

CURTEA EUROPEANĂ A DREPTURILOR OMULUI
MAREA CAMERĂ

Hotărârea
din 4 decembrie 2015
În Cauza Roman Zakharov împotriva Rusiei
(Cererea nr. 47143/06)
Strasbourg

Hotărârea este definitivă. Aceasta poate suferi modificări de formă.

În Cauza Roman Zakharov împotriva Rusiei,
Curtea Europeană a Drepturilor Omului, reunită în Marea Cameră compusă din Dean Spielmann, președinte, Josep Casadevall, Guido Raimondi, Ineta Ziemele, Mark Villiger, Luis López Guerra, Khanlar Hajiyev, Angelika Nußberger, Julia Laffranque, Linos-Alexandre Sicilianos, Erik Møse, André Potocki, Paul Lemmens, Helena Jäderblom, Faris Vehabović, Ksenija Turković, Dmitry Dedov, judecători, și Lawrence Early, jurisconsult,
după ce a deliberat în camera de consiliu, la 24 septembrie 2014 și 15 octombrie 2015,
pronunță prezenta hotărâre, adoptată la cea din urmă dată:

PROCEDURA

1. La originea cauzei se află cererea nr. 47143/06 îndreptată împotriva Federației Ruse, prin care un resortisant al acestui stat, domnul Roman Andreyevich Zakharov („reclamantul”), a sesizat Curtea la 20 octombrie 2006, în temeiul art. 34 din Convenția pentru apărarea drepturilor omului și a libertăților fundamentale (*Convenția*).

2. Reclamantul a fost reprezentat inițial de domnul B. Gruz, avocat în Sankt Petersburg. Ulterior, a fost reprezentat de avocați din partea organizației neguvernamentale EHRAC/Centrul pentru drepturile omului „Memorial”, cu sediul în Moscova. Guvernul rus (Guvernul) a fost reprezentat de domnul G. Matyushkin, reprezentantul Federației Ruse la Curte.

3. Reclamantul a susținut că sistemul de interceptare secretă a comunicațiilor de telefonie mobilă din Rusia a încălcat dreptul său la respectarea vieții sale private și a corespondenței sale și că nu a avut la dispoziție o cale de atac eficientă pentru a formula o plângere în acest sens.

4. La 19 octombrie 2009, cererea a fost comunicată Guvernului.

5. La 11 martie 2014, camera din Secția întâi căreia i-a fost repartizată cauza (art. 52 § 1 din Regulamentul Curții – Regulamentul), compusă din Isabelle Berro-Lefèvre, președinte, Khanlar Hajiyev, Julia Laffranque, Linos-Alexandre Sicilianos, Erik Møse, Ksenija Turković, Dmitry Dedov, judecători, și Søren Nielsen, grefier de secție, s-a desesizat în favoarea Marii Camere; niciuna dintre părți nu a formulat obiecții (art. 30 din Convenție și art. 72 din Regulament).

6. La 24 septembrie 2014, a avut loc o ședință publică la Palatul Drepturilor Omului din Strasbourg (art. 59 § 3 din Regulament).

S-au înfățișat:

– pentru Guvern

dl. G. Matyushkin, reprezentantul Federației Ruse
la Curtea Europeană a Drepturilor Omului,

agent,

d-nele O. Sirotkina,

I. Korieva,

O. Iurchenko,

d-nii O. Afanasev,

A. Lakov,

consilieri;

– pentru reclamant

dl. P. Leach,
d-na. K. Levine,
dl. K. Koroteev,
d-nele. A. Razhikova,
E. Levchishina,

consilieri,
consilieră.

Curtea a ascultat declarațiile prezentate de dl Matyushkin, dl Leach, dna Levine, d-na. Razhikova și dl Koroteev, precum și răspunsurile date de d-nii. Matyushkin și Leach la întrebările adresate de judecători.

ÎN FAPT

I. CIRCUMSTANȚELE CAUZEI

7. Reclamantul s-a născut în 1977 și locuiește în Sankt Petersburg.

8. Acesta este redactor-șef al unei edituri și al unei reviste de aviație. De asemenea, este președintele filialei din Sankt Petersburg a Fundației pentru Apărarea Glasnost, organizație neguvernamentală care monitorizează situația libertății mass-mediei în regiunile Rusiei, apără independența mass-mediei regionale, libertatea de exprimare și respectarea drepturilor jurnaliștilor și le oferă sprijin juridic, inclusiv sub aspect procedural.

9. Acesta era abonat la serviciile mai multor operatori de telefonie mobilă.

10. La 23 decembrie 2003, reclamantul a introdus o acțiune în justiție împotriva a trei operatori de telefonie mobilă, invocând încălcarea dreptului său la respectarea caracterului privat al comunicațiilor sale telefonice. Acesta a susținut că, în conformitate cu Ordinul nr. 70 (*infra*, pct. 115-122) adoptat de Comisia Națională a Comunicațiilor și Tehnologiei Informației – predecesoarea Ministerului Comunicațiilor – operatorii de telefonie mobilă au instalat un echipament care a permis Serviciului Federal de Securitate (FSB) să intercepteze toate comunicațiile telefonice fără autorizație judiciară prealabilă. În opinia acestuia, Ordinul nr. 70, care nu a fost publicat niciodată, restrânge în mod nejustificat dreptul său la respectarea vieții private. Acesta a solicitat instanței emiterea unei dispoziții pentru îndepărtarea echipamentului instalat în conformitate cu Ordinul nr. 70 și acordarea accesului la comunicațiile de telefonie mobilă numai persoanelor autorizate. Ministerul Comunicațiilor și Tehnologiei Informației (Ministerul Comunicațiilor) și secția din Sankt Petersburg și regiunea Leningrad a FSB au intervenit în procedură în calitate de terți.

11. La 5 decembrie 2005, judecătoria districtului Vasileostrovskiy din Sankt Petersburg a respins acțiunea reclamantului pe motiv că acesta nu a demonstrat că operatorii de rețele mobile au transmis vreo informație protejată unor persoane neautorizate ori au permis interceptarea nelimitată sau neautorizată a comunicațiilor. Instanța a indicat că echipamentul vizat de reclamant a fost instalat pentru a permite organelor de aplicare a legii să efectueze cu succes măsuri operative de investigații conform procedurii prevăzute de lege. Aceasta a considerat că instalarea unui astfel de echipament nu constituia în sine o atingere adusă caracterului privat al comunicațiilor reclamantului, care, în opinia sa, nu a stabilit nimic care să justifice constatarea unei încălcări a dreptului său la respectarea caracterului privat al comunicațiilor sale telefonice.

12. Reclamantul a declarat apel. Acesta a afirmat, în special, că judecătoria a respins dintre probe diverse documente, inclusiv două decizii judecătorești privind autorizarea retroactivă a interceptării comunicațiilor de telefonie mobilă, precum și un act adițional la contractul-tip de furnizare de servicii emis de unul dintre operatorii de rețele mobile. Prima decizie judecătorească, pronunțată la 8 octombrie 2002, a autorizat interceptarea comunicațiilor de telefonie mobilă ale mai multor persoane în perioada 1–5 aprilie, 19–23 iunie, 30 iunie – 7 aprilie și 16–20 octombrie 2001. A doua decizie judecătorească, din 18 iulie 2003, a autorizat interceptarea comunicațiilor de telefonie mobilă ale lui M.E. în perioada 11 aprilie – 11 octombrie 2003. În ceea ce privește actul adițional, acesta îl informa pe abonat că, în cazul în care numărul său este folosit pentru a emite amenințări teroriste, operatorul rețelei mobile poate să suspende furnizarea de servicii de telefonie și să transmită datele colectate organelor de aplicare a legii. Potrivit reclamantului, deciziile judecătorești și actul adițional în litigiu dovedesc că operatorii de rețele mobile și organele de aplicare a legii aveau capacitatea tehnică de a intercepta toate comunicațiile telefonice fără a obține în prealabil autorizație judiciară și că recurgeau frecvent la interceptări neautorizate.

13. La 26 aprilie 2006, Tribunalul Sankt Petersburg a confirmat, în apel, hotărârea pronunțată în primă instanță. Instanța a reiterat constatarea instanței districtuale, conform căreia reclamantul nu a demonstrat că i-au fost interceptate comunicațiile telefonice. Instanța a adăugat că reclamantul nu a dovedit nici riscul ca dreptul său la respectarea caracterului privat al comunicațiilor sale telefonice să sufere o ingerință ilegală. Instanța a precizat că, pentru a demonstra existența unui astfel de risc, reclamantul ar fi trebuit să demonstreze că pârâții au acționat contrar legii; or, potrivit instanței de apel, operatorii de rețele mobile erau obligați prin lege să instaleze un echipament care permitea organelor de aplicare a legii să pună în practică măsuri operative de investigații, echipament a cărui existență nu aduce în sine atingere caracterului privat al comunicațiilor reclamantului. Tribunalul Sankt Petersburg a considerat legal refuzul de a admite ca probe deciziile judecătorești din 8 octombrie 2002 și 18 iulie 2003 deoarece au fost luate cu privire la terți și nu îl vizau pe reclamant. De altfel, instanța a admis ca probă și a examinat actul adițional la contractul furnizorului de servicii, dar a concluzionat că documentul nu conținea nicio informație care să justifice reexaminarea hotărârii judecătorești.

14. Dintr-un document prezentat de reclamant rezultă că, în ianuarie 2007, organizația neguvernamentală „Controlul civil” a cerut Parchetului General să examineze ordinele adoptate de Ministerul Comunicațiilor cu privire la interceptarea comunicațiilor, în vederea verificării compatibilității acestora cu legislația federală. În februarie 2007, un membru al Parchetului General a contactat organizația neguvernamentală pentru a-i solicita copii după anexele nepublicate ale Ordinului nr. 70, precizând că parchetul nu a putut să le obțină de la Ministerul Comunicațiilor. În aprilie 2007, Parchetul General a refuzat să efectueze examinarea solicitată.

II. DREPTUL INTERN RELEVANT

A. Dreptul la respectarea vieții private și a corespondenței

15. Constituția garantează oricărei persoane dreptul la respectarea vieții sale private, a secretelor personale și de familie, precum și dreptul de a-și apăra onoarea și reputația (art. 23 alin. 1). Aceasta garantează, de asemenea, dreptul la respectarea corespondenței și a comunicațiilor telefonice, poștale, telegrafice și de alt tip. Acest drept poate fi restrâns doar în temeiul unei decizii judecătorești (art. 23 alin. 2).

16. În plus, Constituția prevede că este interzisă colectarea, păstrarea, utilizarea sau difuzarea de informații despre viața privată a unei persoane fără consimțământul acesteia. Serviciile centrale și municipale trebuie să se asigure că orice persoană are acces la documentele și elementele referitoare la drepturile și libertățile sale, dacă nu există prevederi contrare în lege (art. 24).

17. Legea privind comunicațiile din 7 iulie 2003 (nr. 126-FZ) garantează caracterul privat al comunicațiilor poștale, telegrafice și de alt tip prin intermediul rețelelor de telecomunicații sau al serviciilor de curierat. Restrângerea caracterului privat al comunicațiilor nu este permisă decât în cazurile prevăzute de legislația federală (art. 63 alin. 1). Interceptarea comunicațiilor se face în baza unei autorizații legale prealabile, cu excepția cazurilor prevăzute de legislația federală (art. 63 alin. 3).

18. La 2 octombrie 2003, în Decizia nr. 345-O, Curtea Constituțională a declarat că dreptul la respectarea caracterului privat al comunicațiilor telefonice cuprinde toate datele transmise, păstrate sau aflate cu ajutorul unui aparat de telefon, inclusiv metadatele cum ar fi informațiile privind conexiunile de intrare și de ieșire ale unui anumit abonat. Curtea Supremă a adăugat că supravegherea acestor date se face, de asemenea, în baza unei autorizații legale prealabile.

B. Răspunderea pentru atingerea adusă vieții private

19. Colectarea sau difuzarea neautorizată a informațiilor despre viața privată sau de familie a unei persoane, fără consimțământul acesteia, dacă este făcută din interes financiar sau alte interese personale și încalcă drepturile și interesele legitime ale cetățeanului, se pedepsește cu amendă, cu muncă forțată sau închisoare de până la 4 luni. Aceeași faptă săvârșită de un funcționar public în exercițiul atribuțiilor sale se pedepsește cu amendă, interdicția de a ocupa anumite funcții sau închisoare pe o perioadă de până la 6 luni (art. 137 C. pen.).

20. Orice încălcare a dreptului cetățeanului la respectarea caracterului privat al comunicațiilor sale poștale, telegrafice, telefonice sau de alt tip se pedepsește cu amendă sau muncă forțată. Aceeași faptă săvârșită de un funcționar public în exercițiul atribuțiilor sale se pedepsește cu amendă, interdicția de a ocupa anumite funcții sau închisoare de până la 4 luni (art. 138 C. pen.).

21. Abuzul în serviciu de către un funcționar public, în cazul în care este săvârșit din interes financiar sau din alte interese personale și aduce o atingere gravă drepturilor și intereselor legitime ale unei persoane fizice sau juridice, se pedepsește cu amendă, interdicția de a ocupa anumite funcții sau de a se angaja în anumite activități pentru o perioadă de până la 5 ani, cu muncă forțată pe o perioadă

de până la 4 ani sau cu închisoare de la 4 luni la 4 ani (art. 285 alin. 1 C. pen.).

22. Faptele prin care un funcționar public, depășindu-și în mod evident atribuțiile, încalcă grav drepturile și interesele legitime ale unei persoane fizice sau juridice, se pedepsesc cu amendă, interdicția de a ocupa anumite funcții sau de a se angaja în anumite activități pe o perioadă de până la 5 ani, cu muncă forțată de până la 4 ani sau închisoare de la 4 luni la 4 ani (art. 286 alin. 1 C. pen.).

23. În decizia nr. 19 din 16 octombrie 2009, Plenul Curții Supreme a declarat că, în sensul art. 285 și 286 C. pen., o „ingerință gravă în drepturile și interesele legitime ale unei persoane fizice sau juridice” înseamnă o încălcare a drepturilor și libertăților garantate de principiile în general recunoscute și de prevederile din dreptul internațional și din Constituția Federației Ruse – ca de exemplu dreptul persoanei la respectarea onoarei și demnității sale, a vieții sale private sau de familie, a corespondenței sale, a comunicațiilor sale telefonice, poștale, telegrafice și de alt tip, sau inviolabilitatea domiciliului său. În cazul unei persoane juridice, pentru a stabili dacă ingerința este „gravă”, se ține seama de amploarea prejudiciului suferit ca urmare a fetei ilegale, de natura și valoarea prejudiciului material, de numărul de persoane afectate și de gravitatea prejudiciului fizic, material sau moral suferit de acestea (pct. 18.2 din hotărâre).

24. Acțiunea penală se pune în mișcare dacă există suficiente elemente faptice care arată că s-a săvârșit o infracțiune (art. 140 alin. 2 C. proc. pen.).

C. Dispoziții generale privind interceptarea comunicațiilor

25. Interceptarea comunicațiilor este reglementată de Legea din 12 august 1995 privind măsurile operative de investigații (nr. 144-FZ – LMOI), care se aplică interceptării comunicațiilor atât în cadrul unei proceduri penale, cât și în afara acestui cadru, precum și de Codul de procedură penală din 18 decembrie 2001 (nr. 174 FZ, intrat în vigoare la 1 iulie 2002 – C. proc. pen.), care se aplică numai interceptării comunicațiilor în cadrul unei proceduri penale.

26. Măsurile operative de investigații au mai multe scopuri: 1) depistarea, prevenirea, pedepsirea infracțiunilor și investigarea acestora, precum și identificarea persoanelor care se pregătesc să comită o infracțiune, care comit o infracțiune sau au comis una; 2) localizarea persoanelor care încearcă să se sustragă justiției și a persoanelor date dispărute; 3) obținerea de informații despre fapte sau activități care pun în pericol securitatea națională, militară, economică sau ecologică a Federației Ruse (art. 2 LMOI). La 25 decembrie 2008, art. 2 LMOI a fost modificat prin adăugarea unui nou obiectiv – acela de a obține informații despre bunuri care fac obiectul măsurii confiscării.

27. Funcționarii și organele statului care pun în aplicare măsuri operative de investigații trebuie să dea dovadă de respect față de viața privată și de familie, domiciliul și corespondența cetățenilor. Se interzice recurgerea la astfel de măsuri pentru atingerea altor scopuri sau obiective decât cele prevăzute de lege (art. 5 alin. 1 și 2 LMOI).

28. Funcționarilor și organelor statului nu le este permis: 1) să aplice măsuri operative de investigații în interesul partidelor politice sau al organizațiilor non-profit ori religioase; 2) să aplice în secret măsuri operative de investigații cu privire la servicii federale, regionale sau locale, partide politice sau organizații non-profit ori religioase pentru a influența deciziile sau activitățile acestora; 3) să comunice vreunei persoane datele colectate în cadrul măsurilor operative de investigații dacă aceste date se referă la viața privată sau de familie a unui cetățean sau prejudiciază reputația sau renumele acestuia, cu excepția cazurilor prevăzute de legislația federală; 4) să instige ori să determine pe cineva să comită o infracțiune, ori să îi întindă o capcană în acest scop; 5) să falsifice rezultatele măsurilor operative de investigații (art. 5 alin. 8 LMOI).

