORITATE AL CURȚII

A. Limbaj vag

2. Regretăm să afirmăm de la bun început că limbajul Curții este intolerabil de vag, astfel cum se va demonstra în această opinie. Deși uneori această formulare reflectă intenția deliberată a Curții de a acorda o marjă de manevră pentru executarea discreționară a acestei hotărâri de către statul pârât, în alte momente demonstrează ezitarea judecătorilor în exercitarea funcției lor de a judeca. Procedând astfel, aceștia nu numai că slăbesc autoritatea Curții, ci și atenuează valoarea de standardizare a acestei hotărâri.

3. Întrucât conceptele juridice din dreptul european al drepturilor omului sunt autonome, în sensul că nu sunt strict dependente de sensul și de domeniul de aplicare al conceptelor juridice interne corespunzătoare, și având în vedere caracterul nou al aspectelor juridice în discuție în prezenta cauză din fața Marii Camere, Curtea ar fi trebuit să stabilească, negru pe alb, sensul conceptelor juridice fundamentale pe care le utilizează în prezenta hotărâre², indiferent de sensul lor în Legea din 2000 privind competențele de investigare (RIPA), în Codul de bune practici privind interceptarea comunicațiilor (Codul IC) sau orice alte proceduri „nepublice”. Din motive legate de claritatea conceptuală, vom utiliza termenii enumerați mai jos cu următoarele sensuri:

a) **„subiecții interceptării”**: persoane fizice și persoane juridice, inclusiv servicii publice, corporații private, ONG-uri și orice organizații ale societății civile ale căror comunicații electronice pot fi interceptate, sau au fost interceptate³;

b) **„materiale interceptate” sau „materiale în masă”**: conținutul comunicațiilor electronice și datele aferente comunicațiilor care au fost colectate prin intermediul interceptării în masă⁴;

c) **„date aferente comunicațiilor”**: datele necesare pentru localizarea sursei unei comunicații electronice și a destinației acesteia, pentru stabilirea datei, orei, duratei și tipului de comunicații, pentru identificarea echipamentelor de comunicații utilizate și pentru localizarea echipamentelor terminale și a comunicațiilor, date care cuprind, *inter alia*, numele și adresa utilizatorului, numerele de telefon ale apelantului și ale persoanei apelate, precum și adresa IP pentru serviciile de internet⁵;

interceptare în masă și consecințele nedorite ascunse în josul pantei. Având în vedere discuția purtată în Marea Cameră și după o analiză atentă a tuturor argumentelor contradictorii, putem afirma acum că nu ne-am mișcat nici măcar cu câțiva centimetri față de poziția noastră anterioară. De fapt, suntem și mai convingși că ceea ce scriam în 2016 este, din păcate, încă foarte actual. Prin urmare, prezenta opinie ar trebui citită în coroborare cu ceea ce scriam în urmă cu cinci ani.

² Aceste bune practici pot fi găsite, de exemplu, în *Rohlena împotriva Republicii Ceha* (MC), nr. 59552/08, 27 ianuarie 2015.

³ Conceptul intern este similar. A se vedea art. 20 din RIPA.

⁴ Conceptul intern este diferit. A se vedea art. 20 din RIPA.

⁵ Conceptul intern este mai limitat. A se vedea art. 20 din RIPA. Art. 21 alin. (4), (6) și (7) prevede conceptul de „date de comunicații”.

d) „interceptare în masă”: interceptarea ținută și neținută a comunicațiilor electronice (și a datelor de comunicații aferente) care circulă prin canalele de transmisie, realizată prin intermediul selectorilor și al selectorilor puternici;

e) „canale de transmisie”: transportatoare (în principal cabluri de fibră optică submarine) de comunicații electronice;

f) „selectori puternici”: identificatori specifici (personali) în legătură cu o țință identificată sau identificabilă, care permit colectarea de comunicații electronice către, dinspre sau în legătură cu țința respectivă;

g) „selectori”: identificatori nespecfici (nepersonali);

h) comunicație „către” sau „de la”: comunicația electronică pentru care expeditorul sau destinatarul este utilizatorul selectorului atribuit;

i) comunicație „despre”: comunicația în care selectorul atribuit este menționat în comunicația electronică colectată, dar țința nu este neapărat un participant la comunicare;

j) „comunicație externă”: comunicația trimisă sau primită în afara teritoriului național⁶;

k) „comunicație”: „orice înseamnă expunere, muzică, sunete, imagini vizuale sau date ale oricărei descrieri și semnale care servește fie la a transmite ceva între persoane, între o persoană și un obiect sau între lucruri, fie la acționarea sau controlul oricărui aparat”⁷;

l) „proceduri nepublice”: normele și practicile secrete, interne ale autorității de interceptare.

B. Metodologie pârținitoare

4. Abordarea metodologică a Curții în această cauză este regretabilă, din două motive principale. În primul rând, Curtea a fost dispusă să soluționeze o cauză de această importanță „pe baza unor informații limitate cu privire la modul în care funcționează regimurile [de interceptare în masă ale statelor contractante]”⁸. De exemplu, Guvernul nu a indicat numărul sau gradul de precizie al selectorilor pe care i-a utilizat, numărul de canale de transmisie interceptate sau modul exact în care au fost selecționate aceste canale de transmisie sau tipul de rapoarte de informații care au fost generate cu privire la datele de comunicații aferente, însă Curtea nu a insistat asupra obținerii acestor informații esențiale. Tribunalul cu Competențe de Investigare (IPT) a examinat procedurile „nepublice”⁹, Comisarul pentru Interceptarea Comunicațiilor (Comisarul IC) a avut acces la „probe confidențiale”¹⁰ și chiar și Evaluatorul independent al legislației în materie de combatere a

⁶ Acest concept este similar cu cel de la art. 20 din RIPA.

⁷ Acest concept este consacrat la art. 81 din RIPA, care poate fi utilizat și de către Curte.

⁸ Pct. 323 din prezenta hotărâre.

⁹ Pct. 33 și 50 din prezenta hotărâre.

¹⁰ Pct. 136 din prezenta hotărâre.

terorismului a examinat „materiale confidențiale”¹¹, dar Curtea nu a făcut acest lucru, și nici nu a putut. Curții i-au lipsit în mod evident materialele detaliate necesare pentru a efectua o analiză structurală completă și o evaluare a interceptării în masă în Regatul Unit. Este dezamăgitor faptul că punctul de sensibilitate maximă a obiectului prezentei hotărâri, evidențiat în mod repetat de Curte, nu a avut decât scopul de a insista asupra necesității „eficienței”¹² și „flexibilității”¹³ sistemului de interceptare în masă, dar nu și de a colecta toate probele relevante necesare pentru pronunțarea unei hotărâri solide faptic a Curții. Această limitare autoimpusă asupra competenței Curții de a colecta probe demonstrează că judecătorii de la Strasbourg nu consideră Curtea drept o veritabilă instanță judecătorească, cu competența de a solicita părților să îi acorde acces nelimitat și necondiționat la probele relevante pentru obiectul cauzei. În consecință, Curtea a făcut unele „presupuneri educate” cu privire la gradul probabil de ingerință în drepturile unei persoane, în diferite etape ale procesului de interceptare. Problema elaborării unor standarde de reglementare pe baza unor astfel de „presupuneri educate” este aceea că reflectă ipotezele și prejudecățile autorității de reglementare. Și acestea sunt clare în prezenta cauză. Argumentația Guvernului se rezumă la o simplă propoziție, „credeți-ne!”. Majoritatea a fost pregătită să accepte această propoziție, cu riscul de a alege să se afle de partea colectării excesive de informații. Noi nu suntem. Astfel cum a afirmat Comitetul de evaluare prezidențială al Statelor Unite ale Americii, „americanii nu trebuie să comită greșeala să aibă încredere în oficialități”¹⁴. Am spune că același lucru este valabil pentru europeni.

5. În al doilea rând, limitarea autoimpusă probatorie și jurisdicțională susmenționată determină Curtea să își asume caracterul inevitabil al interceptării în masă și, cu atât mai mult, al unui regim de interceptare generalizat, neîntit, în lipsa unei bănueli, astfel cum susțin statul pârât și părțile terțe atât în prezenta cauză, cât și în *Centrum för rättvisa împotriva Suediei*¹⁵. Prin intermediul unui raționament circular, Guvernul a afirmat că interceptarea în masă este incompatibilă cu cerința unei bănueli întemeiate, deoarece este, prin definiție, neîntită, și este neîntită deoarece nu necesită existența unei

¹¹ Pct. 424 din prezenta hotărâre.

¹² Pct. 353 din prezenta hotărâre.

¹³ Pct. 354 din prezenta hotărâre.

¹⁴ „Liberty and Security in a Changing World” („Libertate și securitate într-o lume în schimbare”), raport și recomandări ale Grupului prezidențial de evaluare a informațiilor și tehnologiilor comunicațiilor, 12 decembrie 2013, pag. 114.

¹⁵ *Centrum för rättvisa împotriva Suediei* (nr. 35252/08), pronunțată în aceeași zi cu prezenta hotărâre. Este de remarcat că guvernele Franței, Țărilor de Jos și Norvegiei s-au concentrat exact asupra acestui aspect: în opinia lor, nu există nici o justificare pentru adăugarea unei bănueli întemeiate la interceptarea în masă (pct. 301, 305 și 309 din prezenta hotărâre).

bănuieli întemeiate¹⁶. Curtea a urmat această pistă și a formulat-o în termeni axiomatici:

„cerința existenței unei «bănuieli întemeiate», care poate fi regăsită în jurisprudența Curții privind interceptarea ținută în contextul cercetărilor penale, este mai puțin relevantă în contextul interceptării în masă, al cărei scop este în principiu unul mai degrabă preventiv decât unul de a investiga o anumită ținută și/sau o infracțiune identificabilă”¹⁷.

Din această nouă paradigmă rezultă că Curtea s-a îndepărtat de la jurisprudența constantă potrivit căreia „nu consideră că există motive pentru a aplica principii diferite privind accesibilitatea și claritatea normelor care reglementează interceptarea comunicațiilor individuale, pe de o parte, și programele de supraveghere mai generale, pe de altă parte”¹⁸. Atât sistemul german, cât și cel britanic de interceptare în masă au fost deja evaluate de Curte exact în temeiul aceluiași criterii aplicabile interceptării ținute: facem trimitere la supravegherea strategică generalizată în temeiul Legii G10 Act în *Weber și Saravia împotriva Germaniei*¹⁹, precum și la colectarea nediscriminatorie a telecomunicațiilor trimise din sau primite în afara Insulelor Britanice în temeiul Legii privind interceptarea comunicațiilor în *Liberty și alții împotriva Regatului Unit*²⁰ și la interceptarea unor cantități mari de comunicații interne în temeiul Legii din 2000 privind competențele de investigare în *Kennedy împotriva Regatului Unit*²¹. Curtea s-a îndepărtat fără un motiv întemeiat de la fundamentele acestei jurisprudențe, astfel cum vom demonstra în continuare.

6. În plus, Curtea nu a acordat greutatea cuvenită faptului că a reformulat și a aplicat efectiv jurisprudența anterioară în trei cauze recente, al căror obiect includea, în una în mod tangențial și în celelalte două în mod specific, interceptarea neținută a comunicațiilor. Facem trimitere la *Roman Zakharov împotriva Rusiei*²², *Szábo și Vissy împotriva Ungariei*²³ și *Mustafa Sezgin Tanrıkulu împotriva Turciei*²⁴. Este semnificativ faptul că *Roman Zakharov*

¹⁶ A se vedea observațiile orale prezentate de guvernul pârât în fața Marii Camere la 10 iulie 2019: „Acestea [bănuiala întemeiată și notificarea ulterioară] sunt fundamental incompatibile cu funcționarea unui regim care nu depinde de existența unor ținte de supraveghere clar definite. Regimul prevăzut la art. 8 alin. (4) este, prin natura sa, un regim neținut. El există pentru a descoperi amenințări necunoscute la adresa securității naționale și infracțiuni grave. Astfel, o bănuială întemeiată pur și simplu nu poate face parte din regim. O astfel de cerință i-ar denatura utilitatea [...]”. În cele din urmă, argumentul se rezumă la „utilitatea” interceptării în masă masive în lipsa unei bănuieli.

¹⁷ Pct. 348 din prezenta hotărâre.

¹⁸ *Liberty și alții împotriva Regatului Unit*, nr. 58243/00, pct. 63, 1 iulie 2008.

¹⁹ *Weber și Saravia împotriva Germaniei* (dec.), nr. 54934/00, pct. 95 și 114, CEDO 2006-XI.

²⁰ *Liberty și alții*, citată anterior, pct. 63-65.

²¹ *Kennedy împotriva Regatului Unit*, nr. 26839/05, pct. 60, 18 mai 2010.

²² *Roman Zakharov împotriva Rusiei* (MC), nr. 47143/06, pct. 231 și 264, CEDO 2015.

²³ *Szábo și Vissy*, citată anterior.

²⁴ *Mustafa Sezgin Tanrıkulu împotriva Turciei*, nr. 27473/06, 18 iulie 2017.

împotriva Rusiei²⁵ a folosit, de asemenea, criteriile *Weber și Saravia* atunci când a evaluat măsurile operative de investigații, inclusiv ingerințele în comunicațiile poștale, telegrafice și de altă natură, care ar putea afecta „orice persoană care utilizează aceste servicii de telefonie mobilă”²⁶, în scopuri legate de securitatea națională, militară, economică sau ecologică²⁷. În această cauză, Marea Cameră a mers până la a critica practica „autorizațiilor de interceptare care nu menționează o anumită persoană sau un anumit număr de telefon, dar care autorizează interceptarea tuturor comunicațiilor telefonice în zona în care a fost săvârșită o infracțiune”²⁸. În *Szábo și Vissy împotriva Ungariei*²⁹ Curtea a fost și mai explicită în cenzurarea „supravegherii nelimitate a unui număr mare de cetățeni”³⁰, în scopul combaterii terorismului și al salvării cetățenilor maghiari aflați în dificultate în străinătate³¹. Deși a admis necesitatea unei interceptări în masă pentru a contracara amenințările interne și externe, Curtea a cerut existența unei „bănuieli individuale”³² pentru fiecare măsură de supraveghere, în lumina criteriilor *Weber și Saravia*³³. În cauza ulterioară *Mustafa Sezgin Tanrıkulu împotriva Turciei*³⁴, Curtea a reproșat instanței interne decizia de a admite interceptarea telefonului și comunicațiilor electronice ale oricărei persoane din Turcia pentru a preveni actele criminale ale organizațiilor teroriste, după ce a reamintit și confirmat jurisprudența *Weber și Saravia*, *Roman Zakharov* și *Szábo și Vissy*.