29. Măsurile operative de investigații includ în special interceptarea comunicațiilor poștale, telegrafice, telefonice sau de alt tip și colectarea de date transmise prin mijloace tehnice de comunicații. Legea prevede că se permite, în cadrul unor astfel de măsuri, realizarea de înregistrări audio și video, fotografierea, filmarea și folosirea altor mijloace tehnice, cu condiția ca acest lucru să nu fie în detrimentul vieții ori sănătății persoanelor vizate sau al mediului. Măsurile operative de investigații care implică interceptarea comunicațiilor poștale, telegrafice, telefonice sau de alt tip și colectarea de date transmise prin mijloace tehnice de comunicație prin intermediul unui echipament instalat de către furnizorii de servicii de comunicații se pun în aplicare cu ajutorul mijloacelor tehnice de către FSB și serviciile Ministerului de Interne, în conformitate cu deciziile și acordurile semnate de serviciile respective (art. 6 LMOI).

30. Decretul prezidențial nr. 891 din 1 septembrie 1995 prevede că interceptarea comunicațiilor poștale, telegrafice sau de alt tip se efectuează de către FSB în interesul și în numele tuturor organelor de aplicare a legii (alin. 1). În situațiile în care FSB nu dispune de echipamentul tehnic necesar, interceptările pot fi făcute de serviciile Ministerului de Interne, în interesul și în numele tuturor organelor de aplicare a legii (alin. 2). Dispoziții similare sunt cuprinse în considerentele 2 și 3 din Hotărârea Guvernului nr. 538 din 27 august 2005.

D. Situații care pot duce la interceptarea comunicațiilor

31. Măsurile operative de investigații care implică o ingerință în dreptul constituțional la respectarea caracterului privat al comunicațiilor poștale, telegrafice și de alt tip transmise printr-o rețea de telecomunicații sau prin servicii de curierat, sau o ingerință în caracterul privat al domiciliului pot fi puse în aplicare în urma primirii unor informații: 1) că o infracțiune a fost comisă, este în curs de comitere sau în curs de pregătire; 2) despre persoane care se pregătesc să comită, comit sau au comis o infracțiune; sau 3) despre fapte sau activități care pun în pericol securitatea națională, militară, economică sau ecologică a Federației Ruse (art. 8 alin. 2 LMOI).

32. LMOI prevede că interceptarea comunicațiilor telefonice și de alt tip se autorizează numai în cazurile în care o persoană este suspectată sau învinuită de săvârșirea unei infracțiuni de gravitate medie, a unei infracțiuni grave ori a unei infracțiuni deosebit de grave, sau este posibil să aibă informații despre o astfel de infracțiune (art. 8 alin. 4 LMOI). Codul de procedură penală prevede, de asemenea, că interceptarea comunicațiilor telefonice și de alt tip ale unui suspect sau acuzat ori ale unei alte persoane poate fi autorizată dacă există motive să se creadă că acestea pot conține informații relevante pentru dosarul aferent unei infracțiuni de gravitate medie, al unei infracțiuni grave sau al unei infracțiuni deosebit de grave (art. 186 alin. 1 C. proc. pen.).

33. Art. 15 C. pen. prevede că „infracțiunile de gravitate medie” sunt acele infracțiuni săvârșite cu premeditare pentru care Codul penal prevede o pedeapsă maximă de la 3 la 5 ani de închisoare, precum și infracțiunile săvârșite fără premeditare pentru care Codul penal prevede o pedeapsă maximă mai mare de 3 ani de închisoare. „Infracțiunile grave” sunt acele infracțiuni săvârșite cu premeditare pentru care Codul penal prevede o pedeapsă maximă de la 5 la 10 ani de închisoare. „Infracțiunile deosebit de grave” sunt acele infracțiuni săvârșite cu premeditare pentru care Codul prevede o pedeapsă maximă mai mare de 10 ani de închisoare sau o pedeapsă mai severă.

E. Procedura de autorizare și termenele

1. Legea privind măsurile operative de investigații

34. Măsurile operative de investigații care implică o ingerință în dreptul constituțional la respectarea caracterului privat al comunicațiilor poștale, telegrafice și de alt tip transmise printr-o rețea de telecomunicații ori prin servicii de curierat, sau o ingerință în caracterul privat al domiciliului – cum ar fi inspectarea locurilor sau clădirilor, interceptarea comunicațiilor poștale, telegrafice, telefonice și de alt tip, sau colectarea de date transmise prin mijloace tehnice de comunicații – necesită o autorizație judiciară prealabilă (art. 8 alin. 2 LMOI).

35. În cazuri de urgență în care există un risc imediat de comitere a unei infracțiuni grave sau deosebit de grave, ori în prezența unor informații despre fapte sau activități care pun în pericol securitatea națională, militară, economică sau ecologică a țării, măsurile operative menționate la art. 8 alin. 2 pot fi aplicate fără autorizație judiciară prealabilă. În astfel de cazuri, este necesar ca în termen de 24 de ore de la începerea măsurilor operative de investigații acestea să fie aduse la cunoștința unui judecător. În cazul în care nu se obține o autorizație judiciară în termen de 48 de ore de la inițierea măsurilor, acestea trebuie să înceteze imediat (art. 8 alin. 3 LMOI).

36. Examinarea cererilor de luare a unor măsuri care implică o ingerință în dreptul constituțional pentru a respecta caracterul privat al comunicațiilor poștale, telegrafice și de alt tip transmise printr-o rețea de telecomunicații ori prin servicii de curierat, sau o ingerință în caracterul privat al domiciliului, este de competența unei instanțe în a cărei rază teritorială se află locul în care trebuie aplicată măsura solicitată sau locul în care își are sediul organul care emite cererea. Cererea se examinează imediat de către un judecător unic (art. 9 alin. 1 LMOI).

37. Judecătorul pronunță decizia pe baza cererii motivate a șefului unuiu dintre serviciile competente să aplice măsuri operative de investigații. Documentele justificative relevante, cu excepția celor care conțin informații despre investigatori sub acoperire sau informatori ai poliției, ori despre organizarea și tactica aferentă măsurilor operative de investigații, pot fi de asemenea prezentate, la cererea judecătorului (art. 9 alin. 2 și 3 LMOI).

38. Judecătorul care examinează cererea decide dacă se impune autorizarea unor măsuri care implică o ingerință în drepturile constituționale sus-menționate, sau dacă – din contră – nu se acordă autorizația; decizia se motivează. Acesta trebuie să precizeze perioada de valabilitate a autorizației, care în principiu nu trebuie să fie mai mare de 6 luni. Dacă este necesar, acesta poate prelungi perioada respectivă după ce reexaminează toate documentele relevante (art. 9 alin. 4 și 5 LMOI).

39. Decizia judecătorească de autorizare a măsurilor operative de investigații și documentele care stau la baza acestei decizii trebuie să rămână în posesia exclusivă a organului statului care aplică măsurile operative de investigații (art. 12 alin. 3 LMOI).

40. Prin Decizia nr. 86-O din 14 iulie 1998, Curtea Constituțională a respins ca inadmisibilă o cerere pentru controlul constituționalității anumitor dispoziții ale LMOI. Instanța a declarat, în special,

că judecătorul nu trebuie să autorizeze măsuri de investigații care implică o ingerință în drepturile constituționale decât dacă are convingerea că astfel de măsuri sunt legale, necesare și justificate, cu alte cuvinte compatibile cu toate cerințele din LMOI. Instanța a precizat că sarcina probei îi revine organului de stat care emite cererea, acesta fiind obligat să demonstreze necesitatea măsurilor respective. De asemenea, instanța constituțională a precizat că, la cererea judecătorului, acestuia trebuie să i se pună la dispoziție documente justificative și că, întrucât unele dintre ele pot conține secrete de stat, doar un judecător care deține certificatul de securitate necesar poate examina cererile de autorizare. În plus, în baza necesității de a păstra secretul măsurilor de supraveghere, Curtea Constituțională a considerat că principiul caracterului public al ședinței și principiul contradictorialității nu sunt aplicabile procedurii de autorizare. În consecință, potrivit înaltei instanțe, faptul că nu se poate ca persoana vizată să participe la procedura de autorizare, să fie informată cu privire la decizia luată ori să declare apel la o instanță superioară nu constituie o încălcare a drepturilor sale constituționale.

41. În Decizia nr. 345-O din 2 octombrie 2003, Curtea Constituțională a declarat că judecătorul este obligat să examineze cu atenție și în detaliu probele prezentate în susținerea unei cereri de interceptare și că, în cazul în care cererea nu este întemeiată suficient, acesta poate solicita informații suplimentare.

42. De asemenea, prin Decizia nr. 1-O din 8 februarie 2007, Curtea Constituțională a respins ca inadmisibilă o cerere pentru controlul constituționalității art. 9 din LMOI. Înalta instanță a considerat că, înainte de a autoriza aplicarea unor măsuri operative de investigații, judecătorul este obligat să verifice temeiul acestora. Instanța a adăugat că decizia judecătorească de autorizare a unor astfel de măsuri trebuie să fie motivată și să facă trimitere la motive specifice pentru a crede că o infracțiune a fost comisă, este în curs de comitere sau în curs de pregătire, ori că au loc anumite activități care pun în pericol securitatea națională, militară, economică sau ecologică a țării, iar persoana vizată în cererea pentru măsuri operative de investigații este implicată în aceste activități criminale sau, din alte motive, periculoase.

43. Prin Decizia nr. 460-O-O din 15 iulie 2008, Curtea Constituțională a respins ca inadmisibilă o cerere pentru controlul constituționalității art. 5, art.11 și art.12 din LMOI. Instanța a considerat că persoana ale cărei comunicații au fost interceptate are posibilitatea de a depune o cerere de revizuire împotriva deciziei judecătorești de autorizare a interceptării. Pentru Curtea Constituțională, faptul că reclamantul nu avea la dispoziție o copie a deciziei judecătorești respective nu îl împiedica pe acesta să depună cererea de revizuire deoarece instanța sesizată putea solicita copie de la autoritățile competente.

2. Codul de procedură penală

44. Măsurile de cercetare penală care implică percheziționarea domiciliului unei persoane sau interceptarea convorbirilor telefonice și a altor comunicații ale acesteia sunt condiționate de obținerea unei autorizații judiciare prealabile. O cerere pentru percheziționarea domiciliului unei persoane sau interceptarea comunicațiilor acesteia trebuie să fie depusă de un investigator cu aprobarea unui procuror și să fie examinată de un judecător unic în termen de 24 de ore. Este permisă prezența procurorului și a investigatorului. Judecătorul care soluționează cererea hotărăște dacă se impune autorizarea măsurii solicitate sau, din contră, respingerea acesteia; acesta motivează decizia (art. 165 C. proc. pen.).

45. O instanță poate acorda autorizația de interceptare a comunicațiilor unui suspect sau învinuit ori ale unei alte persoane dacă există motive să se creadă că în comunicații ar putea fi menționate informații relevante pentru dosarul penal în litigiu (art. 186 alin. 1 C. proc. pen.).

46. O cerere de autorizare a interceptării comunicațiilor trebuie să menționeze în mod clar următoarele informații: 1) dosarul penal corespunzător cererii; 2) motivele care justifică aplicarea măsurilor solicitate; 3) numele de familie, numele patronimic și prenumele persoanei ale cărei comunicații trebuie interceptate; 4) durata măsurii solicitate; 5) organul de stat care va efectua interceptarea (art. 186 alin. 3 C. proc. pen.).

47. Decizia judecătorească de autorizare a interceptării comunicațiilor trebuie să fie transmisă de investigator organului de stat însărcinat cu punerea ei în aplicare. Interceptarea comunicațiilor poate fi autorizată pentru o perioadă de maxim 6 luni, iar investigatorul dispune încetarea măsurii atunci când aceasta nu mai este necesară. În orice caz, măsura trebuie să înceteze când se încheie cercetarea penală (art. 186 alin. 4 și 5 C. proc. pen.).

48. De asemenea, o instanță poate autoriza supravegherea datelor de comunicații corespunzătoare conexiunilor telefonice sau fără fir (*wireless*) ale unei persoane în cazul în care există motive întemeiate pentru a crede că acele date pot fi relevante într-un dosar penal. O cerere de autorizare trebuie să conțină elementele menționate la pct. 46 *supra*. O copie a deciziei judecătorești de autorizare a supravegherii datelor corespunzătoare comunicațiilor unei persoane este transmisă de investigator furnizorului de servicii de comunicații corespunzător; acesta din urmă este obligat apoi ca periodic, cel puțin o dată pe săptămână, să prezinte investigatorului datele solicitate. Supravegherea

datelor de comunicații poate fi autorizată pentru o perioadă de maxim 6 luni, iar investigatorul dispune încetarea măsurii atunci când aceasta nu mai este necesară. În orice caz, aceasta trebuie să înceteze când se încheie cercetarea penală (art. 186.1 C. proc. pen., introdus la 1 iulie 2010).

F. Păstrarea, utilizarea și distrugerea datelor colectate

1. Păstrarea datelor colectate

49. Art. 10 LMOI prevede că organele de aplicare a legii care efectuează măsuri operative de investigații pot crea și folosi baze de date sau pot deschide dosare personale. Un dosar personal se încheie atunci când obiectivele menționate la art. 2 din lege au fost îndeplinite sau în cazul în care se constată că acestea sunt imposibil de realizat.

50. În decizia din 14 iulie 1998 (menționată la pct. 40 *supra*), Curtea Constituțională a observat, cu privire la posibilitatea – prevăzută la art. 10 – ca organele de aplicare a legii care efectuează măsuri operative de investigații să creeze baze de date ori să deschidă dosare personale, că doar datele referitoare la prevenirea infracțiunilor sau la investigarea acestora pot fi introduse în aceste baze de date sau dosare personale. Instanța a adăugat că, din moment ce activitățile infracționale nu intră în sfera vieții private, colectarea de informații despre astfel de activități nu aduce atingere dreptului la respectarea vieții private. În final, instanța a precizat că, în cazul în care informațiile despre activitățile infracționale ale unei persoane introduse într-un dosar personal nu se confirmă ulterior, dosarul respectiv se încheie.

51. Înregistrările comunicațiilor telefonice și de alt tip interceptate trebuie să fie sigilate și păstrate în astfel de condiții încât să se evite orice risc de ascultare sau copiere de către persoane neautorizate (art. 8 alin. 4 LMOI).

52. Informațiile despre echipamentele folosite pentru punerea în aplicare a măsurilor operative de investigații, metodele utilizate, funcționarii implicați și datele colectate constituie secret de stat. Declasificarea acestora este posibilă numai în temeiul unei decizii speciale a șefului organului de stat care efectuează măsurile operative de investigații (art. 12 alin. 1 LMOI și art. 5 alin. 4 din Legea nr. 5485-I din 21 iulie 1993 privind secretele de stat).

53. Pe documentele care conțin secrete de stat se afișează în mod vizibil următoarele informații: nivelul de secretizare, organul de stat care emite decizia de clasificare, numărul de înregistrare și data sau condițiile de declasificării (art. 12 din Legea privind secretele de stat).

2. Utilizarea datelor colectate și condițiile divulgării lor

54. Informațiile care conțin secrete de stat nu pot fi divulgate altui serviciu de stat, unei organizații sau unei persoane decât cu aprobarea serviciului de stat care a emis decizia de clasificare a acestor informații. Acestea nu pot fi comunicate decât serviciilor de stat sau organizațiilor autorizate special în acest sens ori persoanelor care au certificatul de securitate necesar. Serviciul de stat sau organizația care primește informații clasificate trebuie să se asigure că acestea sunt protejate în mod corespunzător. Șeful serviciului de stat sau al organizației în cauză este personal răspunzător pentru protecția informațiilor clasificate împotriva accesului neautorizat sau a divulgării neautorizate (art. 16 și 17 din Legea privind secretele de stat).

55. Numai o organizație sau o întreprindere despre care s-a confirmat faptul că dispune de servicii interne destinate în special protecției datelor, că angajații lor sunt calificați să se ocupe de informații clasificate și că folosesc sisteme agreate pentru protecția datelor pot primi autorizație să acceseze secrete de stat (art. 27 din Legea privind secretele de stat).

56. Certificatul de securitate se acordă numai funcționarilor statului care au cu adevărat nevoie de așa ceva pentru a-și îndeplini sarcinile. De asemenea, certificatul se acordă judecătorilor pe durata mandatelor acestora și avocaților implicați într-o cauză penală dacă dosarul conține elemente legate de secrete de stat. Orice persoană care a primit certificat de securitate trebuie să se angajeze, în scris, să nu comunice informațiile clasificate care i-au fost încredințate (pct. 7, 11 și 21 din Regulamentul nr. 63 adoptat la 6 februarie 2010 de Guvernul Federației Ruse).