7. Pe lângă afirmația potrivit căreia „ambele cauze [*Liberty și alții* și *Weber și Saravia*] au în prezent o vechime de peste zece ani” și că activitatea de supraveghere avută în vedere în respectivele cauze era „mult mai restrânsă”³⁵, Curtea a oferit trei motive pentru a renunța la jurisprudența anterioară³⁶, toate inexacte faptic.

8. Primul argument este acela că „scopul declarat” al interceptării în masă este „în multe cazuri” cel de a monitoriza comunicațiile persoanelor în afara jurisdicției teritoriale a statului „care nu pot fi monitorizate prin alte forme de supraveghere”³⁷. Curtea nu a oferit, și nu ar putea oferi nicio dovadă că „în multe cazuri” interceptarea în masă era limitată, din punctul de vedere al

²⁵ *Roman Zakharov*, citată anterior, pct. 231 și 264.

²⁶ *Ibidem*, pct. 175-178.

²⁷ *Ibidem*, pct. 31, 246-248.

²⁸ *Ibidem*, pct. 265. Cazurile de autorizare a „supravegherii zonei” au implicat în mod clar o potențială supraveghere în masă.

²⁹ *Szábo și Vissy*, citată anterior.

³⁰ *Ibidem*, pct. 67.

³¹ *Ibidem*, pct. 63.

³² *Ibidem*, pct. 71.

³³ *Ibidem*, pct. 56.

³⁴ *Mustafa Sezgin Tanrıkulu*, citată anterior, pct. 56 și 57.

³⁵ Pct. 341 din prezenta hotărâre. Această afirmație trece cu vederea cauza *Roman Zakharov* și *Szábo și Vissy*, deja menționate.

³⁶ Pct. 344-346 din prezenta hotărâre.

³⁷ Pct. 344 din prezenta hotărâre.

„scopului declarat”, cu atât mai puțin al practicii reale, la persoane din afara jurisdicției teritoriale a statului. Dimpotrivă, toate documentele oficiale disponibile privind interceptarea în masă, pe care Curtea a ales să le ignore, relatează o poveste diferită. Este de neînțeles faptul că, având în vedere lipsa de probe din partea guvernului pârât, Curtea a închis ochii la evaluările factice ale Consiliului Europei și ale Uniunii Europene, disponibile public într-o multitudine de documente oficiale privind interceptarea în masă, publicate după ce scandalul Snowden a izbucnit, cum ar fi, de exemplu, rezoluțiile 1954 (2013) și 2045 (2015) ale Adunării Parlamentare a Consiliului Europei (APCE), și Recomandarea 2067 (2015), Declarația Comitetului de Miniștri din 11 iunie 2013 și răspunsul acestuia la Recomandarea 2067 (2015) a APCE, Recomandarea de politică generală nr. 11 a Comisiei Europene împotriva rasismului, comentariile Comisarului pentru drepturile omului din 24 octombrie 2013, documentele sale tematice din 8 decembrie 2014 și din mai 2015, Raportul acestuia privind deficiențele înregistrate în supravegherea serviciilor germane de informații și securitate din 1 octombrie 2015, rezoluțiile Parlamentului European din 12 martie 2014 și din 29 octombrie 2015, avizul Autorității Europene pentru Protecția Datelor din 20 februarie 2014 și avizul 4/2014 al Grupului de lucru „Articolul 29”. De asemenea, a ignorat Rezoluția 68/167 a Adunării Generale a Organizației Națiunilor Unite din 18 decembrie 2013, observațiile finale ale Comitetului pentru Drepturile Omului (CDO) al Organizației Națiunilor Unite cu privire la cel de-al patrulea raport al Statelor Unite ale Americii din 26 martie 2014, precum și declarația comună a Raportorului special al Organizației Națiunilor Unite și a Raportorului special al Comisiei Interamericane pentru Drepturile Omului pentru libertatea de exprimare din 21 iunie 2013³⁸. Cel mai surprinzător, majoritatea nici măcar nu a luat în considerare documentele oficiale internaționale disponibile privind regimul britanic de interceptare în masă, cum ar fi observațiile finale cu privire la cel de-al șaptelea raport al Regatului Unit din 17 august 2015 ale Comitetului pentru Drepturile Omului³⁹, și Memorandumul Comisarului pentru drepturile omului al Consiliului Europei privind mecanismele de supraveghere și control din Regatul Unit din mai 2016⁴⁰.

9. Toate aceste documente, precum și recente hotărâri ale Curții *Szábo și Vissy*⁴¹ și *Mustafa Sezgin Tanrıkulu împotriva Turciei*⁴² și jurisprudența relevantă a Curții de Justiție a Uniunii Europene (CJUE)⁴³, contrazic pretinsa

³⁸ Pentru o analiză detaliată a acestor documente, a se vedea opinia noastră în *Szábo și Vissy împotriva Ungariei*, citată anterior.

³⁹ UN doc. CCPR/C/GBR/CO/7.

⁴⁰ CommDH (2016)20.

⁴¹ *Szábo și Vissy*, citată anterior, pct. 66: „este posibil ca practic orice persoană din Ungaria poate face obiectul unei supravegheri secrete”.

⁴² *Mustafa Sezgin Tanrıkulu*, citată anterior, pct. 7.

⁴³ Pct. 209-241 din prezenta hotărâre. Facem aici trimitere la cauzele *Digital Rights Ireland Ltd* (referitoare la Directiva 2006/24/CE privind păstrarea datelor, care „implică o ingerință

prevalență a monitorizării persoanelor în afara jurisdicției teritoriale a statului. Dimpotrivă, aceste surse de încredere confirmă faptul că supravegherea în masă viza în principal persoanele aflate sub competența teritorială a statului⁴⁴. Guvernul însuși a admis că numărul de cereri de interceptări privind datele de comunicații aferente în temeiul art. 8 alin. (4) din RIPA în ceea ce privește persoanele despre care se știe că se află în Regatul Unit – prin urmare, ca instrument de supraveghere internă – este de până la câteva mii pe săptămână⁴⁵.

10. Al doilea argument care se îndepărtează de la jurisprudența anterioară este acela că statele membre ale Consiliului Europei „par să utilizeze”⁴⁶ interceptarea în masă în alte scopuri decât investigarea infracțiunilor. Linia argumentativă a Curții pare să fie următoarea: întrucât interceptarea ținută este „în cea mai mare parte”⁴⁷ utilizată în interceptarea în masă în scopul depistării și investigării infracțiunilor, însă interceptarea în masă poate fi utilizată și în scopul colectării de informații externe, în cazul în care nu poate exista nici o țință specifică, nicio infracțiune identificabilă, interceptarea în masă nu este (și nu ar trebui) reglementată de aceleași standarde de supraveghere vizată⁴⁸. Acesta este un alt argument care nu este dovedit de Curte, care a ales să decidă mai degrabă pe baza aparențelor decât a faptelor.

11. În realitate, interceptarea în masă neținută este interzisă explicit sau implicit în douăzeci și trei de state europene⁴⁹. Astfel cum au⁵⁰ demonstrat cu

în drepturile fundamentale ale aproape întregii populații europene”), *Maximilian Schrems* (care critica o legislație care permitea autorităților publice să aibă acces „în mod generalizat la conținutul comunicațiilor electronice”), *Privacy International* (care privea o legislație națională care impunea serviciilor de comunicații electronice să divulge datele de trafic și de localizare agențiilor de informații prin intermediul unei transmisii generale și nediferențiate care afecta „toate persoanele care utilizează serviciile de comunicații electronice”) și *La Quadrature du Net și alții* (care cenzurează o legislație care impune furnizorilor de servicii să păstreze „în mod general și nediferențiat” datele privind traficul și localizarea). Primele două cauze priveau prelucrarea datelor cu caracter personal în scopul aplicării legii, iar ultimele două cauze evaluau supravegherii secrete efectuate de serviciile de informații.

⁴⁴ A se vedea mai jos discuția completă privind imposibilitatea ca distincția bazată pe jurisdicția teritorială dintre comunicațiile interne și cele externe să justifice interceptarea în masă a acestora din urmă.

⁴⁵ A se vedea observațiile guvernului pârât în fața Marii Camere din 2 mai 2019, pct. 42 („câteva mii în cursul unei săptămâni dată în legătură cu persoane cunoscute sau despre care se crede că se află doar în Regatul Unit”).

⁴⁶ Pct. 345 din prezenta hotărâre.

⁴⁷ *Ibidem*.

⁴⁸ Trebuie arătat că guvernele Franței și al Țărilor de Jos au insistat, în mod similar Camerei, că presupunerea că interceptarea în masă constituie o intruziune mai mare în viața privată decât interceptarea ținută (pct. 300 și 306 din prezenta hotărâre) este greșită.

⁴⁹ Astfel cum a concluzionat raportul de cercetare al Curții cu privire la Albania, Andorra, Austria, Belgia, Bosnia și Herțegovina, Croația, Republica Cehă, Grecia, Irlanda, Islanda, Italia, Liechtenstein, Macedonia de Nord, Moldova, Monaco, Muntenegru, Polonia, Portugalia, România, San Marino, Serbia, Turcia și Ucraina. Prin urmare, pct. 242-246 din hotărâre nu prezintă o imagine corectă a peisajului european.

⁵⁰ Rezoluția APCE 2031 (2015).

fermitate APCE și Comisarul pentru drepturile omului al Consiliului Europei⁵¹, supravegherea nediferențiată a comunicațiilor în masă s-a dovedit inefficientă în prevenirea terorismului și, prin urmare, nu este doar periculoasă pentru protecția drepturilor omului, ci și o risipă de resurse. Astfel, dacă există un consens în Europa cu privire la interceptarea în masă neîntințită, consensul este că ar trebui interzisă, dar acest fapt a fost ignorat de Curte. Doar șapte state membre ale Consiliului Europei aplică astfel de regimuri⁵², și o fac în principal pentru prevenirea, depistarea și investigarea unor infracțiuni precum terorismul, spionajul, atacurile cibernetice și, mai vag, „infracțiuni grave”⁵³, astfel cum reiese din documentele oficiale menționate mai sus ale Consiliului Europei și Uniunii Europene, din hotărârile Curții *Szábo și Vissy* și *Mustafa Sezgin Tanrikulu* și din jurisprudența relevantă a CJUE. Colectarea de informații externe este doar unul dintre celelalte scopuri, iar Curtea nu dispune de minimul de probe statistice sau de alt gen privind modul în care este urmărit acest scop, fie că se bazează pe monitorizarea unor obiective specifice, fie în alt mod. Chiar presupunând, de dragul discuției, că colectarea de informații externe este realizată în principal prin interceptare în masă neîntințită, acest lucru nu implică neapărat faptul că toate interceptările în masă, inclusiv interceptările în masă cu scopuri legate de depistarea și investigarea infracțiunilor, ar trebui să nu fie ținute. În caz contrar, ceea ce se întâmplă este că interceptarea în masă devine o porțiță de scăpare pentru a eluda protecția unui mandat individual în împrejurări în care un astfel de mandat ar fi perfect adecvat pentru colectarea comunicațiilor în cauză. Acestea fiind spuse, nimic nu exclude posibilitatea ca colectarea de informații externe să poată fi realizată prin intermediul unei interceptări în masă pe baza unei bănuieli întemeiate privind implicarea persoanei vizate sau a unui grup de persoane implicate în activități dăunătoare securității naționale, chiar dacă acestea nu sunt fapte penale⁵⁴.

12. Cel de-al treilea argument se referă exact la această linie delicată între interceptarea ținută de modă veche și noile forme de interceptare în masă utilizate pentru a viza anumite persoane, iar acesta este argumentul cel mai slab al Curții. În cazul interceptării prin intermediul unor selectori puternici,

⁵¹ Memorandumul Comisarului pentru drepturile omului al Consiliului Europei privind mecanismele de supraveghere și control în Regatul Unit, CommDH (2016)20, mai 2016, pct. 10.

⁵² Pct. 242 din prezenta hotărâre.

⁵³ Pct. 345 din prezenta hotărâre. Facem aici trimitere la critica formulată de CJUE cu privire la acest concept de „infracțiune gravă” (pct. 212 din prezenta hotărâre).

⁵⁴ A se vedea raportul Comisiei de la Veneția privind supravegherea democratică a activităților de colectare de informații pe baza semnalelor electromagnetice, 2015, pct. 9, 25 și 26 („trebuie să existe date concrete care să indice comportamentul infracțional/care pune în pericol securitatea, iar investigatorii trebuie să aibă „cauza probabilă”, „o bănuială întemeiată” sau să îndeplinească un criteriu similar”) și memorandumul Comisarului pentru drepturile omului al Consiliului Europei, citat anterior, pct. 6.

Curtea susține că „dispozitivele persoanelor vizate nu sunt monitorizate”⁵⁵ și, prin urmare, interceptarea în masă nu necesită aceleași garanții ca interceptarea ținută clasică. Acest argument nu este convingător. Colectarea și prelucrarea automată prin intermediul unor selectori puternici care permit colectarea de comunicații electronice către, dinspre sau către țintă prin canalele de transmisie alese de serviciile de informații reprezintă o formă potențial mult mai intruzivă de ingerință în drepturile prevăzute la art. 8 decât simpla monitorizare a dispozitivelor persoanelor vizate⁵⁶. Prin urmare, este înșelător să se afirme că „doar” (pct. 346) pachetele de comunicații ale persoanelor vizate vor fi interceptate, lăsând impresia că interceptarea în masă bazată pe selectori puternici este mai puțin intruzivă decât monitorizarea de modă veche a dispozitivelor unei persoane.