57. Șeful serviciului de stat sau al organizației care deține informații ce conțin secrete de stat trebuie să asigure accesul la aceste informații funcționarilor statului și altor persoane autorizate. Acesta trebuie să se asigure că numai informațiile necesare sunt comunicate destinatarului pentru îndeplinirea obligațiilor sale (art. 25 din Legea privind secretele de stat).

58. În cazul în care datele colectate în cadrul măsurilor operative de investigații conțin informații cu privire la comiterea unei infracțiuni, aceste informații și toate elementele justificative necesare (fotografii și înregistrări audio sau video, de exemplu) se comunică serviciilor de investigații competente sau unei instanțe. În cazul în care informațiile au fost colectate în cadrul unor măsuri operative de investigații care implică o ingerință în dreptul la respectarea caracterului privat al comunicațiilor poștale, telegrafice și de alt tip transmise printr-o rețea de telecomunicații ori prin

servicii de curierat, sau o ingerință în caracterul privat al domiciliului, acestea se comunică serviciilor de cercetare sau de urmărire penală, ca și decizia judecătorească de autorizare a măsurilor respective. Informațiile se transmit în conformitate cu procedura specială prevăzută pentru prelucrarea informațiilor clasificate, cu excepția cazului în care organul de stat care a pus în aplicare măsurile operative de investigații a decis să le declassifice (pct. 1, 12, 14 și 16 din Ordinul nr. 776/703/509/507/1820/42/535/ 398/68 din 27 septembrie 2013 al Ministerului de Interne).

59. În cazul în care persoana ale cărei comunicații telefonice și de alt tip au fost interceptate este inculpată pentru o infracțiune, înregistrările se transmit investigatorului și se depun la dosarul penal. Utilizarea și păstrarea lor ulterioară sunt reglementate de normele de procedură penală (art. 8 alin. 5 LMOI).

60. Datele colectate în cadrul unor măsuri operative de investigații pot fi folosite pentru pregătirea și desfășurarea unei cercetări și proceduri judiciare și ca probe în cadrul unei proceduri penale, în conformitate cu prevederile legale privind adunarea, evaluarea și examinarea probelor. Decizia de a transmite datele colectate altor organe de aplicare a legii sau unei instanțe revine șefului organului de stat care a efectuat măsurile operative de investigații (art. 11 LMOI).

61. În cazul în care interceptarea a fost autorizată în cadrul unei proceduri penale, investigatorul poate, în orice moment al perioadei prevăzute în autorizația de interceptare, să obțină înregistrările de la organul care efectuează interceptarea. Înregistrările trebuie să fie sigilate și însoțite de o scrisoare care indică data și ora începerii și încheierii comunicațiilor înregistrate, precum și mijloacele tehnice folosite la interceptare. Înregistrările trebuie să fie ascultate de investigator în prezența martorilor asistenți, a unui expert - după caz - și a persoanelor ale căror comunicații au fost interceptate. Investigatorul întocmește un proces-verbal care conține transcrierea integrală a acelor părți din comunicațiile înregistrate care sunt relevante pentru cauza penală respectivă (art. 186 alin. 6 și 7 C. proc. pen.). La 4 martie 2013, art. 186 alin. 7 a fost modificat, eliminându-se dispoziția referitoare la prezența martorilor asistenți.

62. Înregistrările și datele referitoare la comunicațiile care au fost colectate se depun la dosarul penal. Acestea trebuie să fie sigilate și păstrate în condiții suficiente pentru a preveni orice risc de ascultare sau de copiere de către persoane neautorizate (art. 186 alin. 8 C. proc. pen. și art. 186.1, introdus la 1 iulie 2010).

63. Rezultatele măsurilor operative de investigații care implică o restrângere a dreptului la respectarea corespondenței ori a comunicațiilor telefonice, poștale, telegrafice sau de alt tip pot servi ca probe în cadrul unei proceduri penale doar dacă au fost obținute în temeiul unei decizii judecătorești și dacă măsurile respective au fost puse în aplicare în conformitate cu normele de procedură penală (pct. 14 din hotărârea nr. 8 pronunțată la 31 octombrie 1995 de plenul Curții Supreme a Federației Ruse).

64. Se interzice utilizarea ca probe a datelor care, fiind colectate în cadrul unor măsuri operative de investigații, nu respectă normele din Codul de procedură penală cu privire la admisibilitatea probelor (art. 89 C. proc. pen.). Probele obținute prin încălcarea Codului de procedură penală nu sunt admisibile. Probele inadmisibile sunt lipsite de valoare juridică și nu pot servi ca temei al unor acuzații în materie penală sau pentru a clarifica vreuna din circumstanțele pentru care trebuie prezentate probe în cadrul unei proceduri penale. Probele care au fost respinse de o instanță nu au valoare juridică și nu pot fi invocate într-o hotărâre sau decizie judecătorească și nici examinate sau utilizate în cursul procesului (art. 75 și art. 35 C. proc. pen.).

3. Distrugerea datelor colectate

65. Datele colectate în cadrul măsurilor operative de investigații cu privire la o persoană a cărei vinovăție nu a fost stabilită conform legii se păstrează timp de 1 an după care se distrug, cu excepția cazului în care sunt necesare în interesul serviciului sau al justiției. Înregistrările audio și alte materiale colectate prin interceptarea comunicațiilor telefonice sau de alt tip se păstrează timp de 6 luni, după care se distrug – dacă persoana vizată nu a fost inculpată pentru o infracțiune. Judecătorul care a autorizat interceptarea trebuie să fie informat cu 3 luni înainte de distrugerea planificată (art. 5 alin. 7 LMOI).

66. Dacă persoana vizată a fost inculpată pentru o infracțiune, la sfârșitul procesului penal, judecătorul de fond decide păstrarea sau distrugerea datelor utilizate ca probe. Distrugerea se consemnează într-un raport care va fi semnat de șeful serviciului de investigații și va fi depus la dosarul cauzei (art. 81 alin. 3 C. proc. pen. și pct. 49 din Ordinul nr. 142 din 30 septembrie 2011 al Comisiei de investigații).

G. Controlul asupra interceptării comunicațiilor

67. Șefii organelor care pun în aplicare măsuri operative de investigații sunt răspunzători personal de legalitatea tuturor acestor măsuri (art. 22 LMOI).

68. Controlul general asupra măsurilor operative de investigații se exercită de către Președinte, Parlament și Guvernul Federației Ruse în limitele competențelor lor respective (art. 20 LMOI).
69. Procurorul General și procurorii din subordine competenți pot controla, de asemenea, măsurile operative de investigații. La cererea procurorului competent, șeful organului de stat care pune în aplicare măsuri operative de investigații trebuie să prezinte materialul referitor la aceste măsuri, inclusiv dosarele personale, informațiile despre echipamentul tehnic folosit, registrele și instrucțiunile interne. Materialul care conține informații despre investigatori sub acoperire sau informatori ai poliției poate fi comunicat procurorului numai cu acordul funcționarului sau informatorului respectiv, cu excepția cazurilor de proceduri penale îndreptate împotriva funcționarului sau informatorului respectiv. Răspunderea șefului unui organ de stat poate fi angajată în temeiul legii dacă acesta nu se conformează cererii procurorului. Acesta trebuie să asigure protecția datelor conținute în materialul prezentat (art. 21 LMOI).
70. Legea privind organizarea parchetului (Legea federală nr. 2202-I din 17 ianuarie 1992) prevede că procurorul general este numit și, după caz, demis de Consiliul Federației (Camera superioară a Parlamentului) la propunerea Președintelui (art. 12). Procurorii din subordine sunt numiți de procurorul general după consultarea cu autoritățile executive regionale (art. 13). Pentru a fi numit procuror, persoana trebuie să aibă cetățenie rusă și o diplomă în drept rus (art. 40.1).
71. Pe lângă funcțiile lor de urmărire penală, procurorii sunt însărcinați să se asigure că administrația centrelor de detenție, activitățile executorilor judecătorești, măsurile operative de investigații și urmărirea penală respectă Constituția și legislația Rusiei (art. 1). De asemenea, aceștia coordonează activitățile tuturor serviciilor de aplicare a legii în lupta împotriva criminalității (art. 8).
72. În privința controlului asupra măsurilor operative de investigații, procurorii pot verifica dacă actele efectuate în cursul punerii în aplicare a acestor măsuri au respectat legalitatea și drepturile omului (art. 29). Dispozițiile emise de procurori în cadrul acestui control se aplică în termenul stabilit. Neîndeplinirea acestei obligații poate duce la angajarea răspunderii potrivit legii (art. 6).
73. De asemenea, procurorii pot examina plângerile privind încălcarea legii; aceștia soluționează orice plângere prin decizie motivată. Această decizie nu împiedică persoana interesată să depună o plângere identică la o instanță de judecată. În cazul în care un procuror constată o încălcare a legii, acesta trebuie să ia măsuri pentru a declanșa o acțiune împotriva autorilor încălcării (art. 10).
74. Legea privind FSB din 3 aprilie 1995 (nr. 40-FZ) prevede că informațiile referitoare la investigatorii sub acoperire ai serviciilor de securitate, precum și cele referitoare la tacticile, metodele și mijloacele folosite de aceștia, nu intră în sfera controlului exercitat de procurori (art. 24).
75. Procedurile privind controlul exercitat de procurori asupra măsurilor operative de investigații sunt stabilite în Ordinul Procurorului General nr. 33 din 15 februarie 2011.
76. Această instrucțiune prevede că un procuror poate supune organele care pun în aplicare măsuri operative de investigații unor inspecții sistematice, dar și unor inspecții *ad-hoc* în cazul unei plângeri făcute de o persoană fizică ori în cazul primirii de informații privind eventuale încălcări. Măsurile operative de investigații întreprinse de FSB în contextul contra-informațiilor pot fi supuse inspecției numai în urma unei plângeri individuale (pct. 5 din Ordinul nr. 33).
77. În timpul inspecției, procurorul se asigură de îndeplinirea următoarelor cerințe:
- respectarea drepturilor constituționale ale cetățenilor, precum dreptul la respectarea vieții private și de familie, a domiciliului, a corespondenței, a comunicațiilor telefonice, poștale, telegrafice și de alt tip;
 - caracterul legal și justificat al actelor efectuate în cadrul măsurilor operative de investigații, inclusiv al celor care au fost autorizate de o instanță (pct. 4 și 6 din Ordinul nr. 33).
78. În timpul inspecției, procurorul trebuie să examineze materialul original referitor la măsurile operative de investigații, inclusiv dosarele personale, informațiile despre echipamentul tehnic folosit, registrele și instrucțiunile interne; acesta poate cere explicații funcționarilor competenți. Acesta este obligat să protejeze datele sensibile care îi sunt încredințate împotriva accesului neautorizat sau a divulgării neautorizate (pct. 9 și 12 din Ordinul nr. 33).
79. În cazul în care procurorul constată o încălcare a legii, trebuie să ceară funcționarului responsabil pentru aceasta să o remedieze. De asemenea, acesta trebuie să ia măsuri pentru a opri și a remedia încălcarea drepturilor cetățenilor și pentru a întreprinde o acțiune împotriva autorilor infracțiunii (pct. 9 și 10 din Ordinul nr. 33). Un funcționar al statului care refuză să se conformeze instrucțiunilor unui procuror poate fi supus acțiunilor prevăzute de lege (pct. 11).
80. Procurorul însărcinat cu controlul asupra măsurilor operative de investigații prezintă procurorului general rapoarte semestriale care prezintă detaliat rezultatele inspecțiilor efectuate (pct. 15 din Ordinul nr. 33). Modelul de raport care trebuie completat de procuror este anexat la Ordinul nr. 33. Purtând mențiunea „confidențial”, acest document are două părți, ambele fiind prezentate sub formă de tabel. Prima parte se referă la inspecțiile efectuate în perioada de referință și trebuie să prezinte informații despre numărul de inspecții realizate, dosarele controlate și încălcările depistate. Partea a doua, care se ocupă de plângerile depuse de persoane fizice, trebuie să conțină informații despre numărul de plângeri examinate și admise.

H. Accesul unei persoane fizice la datele colectate despre sine prin interceptarea comunicațiilor

81. Dreptul rus nu prevede obligația de a informa o persoană, în vreo etapă, despre interceptarea comunicațiilor sale. Cu toate acestea, o persoană care are cunoștință de fapte referitoare la măsuri operative de investigații la care a fost supusă, și a cărei vinovăție nu a fost dovedită conform legii – cu alte cuvinte, nu a fost inculpată sau acuzațiile au fost retrase pe motiv că presupusa infracțiune nu a fost săvârșită sau că lipsesc unul sau mai multe dintre elementele constitutive ale unei infracțiuni – are dreptul la informații despre datele colectate în cadrul măsurilor respective, cât timp acest lucru este compatibil cu normele privind confidențialitatea operativă („конспирации”) și excluzându-se datele care ar putea permite divulgarea secretelor de stat (art. 5 alin. 4-6 LMOI).

82. În decizia din 14 iulie 1998 (*supra*, pct. 40), Curtea Constituțională a constatat că orice persoană care are cunoștință de fapte referitoare la măsuri operative de investigații la care a fost supusă are dreptul să primească informații despre datele colectate în cadrul acestor măsuri, cu excepția cazului în datele respective conțin secrete de stat. Înalta instanță a declarat că, în temeiul art. 12 din LMOI, datele colectate în cadrul acestor măsuri – de exemplu, informații despre infracțiuni și persoanele implicate în comiterea lor – constituie secret de stat. Cu toate acestea, instanța a precizat că informațiile referitoare la ingerințe în drepturile cetățenilor sau la acte ilegale comise de autorități nu pot fi clasificate ca secret sub stat și trebuie să fie divulgate. Aceasta a adăugat că, prin urmare, nu se poate invoca art. 12 pentru a refuza accesul la informații care afectează drepturile unei persoane, cu excepția cazului în care informațiile respective privesc obiectivele sau motivele măsurilor operaționale de investigații. În concluzie, în opinia Înaltei instanțe, faptul că în conformitate cu legea atacată o persoană nu poate pretinde acces la toate datele colectate despre sine nu constituie o încălcare a drepturilor constituționale ale acestei persoane.

I. Controlul jurisdicțional

1. Dispozițiile generale din LMOI cu privire la controlul jurisdicțional asupra interceptării comunicațiilor

83. O persoană care consideră că drepturile sale au fost ori sunt încălcate de un funcționar al statului în cadrul aplicării măsurilor operative de investigații poate depune plângere la superiorul ierarhic al acestui funcționar, la parchet sau la instanță. Dacă drepturile unei persoane au fost încălcate de un funcționar al statului în cadrul aplicării măsurilor operative de investigații, superiorul ierarhic al acestuia, procurorul sau instanța trebuie să ia măsuri pentru repararea încălcării și despăgubirea persoanei respective (art. 5 alin. 3 și 9 LMOI).

84. Dacă unei persoane i se refuză accesul la informații privind datele colectate despre sine în cadrul măsurilor operative de investigații, aceasta are dreptul să cunoască motivele refuzului și poate face plângere împotriva acestei decizii la instanță. Sarcina probei revine organelor de aplicare a legii, care trebuie să demonstreze că refuzul este justificat. În vederea unui control complet și aprofundat, organul de aplicare a legii care este însărcinat cu măsurile operative de investigații trebuie, la solicitarea judecătorului, să prezinte materialul aferent măsurilor operative de investigații conținând informații despre datele la care s-a refuzat accesul, cu excepția informațiilor privind investigatorii sub acoperire sau informatorii poliției. În cazul în care instanța consideră nejustificată neacordarea accesului, aceasta poate solicita organului de aplicare a legii să comunice materialul respectiv persoanei în cauză (art. 5 alin. 4-6 LMOI).

85. În decizia din 14 iulie 1998 (*supra*, pct. 40), Curtea Constituțională a hotărât că o persoană care află că a fost supusă unor măsuri operative de investigații și consideră că actele funcționarilor statului i-au încălcat drepturile poate, în temeiul art. 5 LMOI, să conteste în instanță motivele pentru aplicarea măsurilor respective, precum și actele specifice efectuate de serviciile competente în cadrul acestor măsuri, inclusiv cele care au fost autorizate de o instanță.

86. În ceea ce privește aspectele procedurale, Curtea Constituțională a declarat că, într-o procedură în care sunt atacate motivele măsurilor operative de investigații sau ale actelor autorităților competente în cadrul aplicării acestor măsuri, ca și într-o procedură având ca obiect neacordarea accesului la datele colectate, organele de aplicare a legii trebuie să prezinte judecătorului, la cererea acestuia din urmă, orice material relevant referitor la măsurile operative de investigații, cu excepția elementelor care conțin informații despre investigatorii sub acoperire sau informatorii ai poliției.