C. Un regim al garanțiilor deficient

13. Din acest raționament practic nefondat, Curtea a tras două concluzii juridice pentru „abordarea care trebuie urmată în cauzele care privesc interceptarea în masă”⁵⁷: dreptul intern nu trebuie să identifice natura infracțiunilor care pot da naștere unui mandat de interceptare și categoriile de persoane ale căror comunicări pot fi interceptate, și nu este necesară o bănuială întemeiată pentru a justifica un astfel de mandat de interceptare⁵⁸. Potrivit logicii Curții, întrucât „scopul [interceptării în masă] este în principiu mai degrabă unul preventiv, și nu unul de a investiga o anumită țintă și/sau o infracțiune identificabilă”⁵⁹, niciuna dintre cele două garanții de mai sus nu este impusă de dreptul intern, chiar dacă interceptarea în masă vizează o anumită persoană implicată într-o infracțiune identificabilă. Astfel, un mandat de interceptare general, în lipsa unei bănuieli întemeiate, este suficient pentru a declanșa interceptarea în masă, fie doar în scopul detectării și investigării infracțiunilor, fie în alte scopuri.

14. Poziția Curții lasă numeroase întrebări fără răspuns. Care sunt motivele admisibile pentru interceptarea în masă? De exemplu, este investigarea „infracțiunilor grave”, fără nicio altă precizare, un motiv admisibil? Cât de gravă ar trebui să fie infracțiunea investigată? Investigarea furtului unui portofel și a unui telefon mobil reprezintă un motiv admisibil?⁶⁰ Promovarea spionajului economic și industrial în interesul bunăstării economice și al securității naționale a statului care face interceptarea reprezintă un motiv

⁵⁵ Pct. 346 din prezenta hotărâre.

⁵⁶ Astfel cum a explicat CJUE în hotărârea *Digital Rights Ireland*, citată anterior, pct. 55: „necesitatea de [...] garanții este cu atât mai importantă în cazul în care [...] datele cu caracter personal sunt supuse unei prelucrări automate”.

⁵⁷ Lit. c) (iii) din motivarea Curții.

⁵⁸ Pct. 348 din prezenta hotărâre.

⁵⁹ *Ibidem*.

⁶⁰ Exemplul derivă din jurisprudența CJUE (pct. 220 din prezenta hotărâre).

admisibil?⁶¹ Care sunt „circumstanțele” admisibile în care comunicațiile unei persoane pot fi interceptate? Pentru a justifica interceptarea în masă a comunicațiilor unei persoane, care este gradul necesar de interes privind comunicațiile persoanei pentru scopurile urmărite de mandat de interceptare în masă? Este vorba despre standardul individual de bănuială menționat de *Szabo și Vissy*⁶² sau despre criteriul existenței unei bănuieli întemeiate impus de *Roman Zakharov*⁶³? Cum poate solicita Curtea ca dreptul intern să stabilească „cu suficientă claritate”⁶⁴ motivele pentru care poate fi autorizată interceptarea în masă și circumstanțele în care comunicațiile unei persoane pot fi interceptate atunci când Curtea însăși nu este suficient de clară în ceea ce privește la ce tip de „motive” și „circumstanțe” se referă?

15. Întrucât art. 8 se aplică tuturor etapelor interceptării în masă, inclusiv păstrării inițiale a comunicațiilor și a datelor de comunicații aferente⁶⁵, Curtea a stabilit în mod corect „garanții de la un capăt la altul”⁶⁶. Problema este că Curtea nu este clară în ceea ce privește natura juridică a „garanțiilor de la un capăt la altul”. Pe de o parte, a utilizat un limbaj imperativ („trebuie făcută”⁶⁷, „trebuie să facă obiectul”⁶⁸, „trebuie să fie autorizată”⁶⁹, „trebuie să fie informat”⁷⁰, „trebuie să fie justificată”⁷¹, și „trebuie să fie înregistrată cu scrupulozitate”⁷², „trebuie, de asemenea, să facă obiectul”⁷³, „este imperativ ca recursul să”⁷⁴) și le-a denumit „garanții fundamentale”⁷⁵ și chiar „garanții minime”⁷⁶. Dar, pe de altă parte, a diluat aceste garanții într-o „evaluare globală a funcționării regimului”⁷⁷, permițând un compromis între garanții⁷⁸. Se pare că, la sfârșitul zilei, fiecare garanție individuală nu este obligatorie, iar limbajul prescriptiv al Curții nu corespunde cu adevărat caracteristicilor nenegociabile ale sistemului intern. În unele colțuri ale Europei, serviciile

⁶¹ Exemplul derivă din critica aspră adresată de Rezoluția Parlamentului European din 12 martie 2014 referitoare la programul de supraveghere al Agenției Naționale de Securitate a Statelor Unite ale Americii, raportul Comisiei de la Veneția, citat anterior, pct. 18, și din memorandumul Comisarului pentru drepturile omului al Consiliului Europei, citat anterior, pct. 8.

⁶² *Szabo și Vissy*, citată anterior, pct. 71.

⁶³ *Roman Zakharov*, citată anterior, pct. 260, 262 și 263.

⁶⁴ Pct. 348 din prezenta hotărâre.

⁶⁵ Pct. 330 din prezenta hotărâre.

⁶⁶ Pct. 350 din prezenta hotărâre.

⁶⁷ *Ibidem*.

⁶⁸ *Ibidem*.

⁶⁹ Pct. 351 din prezenta hotărâre.

⁷⁰ Pct. 352 din prezenta hotărâre.

⁷¹ Pct. 355 din prezenta hotărâre.

⁷² *Ibidem*.

⁷³ Pct. 356 din prezenta hotărâre.

⁷⁴ Pct. 359 din prezenta hotărâre.

⁷⁵ Pct. 350 din prezenta hotărâre.

⁷⁶ Pct. 348 din prezenta hotărâre.

⁷⁷ Pct. 360 din prezenta hotărâre.

⁷⁸ A se vedea, de exemplu, pct. 370, *in fine*, din prezenta hotărâre.

secrete zeloase vor fi puternic tentate să profite de modul foarte permisiv al Curții de a formula norme juridice, iar persoanele nevinovate vor plăti prețul, mai devreme sau mai târziu.

D. Concluzie preliminară

16. Potrivit Curții, o autoritate independentă⁷⁹, adică independentă de executiv, este necesară de la bun început pentru a evalua scopul interceptării, selecția canalelor de transmisie⁸⁰ și categoriile de selectori⁸¹, în raport cu principiile necesității și proporționalității. Alegerea unor selectori puternici legați de persoane identificabile este deosebit de problematică, întrucât selecția și „utilizarea fiecărui selector atât de puternic”⁸² nu necesită o autorizare independentă prealabilă. În opinia Curții, autorizarea internă este suficientă în acest caz, alături de garanțiile că solicitarea unui selector puternic este justificată și că procesul intern este înregistrat „cu scrupulozitate”⁸³.

17. În plus, executarea mandatului de interceptare, inclusiv reînnoirile sale ulterioare, utilizarea, stocarea, transmiterea ulterioară și ștergerea datelor obținute ar trebui să fie supravegheate de o autoritate independentă de executiv, cu păstrarea unor evidențe detaliate în fiecare etapă a procesului, pentru a facilita această supraveghere⁸⁴.

18. În cele din urmă, controlul *a posteriori* al întregului proces ar trebui să fie efectuat de o autoritate independentă de executiv, în cadrul unei proceduri echitabile și contradictorii, cu competența de a emite decizii obligatorii dispunând încetarea interceptării ilegale și distrugerea datelor obținute sau stocate în mod ilegal, precum și a datelor învechite, echivoce sau disproporționate⁸⁵.

⁷⁹ Deși limbajul Curții nu este uniform, făcând trimitere uneori la noțiunea de autoritate independentă și în alte momente la cea de organ independent, se pare că nu există nicio diferență substanțială între aceste concepte.

⁸⁰ Pct. 352 din prezenta hotărâre.

⁸¹ Pct. 354 din prezenta hotărâre.

⁸² Pct. 355 din prezenta hotărâre.

⁸³ *Ibidem*. Astfel cum indică raportului Comisiei de la Veneția, citat anterior, pct. 28, „controalele interne sunt insuficiente”. Astfel, pct. 199 din hotărâre denaturează poziția Comisiei de la Veneția.

⁸⁴ Pct. 356 din prezenta hotărâre.

⁸⁵ Pct. 359 din prezenta hotărâre.

III. CONSTRUCȚIA REGIMULUI DE INTERCEPTARE ÎN MASĂ *PRO PERSONA*

A. Interceptarea în masă a comunicațiilor

19. Considerăm că regimul sus-menționat nu prezintă un set de garanții suficient pentru drepturile prevăzute la art. 8 și 10. În opinia noastră, a sosit momentul să nu se renunțe la garanțiile fundamentale ale autorizării judiciare, ale supravegherii și ale controlului *a posteriori* în domeniul interceptării în masă⁸⁶. În principiu, controlul judiciar de la un capăt la altul a interceptării în masă este justificat de caracterul extrem de intruziv al acestui proces. Nu înțelegem motivul pentru care un stat de drept nu ar trebui să aibă încredere în judecătorii săi în exercițiu, în cele din urmă cei cu cea mai mare vechime și mai experimentați, pentru a se pronunța cu privire la astfel de probleme. Cu excepția cazului în care Curtea consideră că organele cvasi-judiciare sunt mai independente decât instanțele ordinare [...] În opinia noastră, independența organelor cvasi-judiciare nu reprezintă un dat. În plus, în cazul în care instanțele ordinare sunt competente să autorizeze, să supravegheze și să evalueze interceptarea comunicațiilor în cadrul unor proceduri penale extrem de complexe, cum ar fi investigațiile privind criminalitatea organizată și terorismul, nu înțelegem motivul pentru care nu ar trebui să fie competente să îndeplinească exact aceeași funcție în ceea ce privește funcționarea unui proces de interceptare în masă. Prin urmare, nici independența, nici competența instanțelor ordinare nu ar trebui să fie puse sub semnul întrebării pentru a construi o arhitectură de garanții conforme cu Convenția în cadrul unui regim de interceptare în masă. Un stat care consideră că judecătorii în activitate nu sunt apti să îndeplinească aceste funcții are o problemă gravă cu statul de drept.

20. Pentru a fi clar, intervenția judiciară nu ar trebui să fie un panaceu⁸⁷. Este evident că un control judiciar al întregului proces ar fi lipsit de sens dacă categoriile de infracțiuni și de activități și subiectele interceptării monitorizate nu ar fi prevăzute în dreptul intern cu gradul necesar de claritate și de precizie. În consecință, controlul judiciar trebuie să includă alegerea unor canale de transmisie specifice și a unor selectori puternici. Prin specifice ne referim la canale de transmisie individuale și la selectori puternici, nu la

⁸⁶ Raportul Comisiei de la Veneția, citat anterior, pct. 32 („Pentru statele europene, este de preferat aprobarea judiciară *ex ante* în cazuri individuale”). Pct. 197 din hotărâre denaturează astfel mesajul Comisiei de la Veneția. Comisarul pentru drepturile omului al Consiliului Europei a propus, de asemenea, adoptarea unei autorizări judiciare *ex ante* (Memorandum, citat anterior, pct. 28).

⁸⁷ Faptul că autorizarea judiciară ar putea să nu constituie în sine o protecție suficientă împotriva abuzurilor nu susține concluzia că nu este necesară. Trebuie remarcat faptul că IPA a introdus o autorizare judiciară *ex ante*, dar nu este aici locul să discutăm *ex professo* standardul de control jurisdicțional introdus de IPA, deoarece legea din 2016 nu se află în discuție în fața Curții.

„tipuri” sau „categorii” de canale de transmisie sau selectori, care ar fi un cec în alb prin care autoritatea de interceptare ar putea alege ce-și dorește.

21. În cazul unui sistem cu dublă blocare, în care judecătorul ia în considerare mandate emise anterior de o persoană responsabilă politic sau de un funcționar administrativ, controlul judiciar nu trebuie să se limiteze la posibilitatea de a anula decizia administrativă atunci când judecătorul consideră că persoana responsabilă politic sau funcționarul administrativ a acționat în mod nerezonabil. Aceasta nu ar fi o autorizare cu adevărat judiciară, întrucât criteriile de necesitate și proporționalitate impuse de Convenție sunt mai exigente decât simpla verificare a caracterului rezonabil.

22. Astfel cum am menționat în *Szábo și Vissy*, Convenția nu permite cercetări pentru „căutare de date” sau „exploratorii”, nici sub forma unei supravegheri neștintite bazate pe selectori nespecifici, nici sub forma unui control bazat pe selectori puternici care să vizeze comunicațiile legate de subiectul interceptării țintite⁸⁸. De asemenea, nu este admisibilă nici extinderea numărului de subiecți ai interceptării prin utilizarea unor termeni de căutare mai vagi. Reamintim motivul fundamental pentru care am ajuns la această concluzie. A admite interceptarea în masă neștintită implică o schimbare fundamentală în modul în care vedem prevenirea criminalității și investigarea și colectarea de informații în Europa, de la vizarea unui suspect care poate fi identificat la tratarea tuturor persoanelor ca suspecti potențiali, ale căror date trebuie stocate, analizate și profilate⁸⁹. Desigur, impactul unei astfel de schimbări asupra unei persoane nevinovate ar putea fi atenuat, în cele din urmă, de un grup de arbitri și autorități de reglementare mai mult sau mai puțin flexibile și de o multitudine de legi și coduri de bune practici mai mult sau mai puțin convenabile, dar o societate construită pe astfel de baze este mai apropiată de un stat polițienesc decât de o societate democratică. Aceasta ar fi opusul a ceea ce au dorit părinții fondatori pentru Europa atunci când au semnat Convenția, în 1950.

23. Prin urmare, orice țintă a unei supravegheri trebuie să fie întotdeauna identificată sau identificabilă în prealabil, pe baza unei bănueli întemeiate. Pentru a nu lăsa loc niciunei îndoieli, interceptarea în masă ar trebui să fie admisibilă numai pe baza unor selectori puternici care să vizeze comunicațiile de la și către subiectul interceptării țintite, atunci când există o bănuială întemeiată că persoana respectivă este implicată în categoriile definite de lege

⁸⁸ A se vedea toate lucrările reprezentative internaționale citate în opinia noastră anexată la *Szábo și Vissy*, citată anterior.

⁸⁹ Acesta este motivul pentru care considerăm că colectarea masivă de date ale persoanelor nevinovate acceptate de Curte în prezenta hotărâre contravine principiilor stabilite în *S și Marper împotriva Regatului Unit*, nr. 30562/04 și 30566/04, pct. 135, 4 decembrie 2008; *Shimovolos împotriva Rusiei*, nr. 30194/09, pct. 68 și 69, 21 iunie 2011; *M.K. împotriva Franței*, nr. 19522/09, pct. 37, 18 aprilie 2013; și, cel mai important, *Mustafa Sezgin Tanrıkulu împotriva Turciei*, citată anterior, pct. 57-59.

ca infracțiuni grave sau activități care aduc atingere securității naționale, fără a fi în mod necesar de natură penală⁹⁰.

24. Garanția judiciară trebuie extinsă la autorizarea supravegherii comunicațiilor sau a datelor aferente comunicațiilor, inclusiv a datelor privilegiate și confidențiale, cu singura excepție a cazurilor urgente, atunci când judecătorul competent nu este disponibil de îndată, caz în care autorizația poate fi emisă de un procuror, sub rezerva aprobării ulterioare de către judecătorul competent.

25. Dreptul intern trebuie să prevadă un regim specific de protecție a comunicațiilor profesionale privilegiate ale parlamentarilor, medicilor, avocaților și jurnaliștilor⁹¹. Întrucât o colectare în masă nediferențiată și fără suspiciuni a comunicațiilor ar aduce atingere protecției informațiilor confidențiale și protejate din punct de vedere legal, acest lucru poate fi garantat în mod efectiv numai prin intermediul unei autorizări judiciare de interceptare a unor astfel de comunicații, atunci când sunt prezentate probe care susțin o bănuială întemeiată de participare a acestor profesioniști la o infracțiune gravă sau la o activitate care aduce atingere securității naționale⁹². În plus, orice comunicații ale acestor categorii de profesioniști, care intră sub incidența secretului profesional, în cazul în care este interceptată din greșeală, trebuie să fie distrusă de îndată. Dreptul intern trebuie să prevadă, de asemenea, interzicerea absolută a oricărei interceptări de comunicații care intră sub incidența secretului religios.

26. Controlul judiciar nu trebuie să înceteze la debutul operațiunii de interceptare. În cazul în care funcționarea efectivă a sistemului de interceptare ar fi ascunsă de controlul judecătorului, intervenția inițială a acestuia ar putea fi compromisă cu ușurință și ar putea fi lipsită de orice efect real, transformând-o între garanție pur virtuală și înșelătoare. Dimpotrivă,

⁹⁰ Acesta este standardul universal, astfel cum a fost reprodus în Compilație a Organizației Națiunilor Unite de bune practici în materie de cadre și măsuri juridice și instituționale, inclusiv controlul acestora, care asigură respectarea drepturilor omului de către agențiile de informații în lupta împotriva terorismului, 17 mai 2010 (A/HRC/14/46): „Practica 21. Dreptul intern național precizează tipurile de măsuri de colectare puse la dispoziția serviciilor de informații, obiectivele de colectare a informațiilor admise, categoriile de persoane și activitățile care pot face obiectul colectării de informații, pragul de suspiciune necesar pentru a justifica utilizarea măsurilor de colectare a informațiilor, limitele aduse duratei în care pot fi utilizate măsurile de colectare și procedurile de autorizare, supravegherea și evaluarea utilizării măsurilor de colectare a informațiilor.”

⁹¹ În plus față de *Sanoma Uitgevers B.V. împotriva Țărilor de Jos* (MC), nr. 38224/03, pct. 90-92, 14 septembrie 2010, a se vedea Agenția pentru Drepturi Fundamentale a Uniunii Europene (FRA), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*, vol. II: *Field perspectives and legal updates*, 2017, pag. 12: „Statele membre ale UE trebuie să instituie proceduri juridice specifice pentru a proteja privilegiile profesionale ale unor grupuri precum membrii Parlamentului, membrii sistemului judiciar, avocații și profesioniștii din domeniul mass-media. Punerea în aplicare a acestor proceduri trebuie supravegheată de un organ independent.”

⁹² Raportul Comisiei de la Veneția, citat anterior, pct. 26.

judecătorul trebuie să însoțească întregul proces cu o examinare periodică și vigilentă a necesității și proporționalității mandatului de interceptare, având în vedere datele interceptate obținute. Cu excepția cazului în care primește feedback constant din partea autorității de interceptare, judecătorul care emite autorizația nu va ști cum aceasta e utilizată în fapt. În cazul nerespectării mandatului de interceptare, judecătorul trebuie să poată dispune încetarea imediată a acestuia și distrugerea datelor obținute ilegal. Similar ar trebui să fie și cazul în care continuarea operațiunii nu mai este necesară, de exemplu ca urmare a faptului că datele obținute nu prezintă niciun interes pentru scopurile urmărite de mandatul de interceptare. Numai un judecător investit cu competența de a lua astfel de decizii cu caracter obligatoriu poate oferi o garanție efectivă a legalității materialului care este păstrat. În concluzie, judecătorul trebuie să fie împuternicit să efectueze o reexaminare periodică a funcționării sistemului, inclusiv a tuturor înregistrărilor interceptărilor și a documentelor aferente clasificate⁹³, pentru a evita ingerințele inutile și disproporționate în drepturile prevăzute la art. 8 și 10.

27. În cele din urmă, reexaminarea *ex post* a utilizării unui mandat de interceptare trebuie să fie declanșată și de notificarea persoanei vizate. În cazul în care nimic nu împiedică notificarea persoanei ale cărei comunicații au fost interceptate, acest fapt i-ar permite să conteste în cadrul unei proceduri judiciare echitabile și contradictorii motivele unei astfel de interceptări⁹⁴. Prin urmare, este extrem de speculativ, cel puțin, să se pretindă că un sistem care nu depinde de notificarea subiectului interceptării „poate chiar să ofere garanții mai bune pentru o procedură adecvată decât un sistem bazat pe notificare”⁹⁵. Nimeni nu este mai preocupat de interesele subiectului interceptării decât subiectul însuși.

28. În cazul în care, dintr-un anumit motiv, cum ar fi interesul securității naționale, nu este posibil să fie notificată persoana ale cărei comunicații au fost interceptate, nu există, în mod realist, nicio modalitate ca persoana să

⁹³ Acesta este standardul universal și european, astfel cum a fost reprodus în Compilația Organizației Națiunilor Unite, citată anterior („Practica 25. O instituție independentă există pentru a controla utilizarea datelor cu caracter personal de către serviciile de informații. Această instituție are acces la toate dosarele deținute de serviciile de informații și are competența de a dispune dezvăluirea informațiilor persoanelor vizate, precum și distrugerea dosarelor sau informațiilor personale conținute de acestea”) și FRA, *Surveillance by intelligence services*, citată anterior, pct. 11 („Statele membre trebuie, de asemenea, să acorde organelor de supraveghere competența de a iniția propriile investigații, precum și acces permanent, complet și direct la informațiile și documentele necesare pentru îndeplinirea mandatului acestora”).

⁹⁴ *Szábo și Vissy*, citată anterior, pct. 86: În logica *Szábo și Vissy*, aceasta este o cerință minimă suplimentară față de criteriile *Weber și Saravia*. În ceea ce privește avantajele procesului de notificare „pentru a limita utilizarea excesivă”, a se vedea raportul Comisiei de la Veneția, citat anterior, pct. 35, și rapoartele Comisarului pentru drepturile omului al Consiliului Europei cu privire la Germania, 2015, pct. 17, și cu privire la Regatul Unit, 2016, citate anterior, pct. 5.

⁹⁵ Pct. 358 din prezenta hotărâre.

aibă cunoștință despre măsura de supraveghere luată în privința sa. În acest caz, este imperativ să se impună judecătorului competent sarcina de a evalua, din proprie inițiativă (*ex proprio motu*) sau la inițiativa unui terț (de exemplu, un procuror), modul în care a fost executat mandatul de interceptare pentru a stabili dacă datele în cauză au fost colectate în mod legal și ar trebui păstrate sau distruse; subiectul interceptării trebuie apoi să fie reprezentat de un avocat specialist în protecția vieții private.

29. Nu în ultimul rând, resursele și capacitățile de supraveghere umană și financiară trebuie să corespundă amplitudinii operațiunilor care sunt supravegheate; în caz contrar, întregul sistem va fi o simplă fațadă care acoperă procesul administrativ discreționar al autorităților de interceptare.

B. Schimbul de date interceptate cu serviciile de informații străine

30. Curtea a stabilit un standard de protecție mai scăzut pentru transferul către serviciile de informații străine al datelor obținute prin interceptarea în masă. În primul rând, statul care transferă date nu are obligația de a verifica dacă statul destinatar beneficiază de un grad de protecție comparabil cu cel propriu. În plus, nu este necesar să solicite, înainte de fiecare transfer, o asigurare că statul destinatar, prin transmiterea datelor, va institui garanții capabile să prevină abuzurile și ingerințele disproporționate⁹⁶. Astfel, Curtea nu a exclus posibilitatea unui transfer masiv de date către un serviciu de informații străin în cadrul unui proces continuu bazat pe un singur scop. Având în vedere acest cadru foarte discreționar, nu este clar în ce constă „controlul independent” solicitat de Curte⁹⁷. Care este scopul controlului independent dacă nu este necesar să se evalueze garanțiile aplicate de statul destinatar (inclusiv în sensul că acesta va „garanta stocarea în siguranță a materialelor și va restricționa divulgarea ulterioară a acestora”⁹⁸) înainte de fiecare transfer? Controlul independent este limitat la cauzele în care „este clar că materialele care necesită confidențialitate specială – precum materialele jurnalistice confidențiale – sunt transferate”⁹⁹? Cui ar trebui să i se dea un răspuns clar, serviciului de informații care efectuează transferul sau judecătorului? Există vreo diferență între controlul independent și autorizarea independentă? Caracterul vag al formulării Curții pare să servească la reducerea intenționată a garanțiilor specifice legate de transferul în sine.

31. Nu vedem niciun motiv pentru această reducere a protecției prevăzute de Convenție în cazul partajării de date în masă, și nici Curtea nu oferă vreunul. În conformitate cu normele consolidate ale Consiliului Europei și ale Uniunii Europene, schimbul de date cu caracter personal ar trebui să se limiteze la țările terțe care oferă un nivel de protecție în esență echivalent cu

⁹⁶ Pct. 362 din prezenta hotărâre.

⁹⁷ *Ibidem*.

⁹⁸ *Ibidem*.

⁹⁹ *Ibidem*.

cel garantat în cadrul Consiliului Europei, respectiv al Uniunii Europene¹⁰⁰. În acest caz, controlul judiciar ar trebui să fie la fel de strict ca în orice alt caz. Acest control judiciar atent este justificat în special atunci când un stat membru al Consiliului Europei transferă date unui stat nemembru, pentru motivul evident că utilizarea viitoare a acestor date de către statul nemembru nu este de competența Curții. Un astfel de control judiciar nu ar trebui să fie limitat de „regula terțului”, potrivit căreia este interzis ca un serviciu de informații care a primit date de la un serviciu de informații străin să le comunice unui terț fără consimțământul emitentului¹⁰¹.

C. Interceptarea în masă a datelor de comunicații aferente

32. În sfârșit, Curtea a recunoscut potențialul extrem de intruziv al interceptării în masă a datelor de comunicații aferente¹⁰², dar nu le-a oferit acestora același grad de protecție în prezenta cauză¹⁰³. Pe de o parte, aceasta impune ca „garanțiile menționate anterior [să fie] adoptate”, făcând trimitere la cele prevăzute la pct. 361 din hotărâre, dar, pe de altă parte, recunoaște că statele membre dispun de libertatea de a selecta și de a alege garanțiile specifice care trebuie consacrate în dreptul intern, întrucât „dispozițiile juridice care reglementează [...] tratamentul [datelor de comunicații aferente] pot să nu fie neapărat identice sub orice aspect cu cele care reglementează

¹⁰⁰ Majoritatea ignoră faptul că art. 2 din Protocolul adițional la Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, referitor la autoritățile de control și fluxul transfrontalier al datelor (STE nr. 181), prevede că părțile trebuie să asigure un nivel adecvat de protecție a transferurilor de date cu caracter personal către țări terțe și că derogările sunt admise numai atunci când există interese legitime care prevalează. Raportul explicativ la această convenție adaugă că excepțiile trebuie interpretate în mod restrictiv, „astfel încât excepția să nu devină regulă” (pct. 31). Este important de remarcat faptul că acest protocol a fost ratificat de 44 de state, inclusiv de 8 state care nu sunt membre ale Consiliului Europei. Regatul Unit nu a ratificat-o. Pe lângă această normă a Consiliului Europei, Uniunea Europeană permite doar transferul de date cu caracter personal către o țară terță care oferă un nivel de protecție în esență echivalent cu cel garantat în cadrul Uniunii Europene (pct. 234 din prezenta hotărâre).

¹⁰¹ Raportul Comisiei Veneția, citat anterior, 2015, pct. 34 („Regula inițiatorului sau a «terțului» nu trebuie să se aplice organului de supraveghere”), precum și FRA, *Surveillance by intelligence services*, citată anterior, 2017, pct. 13 și 106 („Fără a aduce atingere regulii terțului, statele membre ale UE trebuie să ia în considerare posibilitatea de a acorda organelor de supraveghere acces deplin la datele transferate prin cooperare internațională. Acest fapt ar extinde competențele de supraveghere a tuturor datelor disponibile și prelucrate de serviciile de informații”).

¹⁰² Pct. 342 din prezenta hotărâre.