87. O persoană care dorește să facă plângere împotriva interceptării comunicațiilor sale poate să solicite un control jurisdicțional în temeiul art. 125 C. proc. pen., să solicite un control jurisdicțional în temeiul capitolului 25 din Codul de procedură civilă și al Legii privind controlul jurisdicțional, înlocuite din data de 15 septembrie 2015 prin Codul de procedură administrativă, ori să introducă o acțiune în răspundere în conformitate cu art. 1069 din Codul civil.

2. Cererea de control jurisdicțional în temeiul art. 125 C. proc. pen.

88. În hotărârea nr. 1 din 10 februarie 2009, Plenul Curții Supreme a declarat că actele funcționarilor sau organelor statului care efectuează măsuri operative de investigații la cererea unui investigator pot fi contestate conform procedurii prevăzute la art. 125 C. proc. pen. (pct. 4). Plângerile întemeiate pe această dispoziție pot fi examinate numai în contextul unei urmăriri penale în desfășurare. În cazul în care cauza a fost înaintată instanței de judecată, judecătorul declară plângerea inadmisibilă și informează reclamantul că va putea depune plângere la instanța de fond competentă (pct. 9).

89. Art. 125 C. proc. pen. prevede controlul jurisdicțional asupra deciziilor și actelor sau omisiunilor unui investigator sau procuror care sunt de natură să aducă atingere drepturilor sau libertăților constituționale ale participanților la o procedură penală. Cu excepția unei dispoziții contrare din partea investigatorului, procurorului sau a instanței, depunerea unei plângeri nu are efect suspensiv asupra deciziei atacate ori a actului atacat. Instanța examinează plângerea în termen de 5 zile. Autorul plângerii, avocatul său, investigatorul și procurorul pot asista la ședință. Reclamantul trebuie să-și justifice plângerea (art. 125 alin. 1-4 C. proc. pen.).

90. Părțile prezente pot să studieze tot materialul prezentat instanței și să prezinte probe suplimentare referitoare la plângere. Divulgarea elementelor dosarului penal nu este permisă decât în cazul în care aceasta nu contravine intereselor cercetării penale și nu încalcă drepturile participanților la procedura penală. Judecătorul poate invita părțile să prezinte probele pe care se bazează decizia atacată, sau orice altă probă relevantă (pct. 12 din hotărârea nr. 1 din 10 februarie 2009 a Plenului Curții Supreme a Federației Ruse).

91. După examinarea plângerii, instanța fie respinge plângerea, fie constată caracterul nelegal sau nejustificat al deciziei, actului sau omisiunii în litigiu și dispune ca funcționarul răspunzător să remedieze neregula constatată (art. 125 alin. 5 C. proc. pen.). În cazul în care dispune ca funcționarul să remedieze neregula constatată, instanța nu poate să îi impună adoptarea unei anumite măsuri, dar nici să anuleze ori să impună funcționarului să anuleze decizia care este declarată ilegală sau nejustificată (pct. 21 din hotărârea nr. 1 din 10 februarie 2009 a Plenului Curții Supreme a Federației Ruse).

3. Cererea de control jurisdicțional întemeiată pe capitolul 25 din Codul de procedură civilă, Legea privind controlul jurisdicțional și Codul de procedură administrativă

92. Conform hotărârii nr. 2 din 10 februarie 2009 a Plenului Curții Supreme a Federației Ruse, plângerile împotriva deciziilor sau actelor funcționarilor sau organelor care întreprind măsuri operative de investigații ce nu pot fi contestate în cadrul unei proceduri penale, ca și plângerile împotriva neacordării de acces la informații despre datele colectate în cadrul măsurilor operative de investigații pot fi examinate în conformitate cu procedura prevăzută în capitolul 25 din Codul de procedură civilă (C. proc. civ.) (pct. 7).

93. Capitolul 25 C. proc. civ., în vigoare până la 15 septembrie 2015, a definit procedura pentru examinarea plângerilor împotriva deciziilor și actelor funcționarilor care încalcă drepturile și libertățile cetățenilor, procedură care a fost detaliată în Legea nr. 4866-1 din 27 aprilie 1993 privind controlul jurisdicțional asupra deciziilor și actelor care încalcă drepturile și libertățile cetățenilor (*Legea privind controlul jurisdicțional*). La 15 septembrie 2015, capitolul 25 C. proc. civ. și Legea privind controlul jurisdicțional au fost abrogate și înlocuite prin Legea nr. 21-FZ din 8 martie 2015 (Codul de procedură administrativă, C. proc. admin.), care a intrat în vigoare la acea dată. Codul de procedură administrativă, în esență, a confirmat și a clarificat dispozițiile din capitolul 25 C. proc. civ. și din Legea privind controlul jurisdicțional.

94. Codul de procedură civilă, Legea privind controlul jurisdicțional și Codul de procedură administrativă prevăd că un cetățean poate depune plângere la o instanță cu privire la un act sau o decizie a unui serviciu sau funcționar al autorităților centrale ori locale în cazul în care consideră că actul sau decizia i-au încălcat drepturile și libertățile (art. 254 C. proc. civ. și art. 1 Legea privind controlul jurisdicțional). Plângerea poate viza orice decizie, act sau omisiune care a încălcat drepturile sau libertățile cetățeanului, l-a împiedicat pe acesta să-și exercite drepturile și libertățile, sau i-a impus o obligație sau responsabilitate (art. 255 C. proc. civ., art. 2 Legea privind controlul jurisdicțional și art. 218 alin. 1 C. proc. admin.).

95. Plângerea se depune la o instanță de drept comun în termen de 3 luni de la data la care autorul ei a luat cunoștință de încălcarea drepturilor sale. Termenul se poate prelungi pentru motive întemeiate (art. 254 C. proc. civ., art. 4-5 din Legea privind controlul jurisdicțional și art. 218 alin. 5 și art. 219 alin. 1 și 7 C. proc. admin.). Plângerea trebuie să indice numărul de înregistrare și data deciziei atacate sau data și locul comiterii actului în litigiu (art. 220 alin. 2 pct. 3 C. proc. admin.). Autorul plângerii trebuie să prezinte documente justificative ori să explice de ce nu este în măsură să le prezinte (art. 220 alin. 2 pct. 8 și alin. 3 C. proc. admin.). În cazul în care autorul plângerii nu-și îndeplinește obligațiile de mai sus, judecătorul declară plângerea inadmisibilă (art. 222 alin. 3 C. proc. admin.).

admin.).

96. Serviciul sau funcționarul vizat este cel care are sarcina de a dovedi legalitatea deciziei, a actului sau a omisiunii în litigiu. La rândul său, autorul plângerii trebuie să demonstreze că decizia, actul sau omisiunea i-a încălcat drepturile și libertățile (art. 6 din Legea privind controlul jurisdicțional și art. 226 alin. 11 C. proc. admin.).

97. Conform Codului de procedură civilă, plângerea se examinează în termen de 10 zile (art. 257 C. proc. civ.), deși Codul de procedură administrativă prevede în prezent un termen de 2 luni (art. 226 alin. 1 C. proc. admin.). În cazul în care consideră plângerea justificată, instanța pronunță o decizie prin care anulează decizia sau actul în litigiu și obligă serviciul sau funcționarul în cauză să remedieze în totalitate ingerința în drepturile reclamantului (art. 258 alin. 1 C. proc. civ., art. 7 din Legea privind controlul jurisdicțional și art. 227 alin. 2 și 3 C. proc. admin.). Instanța poate stabili termenul în care trebuie să fie reparată încălcarea și/sau să definească măsurile speciale pentru a repara în totalitate încălcarea (pct. 28 din hotărârea nr. 2 din 10 februarie 2009 a Plenului Curții Supreme a Federației Ruse și art. 227 alin. 3 C. proc. admin.). Autorul plângerii poate apoi, în cadrul unei acțiuni civile separate, să solicite repararea prejudiciului material sau moral suferit (art. 7 din Legea privind controlul jurisdicțional).

98. Instanța poate respinge plângerea în cazul în care consideră că actul sau decizia în litigiu aparține unui serviciu sau funcționar competent, are caracter legal și nu încalcă drepturile reclamantului (art. 258 alin. 4 C. proc. civ. și art. 226 alin. 9 și art. 227 alin. 2 C. proc. admin.).

99. O parte la proces poate declara apel la o instanță superioară (art. 336 C. proc. civ. în versiunea în vigoare până la 1 ianuarie 2012, art. 320 C. proc. civ. în versiunea în vigoare de la această dată și art. 228 C. proc. admin.). Decizia pronunțată în apel intră în vigoare la data emiterii sale (art. 367 C. proc. civ. în versiunea în vigoare până la 1 ianuarie 2012, art. 329 alin. 5 în versiunea în vigoare de la această dată și art. 186 și art. 227 alin. 5 C. proc. admin.).

100. Codul de procedură civilă prevedea că decizia judecătorească prin care se admite o plângere și se impune unui serviciu sau funcționar să repare încălcarea drepturilor unui cetățean trebuie să fie adresată șefului serviciului respectiv, funcționarului respectiv ori superiorilor acestora în termen de 3 zile de la data intrării în vigoare (art. 258 alin. 2 C. proc. civ.). Legea privind controlul jurisdicțional prevedea trimiterea deciziei judecătorești în termen de 10 zile de la data intrării în vigoare (art. 8). Codul de procedură administrativă prevede că decizia judecătorească se trimite în ziua intrării în vigoare (art. 227 alin. 7). Instanța de judecată și autorul plângerii trebuie să fie informați cu privire la executarea deciziei în luna următoare primirii acesteia (art. 258 alin. 3 C. proc. civ., art. 8 din Legea privind controlul jurisdicțional și art. 227 alin. 9 C. proc. admin.).

4. Acțiunea în răspundere întemeiată pe art. 1069 din Codul civil

101. Un prejudiciu cauzat unei persoane sau bunurilor acesteia atrage după sine o despăgubire integrală din partea autorului prejudiciului. Acesta nu este obligat să ofere despăgubire în cazul în care dovedește că prejudiciul nu este cauzat din vina sa (art. 1064 alin. 1 și 2 din Codul civil).

102. Organele și funcționarii autorităților centrale și locale sunt răspunzătoare pentru orice prejudiciu cauzat unui cetățean ca urmare a acțiunilor sau omisiunilor lor nelegale (art. 1069 C. civ.). Indiferent dacă există sau nu o eroare a unui funcționar, Trezoreria federală sau regională este obligată să repare orice prejudiciu cauzat unui cetățean ca urmare i) a unei condamnări sau urmăriri penale ilegale, ii) a aplicării ilegale a unei măsuri preventive, sau iii) a unei sancțiuni administrative ilegale (art. 1070 C. civ.).

103. O instanță poate impune autorului prejudiciului obligația de a repara prejudiciul moral (suferință fizică sau morală). Despăgubirea pentru prejudiciul moral nu este legată de eventuala reparație a prejudiciului material (art. 151 alin. 1 și art. 1099 C. civ.). Quantumul despăgubirii se stabilește în funcție de gravitatea culpei comise de autorul prejudiciului, dar și în funcție de alte elemente importante. De asemenea, instanța ține seama de amploarea suferinței fizice sau morale, având în vedere caracteristicile victimei (art. 151 alin. 2 și art. 1101 C. civ.).

104. Indiferent de existența unei culpe a autorului prejudiciului, prejudiciul moral necesită reparație dacă a fost cauzat i) printr-un echipament periculos, ii) ca urmare a unei condamnări sau urmăriri penale ilegale sau a aplicării ilegale a unei măsuri preventive ori a unei sancțiuni administrative ilegale, sau iii) prin difuzarea de informații care au adus atingere onoarei, demnității sau reputației unei persoane (art. 1100 C. civ.).

105. Într-o procedură civilă, sarcina probei revine celui care afirmă, dacă nu există prevederi contrare în legislația federală (art. 56 alin. 1 C. proc. civ.).

5. Acțiunea introdusă la Curtea Constituțională

106. Conform Legii privind Curtea Constituțională (Legea nr. 1-FKZ din 21 iulie 1994), în cazul în care instanța constituțională pronunță într-o hotărâre o opinie pentru a stabili dacă interpretarea dată unei prevederi legale în practica organelor judiciare și de aplicare a legii este în concordanță cu

Constituția, opinia trebuie să fie aplicată de instanțe și organele de aplicare a legii cu începere de la data pronunțării hotărârii (art. 79 alin. 5).

J. Obligațiile furnizorilor de servicii de comunicație

1. Obligația de protejare a datelor cu caracter personal și a caracterului privat al comunicațiilor

107. În conformitate cu Legea privind comunicațiile, furnizorii de servicii de comunicații trebuie să asigure respectarea caracterului privat al comunicațiilor. Informațiile privind comunicațiile transmise prin intermediul rețelelor de telecomunicații sau al serviciilor de curierat și conținutul acestor comunicații nu pot fi divulgate decât expeditorului și destinatarului sau reprezentanților autorizați ai acestora, cu excepția cazurilor prevăzute de legislația federală (art. 63 alin. 2 și 4 din Legea privind comunicațiile).

108. Informațiile despre abonați și serviciile furnizate acestora sunt confidențiale. Informațiile despre un abonat includ: numele de familie, patronimul, prenumele și supranumele, dacă este persoană fizică; denumirea societății, precum și numele de familie, patronimele și prenumele directorului și ale angajaților, dacă este persoană juridică; adresa și numărul abonatului și alte informații pentru a putea identifica persoana vizată sau terminalul acesteia; datele conținute în bazele de date de plată, inclusiv informațiile privind comunicațiile, traficul și plățile abonatului. Informațiile despre un abonat nu pot fi dezvăluite unor terți fără consimțământul abonatului, cu excepția cazurilor prevăzute de legislația federală (art. 53 din Legea privind comunicațiile).

2. Obligația de colaborare cu organele de aplicare a legii

109. Legea privind comunicațiile impune furnizorilor de servicii de comunicații obligația de a furniza organelor de aplicare a legii, în cazurile prevăzute de legislația federală, informații despre abonați și serviciile de care beneficiază, precum și orice altă informație necesară organelor respective pentru a-și atinge scopurile și obiectivele (art. 64 alin. 1 din Legea privind comunicațiile).

110. La 31 martie 2008, Consiliul Municipiului Moscova a examinat o propunere de modificare a art. 64 alin. 1 din Legea privind comunicațiile, urmărind să oblige organele de aplicare a legii să prezinte o autorizație judiciară furnizorilor de servicii de comunicații cărora le cer informații despre abonați. Reprezentanții FSB și ai Ministerului de Interne au comunicat celor prezenți că o decizie judecătorească de autorizare a interceptării este un document clasificat care, prin urmare, nu poate fi prezentat furnizorilor de servicii de comunicații. În consecință, modificarea propusă a fost respinsă.

111. Furnizorii de servicii de comunicații trebuie să se asigure că rețelele și echipamentele lor sunt conforme cu specificațiile tehnice stabilite de Ministerul Comunicațiilor în colaborare cu organele de aplicare a legii. De asemenea, furnizorii de servicii de comunicații trebuie să se asigure că metodele și tacticile folosite de aceste organe sunt confidențiale (art. 64 alin. 2 din Legea privind comunicațiile).

112. În cazurile prevăzute de legislația federală, un furnizor de servicii de comunicații este obligat să suspende serviciile sale către un abonat la primirea unui ordin scris și motivat în acest sens, emis de șeful unui organ de aplicare a legii care întreprinde măsuri operative de investigații sau apără securitatea națională (art. 64 alin. 3 din Legea privind comunicațiile).

113. Legea privind FSB obligă furnizorii de servicii de comunicații să instaleze un echipament care să permită FSB să efectueze măsuri operative de investigații (art. 15).

3. Specificațiile tehnice privind echipamentul pe care furnizorii de servicii de comunicații trebuie să îl instaleze

114. Principalele caracteristici ale sistemului de instalații tehnice pentru punerea în aplicare a măsurilor operative de investigații (*Система технических средств для обеспечения функций оперативно-разыскных мероприятий „СОПМ” – „SORM”*) sunt prezentate în câteva ordine și regulamente emise de Ministerul Comunicațiilor.

a) Ordinul nr. 70

115. Ordinul nr. 70 privind specificațiile tehnice pentru sistemul de instalații tehnice pentru punerea în aplicare a măsurilor operative de investigații în cadrul rețelelor de telecomunicații, emis de Ministerul Comunicațiilor la 20 aprilie 1999, prevede că echipamentul instalat de furnizorii de servicii de comunicații trebuie să îndeplinească anumite specificații prezentate în anexele ordinului. Acest ordin, inclusiv anexele, a fost publicat în revista oficială a Ministerului Comunicațiilor *SvyazInform*, distribuit pe bază de abonament. Acesta poate fi accesat și printr-o bază de date juridică și privată disponibilă pe internet, care l-a preluat de la *SvyazInform*.

116. Anexele nr. 1 și 3 descriu specificațiile tehnice ale SORM cu privire la rețelele de telefonie

mobilă. Acestea precizează că interceptarea comunicațiilor se efectuează de către un organ de aplicare a legii de la un terminal de control la distanță conectat la echipamentul de interceptare instalat de operatorul rețelei de telefonie mobilă. Acest echipament trebuie să permită în special: a) crearea unor baze de date privind persoanele supuse interceptărilor, care se administrează de la terminalul de control la distanță; b) interceptarea comunicațiilor și transmiterea datelor astfel colectate la terminalul de control la distanță; c) protejarea datelor împotriva oricărui acces neautorizat, inclusiv din partea angajaților operatorului rețelei de telefonie mobilă; d) asigurarea accesului la bazele de date cu adresele abonaților (pct. 1.1. și 1.6 din actul adițional nr.1).

117. Mai precis, echipamentul trebuie să permită: a) interceptarea tuturor apelurilor primite și efectuate de persoana supusă interceptării; b) accesul la informațiile privind locul unde se află aceasta; c) menținerea capacității de interceptare în cazul în care o conexiune în curs este transferată de la rețeaua unui operator de rețea de telefonie mobilă la cea a altui operator; d) menținerea capacității de interceptare în cazul utilizării unor servicii suplimentare, cum ar fi redirectionarea apelului, transferul apelului sau conferința multiplă, cu posibilitatea de a înregistra numărul sau numerele la care apelul este direcționat; e) colectarea datelor de comunicații pentru orice tip de conexiune – fax, mesagerie (SMS) sau orice alt tip; f) accesul la informații privind serviciile furnizate persoanei supuse interceptării (pct. 2.1.2 din Anexa nr. 1).

118. Există două tipuri de interceptare: „interceptarea totală” și „supravegherea statistică”. Interceptarea totală este interceptarea, în timp real, a datelor și conținutului tuturor comunicațiilor primite sau efectuate de persoana supusă interceptării. Supravegherea statistică este supravegherea, în timp real, doar a datelor de comunicații, fără interceptarea conținutului comunicațiilor. Datele de comunicații includ numărul de telefon apelat, data și ora de începere și de încheiere a conexiunii, serviciile suplimentare utilizate, locul unde se află persoana supusă interceptării și starea conexiunii sale (pct. 2.2 și 2.4 din actul adițional nr. 1).

119. Echipamentul montat trebuie să permită începerea interceptării comunicațiilor în 30 de secunde de la primirea unei dispoziții de la terminalul de control la distanță (pct. 2.5 din Anexa nr. 1).

120. Informațiile despre persoanele supuse interceptărilor sau despre transmiterea de date către terminalul de control la distanță nu pot fi consemnate ori înregistrate (pct. 5.4 din Anexa nr. 1).

121. Terminalul de control la distanță recepționează de la operatorul rețelei mobile o parolă care îi acordă acces total la SORM. În continuare, terminalul schimbă parola pentru a împiedica persoanele neautorizate să acceseze SORM. De la terminalul de control la distanță, se poate activa SORM în special pentru ca acesta să lanseze, să suspende ori să oprească interceptarea unui abonat, să intercepteze apelul în curs al unui abonat și să prezinte informații specifice despre un abonat (pct. 3.1.2 din Anexa nr. 3).

122. Centrul de control la distanță primește următoarele notificări automate cu privire la subiectul interceptării: mesaje scurte (SMS) trimise sau primite, inclusiv conținutul lor; apelarea unui număr; stabilirea unei conexiuni; întreruperea unei conexiuni; utilizarea unor servicii suplimentare; schimbarea stării conexiunii sau poziția subiectului interceptării (pct. 3.1.4 din Anexa nr. 3).

b) Ordinul nr. 130

123. Ordinul nr. 130 privind procedurile de instalare aplicabile sistemului tehnic pentru punerea în aplicare a măsurilor operative de investigații, emis de Ministerul Comunicațiilor la 25 iulie 2000, prevedea că furnizorii de servicii de comunicații trebuie să instaleze un echipament care respectă specificațiile tehnice stabilite prin Ordinul nr. 70. Procedura și programul de instalare necesită aprobare din partea FSB (pct. 1.4).

124. Furnizorii de servicii de comunicații ar trebui să ia măsuri pentru protecția informațiilor despre metodele și tacticile folosite în cadrul măsurilor operative de investigații (pct. 2.4).

125. Furnizorii de servicii de comunicații trebuiau să se asigure că orice interceptare a comunicațiilor sau orice acces la date de comunicații se acordă numai în temeiul unei decizii judecătorești și în conformitate cu procedura stabilită de LMOI (pct. 2.5).

126. Nu era necesară informarea furnizorilor de servicii de comunicații cu privire la interceptările care îi vizau pe abonații lor. De asemenea, nu era necesar să le fie prezentate deciziile judecătorești de autorizare a interceptărilor (pct. 2.6).

127. Interceptările erau realizate de personalul și prin intermediul echipamentelor FSB și ale serviciilor Ministerului de Interne (pct. 2.7).

128. Punctele 1.4 și 2.6 din Ordinul nr. 130 au fost contestate la Curtea Supremă de domnul N. Acesta a invocat lipsa de legalitate a trimiterii la Ordinul nr. 70, prevăzută la pct. 1.4, susținând că acest ordin nu era publicat și era lipsit de validitate. În ceea ce privește pct. 2.6, domnul N. l-a considerat incompatibil cu legea privind comunicațiile, care prevedea că furnizorii de servicii de comunicații erau obligați să asigure respectarea caracterului privat al comunicațiilor. La 25 septembrie 2000, Curtea Supremă a declarat că trimiterea la Ordinul nr. 70 prevăzută la pct. 1.4 este legală deoarece ordinul avea caracter tehnic și nu era așadar necesar să apară într-o publicație oficială

disponibilă tuturor, motiv pentru care a fost publicat doar într-o revistă de specialitate. În ceea ce privește pct. 2.6, Curtea Supremă a considerat că acesta putea fi interpretat în sensul că obligă furnizorii de servicii de comunicații să acorde organelor de aplicare a legii, fără autorizație judiciară, accesul la informații despre abonați. Considerând că o astfel de cerință este în contradicție cu legea privind comunicațiile, instanța supremă a ajuns la concluzia că pct. 2.6 este ilegal și inaplicabil.

129. La 25 octombrie 2000, Ministerul Comunicațiilor a abrogat pct. 2.6 din Ordinul nr. 130.

130. Ca răspuns la o solicitare de informații din partea organizației neguvernamentale „Controlul civil”, Ministerul Comunicațiilor a declarat, în scrisoarea din 20 august 2006, că abrogarea pct. 2.6 din Ordinul nr. 130 nu înseamnă că furnizorii de servicii de comunicații trebuie să fie informați cu privire la măsurile operative de investigații aplicate unui abonat ori să primească o copie a deciziei prin care s-a acordat autorizația legală pentru o astfel de supraveghere.

131. Ordinul nr. 130 a fost abrogat la 16 ianuarie 2008 (*infra*, pct. 134).

c) Ordinul nr. 538

132. Conform Ordinului nr. 538 privind colaborarea dintre furnizorii de servicii de comunicații și organele de aplicare a legii, adoptate de Guvern la 27 august 2005, furnizorii de servicii de comunicații trebuie să dea dovadă de diligență la actualizarea bazelor de date conținând informații despre abonați și serviciile oferite acestora. Aceste informații se păstrează timp de 3 ani. Organele de aplicare a legii trebuie să aibă, în permanență, acces la distanță la aceste baze de date (pct. 12).

133. Bazele de date trebuie să conțină următoarele informații despre abonați: a) prenumele, patronimul și numele de familie, adresa de domiciliu și numărul de pașaport, în cazul unei persoane fizice; b) denumirea societății, adresa și lista persoanelor cu acces la echipamentul terminal, precum și prenumele, patronimul, numele de familie, adresa de domiciliu și numărul de pașaport, în cazul unei persoane juridice; c) informații despre conexiuni, trafic și plăți (pct. 14).

d) Ordinul nr. 6

134. Ordinul nr. 6 privind specificațiile pentru rețelele de telecomunicații cu privire la punerea în aplicare a măsurilor operative de investigații (prima parte), emis de Ministerul Comunicațiilor la 16 ianuarie 2008, a înlocuit Ordinul nr. 130.

135. Ordinul nr. 6 a menținut obligația ca furnizorii de servicii de comunicații să asigure transmiterea, către terminalul de control la distanță al organului de aplicare a legii competent, informații cu privire la: a) numerele și codurile de identificare ale abonaților și b) conținutul comunicațiilor acestora. Aceste informații trebuie să fie transmise în timp real, la cererea provenită de la terminalul de control de la distanță. Furnizorii de servicii de comunicații trebuie să asigure, de asemenea, identificarea locului unde se află un abonat (pct. 2, 3 și 5).

136. Terminalul de control la distanță trebuie să aibă acces la bazele de date conținând informații despre abonați, inclusiv numerele și codurile de identificare ale acestora (pct. 7 și 8).

137. Furnizorii de servicii de comunicații trebuie să se asigure că subiectul interceptării nu află despre interceptarea comunicațiilor sale. Informațiile privind interceptările anterioare sau în desfășurare trebuie să fie protejate împotriva accesului neautorizat de către angajații furnizorilor de servicii de comunicații (pct. 9).

e) Ordinul nr. 73

138. Ordinul nr. 73 privind specificațiile pentru rețelele de telecomunicații cu privire la punerea în aplicare a măsurilor operative de investigații (Partea a II-a), emis de Ministerul Comunicațiilor la 27 mai 2010, oferă precizări privind anumite specificații din Ordinul nr. 6. Se precizează în special faptul că echipamentul instalat de furnizorii de servicii de comunicații trebuie să permită organelor care efectuează măsuri operative de investigații să aibă acces la toate datele transmise prin intermediul rețelelor telecomunicații și să fie capabil să selecteze datele și să transmită datele selectate la terminalul său de control (pct. 2).

III. INSTRUMENTE INTERNAȚIONALE ȘI EUROPENE RELEVANTE

A. Organizația Națiunilor Unite

139. Rezoluția nr. 68/167 privind dreptul la viață privată în era digitală, adoptată de Adunarea generală la 18 decembrie 2013, prevede următoarele:

„Adunarea generală,

(...)

4. *Invită* toate statele:

(...)

c) să-și revizuiască procedurile, practicile și legile referitoare la supravegherea și interceptarea comunicațiilor, precum și la colectarea de date cu caracter personal, în special pe scară largă, pentru a apăra dreptul la viață privată asigurând respectarea în totalitate a tuturor obligațiilor lor prevăzute de dreptul internațional [al drepturilor omului];

d) să înființeze mecanisme naționale de control independente și eficiente, capabile să asigure transparența și, după caz, răspunderea în cadrul operațiunilor lor de supraveghere și interceptare a comunicațiilor și colectare de date cu caracter personal, ori să mențină mecanismele existente [...]”

B. Consiliul Europei

140. Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal din 28 ianuarie 1981 (STCE nr. 108 – „Convenția nr. 108”) a stabilit norme pentru protejarea datelor în cadrul prelucrării automatizate a datelor cu caracter personal în sectorul public și cel privat. Aceasta prevede:

ART. 8

Garanții complementare pentru persoana în cauză

Orice persoană trebuie:

a) să aibă cunoștință 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).

ART. 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.

(...)

ART. 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.”

141. Convenția nr. 108 a fost ratificată de Federația Rusă la 15 mai 2013 și a intrat în vigoare, pentru acest stat, la 1 septembrie 2013. Instrumentul de ratificare depus la 15 mai 2013 de Federația Rusă conține următoarele declarații:

„Federația Rusă declară că, în conformitate cu art. 3 alineatul 2 litera a) din Convenție, nu va aplica această Convenție datelor cu caracter personal:

(...)

b) care constituie secret de stat, în conformitate cu legislația Federației Ruse privind secretul de stat.

Federația Rusă declară că, în conformitate cu art. 3 alineatul 2 litera a) din Convenție, va aplica această Convenție datelor cu caracter personal care nu sunt prelucrate automatic, dacă aplicarea Convenției corespunde naturii acțiunilor efectuate cu datele cu caracter personal, fără ajutorul unor mijloace automate.

Federația Rusă declară că, în conformitate cu art. 9 alineatul 2 litera a) din Convenție, își rezervă dreptul de a limita accesul unei persoane la propriile sale date cu caracter personal în vederea protejării securității statului și a ordinii publice.”

142. 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, adoptat la 8 noiembrie 2001 (STCE nr. 181), care a fost semnat dar nu și ratificat de Federația Rusă, prevede:

„ART. 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 ale 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.

(...)”

143. Recomandarea nr. R (87) 15 a Comitetului de Miniștri referitoare la reglementarea utilizării datelor cu caracter personal în domeniul polițienesc, adoptată la 17 septembrie 1987,

„1.1. Fiecare stat membru ar trebui să aibă o autoritate control independentă și externă a poliției, însărcinată cu asigurarea respectării principiilor formulate în prezenta recomandare.

(...)

2.1. Colectarea datelor cu caracter personal în domeniul polițienesc ar trebui să se limiteze la ceea ce este necesar pentru a preveni un pericol real sau pedepsirea unei infracțiuni specifice. Orice excepție de la această dispoziție ar trebui să facă obiectul unei legislații naționale specifice.

2.2. În cazul în care datele referitoare la o persoană au fost colectate și înregistrate fără cunoștința sa, aceasta ar trebui, dacă datele nu sunt distruse, să fie informată, dacă este posibil, că se dețin informații despre aceasta, și asta de îndată ce obiectul activităților poliției nu mai riscă să fie afectat.

(...)

3.1. Pe cât posibil, înregistrarea datelor cu caracter personal în domeniul polițienesc ar trebui să vizeze doar date exacte și să se limiteze la datele necesare pentru a permite organelor de poliție să își îndeplinească sarcinile legale, în cadrul dreptului intern și al obligațiilor care decurg din dreptul internațional.

(...)

5.2.i. Comunicarea datelor către organe publice ar trebui să fie permisă dacă, într-un caz particular:

a) există o obligație sau autorizație judiciară clară ori aprobare a autorității de supraveghere,

sau dacă

b) aceste date sunt indispensabile destinatarului pentru a-i permite să își îndeplinească propriile atribuții legale și cu condiția ca scopul colectării sau prelucrării efectuate de către destinatar să nu fie incompatibil cu cel inițial și ca obligațiile legale ale organului de comunicare să nu fie contrare acesteia.

5.2.ii. Mai mult, comunicarea este permisă, ca excepție, dacă într-un caz particular:

a) comunicarea este, fără îndoială, în interesul persoanei vizate și fie persoana vizată și-a dat consimțământul, fie circumstanțele permit o presupunere clară a consimțământului, sau dacă

b) comunicarea este necesară pentru a preveni un pericol grav și iminent.

5.3.i. Comunicarea datelor către persoane private ar trebui permisă doar dacă, într-un caz particular, există o obligație sau autorizație judiciară clară sau cu aprobarea autorității de control.

(...)

6.4. Exercițarea [de către persoana vizată a] drepturilor de acces, de rectificare sau de ștergere ar trebui să fie restrânsă doar în cazul în care o restricție este indispensabilă pentru exercitarea atribuțiilor legale ale poliției sau necesară pentru protejarea persoanei vizate ori a drepturilor și libertăților altora.

(...)

6.5. Refuzarea sau restrângerea acestor drepturi ar trebui să fie motivată în scris. Comunicarea motivării poate fi refuzată doar dacă aceasta este indispensabilă pentru exercitarea unei atribuții legale a poliției sau este necesară pentru protejarea drepturilor și libertăților altora.

6.6. În cazul în care se refuză accesul, persoana în cauză ar trebui să aibă la dispoziție o cale de atac la autoritatea de control sau alt organism independent care se va asigura că refuzul este bine întemeiat.

7.1. Ar trebui luate măsuri pentru ca datele cu caracter personal păstrate în domeniul polițienesc să fie șterse dacă nu mai sunt necesare scopului pentru care au fost stocate.

În acest scop, în special, se vor lua în considerare următoarele criterii: necesitatea de a stoca datele în vederea terminării urmăririi penale într-un caz determinat; pronunțarea unei hotărâri judecătorești definitive, în special de achitare; reabilitare; prescripție; amnistie; vârsta persoanei vizate; categorii speciale de date.

7.2. Regulile privind stabilirea termenelor de stocare a diferitelor categorii de date cu caracter personal, precum și verificările periodice asupra calității acestora ar trebui să fie stabilite de comun acord cu autoritatea de supraveghere sau în conformitate cu dreptul intern.

8. Organul competent trebuie să ia toate măsurile necesare pentru a asigura securitatea fizică și logică adecvată a datelor, precum și pentru a împiedica accesul neautorizat, comunicarea neautorizată sau modificarea acestora. În acest scop, este necesar să se țină seama de conținutul și caracteristicile diferite ale fișierelor."