¹⁰³ În cele din urmă, Curtea s-a lăsat influențată de amenințarea Guvernului, potrivit căruia „în cazul în care statele membre care operează un regim de interceptare în masă ar fi obligate să aplice aceleași protecții în ceea ce privește conținutul [datelor de comunicații conexe], atunci rezultatul probabil ar fi pur și simplu o diluare a protecției conținutului.” (observațiile guvernului pârât în fața Marii Camere din 2 mai 2019, pct. 42).

tratamentul conținutului”¹⁰⁴. Mesajul neclar al Curții este atât de ambiguu încât nu oferă statelor orientări adecvate privind care dintre „garanțiile menționate anterior” sunt obligatorii, dacă există, pentru interceptarea în masă a datelor aferente comunicațiilor. În consecință, poziția ezitantă a Curții nu înlătură riscul, pe care Curtea însăși l-a identificat, ca aceste date să prezinte un proces detaliat al întregii vieți sociale a unei persoane.

D. Concluzie preliminară

33. Nu suntem de acord că „statele se bucură de o marjă largă de apreciere atunci când decid ce tip de regim de interceptare este necesar, în aceste scopuri [pentru a proteja securitatea națională și alte interese naționale esențiale împotriva amenințărilor externe grave], [dar] în ceea ce privește operarea unui astfel de sistem, marja de apreciere acordată acestora trebuie să fie mai restrânsă”¹⁰⁵. Dacă marjele puterii discreționare a statului sunt largi, chiar și cel mai strict control al acestora nu protejează suficient împotriva abuzurilor. Marja de apreciere trebuie să fie aceeași, atât pentru conceperea sistemului, cât și pentru operarea sa, iar această marjă este limitată, având în vedere caracterul profund intruziv al competențelor de supraveghere ale statului în cauză, riscul inherent ridicat de a abuza de aceste puteri și – a nu se uita – consensul european privind interzicerea interceptării în masă neîntinse. Acest risc este amplificat de unele guverne obsedate de securitate cu un apetit nelimitat pentru date, care au acum mijloacele tehnologice pentru a controla comunicațiile digitale la nivel mondial.

34. În concluzie, dreptul intern trebuie să fie suficient de clar în ceea ce privește termenii săi pentru a oferi persoanelor fizice și persoanelor juridice¹⁰⁶ indicații adecvate cu privire la condițiile obligatorii și procedurile pe mai multe niveluri potrivit cărora autoritățile sunt împuternicite să recurgă la interceptarea în masă; aceste condiții și proceduri includ următoarele¹⁰⁷:

a) Definirea motivelor care pot justifica adoptarea unui mandat de interceptare, cum ar fi: detectarea de activități care reprezintă o amenințare la adresa securității naționale sau prevenirea, detectarea sau investigarea infracțiunilor grave, caz în care infracțiunile care pot declanșa interceptarea trebuie să corespundă fie unei liste de infracțiuni grave

¹⁰⁴ Pct. 364 din prezenta hotărâre, coroborat cu pct. 361.

¹⁰⁵ Pct. 347 din prezenta hotărâre.

¹⁰⁶ În *Liberty și alții*, citată anterior, toate reclamantele erau ONG-uri care au susținut că dreptul lor la protecția corespondenței a fost încălcat. Aceste drepturi sunt, de asemenea, implicate în prezenta cauză.

¹⁰⁷ În acest scop, în afară de autoritățile sus-menționate la pct. 8, am luat, de asemenea, în considerare Compilația Organizației Națiunilor Unite, citată anterior, 2010, Raportul Comisiei de la Veneția, citat anterior, 2015, și Raportul FRA, citat anterior, 2017.

specifice, fie, în general, infracțiunilor pedepsite cu cel puțin patru ani de închisoare¹⁰⁸.

b) Definirea subiecților interceptării, cu alte cuvinte, a persoanelor sau a instituțiilor care pot face obiectul interceptării comunicațiilor, după cum urmează:

(i) interzicerea strictă a cercetărilor pentru „căutare de date sau exploratorii, pentru a descoperi „necunoscute necunoscute”, inclusiv orice formă de supraveghere neîntințită bazată pe selectori nespecfici;

(ii) interzicerea strictă a utilizării unor selectori puternici în comunicațiile despre subiectul interceptării țintite;

(iii) admisibilitatea unor selectori puternici care să vizeze comunicațiile de la și către subiectul interceptării țintite atunci când există o bănuială întemeiată că subiectul interceptării este implicat în infracțiunile sau activitățile menționate mai sus.

c) Un catalog al formelor de comunicații electronice care pot fi interceptate, cum ar fi telefon, telex, fax, e-mail, căutare Google, navigare pe internet, platforme de comunicare socială și stocare în cloud.

d) Respectarea principiului necesității, care impune ca:

(i) ingerința în drepturile subiecților interceptării trebuie să servească în mod adecvat scopurilor urmărite și să nu depășească ceea ce este necesar pentru atingerea obiectivelor respective;

(ii) interceptarea trebuie să fie justificată numai ca măsură de ultimă instanță, și anume atunci când nu sunt disponibile alte mijloace de obținere a probelor sau a informațiilor, întrucât recursul la alte metode mai puțin invazive s-a dovedit a fi nereușit sau, în mod excepțional, în cazul în care se consideră că este puțin probabil ca alte metode mai puțin invazive să aibă succes;

(iii) interceptarea trebuie adaptată pentru a evita, pe cât posibil, vizarea unor persoane sau instituții care nu sunt responsabile de infracțiunile sau activitățile sus-menționate;

(iv) interceptarea trebuie să înceteze de îndată ce nu mai servește scopurilor urmărite.

e) Respectarea principiului proporționalității, care impune ca:

(i) să fie asigurat un just echilibru între drepturile concurente ale subiecților interceptării și scopurile urmărite, în conformitate cu principiul potrivit căruia cu cât mai grave sunt infracțiunile sau activitățile sus-menționate și consecințele lor trecute sau viitoare, cu atât mai intruzivă și mai extinsă poate fi interceptarea; și

(ii) în orice caz, interceptarea trebuie să asigure respectarea esenței (sau minimul nucleu al) drepturilor subiecților interceptării, cum ar fi dreptul la viață privată intimă,

¹⁰⁸ Articolul 2 litera b) din Convenția Națiunilor Unite împotriva criminalității transnaționale organizate definește „infracțiunea gravă” ca fiind o faptă pasibilă de o pedeapsă privată de libertate al cărei maxim este de cel puțin patru ani sau o pedeapsă mai grea. Raportul explicativ privind Recomandarea Rec (2005)10 a Comitetului de Miniștri urmează această trimitere.

în cazul persoanelor fizice. Interceptarea trebuie să înceteze de îndată ce devine evident că afectează nucleul vieții private.

f) O limită a duratei mandatului de interceptare, care poate fi prelungită de una sau mai multe ori, după o evaluare a rezultatelor operațiunii, dar, în orice caz, cu un termen maxim impus pentru întreaga operațiune.

g) Controlul judiciar de la un capăt la altul, care include:

(i) autorizarea interceptării, inclusiv a canalelor de transmisie specifice și a selectorilor puternici care urmează să fie utilizați;

(ii) controlul periodic al punerii în aplicare a mandatului de interceptare, la intervale suficient de scurte, inclusiv prelungirea duratei mandatului de interceptare și transmiterea datelor obținute către terți; și

(iii) controlul *a posteriori* al procesului de interceptare și a datelor interceptate.

h) În caz de urgență, un procuror poate emite un mandat special de interceptare, dar trebuie să fie confirmat de un judecător într-o perioadă scurtă de timp.

i) Procedura care trebuie urmată pentru examinarea, utilizarea, stocarea și distrugerea datelor obținute, cu o descriere detaliată a domeniului de aplicare a controlului exercitat de judecător pe parcursul etapei de punere în aplicare și după încetarea interceptării, precum și documentarea principalelor etape ale ștergerii datelor, în măsura în care acest lucru este necesar controlului exercitat de judecător.

j) Condițiile care trebuie îndeplinite și măsurile de precauție care trebuie luate atunci când se face schimbul de date interceptate cu serviciile de informații străine, după cum urmează:

(i) interzicerea absolută a externalizării operațiunilor de supraveghere care eludează normele interne;

(ii) interzicerea absolută, în cazul unui serviciu de informații care a primit date de la un serviciu de informații străin, de a le transmite unui terț fără consimțământul emitentului, această regulă nelimitând accesul judecătorului intern al statului destinatar la datele transferate;

(iii) interzicerea absolută a schimbului de date cu servicii străine de informații care nu asigură un nivel de protecție echivalent în esență cu cel garantat de Convenție;

(iv) interzicerea absolută a transferului în masă de date, sau a primirii, de la sau către un serviciu de informații străin în cadrul unui proces continuu, bazat pe un singur scop;

(v) autorizarea judiciară înainte de fiecare transfer/primire de date în conformitate cu exact aceleași principii și norme privind interceptarea în masă la nivel național, inclusiv, printre altele, respectarea principiilor necesității și proporționalității;

(vi) aceste norme se aplică fără distincție între datele solicitate și cele nesolicitate, datele „brute” (neevaluate) și datele evaluate.

k) Obligația de a notifica subiectul interceptării atunci când interceptarea încetează, cu excepția cazului în care interesele de securitate

națională ar fi amenințate de o astfel de divulgare, caz în care judecătorul competent trebuie să aibă competența de a examina din proprie inițiativă (*ex proprio motu*) sau din inițiativa unui terț (de exemplu, un procuror) întregul proces de interceptare pentru a stabili dacă datele au fost obținute în mod legal și dacă trebuie păstrate sau distruse, persoana interceptată fiind apărută ulterior de un avocat specializat în protecția vieții private.

l) Garanții speciale în ceea ce privește confidențialitatea comunicațiilor profesionale ale persoanelor ale căror comunicații sunt acoperite de secretul profesional, cum ar fi parlamentarii, medicii, avocații, jurnaliștii și preoții.

m) Garanția că o condamnare penală nu se poate baza exclusiv sau într-o măsură decisivă pe probe colectate prin interceptarea în masă.

n) Aceste principii se aplică supravegherii efectuate pe teritoriul părții contractante, precum și supravegherii efectuate extrateritorial, indiferent de scopul supravegherii, de starea datelor (stocate sau în tranzit) sau de posesia datelor (date aflate în posesia subiectului interceptării sau în posesia unui furnizor de servicii).

o) Obligația statului de a respecta și de a face să fie respectate drepturile persoanelor fizice este completată de obligația de a proteja drepturile persoanelor împotriva abuzurilor comise de actori nestatali, inclusiv de entități corporative.

IV. CRITICILE ADUSE REGIMULUI DE INTERCEPTARE ÎN MASĂ DIN REGATUL UNIT ÎN LITIGIU ÎN PREZENTA SPEȚĂ

A. Interceptarea în masă a comunicațiilor în temeiul RIPA 2000

35. Având în vedere cele de mai sus, avem o obiecție principală, ce depășește cu mult critica inconsistentă făcută de Marea Cameră regimului de interceptare în masă din Regatul Unit, astfel cum era în vigoare la 7 noiembrie 2017, ceea ce înseamnă înainte de intrarea deplină în vigoare a Legii privind competențele de investigare din 2016 (IPA)¹⁰⁹.

36. Scopul interceptării în masă în detectarea și investigarea infracțiunilor grave, astfel cum sunt definite la art. 81 alin. (2) lit. b) din RIPA, nu este în mod definitiv compatibil cu noțiunea de infracțiune gravă care prevalează în dreptul internațional, în măsura în care dreptul conceptul intern include infracțiuni pedepsite cu închisoarea mai mică de patru ani. În plus, scopul de a proteja bunăstarea economică a Regatului Unit, în măsura în care acest interes este relevant și pentru interesele securității naționale, nu este suficient

¹⁰⁹ Pct. 270 din prezenta hotărâre. Aceasta înseamnă că, la fel ca Marea Cameră, nu am luat în considerare modificările introduse de IPA și de noul Cod IC 2018. Acestea nu s-au aflat în discuție în fața Curții.

de precis, permițând utilizarea interceptării în masă, de exemplu, în scopuri legate de spionajul economic și industrial și „războiul comercial”¹¹⁰.

37. Termenii foarte generali ai mandatelor emise de ministru de la art. 8 alin. (4) au fost, de asemenea, criticați, în mod corect, de Comisia pentru Informații și Securitate a Parlamentului (ISC)¹¹¹.

38. Distincția dintre comunicațiile interne și cele externe, astfel cum este prevăzută la art. 20 din RIPA, este fundamental deficientă și nu delimitează suficient categoriile de persoane susceptibile să le fie interceptate comunicațiile. După cum a concluzionat ISC, această distincție era confuză și lipsită de transparență¹¹².

39. Justificarea Guvernului pentru această distincție a fost aceea că „[î]n momentul în care obțin informații cu privire la activitățile din străinătate, serviciile de informații nu au aceeași capacitate de a identifica ținte sau amenințări cu cele pe care le au în Regatul Unit”¹¹³. IPT a reiterat argumentul, afirmând că „este mai dificil să se investigheze amenințările teroriste și infracționale din străinătate”¹¹⁴. Această justificare trebuie înțeleasă în contextul informațiilor prezentate de Guvern în 2014, care a recunoscut că solicitările de a primi materiale în masă au fost adresate unui serviciu de informații străin „altfel decât în conformitate cu un acord internațional de asistență juridică reciprocă”¹¹⁵. Astfel, sistemul de interceptare în masă în litigiu a fost creat pentru a evita proceduri de durată și o utilizare intensivă a resurselor și obligațiilor „mai stricte” care decurg din cadrul juridic internațional existent privind asistența juridică reciprocă, cu alte cuvinte, pentru a evita garanțiile din cadrul actualului sistem de tratate internaționale de asistență reciprocă și pentru a profita de lipsa reglementării noilor tehnologii de supraveghere transnațională.

40. În plus, având în vedere că un volum tot mai mare de comunicații este tratat¹¹⁶ ca extern, precum și creșterea exponențială a interceptării în masă a tot mai multor persoane care se află în Insulele Britanice¹¹⁷, distincția

¹¹⁰ A se vedea interesanta discuție dintre părți în ședința Marii Camere din 10 iulie 2019 cu privire strict la acest aspect. Curtea a susținut puncte de vedere diferite cu privire la precizia scopului privind securitatea națională (a se compara și *a contrario*, *Iordachi și alții împotriva Moldovei*, nr. 25198/02, pct. 46, 10 februarie 2009, și *Kennedy împotriva Regatului Unit*, citată anterior, pct. 159).