144. Recomandarea nr. R (95) 4 a Comitetului de Miniștri privind protecția datelor cu caracter personal în domeniul serviciilor de telecomunicații, cu referire specială la serviciile de telefonie, adoptată la 7 februarie 1995, prevede următoarele:

„2.4. Nu se permite nicio ingerință a autorităților publice în conținutul unei comunicații, inclusiv utilizarea unor echipamente de interceptări telefonice sau a altor mijloace de supraveghere ori de interceptare a comunicațiilor, dacă această ingerință nu este prevăzută de lege și nu constituie o măsură necesară într-o societate democratică:

a) pentru protejarea securității statului, a siguranței publice, a intereselor monetare ale statului sau pedepsirea infracțiunilor;

b) pentru protejarea persoanei vizate sau a drepturilor și libertăților altora.

2.5. În caz de ingerință a autorităților publice în conținutul unei comunicări, dreptul intern ar trebui să reglementeze:

a) exercitarea drepturilor de acces și de rectificare de către persoana în cauză;

b) condițiile în care autoritățile publice competente vor avea dreptul să refuze să dea informații persoanei vizate ori să amâne acordarea lor;

c) păstrarea sau distrugerea acestor date.

Atunci când un operator de rețea sau un furnizor de servicii este obligat de o autoritate publică să comită o ingerință, datele colectate în acest mod ar trebui să fie comunicate doar organului desemnat în autorizația pentru acea interferență. [...]"

C. Uniunea Europeană

145. Rezoluția Consiliului din 17 ianuarie 1995 privind interceptarea legală a telecomunicațiilor (96/C 329/01) prevede:

„Această secțiune prezintă specificațiile serviciilor autorizate cu privire la interceptarea legală a telecomunicațiilor. Specificațiile se supun legislației naționale și se interpretează în conformitate cu politicile naționale aplicabile.

(...)

1.3. Telecomunicațiile efectuate de persoana supusă interceptării sau adresate acesteia trebuie să fie accesibile serviciilor autorizate, cu excluderea tuturor telecomunicațiilor care nu au legătură cu serviciul țintă specificat în autorizația de interceptare.

(...)

2. Serviciile autorizate trebuie să aibă posibilități de supraveghere în timp real și în permanență pentru interceptarea transmisiunilor de telecomunicații. Tot în timp real trebuie să fie furnizate date suficiente aferente apelurilor. Dacă nu pot fi furnizate în timp real date suplimentare aferente apelului, serviciile autorizate trebuie să dispună de aceste date cât mai curând posibil după terminarea apelului.

3. Operatorii de rețele sau furnizorii de servicii trebuie să ofere serviciilor autorizate o interfață sau mai multe interfețe de la care comunicațiile interceptate pot fi transmise la sistemele lor de supraveghere. Aceste interfețe trebuie să facă obiectul unui acord între autoritățile care interceptează comunicațiile și operatorii de rețele sau furnizorii de servicii. Celelalte probleme legate de aceste interfețe vor fi abordate în conformitate cu practicile acceptate în fiecare țară.

(...)

5. Interceptarea trebuie să fie concepută și pusă în aplicare pentru a împiedica utilizarea neautorizată sau abuzivă și pentru a proteja informațiile despre interceptare.

(...)

5.2. Operatorii de rețele sau furnizorii de servicii trebuie să se asigure că comunicațiile interceptate sunt transmise numai la serviciul de supraveghere specificat în autorizația de interceptare.

(...)"

146. Specificațiile sus-menționate au fost confirmate și explicate în Rezoluția nr. 9194/01 a Consiliului din 20 iunie 2001 privind nevoile operaționale ale serviciilor autorizate în materie de rețele și servicii publice de telecomunicații.

147. În hotărârea pronunțată la 8 aprilie 2014 în cauzele conexe *Digital Rights Ireland* și *Seitlinger ș.a.*, Curtea de Justiție a Uniunii Europene (CJUE) a declarat nevalidă Directiva 2006/24/CE privind păstrarea datelor, care impunea furnizorilor de servicii de comunicații electronice accesibile publicului sau de rețele de comunicații publice obligația de a păstra datele privind traficul și locația pentru o perioadă de la 6 luni la 2 ani, pentru ca datele respective să fie disponibile în scopul cercetării, depistării și urmăririi penale a infracțiunilor grave, după cum au fost definite de fiecare stat membru în dreptul intern. CJUE a constatat că, deși directiva nu autorizează păstrarea conținutului comunicației, datele privind traficul și locația vizate de acest text pot permite deducerea unor concluzii foarte precise privind viața privată a persoanelor ale căror date au fost păstrate. În consecință, în opinia CJUE, obligația de a păstra datele respective constituie în sine o ingerință în exercitarea dreptului la respectarea vieții private și a comunicațiilor, garantat de art. 7 din Carta drepturilor fundamentale a Uniunii Europene, precum și a dreptului la protecția datelor cu caracter personal, întemeiat pe art. 8 din Cartă. De asemenea, în opinia CJUE, accesul autorităților naționale competente la date constituie o ingerință suplimentară în exercitarea acestor drepturi fundamentale. CJUE a adăugat că ingerința este deosebit de gravă și că împrejurarea că păstrarea datelor și utilizarea lor ulterioară sunt efectuate fără ca abonatul sau utilizatorul înregistrat să fie informați cu privire la aceasta este susceptibilă să genereze în mintea persoanelor vizate sentimentul că viața lor

privată face obiectul unei supravegheri constante. Instanța consideră că, deși ingerința răspunde unui obiectiv de interes general - de a contribui la combaterea criminalității grave și a terorismului și astfel, în final, la siguranța publică - aceasta nu respectă totuși cerința de proporționalitate. CJUE a constatat în primul rând că Directiva acoperă în mod generalizat toate persoanele și toate mijloacele de comunicare electronică, precum și ansamblul datelor de trafic, fără a face vreo diferențiere, limitare sau excepție în funcție de obiectivul combaterii infracțiunilor grave. Astfel, potrivit CJUE, Directiva conține o ingerință în drepturile fundamentale ale cvasitotalității populației europene și se aplică, așadar, chiar și acelor persoane în privința cărora nu există niciun indiciu de natură să sugereze că comportamentul lor poate avea o legătură, chiar indirectă sau îndepărtată, cu infracțiuni grave. CJUE a declarat că, în al doilea rând, Directiva nu conține condițiile materiale și procedurale în ceea ce privește accesul autorităților naționale competente la date și utilizarea lor ulterioară și, prin faptul că se limitează la a face trimitere în general la infracțiunile grave, astfel cum sunt definite de fiecare stat membru în dreptul său intern, Directiva nu prevede niciun criteriu obiectiv care să permită identificarea infracțiunilor care pot fi considerate ca fiind suficient de grave pentru a justifica o ingerință atât de mare în drepturile fundamentale consacrate la articolele 7 și 8 din cartă. Mai ales, în opinia CJUE, accesul la datele păstrate de autoritățile naționale competente nu este condiționat de un control prealabil efectuat fie de o instanță, fie de o entitate administrativă independentă prin a căror decizie se urmărește limitarea accesului la date și a utilizării lor la ceea ce este strict necesar în vederea atingerii obiectivului urmărit. În al treilea rând, CJUE a constatat că Directiva 2006/24 impune păstrarea tuturor datelor pentru o perioadă de cel puțin 6 luni, fără a se face vreo distincție între categoriile de date în funcție de utilitatea lor eventuală în scopul realizării obiectivului urmărit sau în funcție de persoanele vizate. CJUE a concluzionat că Directiva conține o ingerință în drepturile fundamentale prevăzute la articolele 7 și 8 din cartă, ingerință care este de o mare amploare și de o gravitate deosebită în ordinea juridică a Uniunii, fără ca această ingerință să fie încadrată în mod precis de dispoziții care să poată garanta faptul că ea este limitată efectiv la strictul necesar. CJUE a mai observat că Directiva nu prevede garanții suficiente — prin intermediul unor măsuri tehnice și organizaționale — care să permită asigurarea unei protecții eficiente a datelor păstrate împotriva riscurilor de abuz, precum și împotriva oricărui acces și a oricărei utilizări ilicite a acestor date.

ÎN DREPT

I. CU PRIVIRE LA PRETINSA ÎNCĂLCARE A ART. 8 DIN CONVENȚIE

148. Reclamantul susține că sistemul de interceptare secretă a comunicațiilor de telefonie mobilă din Rusia nu respectă cerințele de la art. 8 din Convenție, formulat astfel:

„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.”

A. Cu privire la admisibilitate

149. Guvernul susține că reclamantul nu se poate considera victimă a încălcării dreptului său la respectarea vieții sale private sau a corespondenței sale (*infra*, pct. 152-157). De asemenea, acesta consideră că reclamantul nu a epuizat căile de atac interne (*infra*, pct. 219-226).

150. Curtea consideră că excepțiile ridicate de Guvern sunt atât de strâns legate de fondul capătului de cerere formulat de reclamant încât este necesar să fie conexe cu fondul.

151. De asemenea, constatând că acest capăt de cerere nu este în mod vădit nefondat în sensul art. 35 § 3 lit. a) din Convenție și nu prezintă niciun alt motiv de inadmisibilitate, Curtea îl declară admisibil.

B. Cu privire la fond

1. Cu privire la calitatea de victimă a reclamantului și existența unei „ingerințe”

a) Argumentele părților

i. Guvernul

152. Guvernul consideră că reclamantul nu se poate considera victima încălcării art. 8 din Convenție și că nu a existat nicio ingerință în exercitarea drepturilor sale. Reclamantul nu s-a plâns de o interceptare a comunicațiilor sale telefonice. Capătul de cerere formulat în fața instanțelor naționale și a Curții constă, în esență, în afirmația că furnizorii de servicii de comunicații au instalat un echipament special care permite autorităților să pună în aplicare măsuri operative de investigații. Or, cauza *Orange Slovensko, A.S. împotriva Slovaciei* [(dec.), nr. 43983/02, 24 octombrie 2006] a confirmat faptul că instalarea, sau chiar finanțarea, unui echipament de interceptare de către societățile private nu este, în sine, contrar Convenției.

153. Guvernul adaugă că art. 34 nu poate fi invocat pentru a introduce o cerere de tip *actio popularis*, nici pentru a servi ca temeiul unei plângeri în *abstracto* conform căreia o lege contravine Convenției [Guvernul menționează *Aalmoes și alți 112 împotriva Țărilor de Jos* (dec.), nr. 16269/02, 25 noiembrie 2004]. Acesta consideră că noțiunea de calitate de victimă definită în hotărârile *Klass și alții împotriva Germaniei* (6 septembrie 1978, pct. 34, seria A nr. 28) și *Malone împotriva Regatului Unit* (2 august 1984, pct. 64, seria A nr. 82) – conform căreia o persoană poate, în anumite condiții, să se pretindă victimă a unei încălcări determinate de simpla existență a unor măsuri secrete sau a unei legislații care permite astfel de măsuri, fără a fi nevoie să pretindă că i-au fost aplicate în realitate – nu trebuie să fie interpretată în sens larg pentru a cuprinde orice persoană din statul pârât care se teme că serviciile de securitate au fost în măsură să adune informații despre ele. În opinia Guvernului, reclamantul trebuie să demonstreze existența unei „probabilități rezonabile” că serviciile de securitate au colectat și au păstrat informații despre viața sa privată [acesta se referă la *Esbuster împotriva Regatului Unit*, nr. 18601/91, decizia Comisiei din 2 aprilie 1993; *Redgrave împotriva Regatului Unit*, nr. 20271/92, decizia Comisiei din 1 septembrie 1993; *Matthews împotriva Regatului Unit*, nr. 28576/95, decizia Comisiei din 16 octombrie 1996; *Halford împotriva Regatului Unit*, 25 iunie 1997, pct. 17, *Culegere de hotărâri și decizii 1997-III*; *Weber și Saravia împotriva Germaniei* (dec.), nr. 54934/00, pct. 4-6 și 78, CEDO 2006-XI; și *Kennedy împotriva Regatului Unit*, nr. 26839/05, pct. 122 și 123, 18 mai 2010].

154. Guvernul consideră că derogările de la principiul „probabilității rezonabile” sunt acceptabile numai pentru motive speciale. În opinia sa, o persoană se poate plânge de o ingerință cauzată de simpla existență a unei legislații care permite măsuri de supraveghere secretă numai în circumstanțe excepționale, și este necesar să se țină seama de disponibilitatea unei eventuale căi de atac interne, precum și de riscul ca persoanei în cauză să i se aplice măsuri de supraveghere secretă (acesta citează *Kennedy*, citată anterior, pct. 124). Or, pentru Guvern, nu se poate stabili niciun astfel de motiv în prezenta cauză.

155. În primul rând, potrivit Guvernului, dat fiind că reclamantul nu a fost bănuit de nicio infracțiune, nu există nicio „probabilitate rezonabilă”, nici măcar cel mai mic risc, ca acesta să fi fost supus unor măsuri de supraveghere. Profesia sa – redactor-șef al unei edituri – nu poate justifica o măsură de interceptare în conformitate cu dreptul rus. Guvernul asigură că nu au fost niciodată interceptate convorbirile telefonice ale reclamantului și că acesta nu a prezentat nicio dovadă în sens contrar. Documentele prezentate de acesta în cadrul procedurii interne se referă la terți și nu conțin nicio dovadă că ar fi fost interceptat.

156. În al doilea rând, există căi de atac interne care permit denunțarea atât a pretensei insuficiențe a garanțiilor acordate de dreptul rus împotriva abuzurilor, precum și a oricărei măsuri de supraveghere specială aplicate unei persoane. Există posibilitatea de a solicita Curții Constituționale să verifice constituționalitatea LMOI, și, de asemenea, de a sesiza Curtea Supremă, așa cum a procedat cu succes domnul N., care a obținut constatarea nelegalității unei dispoziții din Ordinul nr. 130 al Ministerului Comunicațiilor (*supra*, pct. 128). În ceea ce privește Ordinul nr. 70, contrar afirmațiilor reclamantului, acesta a fost publicat în mod corespunzător (*infra*, pct. 181) și, prin urmare, poate fi atacat în instanță. De asemenea, persoana ale cărei comunicații au fost interceptate ilegal în absența unei autorizații legale prealabile poate obține despăgubire în fața unei instanțe civile. Guvernul face trimitere la hotărârea din 15 iulie 2009, în care Curtea Supremă a considerat că instalarea unei camere video în biroul petentului și interceptarea telefonului său de serviciu au fost ilegale, aceste măsuri de supraveghere fiind puse în aplicare fără nicio autorizație judiciară prealabilă (a se vedea, de asemenea, pct. 219-224 *infra*). În cele din urmă, Guvernul afirmă că, în dreptul rus, măsurile de interceptare sunt controlate de un organism independent, parchetul.

157. Guvernul concluzionează astfel că prezenta cauză este diferită de cauza *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiiev împotriva Bulgariei* (nr. 62540/00, 28 iunie 2007), în care Curtea a refuzat să aplice criteriul „probabilității rezonabile” din cauza lipsei de garanții împotriva interceptării ilegale în Bulgaria. În opinia Guvernului, întrucât dreptul rus oferă garanții adecvate și suficiente – inclusiv căi de atac – împotriva abuzurilor în materie de interceptare a

comunicațiilor, reclamantul nu poate să se plângă de o ingerință pe motivul existenței unei legislații care permite supravegherea secretă. Din lipsă de „probabilitate rezonabilă” că i-au fost interceptate comunicațiile telefonice, acesta nu se poate pretinde victima încălcării art. 8 din Convenție pe care o invocă.

ii. Reclamantul

158. Reclamantul consideră că se poate pretinde victimă a încălcării art. 8 cauzate de simpla existență a legislației care autorizează un sistem de interceptări secrete ale comunicațiilor, fără a fi nevoie să demonstreze că aceste măsuri secrete i-au fost aplicate efectiv. În opinia sa, existența unei astfel de legislații înseamnă că toți utilizatorii serviciilor de telecomunicații riscă să fie supravegheați și, prin urmare, se interpretează în sine ca o ingerință în exercitarea drepturilor sale care decurg de la art. 8. Reclamantul își susține poziția invocând hotărârile *Klass și alții* (citată anterior, pct. 34 și 37), *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhev* (citată anterior, pct. 58) și *Kennedy* (citată anterior, pct. 123).

159. Acesta susține că astfel, Curtea a utilizat criteriul „probabilității rezonabile” numai în cauzele în care reclamantul s-a plâns de interceptări care au avut loc în realitate, pe când în cauzele având ca obiect un capăt de cerere general cu privire la legislația și practica prin care se autorizează supravegherea secretă, Curtea a aplicat – în opinia acestuia – criteriul „simplei existențe”, stabilit în hotărârea *Klass și alții* (*Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhev*, citată anterior, pct. 59; și *Kennedy*, citată anterior, pct. 122 și 123, împreună cu alte trimiteri). Acesta adaugă că, în cauza *Liberty și alții împotriva Regatului Unit* (nr. 58243/00, pct. 56 și 57, 1 iulie 2008), Curtea a considerat că existența unor atribuții care permit autorităților să intercepteze comunicațiile se interpretează ca o ingerință în drepturile reclamantelor prevăzute la art. 8 deoarece exista posibilitatea ca acestora să li se aplice atribuțiile în litigiu. De asemenea, Guvernul precizează că, în hotărârea *Kennedy* (citată anterior, pct. 124), Curtea a completat acest criteriu adăugând o evaluare a disponibilității unei căi de atac la nivel intern, precum și a riscului ca persoanei în cauză să i se aplice măsuri de supraveghere secretă. În fine, în cauza *Mersch și alții împotriva Luxemburgului* (nr. 10439/83 etc., decizia Comisiei din 10 mai 1985), Comisia a considerat că, în situațiile în care autoritățile nu sunt obligate să notifice persoanelor vizate măsurile de supraveghere la care au fost supuse, acestea se pot considera „victime” ale încălcării Convenției prin simpla existență a legislației privind supravegherea secretă, chiar dacă acestea nu pot invoca în susținerea cererilor lor faptul că au fost într-adevăr supuse unor măsuri de supraveghere.

160. Reclamantul consideră că se poate pretinde victima unei încălcări a art. 8 din cauza atât a simplei existențe a legislației privind supravegherea secretă, cât și a situației sale personale. Acesta susține că LMOI, împreună cu legea privind FSB, legea privind comunicațiile și ordinele emise de Ministerul Comunicațiilor – în special Ordinul nr. 70 – permite serviciilor de securitate să intercepteze prin mijloace tehnice comunicațiile oricărei persoane fără să fie obligate să obțină o autorizație judiciară prealabilă în acest scop. Mai precis, serviciile de securitate nu au nicio obligație să prezinte o autorizație de interceptare cuiva, nici măcar furnizorului de servicii de comunicații. Reclamantul concluzionează astfel că legislația în litigiu permite interceptarea generalizată a comunicațiilor.

161. Dreptul rus nu oferă nicio cale de atac pentru a putea contesta legislația în litigiu. Astfel, în ceea ce privește posibilitatea de a contesta Ordinul nr. 70, reclamantul face trimitere la hotărârea Curții Supreme din 25 septembrie 2000 privind plângerea domnului N. (*supra*, pct. 128), în care înalta instanță a declarat că ordinul în litigiu are un caracter mai mult tehnic decât juridic și, prin urmare, nu putea să apară într-o publicație oficială. De asemenea, reclamantul a prezentat o copie a deciziei din 24 mai 2010 a Tribunalului Superior Comercial, în care s-a constatat că ordinele Ministerului Comunicațiilor care impun furnizorilor de servicii de comunicații obligația de a instala un echipament care să permită autorităților să pună în aplicare măsuri operative de investigații nu intră sub controlul instanțelor comerciale. Acesta adaugă că procedura internă pe care a inițiat-o a arătat că Ordinul nr. 70 nu putea fi contestat în mod efectiv în fața instanțelor ruse. În ceea ce privește LMOI, Curtea Constituțională a examinat de mai multe ori constituționalitatea acesteia și a concluzionat că legea era compatibilă cu Constituția. În ceea ce privește posibilitatea de a ataca măsurile de supraveghere individuală, reclamantul susține că persoana vizată nu este informată despre măsura de interceptare decât în cazul în care informațiile interceptate sunt prezentate ca probe în cadrul unei proceduri penale îndreptate împotriva sa. În lipsa notificării, căile de atac interne sunt inefficiente (a se vedea, de asemenea, pct. 217 *infra*).

162. Cu privire la situația sa personală, reclamantul afirmă că este jurnalist și președintele filialei din Sankt Petersburg a Fundației pentru Apărarea Glasnost, care monitorizează situația libertății mass-mediei și oferă sprijin juridic jurnaliștilor ale căror drepturi profesionale au fost încălcate (*supra*, pct. 8). Riscul de interceptare a comunicațiilor sale este așadar mai mare. În acest sens, reclamantul menționează importanța crucială a protejării surselor jurnalistice, pe care Marea Cameră a subliniat-o în hotărârea *Sanoma Uitgevers B.V. împotriva Țărilor de Jos* [(MC), nr. 38224/03, pct. 50, 14

septembrie 2010].

b) Motivarea Curții

163. Curtea observă că reclamantul din prezenta cauză invocă o ingerință în exercitarea drepturilor sale, ingerință care rezultă nu din măsurile specifice de interceptare care i-au fost aplicate, ci din simpla existență a legislației care autorizează interceptarea secretă a comunicațiilor de telefonie mobilă, precum și cea a riscului de a fi el însuși supus unor măsuri de interceptare.

i. Rezumatul jurisprudenței Curții

164. Conform jurisprudenței constante a Curții, Convenția nu recunoaște *actio popularis*, iar Curtea nu are în mod normal sarcina de a examina *in abstracto* legislația și practica relevante, ci de a verifica dacă modul în care acestea au fost aplicate reclamantului ori l-au afectat, a cauzat o încălcare a Convenției [a se vedea, printre altele, *N.C. împotriva Italiei* (MC), nr. 24952/94, pct. 56, CEDO 2002-X; *Krone Verlag GmbH & Co. KG împotriva Austriei* (nr. 4), nr. 72331/01, pct. 26, 9 noiembrie 2006; și *Centrul de Resurse Juridice în numele lui Valentin Câmpeanu împotriva României* (MC), nr. 47848/08, pct. 101, CEDO 2014]. Rezultă că, pentru a putea introduce o cerere în temeiul art. 34, o persoană trebuie să poată demonstra că „a suportat în mod direct efectele” măsurii în litigiu. Această condiție este necesară pentru declanșarea mecanismului de protecție prevăzut de Convenție, chiar dacă acest criteriu nu ar trebui aplicat într-un mod rigid, mecanic și inflexibil pe tot parcursul procedurii (*Centrul de Resurse Juridice în numele lui Valentin Câmpeanu*, citată anterior, pct. 96).

165. Astfel, având în vedere particularitățile măsurilor secrete de supraveghere și importanța de a garanta că acestea sunt supuse unui control și unei supravegheri efective, Curtea admite căile de atac generale îndreptate împotriva legislației care reglementează acest domeniu. În cauza *Klass și alții*, Curtea a hotărât că o persoană poate, în anumite condiții, să se pretindă victima unei încălcări cauzate prin simpla existență a unor măsuri secrete sau a unei legislații care permite astfel de măsuri, fără a fi nevoie să pretindă că acestea i-au fost aplicate în realitate. În plus, condițiile necesare trebuie să fie definite în fiecare cauză în parte, în funcție de dreptul/drepturile din Convenție a cărui/căror încălcare a fost invocată, caracterul secret al măsurilor în litigiu și relația dintre reclamant și măsurile respective (*Klass și alții*, citată anterior, pct. 34). Curtea și-a justificat abordarea după cum urmează:

„36. Curtea constată că, atunci când un stat introduce o supraveghere secretă, a cărei existență rămâne necunoscută de persoanele supravegheate și care astfel rămâne inatacabilă, art. 8 ar putea fi anulat în totalitate. Într-o astfel de situație, este posibil ca o persoană să fie tratată într-un mod contrar art. 8, ba chiar să fie lipsită de dreptul garantat de acest articol, fără să știe acest fapt și, prin urmare, fără să aibă posibilitate de acțiune la nivel național sau în fața organelor Convenției.

(...)

Curtea nu poate admite faptul că asigurarea exercitării unui drept garantat de Convenție poate fi astfel eliminată prin simplul fapt de a menține persoana respectivă neinformată despre încălcarea acestuia. Dreptul de a sesiza Comisia, care le aparține persoanelor eventual afectate de supravegherea secretă, decurge de la art. 25 [în prezent art. 34]; în caz contrar, art. 8 ar risca să-și piardă orice aplicare.

37. În ceea ce privește faptele cauzei, Curtea constată că legislația în litigiu stabilește un sistem de supraveghere care expune orice persoană, în Republica Federală Germania, controlării corespondenței sale, a expedierilor sale poștale și a telecomunicațiilor sale fără să afle acest lucru vreodată, în lipsa unei indiscreții sau notificări ulterioare în circumstanțele indicate în hotărârea Curții Constituționale Federale (...) Legislația respectivă afectează astfel în mod direct orice utilizator sau utilizator virtual al serviciilor de poștă și telecomunicații din Republica Federală Germania. În plus, așa cum delegații au constatat în mod întemeiat, această amenințare a supravegherii poate fi denunțată ca restrângând în sine libertatea de comunicare prin intermediul acestor servicii și ca reprezentând așadar, pentru fiecare utilizator sau utilizator virtual, o ingerință directă în dreptul garantat de art. 8.

(...)

38. Având în vedere particularitățile cauzei, Curtea decide că reclamantii au fiecare dreptul «să se pretindă victimă a unei încălcări» a Convenției, chiar dacă nu pot invoca în sprijinul cererii lor faptul că au fost supuși unei măsuri concrete de supraveghere. Pentru a stabili dacă au fost într-adevăr victime ale unei încălcări, trebuie verificat dacă legislația în litigiu este în sine în concordanță cu prevederile Convenției.

(...)”

166. În urma cauzei *Klass și alții*, două concepții privind calitatea de victimă în cauzele privind supravegherea secretă s-au dezvoltat în paralel în jurisprudența organelor Convenției.

167. În mai multe cauze, Comisia și Curtea au declarat că aceste criterii formulate în hotărârea *Klass și alții* nu trebuie să fie interpretate în sens larg pentru a include orice persoană care se teme în statul pârât că serviciile de securitate au colectat informații în privința sa. Cu toate acestea, Comisia și Curtea au considerat că nu este o așteptare rezonabilă ca un reclamant să demonstreze că au fost colectate și păstrate informații despre viața sa privată. Comisia și Curtea au adăugat că, în privința măsurilor secrete, este suficient să se demonstreze existența unor practici care permit supravegherea secretă și existența unei probabilități suficiente că serviciile de securitate au colectat și au păstrat informații despre viața privată a persoanei vizate (*Esbester*, decizia citată anterior; *Redgrave*, decizia citată anterior; *Christie împotriva Regatului Unit*, nr. 21482/93, decizia Comisiei din 27 iunie 1994; *Matthews*, decizia citată anterior; *Halford*, citată anterior, pct. 47 și 55-57; și *Iliya Stefanov împotriva Bulgariei*, nr. 65755/01, 22 mai 2008, pct. 49 și 50). În toate aceste cauze, reclamantii au pretins că într-adevăr le-au fost interceptate comunicațiile. În unele cauze, aceștia s-au mai plâns, în general, de legile și practicile care autorizau măsuri secrete de supraveghere (*Esbester*, *Redgrave*, *Matthews* și *Christie*, decizii citate anterior).

168. În alte cauze, Curtea a reiterat abordarea adoptată în hotărârea *Klass și alții*, conform căreia legile și practicile care autorizează și instituie un sistem de supraveghere secretă a comunicațiilor generează, prin simpla lor existență, în rândul tuturor celor cărora li s-ar putea aplica legislația, un risc de supraveghere care în mod necesar restrânge libertatea de comunicare între utilizatorii serviciilor de telecomunicații și astfel constituie, în sine, o ingerință în exercitarea de către reclamantii a drepturilor lor care decurg de la art. 8, indiferent de măsurile luate în fapt în privința lor (*Malone*, citată anterior, pct. 64; *Weber și Saravia*, decizia citată anterior, pct. 78; *Asociația pentru Integrarea Europeană și Drepturile Omului și Ekimdzhiev*, citată anterior, pct. 58, 59 și 69; *Liberty și alții*, citată anterior, pct. 56 și 57; precum și *Lordachi și alții împotriva Moldovei*, nr. 25198/02, pct. 30-35, 10 februarie 2009). În toate aceste cauze, reclamantii au formulat plângeri generale cu privire la legislația și practica prin care se autorizau măsurile de supraveghere secretă. În unele cauze, aceștia au invocat totodată interceptarea în realitate a comunicațiilor lor (*Malone*, citată anterior, pct. 62; și *Liberty și alții*, citată anterior, pct. 41 și 42).

169. În fine, în cauza *Kennedy împotriva Regatului Unit*, cea mai recentă în materie, Curtea a declarat că trebuie avute în vedere considerațiile speciale care justifică, în cauzele având ca obiect măsuri de supraveghere secretă, derogarea de la abordarea sa generală constând în a nega persoanelor dreptul de a se plânga în abstracto de o anumită lege. Curtea a precizat că principala considerație este aceea că este necesară asigurarea că natura secretă a acestor măsuri nu face ca acestea să fie inatacabile în practică și să fie exceptate de la controlul exercitat de autoritățile judiciare naționale și de Curte. Aceasta a considerat că, pentru a hotărî într-o anumită cauză dacă o persoană se poate plânga de o ingerință ca urmare a simplei existențe a unei legislații care permite măsuri de supraveghere secretă, trebuie să ia în considerare disponibilitatea unei căi de atac interne, dar și riscul ca măsurile de supraveghere secretă să fi fost aplicate persoanei respective. Curtea a adăugat că, atunci când nu există nicio posibilitate de a contesta aplicarea unor măsuri de supraveghere secretă la nivel intern, nu sunt nejustificate suspiciunile și temerile populației cu privire la modul abuziv în care pot fi folosite atribuțiile de supraveghere secretă. Curtea a concluzionat că, în acest caz, este necesar un control mai amplu din partea sa, chiar dacă, în practică, riscul de supraveghere nu este mare (*Kennedy*, citată anterior, pct. 124).

ii. Armonizarea abordărilor

170. În acest context, Curtea consideră că trebuie precizate condițiile în care un reclamant se poate pretinde victimă a unei încălcări a art. 8 fără a fi nevoie să demonstreze că măsurile de supraveghere secretă i-au fost aplicate în realitate, pentru a permite adoptarea unei abordări uniforme și previzibile.

171. În opinia Curții, abordarea din cauza *Kennedy* este cea mai potrivită pentru necesitatea de a asigura faptul că natura secretă a măsurilor de supraveghere nu face ca acestea să fie inatacabile în practică și exceptate de la controlul exercitat de autoritățile judiciare naționale și de Curte. Prin urmare, Curtea admite că un reclamant se poate pretinde victimă a unei încălcări cauzate de simpla existență a unor măsuri de supraveghere secretă sau a unei legislații care autorizează astfel de măsuri dacă sunt îndeplinite următoarele condiții. În primul rând, Curtea va lua în considerare domeniul de aplicare a legislației care autorizează măsuri de supraveghere secretă și va cerceta dacă reclamantul poate fi, eventual, afectat de legislația în litigiu, fie pentru că acesta aparține unui grup de persoane vizate de legislație, fie pentru că aceasta vizează în mod direct toți utilizatorii serviciilor de comunicații prin introducerea unui sistem în care oricărei persoane i se pot intercepta comunicațiile. În al doilea rând, Curtea va ține seama de disponibilitatea unei căi de atac la nivel național și va ajusta nivelul controlului său în funcție de eficacitatea acestor căi de atac. După cum a subliniat în hotărârea

Kennedy, atunci când ordinea internă nu oferă o cale de atac efectivă persoanei care crede că a fost supusă unei supravegheri secrete, nu sunt nejustificate suspiciunile și temerile populației cu privire la modul abuziv în care pot fi folosite atribuțiile de supraveghere secretă (*Kennedy*, citată anterior, pct. 124). În aceste circumstanțe, este întemeiată afirmația că însuși riscul de supraveghere restrânge libertatea de comunicare prin intermediul serviciilor de poștă și telecomunicații și constituie așadar, pentru fiecare utilizator sau utilizator virtual, o ingerință directă în dreptul garantat de art. 8. Prin urmare, controlul mai amplu exercitat de Curte este necesar și justifică derogarea de la regula că persoanele nu au dreptul să se plângă de o lege *in abstracto*. În acest caz, persoana respectivă nu trebuie să dovedească existența unui risc de aplicare a măsurilor de supraveghere secretă în privința sa. Cu toate acestea, dacă ordinea internă dispune de căi de atac efective, suspiciunile generalizate cu privire la abuzuri sunt mai greu de justificat. În această ipoteză, persoana respectivă se poate pretinde victimă a unei încălcări cauzate prin simpla existență a unor măsuri secrete sau a unei legislații care autorizează astfel de măsuri numai dacă poate să demonstreze că, din cauza situației sale personale, este potențial expusă riscului de a i se aplica astfel de măsuri.

172. Abordarea definită în hotărârea *Kennedy* oferă așadar Curții flexibilitatea necesară pentru a soluționa toate tipurile de situații care pot apărea în materie de supraveghere secretă, având în vedere particularitățile sistemelor juridice ale statelor membre, și anume căile de atac existente, precum și situația personală a fiecărui reclamant.

iii. Aplicarea în prezenta cauză

173. Nimeni nu contestă faptul că toate comunicațiile de telefonie mobilă intră în sfera noțiunilor de „viață privată” și „corespondență” în sensul art. 8 § 1 (a se vedea, de exemplu, *Liberty și alții*, citată anterior, pct. 56).

174. Curtea observă că reclamantul invocă, în prezenta cauză, o ingerință în exercitarea drepturilor sale, ingerință care nu rezultă din măsuri specifice de supraveghere care i-ar fi fost aplicate, ci din simpla existență a legislației care autorizează măsurile de supraveghere secretă și din riscul de a fi el însuși supus unor astfel de măsuri.