¹¹¹ Pct. 146 din prezenta hotărâre.

¹¹² Pct. 145 din prezenta hotărâre.

¹¹³ A se vedea observațiile guvernului pârât prezentate în fața Marii Camere la 2 mai 2019, pct. 9.

¹¹⁴ Pct. 51 din prezenta hotărâre, pe care Curtea l-a reiterat la pct. 375.

¹¹⁵ Pct. 36 și 116 din prezenta hotărâre, care fac trimitere la pct. 12.2 din Codul IC.

¹¹⁶ Pct. 47 din prezenta hotărâre.

¹¹⁷ Astfel cum a indicat guvernul pârât, „cu toate acestea, faptul că comunicațiile electronice pot utiliza orice rută pentru a ajunge la destinație înseamnă în mod inevitabil că o parte din comunicațiile care circulă printr-un canal de transmisie între Regatul Unit și un alt stat vor consta în «comunicații interne»: și anume comunicații între persoane localizate în Insulele Britanice” (a se vedea observațiile prezentate în fața Marii Camere la 2 mai 2019, pct. 20).

comunicare externă/internă nu este pur și simplu fezabilă din punct de vedere tehnic și, prin urmare, este lipsită de sens. Distincția bazată pe jurisdicția teritorială între comunicațiile externe și cele interne este în mod inerent în contradicție cu realitatea fluxului actual de comunicare pe internet, unde un mesaj Facebook schimbat în cadrul unui grup de prieteni din Londra este transmis prin California și, prin urmare, este „extern” pentru Regatul Unit¹¹⁸. Astfel cum a reamintit Law Society Curții, comunicațiile confidentiale dintre avocați și clienți, chiar și atunci când ambii se aflau în Regatul Unit, puteau fi interceptate în temeiul regimului prevăzut la art. 8 alin. (4)¹¹⁹. În practică, conceptul extins al Guvernului în ceea ce privește comunicațiile externe include, de asemenea, stocarea în cloud, căutările pe Google, navigarea pe Internet și activitățile de pe platformele de comunicare socială¹²⁰. Pentru multe tipuri de comunicații, este posibil să nu se poată face distincția între comunicațiile externe și cele interne, întrucât localizarea destinatarului vizat nu va fi întotdeauna evidentă din datele de comunicații aferente. Analiza faptică prin care se determină dacă o anumită comunicație este externă sau internă poate fi efectuată în cazuri individuale numai printr-o analiză retrospectivă.¹²¹ Gradul mai mare actual de interconectare a condițiilor de viață și de comunicare la nivel transfrontalier nu constituie, cu siguranță, un argument pentru a trata în mod diferit comunicațiile interne și externe, ci mai degrabă un argument contrar. Bineînțeles, acest lucru nu ar trebui înțeles ca o invitație de a reduce nivelul de protecție a comunicațiilor interne, ci de a crește nivelul de protecție a comunicațiilor externe.

41. În această privință, nu este evident că o comunicație efectuată între o persoană din Strasbourg și o persoană din Londra ar trebui să beneficieze de protecție mai limitată în temeiul Convenției decât o comunicație efectuată între două persoane din Londra. Prin urmare, nu pare să existe nicio justificare obiectivă pentru a trata aceste persoane în mod diferit, cu excepția ipotezei că amenințările apar mai frecvent din străinătate și că străinii sunt de mai puțină încredere decât resortisanții naționali, întrucât prezintă un risc mai grav pentru securitatea națională și siguranța publică decât resortisanții naționali, justificând astfel necesitatea de a monitoriza comunicațiile trimise sau primite din afara Insulelor Britanice¹²². Acest lucru se reflectă, de asemenea, în modul

¹¹⁸ Pct. 75 din prezenta hotărâre.

¹¹⁹ Pct. 321 din prezenta hotărâre. A se vedea și hotărârea IPT *Belhadj și alții împotriva Security Service și altora*, IPT/13/132-9/H.

¹²⁰ Pct. 75 din prezenta hotărâre. Această practică pare să contrazică pct. 6.5 din Codul IC.

¹²¹ Guvernul pârât însuși a admis acest lucru (a se vedea observațiile prezentate în fața Marii Camere la 2 mai 2019, pct. 37).

¹²² Nu este suficient să se susțină că, întrucât legislația britanică „împiedică selectarea materialelor interceptate spre examinare în funcție de un factor «care are legătură cu o persoană despre care se știe că se află deocamdată în Insulele Britanice», orice diferență de tratament care rezultă nu ar fi bazată în mod direct pe naționalitate sau pe originea națională, ci mai degrabă pe localizarea geografică”, astfel cum se afirmă în hotărârea pronunțată de Camera (pct. 517), pentru motivul evident că marea majoritate a persoanelor despre care se

în care străinii sunt tratați în instanță atunci când doresc să își susțină dreptul la viață privată. IPT nu acceptă plângerile formulate de reclamanți din afara teritoriului național¹²³. Acest *Weltanschauung* ostil străinilor nu ar putea fi mai îndepărtat de spiritul și litera Convenției¹²⁴. Convenția plasează în centrul său persoana, nu cetățeanul unui stat, ceea ce înseamnă că drepturile conferite de Convenție ca drepturi ale persoanei ar trebui să ofere protecție ori de câte ori o parte contractantă acționează și, prin urmare, creează nevoia unei protecții – indiferent de locul, de cine și de modul în care face acest lucru. În plus, drepturile conferite de Convenție ar trebui să transpară în participarea statelor membre ale Consiliului Europei la comunitatea internațională, în măsura în care „ordinea juridică a Consiliului Europei nu mai poate fi confundată cu acordul internațional tradițional al unor egoisme juxtapuse. Suveranitatea nu mai este un dat absolut, la fel ca în perioada westfaliană, ci face parte integrantă dintr-o comunitate care servește drepturilor omului”¹²⁵.

42. În definitiv, distincția RIPA nu era adecvată scopului într-o perioadă de dezvoltare a internetului și servea strict obiectivului politic de a legitima sistemul în ochii publicului britanic, oferind iluzia că persoanele aflate sub jurisdicția teritorială a Regatului Unit vor fi scutite de „Big Brother”-ul guvernamental. În fapt, nu s-a întâmplat așa. Ministrul avea posibilitatea, atunci când considera necesar, să decidă examinarea materialelor selectate în funcție de factori care să aibă legătură cu o persoană care se afla în Insulele Britanice¹²⁶ și să modifice un mandat pentru a autoriza selectarea comunicațiilor respectivei persoane¹²⁷. În plus, captarea accidentală a comunicațiilor interne neidentificate în mandatul ministrului era permisă ori de câte ori era necesar pentru a obține comunicații externe care făcuseră

cunoaște că se află pentru moment în Insulele Britanice sunt resortisanți britanici, și viceversa, majoritatea celor care se află în afara insulelor sunt străini. Tratatul mai avantajos aplicat resortisanților a fost, de asemenea, remarcat de către FRA (*Surveillance by intelligence services*, citată anterior, pag. 45: „Atunci când serviciile de informații desfășoară activități de supraveghere pe plan intern, garanțiile juridice aplicabile sunt consolidate în comparație cu cele existente pentru supravegherea externă”).

¹²³ IPT, *Human Rights Watch & Ors împotriva SoS for the Foreign & Commonwealth Office & Ors*, 16 mai 2016: „În ceea ce privește orice presupunere afirmată că orice activitate care intră sub incidența art. 68 alin. (5) din RIPA a fost săvârșită de către sau în numele oricăruia dintre serviciile de informații, reclamantul trebuie să demonstreze că există o bază pentru o astfel de convingere, astfel încât să poată demonstra că este potențial expus riscului de a fi supus unei astfel de activități. În plus, un astfel de reclamant trebuie să demonstreze, în legătură cu o astfel de plângere că se află sau s-a aflat la momentul faptelor în Regatul Unit”.

¹²⁴ Raportul Comisiei de la Veneția, citat anterior, pct. 17, formulează aceeași critică „din motive fundamentale”, la fel ca și Raportorul special al ONU pentru promovarea și protecția dreptului la libertatea de opinie și de exprimare, făcând trimitere la PIDCP (pct. 313 din prezenta hotărâre).

¹²⁵ Pct. 22 din opinia noastră formulată în *Mursić împotriva Croației* (MC), nr. 7334/13, 20 octombrie 2016.

¹²⁶ Art. 16 alin. (3) of RIPA.

¹²⁷ Pct. 6.2 din Codul IC.

obiectul mandatului¹²⁸, și potrivit însuși Guvernului, acest lucru „este în practică inevitabil”¹²⁹. Acestea fiind spuse, trebuie arătat că, în ceea ce privește interceptarea în masă a datelor privind comunicațiile aferente, nu a existat nici măcar o restricție în ceea ce privește comunicațiile externe.

43. Chiar dacă interceptarea în masă a fost menită să fie o capacitate pentru colectarea de informații externe¹³⁰, și nu un instrument pentru prevenirea, detectarea și investigarea infracționalității¹³¹, nu justifică lipsa reglementărilor sau întinderea acordată puterilor autorităților de interceptare. În orice caz, drept rezultat al dezvoltării comunicațiilor digitale, garanția care limitează interceptarea comunicațiilor externe nu mai acționează ca o constrângere semnificativă¹³², dacă acest lucru s-a întâmplat vreodată. Și considerăm că nu s-a întâmplat niciodată, pentru următoarele motive.

44. Ministrul nu a emis nicio autorizație independentă pentru un mandat în temeiul art. 8 alin. (4)¹³³, mandatul său de interceptare fiind un cec în alb, care nu menționa numele și nici nu descria subiectul interceptării, nu impunea o limită expresă a numărului de comunicații care puteau fi interceptate și nu specifica canalele de transmisie sau selectorii. Nicio prevedere specifică nu reglementa situațiile în care erau formulate cererile de interceptare a comunicațiilor unui jurnalist, ale unui medic sau ale unui preot sau în care era posibilă o astfel de intruziune colaterală, cu excepția anodinelor puncte 4.28-4.31 din Codul IC¹³⁴. Alegerea canalelor de transmisie și aplicarea selectorilor, inclusiv a selectorilor puternici la comunicațiile externe, depindeau în ultimă instanță de autoritatea de interceptare¹³⁵. Cu alte cuvinte, comunitatea serviciilor de informații deținea controlul deplin asupra procedurii de autorizare, ținându-l la distanță pe ministru de informații esențiale, astfel încât acesta nu putea realiza o analiză adecvată a proporționalității și necesității, ci doar cauționa politic funcționarea sistemului¹³⁶.

¹²⁸ Art. 5 alin. (6) lit. a) din RIPA și pct. 6.6 din Codul IC.

¹²⁹ A se vedea observațiile guvernului pârât prezentate în fața Marii Camere la 2 mai 2019, pct. 37.

¹³⁰ În temeiul pct. 6.2 din Codul IC, „interceptarea în temeiul art. 8 alin. (4) reprezintă capacitatea de a colecta informații”.

¹³¹ Art. 81 din RIPA definește prevenirea și depistarea infracțiunilor, nu și investigarea lor.

¹³² Raportul Comisiei de la Veneția, citat anterior, pct. 11, face aceeași constatare.

¹³³ Parlamentul Regatului Unit a recunoscut, în raportul ISC din 2015, lipsa de independență a ministrului internelor, înainte de schimbarea creării IPA în 2016.

¹³⁴ Dispoziții aplicabile art. 8 alin. (4) în ceea ce privește materialele selectate spre examinare și care constituie informații confidențiale (pct. 4.32 din Codul IC). Guvernul pârât recunoaște acum că „cererile de date privind comunicațiile destinate identificării surselor jurnalistice ar trebui să facă obiectul aprobării judiciare” (răspunsul Regatului Unit către Comisarul pentru drepturile omului al Consiliului Europei – Memorandum privind mecanismele de supraveghere și control în Regatul Unit, pct. 24).

¹³⁵ Pct. 146-147 din prezenta hotărâre.

¹³⁶ Aceasta a fost și concluzia raportului ISC din 2015 (pct. 147 din prezenta hotărâre). Nu este surprinzător că, în 2016, au fost emise 3 007 mandate de interceptare și numai 5 cereri

45. Pe de altă parte, Codul de bune practici emis de ministru nu era obligatoriu, permițând o derogare de la acesta pentru motive întemeiate. Și mai grav, activitatea cotidiană era guvernată de „proceduri nepublice”, care nu erau disponibile publicului, nici măcar într-o formă sumară sau obscurată¹³⁷. Această marjă de manevră administrativă a autorității de interceptare încălca scopul principiului legalității, potrivit căruia normele care reglementează interceptarea în masă trebuie să aibă un temei în dreptul intern și că legea trebuie să fie accesibilă și previzibilă în ceea ce privește efectele sale.

46. Deficiențele de reglementare ale sistemului erau și mai mult agravate de statutul Comisarului pentru Interceptarea Comunicațiilor (Comisarul IC), care nu era o autoritate independentă și care nu exercita un control efectiv în ceea ce privește punerea în aplicare a mandatului de interceptare¹³⁸. Astfel cum indică raportul ISC din 2015, „deși cei doi comisari sunt foști judecători, în calitatea lor de comisari, aceștia își desfășoară activitatea în afara cadrului judiciar oficial”, concluzionând că „o parte dintre aceste responsabilități se exercită în prezent pe o bază nestatutară. Acest lucru este nesatisfăcător și inadecvat”¹³⁹. Acesta nu este cel mai grav aspect al statutului juridic al Comisarului IC. Conform dispozițiilor legale, prim-ministrul numea Comisarul CI, care îi raporta și depindea de personalul pus la dispoziția sa de ministru¹⁴⁰. În plus, era o poziție cu fracțiune de normă, iar Comisarul IC putea fi demis de către prim-ministru în orice moment¹⁴¹. Evident, acest statut nu era compatibil cu independența necesară pentru o supraveghere efectivă a funcționării regimului prevăzut la art. 8 alin. (4). Pe scurt, comisarii nu erau „independenți din punct de vedere instituțional, operațional și financiar de instituțiile pe care [erau] mandatați să le supravegheze”, astfel cum prevăd principiile Tshwane¹⁴².

47. Presupunând chiar, de dragul discuției, că era independent controlul exercitat de Comisar în Regatul Unit, trebuie să constatăm că acesta nu era unul efectiv, pentru simplul motiv că, atunci când se confrunta cu o eroare

au fost respinse de ministru (pct. 170 din prezenta hotărâre). Cifrele sunt elocvente: rolul ministrului era doar acela de a aproba cererile.

¹³⁷ Pct. 33 din prezenta hotărâre.

¹³⁸ A se vedea pct. 347 din hotărârea Camerei și pct. 26 din opinia separată a doamnei judecător Koskela, susținută de doamna judecător Turković, care subliniază faptul că sistemul britanic era mai deficitar decât sistemul de garanții german în vigoare în perioada cauzelor *Klass și alții* și *Weber și Saravia*.

¹³⁹ Din păcate, acest pasaj al raportului ISC din 2015, menționat la pct. 142 din hotărâre, a fost neglijat de majoritate.

¹⁴⁰ Pct. 57 din RIPA 2000.

¹⁴¹ Critica formulată de reclamanti în cadrul ședinței în fața Marii Camere din 10 iulie 2019 este legitimă: un judecător unic pensionat care lucrează cu fracțiune de normă și cu un secretariat redus și care realizează analize prin sondaje „nu poate spera să exercite un control semnificativ”.

¹⁴² Cu privire la aceste principii și rolul lor în cadrul Consiliului Europei, a se vedea concluziile noastre separate formulate în *Szabo și Vissy*, citată anterior.

gravă, Comisarul avea doar competența de a prezenta un raport prim-ministrului pentru a-i atrage atenția asupra respectivei erori și, în cazul unui răspuns afirmativ, de a decide în ce măsură era posibil să se publice eroarea respectivă¹⁴³. De exemplu, nu putea nici să trimită cauza în fața IPT, nici să informeze victima cu privire la interceptarea excesivă. În fapt, Comisarul nici măcar nu a constatat că reclamantele Amnesty International și Centrul de Resurse Juridice din Africa de Sud făcuseră obiectul unei supravegheri ilegale!

48. Durata perioadelor de interceptare și de păstrare a datelor nu avea un termen maxim specificat în lege, iar practica nu acoperea această lacună¹⁴⁴. Mandatele în temeiul art. 8 alin. (4) puteau fi reînnoite *ad aeternum*¹⁴⁵. În plus, perioadele de păstrare a datelor erau diferite de la o autoritate de interceptare la alta¹⁴⁶, iar termenul maxim „normal” de păstrare a datelor în temeiul pct. 7.9 din Codul IC (și anume doi ani) putea fi suspendat de către un înalt funcționar al autorității de interceptare. Asta spune multe despre cine avea controlul în sistemul de interceptare în masă britanic¹⁴⁷.

49. Nu exista nicio obligație de notificare la finalul procesului de interceptare¹⁴⁸. În lipsa unei astfel de notificări, dreptul de acces la o instanță era în mare măsură inutil. Aceasta era situația în Regatul Unit¹⁴⁹. IPT acționa numai ca urmare a unei plângeri a unei persoane care credea că a făcut obiectul unei supravegheri secrete, ceea ce însemna că IPT constituia o garanție pur teoretică pentru toți subiecții interceptării care nu aveau nicio idee că comunicațiile lor au fost interceptate¹⁵⁰. Insuficiența controlului din partea IPT era agravată de faptul că nu avea competența de a formula o declarație de incompatibilitate în cazul în care constata că legislația primară

¹⁴³ Astfel cum a recunoscut guvernul pârât în ședința Marii Camere din 10 iulie 2019.

¹⁴⁴ Astfel cum a indicat guvernul pârât (pct. 403 din prezenta hotărâre). Se pare că nici măcar politicile interne nu erau respectate (pct. 59 din prezenta hotărâre).

¹⁴⁵ Pct. 6.22-6.24 din Codul IC.

¹⁴⁶ Pct. 176 din hotărâre.

¹⁴⁷ Este destul de surprinzător faptul că majoritatea, la pct. 405 din hotărâre, a considerat că este „de dorit” ca practica descrisă de guvernul pârât în fața Marii Camere să fie consacrată de lege.

¹⁴⁸ IPA a introdus obligația Comisarului de a analiza dacă a existat o eroare gravă și dacă ar fi în interesul public să fie notificată persoana în cauză, dar această regulă nu face obiectul analizei Curții în prezenta cauză. Alegerea politicii IPA reprezintă o recunoaștere a faptului că sistemul anterior era insuficient și că va mai trece timp până se va vedea dacă soluția IPA este suficientă.

¹⁴⁹ Acest lucru este agravat de politica NCNN („nici nu confirmă, nici nu neagă”) a Guvernului, care „împiedică o persoană să știe vreodată dacă a fost ținta unei supravegheri” și „nu permite ca deciziile de supraveghere să fie supuse unui control efectiv”, astfel cum a concluzionat Comisarul pentru drepturile omului al Consiliului Europei (Memorandum, citat anterior).

¹⁵⁰ Astfel, concluzia majorității potrivit căreia IPT oferea „o cale de atac solidă pentru oricine ar fi suspectat că comunicațiile sale au fost interceptate” (pct. 415) nu identifică deficiența evidentă a sistemului: caracterul său virtual pentru cei care nu au niciun motiv să suspecteze că ar fi făcut obiectul unei supravegheri secrete.

era incompatibilă cu CEDO, întrucât nu era o „instanță” în sensul art. 4 din Legea drepturilor omului din 1998, deciziile sale nu puteau fi contestate și, în mod ciudat, ministrul avea competența de a adopta normele procedurale ale IPT, ceea ce în practică însemna că entitatea supravegheată avea competența de a stabili normele care guvernau organul de control.¹⁵¹

B. Schimbul de date interceptate cu serviciile de informații străine

50. Nu există un cadru statutar expres analog cu RIPA care să reglementeze modul în care guvernul britanic putea utiliza datele interceptate dintr-o țară străină. Abia în ianuarie 2016 Capitolul 12 din Codul IC a stabilit cadrul unui astfel de schimb¹⁵². În temeiul pct. 12.5 din Codul IC și al notei sale de subsol aferente, cererile privind comunicațiile interceptate și datele aferente comunicațiilor de la un serviciu de informații străin puteau fi formulate pentru „materiale către, dinspre și cu privire la anumiți selectori”¹⁵³. NSA a renunțat la colectarea de date „despre” în aprilie 2017, deoarece aceasta nu putea fi efectuată în mod legal din cauza depășirii masive la un nivel inadmisibil a intruziunii¹⁵⁴. Cu toate acestea, disponibilitatea surprinzătoare a Curții de a accepta politica de „colectare completă” a guvernului pârât¹⁵⁵ depășește chiar și ansamblul de tactici al NSA, admitând nu doar solicitări de colectări de date „despre”, ci și solicitări de materiale altele decât cele referitoare la selectori specifici¹⁵⁶.

51. Potrivit Curții, transferul de materiale în masă către servicii de informații străine partenere ar trebui să facă obiectul unui „control independent”¹⁵⁷, nu și primirea de materiale în masă colectate de servicii de informații străine¹⁵⁸. În cazul în care garanțiile nu sunt adecvate în ceea ce privește supravegherea directă de către autoritățile de interceptare ale Regatului Unit, acestea ar trebui considerate inadecvate și în ceea ce privește supravegherea indirectă efectuată, care rezultă din schimbul de informații despre materialele interceptate de terți, cu atât mai mult cu cât astfel de materiale sunt colectate de un terț care nu este obligat prin Convenție. Atunci când riscul ca materialele colectate și stocate într-un mod neconform cu

¹⁵¹ Art. 69 alin. (1) of RIPA.

¹⁵² Guvernul pârât a afirmat că, „chiar înainte de publicarea Capitolului 12 din cod, acesta era «accesibil» ca urmare a divulgării”, făcând referire la divulgarea din octombrie 2014 (a se vedea observațiile prezentate în fața Marii Camere la 2 mai 2019, pct. 49). Acest lucru arată că până și Guvernul admite că, înainte de acel moment, legea nu era accesibilă.

¹⁵³ Pct. 116 din prezenta hotărâre.

¹⁵⁴ Pct. 263 din prezenta hotărâre.

¹⁵⁵ Potrivit afirmațiilor guvernului pârât în ședința Marii Camere din 10 iulie 2019: „prin urmare, dacă întrebarea problematică este dacă avem foarte multe date, chiar și după procesul de filtrare, răspunsul este «da», iar acesta este un lucru foarte bun, în opinia noastră.”

¹⁵⁶ Pct. 502 și 503 din prezenta hotărâre.

¹⁵⁷ Pct. 362 din prezenta hotărâre.

¹⁵⁸ Pct. 513 din prezenta hotărâre.

Convenția este mai mare și, prin urmare, controlul independent este cel mai necesar, Curtea a renunțat la această garanție, fără nicio justificare plauzibilă¹⁵⁹. În această privință, controlul Comisarului IC și al IPT, invocat de Guvern și de majoritatea din Marea Cameră, a fost practic inoperant în ceea ce privește controlul schimbului de materiale provenite de la terți, nu mai puțin important decât în cazul controlului supravegherii interne, întrucât intervenția IPT depindea de o plângere, iar Comisarul IC nu avea altă competență decât să prezinte un raport prim-ministrului pentru a-i atrage acestuia atenția asupra unei erori grave.

52. Consecințele absurde ale raționamentului majorității sunt și mai numeroase în exemplul următor: dacă un londonez transmite un mesaj pe Twitter unui alt londonez, iar această comunicare este transmisă prin intermediul unui server din Statele Unite ale Americii, Curtea acceptă că interceptarea de către Cartierul General pentru Comunicații al Guvernului (GCHQ) a mesajului respectiv și a datelor de comunicații aferente, atunci când părăsește Regatul Unit pe un cablu legat de Statele Unite ale Americii, obține garanția unei autorizări independente. Cu toate acestea, în cazul în care NSA interceptează același mesaj la celălalt capăt al aceluiași cablu și transmite apoi către GCHQ o copie sau datele de comunicații aferente, garanția unei autorizări independente nu se aplică. Este complet arbitrar să existe protecții juridice diferite pentru aceleași date numai în funcție de localizarea accidentală a persoanei care a efectuat interceptarea inițială. Lipsa unui sistem legal de garanții pentru utilizarea datelor interceptate dintr-o țară străină care să fie la fel de protectoare ca și în cazul datelor interceptate colectate în țara de origine înseamnă că legislația Regatului Unit este insuficientă pentru a proteja împotriva arbitrariului și abuzurilor¹⁶⁰.

53. În plus, conform pct. 12.6 din Codul IC, art. 15 și 16 din RIPA nu se aplicau tuturor materialelor primite de la serviciile de informații străine care puteau fi rezultatul unei interceptări în masă, ci numai materialele interceptate solicitate sau „în cazul în care materialele identificate ca fiind însuși produsul interceptării”, ceea ce făcea ca declanșarea garanțiilor naționale ale statului destinatar (Regatul Unit) să depindă de o decizie a serviciilor de informații străine.

54. Descrierea schimbului de materiale interceptate în masă cu alte părți ar fi incompletă fără a menționa o altă caracteristică notabilă. Trebuie adăugat că pct. 7.3 din Codul IC permitea divulgarea către alte părți a materialelor interceptate în conformitate cu simpla utilitate a serviciului, un criteriu

¹⁵⁹ Din păcate, Curtea a ignorat poziția Comitetului pentru Drepturile Omului în observațiile sale finale din 2015 cu privire la Regatul Unit, documentul ONU CCPR/C/GBR/CO/7, 17 august 2015, pct. 24, unde Comitetul își exprima îngrijorarea cu privire la „lipsa unor garanții suficiente în ceea ce privește obținerea de comunicații private de la serviciile de securitate străine și schimbul de date privind comunicațiile personale cu astfel de servicii”.

¹⁶⁰ Este exact ceea ce preconizează Comisia de la Veneția (pct. 201 din prezenta hotărâre).

extrem de simplist. Principiul „nevoii de a cunoaște”¹⁶¹ este opusul logic al criteriilor necesității și proporționalității: principiul potrivit căruia numai o mare parte din materialele interceptate pot fi dezvăluite pentru că destinatarul are nevoie de ele reprezintă antiteza acestor criterii. Utilizarea acestei competențe de a divulga nu este supusă unui prag legal obiectiv, ci doar ghidată, și eventual ascunsă, de scopul urmărit. Astfel, considerații pur oportuniste au prevalat asupra aprecierii necesității și proporționalității ingerinței suplimentare în drepturile subiectului interceptat, constând în divulgarea materialelor interceptate către alte părți. În termeni simpli, comunicațiile persoanei sunt tratate ca o posesie a statului, un bun pe care statul îl poate împărtăși cu alte părți, la discreția sa, pentru a „căuta acul în carul cu fân”¹⁶².

C. Interceptarea în masă a datelor de comunicații aferente

55. În sfârșit, art. 16 alin. (2) din RIPA nu se aplică interceptării în masă a datelor de comunicare aferente, ceea ce înseamnă că orice analist putea utiliza un selector puternic care făcea referire la o persoană despre care se cunoștea că se află în Insulele Britanice fără o certificare prealabilă din partea ministrului și, mai rău decât atât, datele interceptate puteau fi stocate timp de „câteva luni”, dacă și cât timp era necesar pentru a descoperi „necunoscute necunoscute”¹⁶³. În termeni practici, interceptarea și prelucrarea datelor de comunicații aferente era limitată doar de capacitatea de stocare a serviciilor de interceptare. În fapt, RIPA nu consacră cu adevărat puterea de a colecta informații externe, întrucât dezvoltarea tehnologică a transformat-o într-o putere de supraveghere internă, motiv pentru care Guvernul pretinde acum că garanția aplicabilă Insulelor Britanice de la art. 16 din RIPA nu este „necesară” pentru compatibilitatea cu Convenția¹⁶⁴.

56. Nici argumentul Guvernului privind fezabilitatea¹⁶⁵ nu ne convinge. Este perfect posibil ca un judecător să evalueze, în timp util, necesitatea și proporționalitatea unei cereri de autorizare de a ținti datele de comunicații ale persoanei în discuție în fiecare cauză, fără vreun risc grav de a-i submina utilizarea¹⁶⁶. Dacă acest proces de autorizare poate fi instituit pentru a ținti

¹⁶¹ Pct. 7.3 din Codul IC (pct. 96 și 390 din prezenta hotărâre).

¹⁶² Potrivit afirmațiilor guvernului pârât în ședința Marii Camere din 10 iulie 2019:

¹⁶³ Pct. 422-423 din prezenta hotărâre.

¹⁶⁴ A se vedea observațiile orale prezentate de guvernul pârât în fața Marii Camere la 10 iulie 2019. Astfel, autoritatea de interceptare putea obține, prin intermediul unui mandat colectiv, un conținut pe care ar fi trebuit să îl obțină prin intermediul unui mandat individual și specific în temeiul art. 8 și putea, prin urmare, să eludeze hotărârea Curții în *Kennedy împotriva Regatului Unit*, citată anterior.

¹⁶⁵ Pct. 420 din prezenta hotărâre.

¹⁶⁶ Opinia noastră se bazează pe propria experiență de judecător al curții penale în cauze penale extrem de complexe, în care poliția a cerut adesea interceptarea unor cantități mari de date legate de comunicații.

jurnaliști și alți profesioniști ale căror date de comunicații aferente sunt privilegiate din punct de vedere juridic, după cum acceptă Curtea¹⁶⁷, de ce nu poate fi stabilit pentru a ținti datelor de comunicare aferente ale muritorului de rând? Astfel de sisteme de omologare funcționale la scară largă sunt perfect posibile. Ideea este că ingerințele la scară largă în viața privată necesită un sistem de garanții la scară largă.

57. În pofida gradului lor de intruziune, atât în interiorul, cât și în afara Insulelor Britanice, toleranța Curții față de aceste practici este de neînțeles, ținând seama de faptul că art. 16 alin. (2) este considerat chiar de către Curte ca fiind „principala garanție statutară care circumscrie procesul de selectare a materialelor interceptate în vederea examinării”¹⁶⁸.

D. Concluzie preliminară

58. În concluzie, faptul că domeniul de aplicare al activității de supraveghere avute în vedere în *Weber și Saravia* (2006) și *Liberty și alții* (2008) era mult mai restrâns decât în prezent nu ar fi trebuit să determine Curtea să fie mai puțin exigentă în ceea ce privește nivelul necesar de protecție a drepturilor la viață privată în prezent. Creșterea exponențială a activității de supraveghere în ultimul deceniu și promisiunea publică pe care a lansat-o justifică un control mai strict al activităților serviciilor de informații, în scopul menținerii democrației și al apărării statului de drept. Nu invers. Atunci când riscul abuzurilor din partea statului crește, garanțiile prevăzute de Convenție și garanțiile corespunzătoare din dreptul intern ar trebui să crească, nu să se diminueze¹⁶⁹. Cu alte cuvinte, standardele actuale ale Curții ar trebui să fie mai exigente decât cele din 2006 sau 2008. Este exact opusul a ceea ce a decis prezenta hotărâre. În prezenta hotărâre, Curtea a cedat în fața faptului împlinit al interceptării generale în masă, acceptând în mod periculos că acest lucru trebuie să fie admisibil dacă este util. Utilitatea nu este aceeași cu necesitatea și proporționalitatea într-o societate democratică. Astfel cum a afirmat domnul judecător Brandeis în *Olmstead*

¹⁶⁷ Pct. 450 din prezenta hotărâre.

¹⁶⁸ A se compara și *a contrario*, pct. 420 și 421. A se observa că, la pct. 420, formularea este „principala garanție legală”, iar la pct. 421 este redusă la „o garanție importantă”. Limbajul imprecis de la punctul 421 este consternant, dar și mai îngrijorătoare este lipsa de substanță. Pura manipulare a limbajului este esențială pentru ponderea diferită acordată de Curte „preocupărilor” menționate la pct. 381 și 382 în ceea ce privește interceptarea în masă a datelor de comunicații aferente. Cireașa de pe tort o reprezintă în mod evident „evaluarea generală”, care îi permite Curții să ajungă la orice rezultat dorește [a se vedea analiza acestui criteriu al „caracterului echitabil general” din opiniile noastre anexate la *Muhammad și Muhammad împotriva României* (MC), nr. 80982/12, 15 octombrie 2020, și *Murtazaliyeva împotriva Rusiei* (MC), nr. 36658/05, 18 decembrie 2018].

¹⁶⁹ *Szábo și Vissy*, citată anterior, pct. 70: „Garanțiile impuse de jurisprudența actuală a Convenției în ceea ce privește interceptările trebuie îmbunătățite pentru a aborda problema acestor practici de supraveghere.” În mod similar, Rezoluția APCE 2045 (2015) insistă asupra necesității unui control consolidat al supravegherii în masă.

*împotriva Statelor Unite ale Americii*¹⁷⁰, „este, de asemenea, lipsit de relevanță faptul că intruziunea [în ceea ce privește convorbirile telefonice] a fost în sprijinul aplicării legii”. Experiența ar trebui să ne învețe să fim foarte vigilenți să ne protejăm libertatea atunci când obiectivele guvernului sunt bine intenționate”.

V. CONCLUZIE

59. Această hotărâre modifică fundamental echilibrul existent în Europa între dreptul la respectarea vieții private și interesele de securitate publică, prin faptul că permite supravegherea neindividualizată a conținutului comunicațiilor electronice și a datelor aferente comunicațiilor și, chiar mai rău, schimbul de date cu țări terțe care nu beneficiază de o protecție comparabilă cu cea a statelor membre ale Consiliului Europei. Această concluzie este cu atât mai justificată având în vedere respingerea de către CJUE într-un mod categoric a accesului generalizat la conținutul comunicațiilor electronice¹⁷¹, reticența sa vădită față de păstrarea generală și nediscriminatorie a datelor privind traficul și locația¹⁷² și limitarea schimburilor de date cu serviciile străine de informații care nu asigură un nivel de protecție echivalent în esență cu cel garantat de Carta drepturilor fundamentale¹⁷³. Cu privire la toate aceste trei aspecte, Curtea de la Strasbourg a rămas în urma Curții de la Luxemburg, care rămâne farul călăuzitor pentru drepturile la viața privată în Europa.

60. De bine sau de rău, cred ca mai curând de rău decât de bine, prin prezenta hotărâre, Curtea de la Strasbourg tocmai a deschis porțile pentru un „Big Brother” electronic în Europa. Dacă aceasta este noua normalitate pe care eminentii noștri colegi care formează majoritatea o doresc pentru Europa, nu ne putem alătura lor, iar acest lucru îl spunem cu inimă grea, cu aceeași dezolare ca și cea care emană din *Miserere mei, Deus* a lui Gregorio Allegri.

¹⁷⁰ 277 US 438.

¹⁷¹ Pct. 226 din prezenta hotărâre.

¹⁷² Pct. 211, 217, 239-241 din prezenta hotărâre.

¹⁷³ Pct. 234 din prezenta hotărâre.

OPINIA COMUNĂ PARȚIAL DIZIDENTĂ A DOMNILOR JUDECĂTORI LEMMENS, VEHABOVIĆ ȘI BOŠNJAK

1. Suntem de acord cu prezenta hotărâre, cu excepția aprecierii capătului de cerere cu privire la primirea de către autoritățile statului pârât a unor materiale interceptate solicitate de la servicii de informații străine, în temeiul art. 8 și 10 din Convenție (pct. 3 și 5 din dispozitivul hotărârii).

2. În prezenta hotărâre – precum și în hotărârea de astăzi *Centrum för rättvisa împotriva Suediei* de astăzi (nr. 35252/08) – Marea Cameră a instituit pentru regimurile de interceptare în masă un sistem eficient de garanții „de la un capăt la altul”, cu trei piloni principali sau pietre de temelie principale, pentru a reduce la minimum riscul de a abuza de o astfel de putere. Acești piloni fundamentali sunt: (1) autorizarea interceptării în masă de la început, atunci când obiectul și amploarea operațiunii sunt definite, de către un organism independent de executiv; (2) autorizarea internă prealabilă, atunci când sunt utilizați selectori puternici legați de persoane identificabile; și (3) supravegherea operațiunii de către o autoritate independentă, precum și un control *a posteriori* efectiv efectuat de un organism independent de executiv (pct. 350-359 din hotărâre).

3. Aceleași garanții „de la un capăt la altul” stabilite pentru un regim de interceptare în masă ar trebui să se aplice, de asemenea, unui regim în care autoritățile nu interceptează ele însele datele de comunicații transfrontaliere și cele de comunicații aferente, ci mai degrabă solicită serviciilor de informații străine să intercepteze aceste date sau să transmită date deja interceptate. Cu toate acestea, deși, la primirea materialelor interceptate, garanțiile privind examinarea, utilizarea și stocarea acestora, transmiterea lor ulterioară, precum și ștergerea și distrugerea lor sunt, de asemenea, aplicabile (pct. 498 din hotărâre), primul pilon, respectiv autorizarea independentă prealabilă, dispare complet în viziunea majorității. Motivarea sa în această privință nu ne convinge. De ce ar trebui făcută o distincție în funcție de modul în care autoritățile au intrat în posesia datelor interceptate, indiferent dacă au interceptat ele datele sau de către o autoritate străină? Prin urmare, în opinia noastră, inclusiv în ceea ce privește primul pilon, ar trebui să se aplice aceleași garanții precum cele stabilite pentru interceptarea în masă.

4. Putem subscrie pe deplin la motivarea Curții de la pct. 496 și 497 din hotărâre, în special că o ingerință în art. 8 se regăsește deja în cererea inițială adresată autorităților străine, iar protecția conferită de Convenție ar fi lipsită de obiect dacă statele ar putea eluda obligațiile care le revin în temeiul Convenției, solicitând astfel de date de la state necontractante. Prin urmare, statele membre trebuie să dispună de norme clare și detaliate care să ofere garanții efective împotriva utilizării competenței lor de a eluda dreptul intern și/sau obligațiile care le revin în temeiul Convenției.

5. Acolo unde ne îndepărtăm cu respect de majoritate este întrebarea în ce constau „garanțiile efective”.

6. Majoritatea face trimitere, în primul rând, la faptul că cererile fie erau întemeiate pe mandate deja autorizate de ministru, fie aprobate explicit de acesta (pct. 505 din hotărâre). Cu toate acestea, susținem că ministrul nu este independent de executiv și, în acest sens, regimul care guvernează primirea de informații de la servicii de informații străine este afectat de aceeași deficiență ca regimul de interceptare în masă (pct. 377 din hotărâre).

7. În al doilea rând, majoritatea pare să presupună că o lege națională care interzice eludarea dispozițiilor sale constituie, în sine, o garanție efectivă (pct. 506 din hotărâre). Cu respect, nu suntem de acord. După cum s-a subliniat deja, de exemplu, în opinia separată a domnului judecător Ranzoni în *Breyer împotriva Germaniei* (nr. 50001/12, 30 ianuarie 2020), dreptul intern nu prevede decât baza legală care determină legalitatea ingerinței: nu constituie, în plus și în sine, o protecție efectivă pentru a proteja persoana de aplicarea dreptului intern în mod arbitrar și contra utilizării abuzive a puterilor conferite prin lege. O astfel de protecție trebuie să depășească normele juridice, în special atunci când aceste norme și competențe juridice sunt formulate în termeni generali.

8. Cu alte cuvinte, o dispoziție legală care interzice eludarea sau orice altă utilizare abuzivă nu poate, în același timp, să constituie o garanție pentru ca acest lucru să nu se întâmple. O garanție efectivă presupune disponibilitatea unui mecanism capabil să asigure aplicarea corectă a dispoziției respective. Cu toate acestea, nu există o astfel de garanție în ceea ce privește cererile de interceptare și transmitere de date adresate unor servicii de informații străine. În opinia noastră, la fel ca în cazul regimului de interceptare în masă, primul pilon din cadrul garanțiilor „de la un capăt la altul” ar trebui să se aplice în mod similar. În consecință, orice astfel de cerere ar trebui să facă obiectul unei autorizări prealabile din partea unui organism independent capabil să evalueze dacă este atât necesară, cât și proporțională cu scopul urmărit (pct. 350 și 351 din hotărâre) și să se asigure că această competență nu este utilizată pentru a eluda dreptul intern și/sau obligațiile care îi revin statului în temeiul Convenției.

9. Din aceste motive, am votat împotriva constatării neîncălării art. 8 din Convenție în ceea ce privește obținerea de informații de la servicii de informații străine.

10. Întrucât majoritatea concluzionează că regimul schimbului de informații nu încalcă art. 10 din Convenție, pe baza acelorași motive care a determinat-o să concluzioneze o neîncălcare a art. 8 (pct. 516 din hotărâre), nu putem adera la concluzia la care a ajuns în temeiul art. 10.

ANEXĂ

Lista părților reclamante

Anexa nr.	Părți reclamante
58170/13	Big Brother Watch
58170/13	English PEN
58170/13	Open Rights Group
58170/13	Dr. Constanze Kurz
62322/14	Bureau of Investigative Journalism (Biroul de Jurnalism de Investigație)
62322/14	Alice Ross
24960/15	Amnesty International Limited
24960/15	Bytes For All
24960/15	The National Council for Civil Liberties („Liberty”) (Consiliul Național pentru Libertăți Civile)
24960/15	Privacy International
24960/15	The American Civil Liberties Union (Uniunea Americană pentru Libertăți Civile)
24960/15	The Canadian Civil Liberties Association (Asociația Canadiană pentru Libertăți Civile)
24960/15	The Egyptian Initiative For Personal Rights (Inițiativa Egipteană pentru Drepturile Personale)

HOTĂRÂREA BIG BROTHER WATCH ȘI ALȚII ÎMPOTRIVA REGATULUI UNIT

24960/15	The Hungarian Civil Liberties Union (Uniunea Maghiară pentru Libertăți Civile)
24960/15	Irish Council for Civil Liberties Limited (Consiliul Irlandez pentru Libertăți Civile, Ltd.)
24960/15	Centrul de Resurse Juridice