175. Curtea observă că legislația în litigiu a introdus un sistem de supraveghere secretă în cadrul căruia pot fi interceptate comunicațiile de telefonie mobilă ale tuturor utilizatorilor serviciilor de telefonie mobilă oferite de furnizori ruși, fără ca utilizatorii să fie informați vreodată despre această supraveghere. Ca atare, legislația în litigiu afectează în mod direct orice utilizator al serviciilor de telefonie mobilă.

176. În plus, pentru motivele expuse în continuare (pct. 286-300), dreptul rus nu oferă căi de atac efective unei persoane care crede că a fost supusă unei supravegheri secrete.

177. Prin urmare, reclamantul nu a reușit să demonstreze că riscă să fie supus supravegherii secrete din cauza situației sale personale.

178. Având în vedere caracterul secret al măsurilor de supraveghere prevăzute de legislația în litigiu, aplicarea lor pe scară largă, din moment ce afectează toți utilizatorii serviciilor de comunicații de telefonie mobilă, precum și lipsa căilor de atac efective care permit contestarea în plan intern a presupusei aplicări a unor astfel de măsuri, Curtea consideră justificată examinarea *in abstracto* a acestei legislații.

179. Prin urmare, Curtea consideră că reclamantul are dreptul să se pretindă victima unei încălcări a Convenției, chiar dacă nu poate argumenta în susținerea cererii sale faptul că a fost supus unei măsuri concrete de supraveghere. Pentru aceleași motive, simpla existență a legislației în litigiu constituie, în sine, o ingerință în exercitarea de către reclamant a drepturilor derivate de la art. 8. În consecință, Curtea respinge obiecția ridicată de Guvern cu privire la lipsa calității de victimă a reclamantului.

2. Cu privire la justificarea ingerinței

a) Observațiile părților

i. Accesibilitatea dreptului intern

180. Reclamantul susține că Anexele la Decretul nr. 70 care prezintă specificațiile tehnice ale echipamentului ce trebuie instalat de furnizorii de servicii de comunicații nu au fost niciodată publicate oficial și nu sunt accesibile cetățenilor. În opinia sa, în măsura în care acestea stabilesc atribuțiile organelor de aplicare a legii în materie de supraveghere secretă, aceste acte adiționale au efect asupra drepturilor cetățenilor și ar fi trebuit așadar să fie publicate. Potrivit acestuia, nu faptul că a putut în cele din urmă să le consulte în cursul procedurii interne a remediat absența unei publicări oficiale (reclamantul face trimitere la *Kasymakhunov și Saybatalov împotriva Rusiei*, nr. 26261/05 și 26377/06, pct. 92, 14 martie 2013). În opinia sa, cetățenii nu trebuie să fie constrânși să declanșeze o acțiune în justiție pentru a avea acces la o reglementare care îi este aplicabilă. Curtea a concluzionat

deja că este esențial să se stabilească norme clare, detaliate și accesibile cu privire la aplicarea măsurilor de supraveghere secretă (*Shimovolos împotriva Rusiei*, nr. 30194/09, pct. 68, 21 iunie 2011).

181. Potrivit Guvernului, Ordinul nr. 70 are caracter tehnic și, prin urmare, nu se pretează publicării oficiale. Acesta a fost publicat într-o revistă de specialitate, *SvyazInform* (nr. 6 din 1999) și este inclus totodată în baza de date juridică disponibilă pe internet *ConsultantPlus*, unde poate fi consultat gratuit. Guvernul observă că reclamantul a prezentat Curții o copie a ordinului, împreună cu actele adiționale, ceea ce demonstrează că el a avut acces la acesta. În consecință, dreptul intern este accesibil.

ii. Domeniul de aplicare a măsurilor de supraveghere secretă

182. Reclamantul susține că anterior Curtea a constatat că LMOI nu a îndeplinit cerința de „previzibilitate” pe motiv că atribuțiile discreționare legale de care beneficiază autoritățile pentru a dispune o „operațiune de testare” – care implică înregistrarea comunicațiilor private cu ajutorul unui aparat de transmisie radio – nu erau supuse niciunei condiții și că întinderea și modurile de exercitare a acestor atribuții nu erau definite [*Bykov împotriva Rusiei* (MC), nr. 4378/02, pct. 80, 10 martie 2009]. Potrivit reclamantului, prezenta cauză este similară cu cauza *Bykov*. În special, dreptul rus nu indică în mod clar categoriile de persoane care pot fi supuse unor măsuri de interceptare. Astfel, măsurile de supraveghere nu se limitează la persoanele bănuite sau învinuite de infracțiuni: orice persoană care deține informații despre o infracțiune ar putea fi interceptată. În plus, măsurile de interceptare nu se limitează la infracțiunile grave sau deosebit de grave. Dreptul rus autorizează aceste măsuri și în contextul infracțiunilor de gravitate medie, cum ar fi furtul din buzunare.

183. Guvernul susține că interceptarea comunicațiilor poate fi făcută numai după primirea unor informații că o infracțiune a fost comisă, este în curs de comitere sau în pregătire, a unor informații despre persoane care se pregătesc să comită o infracțiune, care comit o infracțiune ori au comis-o deja, sau a unor informații despre fapte sau activități care pun în pericol securitatea națională, militară, economică sau ecologică a Federației Ruse. În decizia din 14 iulie 1998, Curtea Constituțională a declarat că activitatea de colectare a informațiilor despre viața privată a unei persoane este autorizată numai în vederea prevenirii sau depistării infracțiunilor ori în vederea cercetării penale a acestora, ori în vederea atingerii altor scopuri legitime enumerate în LMOI.

184. Guvernul adaugă că numai infracțiunile de gravitate medie, infracțiuni grave și infracțiunile deosebit de grave pot duce la adoptarea unei decizii de interceptare și că numai persoanele care sunt bănuite de astfel de infracțiuni sau care pot avea informații despre aceste infracțiuni pot fi supuse măsurilor de interceptare. În acest sens, Curtea a concluzionat deja că măsurile de supraveghere aplicate unei persoane nesuspectate de săvârșirea unei infracțiuni pot fi justificate în temeiul Convenției [Guvernul se referă la *Greuter împotriva Țărilor de Jos* (dec.), nr. 40045/98, 19 martie 2002].

185. În ceea ce privește interceptările în vederea protejării securității naționale, Guvernul susține că cerința de „previzibilitate” a legii nu include obligarea statelor la adoptarea unor dispoziții legale care enumeră în detaliu toate comportamentele ce pot duce la decizia de a supune o persoană supravegherii din motive de „securitate națională” (Guvernul se referă la *Kennedy*, citată anterior, pct. 159).

iii. Durata măsurilor de supraveghere secretă

186. Reclamantul susține că LMOI nu precizează circumstanțele în care interceptarea poate fi prelungită după termenul de 6 luni și că legea nu stabilește durata maximă a unei măsuri de interceptare.

187. Guvernul declară că, în dreptul rus, interceptarea poate fi autorizată de un judecător pentru o perioadă de maxim 6 luni și poate fi prelungită dacă este necesar. Acesta adaugă că măsura trebuie ridicată în cazul în care urmărirea penală este finalizată. Acesta consideră că este rezonabil să lase durata interceptărilor la discreția autorităților naționale, având în vedere complexitatea și durata urmăririi penale într-o anumită cauză (*Kennedy*, citată anterior). De asemenea, Guvernul menționează cauza *Van Pelt împotriva Țărilor de Jos* (nr. 20555/92, decizia Comisiei din 6 aprilie 1994), în care Comisia a ajuns la concluzia că interceptările telefonice la care reclamantul a fost supus timp de aproape 2 ani nu au constituit o încălcare a Convenției.

iv. Proceduri de urmat pentru păstrarea, consultarea, examinarea, folosirea, transmiterea și distrugerea datelor interceptate

188. Reclamantul afirmă că LMOI nu stabilește nici procedurile de urmat pentru examinarea, păstrarea, consultarea sau folosirea datelor interceptate, nici măsurile de precauție de luat în ceea ce privește transmiterea acestora către alte părți. Legea prevede că acestea trebuie să fie distruse în termen de 6 luni, cu excepția cazului în care sunt necesare în interesul serviciului sau al justiției. Însă

nu există nicio definiție a noțiunii „interesul serviciului sau al justiției”. De asemenea, dreptul rus lasă o libertate deplină instanței de fond pentru a decide, la finalul procesului, dacă se impune păstrarea sau distrugerea datelor utilizate ca probe.

189. Guvernul susține că LMOI impune ca înregistrările comunicațiilor interceptate să fie păstrate în condiții care exclud orice risc de ascultare sau copiere de către persoane neautorizate. Acesta adaugă că decizia judecătorească de autorizare a interceptării comunicațiilor, documentele care au stat la baza acestei hotărâri, precum și datele colectate prin interceptare constituie secret de stat și trebuie să rămână în posesia exclusivă a organului de stat care efectuează interceptările. În cazul în care este necesară transmiterea lor la un investigator, un procuror sau o instanță, aceste elemente pot fi declassificate de șefii organelor care îndeplinesc măsurile operative de investigații. Autorizațiile de interceptare vor fi declassificate de instanțele care le-au emis. Procedura de urmat pentru a trimite datele colectate în cadrul măsurilor operative de investigații la organele de cercetare competente sau la o instanță este definită prin Ordinul Ministerului de Interne din 27 septembrie 2013 (*supra*, pct. 58).

190. Potrivit Guvernului, datele colectate în cadrul măsurilor operative de investigații se păstrează timp de 1 an, apoi se distrug, cu excepția cazului în care acestea sunt necesare în interesele serviciului sau justiției, iar înregistrările se păstrează timp de 6 luni, apoi se distrug. Prin urmare, dreptul rus este previzibil și oferă garanții suficiente.

v. Autorizarea măsurilor de supraveghere secretă

α) Reclamantul

191. Reclamantul susține că, deși dreptul intern impune pentru orice interceptare o autorizație judiciară prealabilă, procedura de autorizare nu oferă garanții suficiente împotriva abuzurilor. În primul rând, în cazurile urgente, se permite interceptarea comunicațiilor fără autorizație judiciară pe o durată de cel mult 48 de ore. În al doilea rând, contrar dispozițiilor din Codul de procedură penală, LMOI nu prevede nicio condiție referitoare la conținutul autorizației de interceptare. În special, legea nu prevede că subiectul interceptării trebuie identificat clar în autorizație prin nume, număr de telefon sau adresă (a se vedea, *a contrario*, legislația britanică și cea bulgară citate în *Kennedy*, *supra*, pct. 41 și 160; a se vedea, de asemenea, *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiev*, citată anterior, pct. 13). De asemenea, dreptul intern nu impune ca autorizația să precizeze ce comunicații sau ce tipuri de comunicații trebuie să fie înregistrate, pentru a restrânge astfel competențele discreționare de care beneficiază organele de aplicare a legii la stabilirea întinderii măsurilor de supraveghere. Legislația rusă nu stabilește nici norme speciale pentru supraveghere în situații delicate, de exemplu în cazuri care implică confidențialitatea surselor jurnalistice sau atunci când supravegherea vizează comunicațiile dintre un avocat și clientul său, care fac parte din secretul profesional.

192. În plus, reclamantul precizează că dreptul intern nu impune judecătorului obligația de a verifica existența unei „suspiciuni întemeiate” în privința persoanei ori de a aplica criteriile de „necesitate” și „proporționalitate”. Serviciile solicitante nu sunt obligate să atașeze documente justificative la cererile de interceptare. În plus, LMOI prevede interdicția expresă de a prezenta judecătorului anumite documente – cele care conțin informații despre investigatori infiltrați ori informatori ai poliției, sau despre tactica și organizarea corespunzătoare măsurilor operative de investigații –, ceea ce îl împiedică pe judecător să verifice în mod concret existența unei „suspiciuni întemeiate”. Dreptul rus nu prevede că judecătorul trebuie să limiteze autorizația exclusiv la cazurile în care scopurile legitime urmărite nu pot fi atinse prin alte mijloace mai puțin invazive.

193. În susținerea afirmației sale că judecătorii nu verifică dacă o „suspiciune întemeiată” planează asupra persoanei și nu aplică criteriile de „necesitate” și „proporționalitate”, reclamantul a prezentat copia notelor analitice emise de trei instanțe districtuale situate în diferite regiuni ale Rusiei (regiunea Tambov, regiunea Tula și Republica Dagestan). În opinia reclamantului, aceste instanțe fac acolo rezumatul pentru 2010-2013 al propriei jurisprudențe privind măsurile operative de investigații care implică încălcări ale caracterului privat al comunicațiilor sau ale caracterului privat al domiciliului. O instanță a declarat că nu acordă autorizația pentru a desfășura o măsură operativă de investigații dacă aceasta nu se află în lista de măsuri prevăzute în LMOI, dacă cererea de autorizare nu este semnată de un funcționar competent sau nu este motivată, sau dacă respectiva cauză intră sub incidența unei restricții legale care împiedică folosirea unei astfel de măsuri (de exemplu, din cauza situației persoanei vizate sau a naturii infracțiunii). Aceeași instanță a declarat că acordă autorizația atunci când sunt îndeplinite toate condițiile sus-menționate. O altă instanță precizează că autorizația poate fi refuzată în cazul în care cererea nu este motivată suficient, adică în cazul în care aceasta nu conține suficiente informații pentru a permite judecătorului să se asigure că măsura este legală și justificată. Cea de a treia instanță a declarat că acordă autorizația atunci când o solicită un organ de aplicare a legii. Aceasta declară că nu a respins niciodată o astfel de cerere. Cele trei instanțe au considerat că această cerere este motivată suficient dacă se referă la existența informațiilor

menționate la art. 8 § 2 din LMOI (*supra*, pct. 31). Una dintre ele a precizat că niciodată cererile de autorizare nu sunt însoțite de documente justificative; alta a observat că unele cereri includ astfel de documente, dar nu toate; a treia a declarat că toate cererile sunt însoțite de astfel de documente. Cele trei instanțe au declarat că nu solicită niciodată organelor de aplicare a legii să prezinte documente justificative suplimentare, care să confirme, de exemplu, motivele interceptării ori să demonstreze că numerele de telefon interceptate aparțin persoanei vizate. Două instanțe declară că acordă autorizații de interceptare care vizează persoane neidentificate; una dintre ele precizează că aceste autorizații vizează doar colectarea de date provenite de la mijloace tehnice de comunicații. Astfel de autorizații nu menționează o anumită persoană sau un număr de telefon de interceptat, dar permit interceptarea tuturor comunicațiilor telefonice din zona în care a fost comisă o infracțiune. Una dintre instanțe declară că nu acordă o asemenea autorizație niciodată. Două instanțe declară că autorizațiile indică întotdeauna perioada de timp în care este permisă interceptarea; a treia declară că durata operațiunii nu este specificată niciodată în autorizațiile pe care le emite. În fine, niciuna dintre cele trei instanțe nu a examinat vreo plângere depusă de persoane ale căror comunicări au fost interceptate.

194. Reclamantul prezintă, de asemenea, statistici oficiale întocmite de Curtea Supremă în perioada 2009-2013. Rezultă că, în 2009, instanțele ruse au primit 130 083 de cereri de interceptare depuse în temeiul Codului de procedură penală dintr-un total de 132 821 și 245 645 de cereri depuse în temeiul LMOI din 246 228 (adică 99 %). În 2010, instanțele au admis 136 953 de cereri de interceptare depuse în temeiul Codului de procedură penală din 140 372 și alte 276 682 de cereri depuse în temeiul LMOI din 284 137. În 2011, au primit 140 047 de cereri de interceptare depuse în temeiul Codului de procedură penală din 144 762 și alte 326 105 de cereri depuse în temeiul LMOI din 329 415. În 2012, instanțele au admis 156 751 de cereri de interceptare depuse în temeiul Codului de procedură penală din 163 469 și alte 372 744 de cereri depuse în temeiul LMOI din 376 368 (adică 99 %). În 2013, instanțele au admis 178 149 de cereri de interceptare depuse în temeiul Codului de procedură penală din 189 741 (adică 93 %) și alte 416 045 de cereri depuse în temeiul LMOI din 420 242 (adică 99 %). Reclamantul subliniază că numărul de autorizații de interceptare aproape că s-a dublat din 2009 până în 2013. De asemenea, acesta susține că procentul foarte ridicat de autorizații emise arată că instanțele nu verifică dacă există o „suspiciune întemeiată” în privința subiectului interceptării și nu exercită un control atent și riguros. În consecință, potrivit reclamantului, măsurile de interceptare sunt dispuse în cazul foarte multor persoane în situații în care informațiile ar fi putut fi obținute prin mijloace mai puțin invazive.

195. Reclamantul concluzionează de aici că procedura de autorizare este viciată și, prin urmare, necorespunzătoare pentru a limita folosirea unor măsuri de supraveghere secretă la ceea ce este necesar într-o societate democratică.

196. În ceea ce privește garanțiile împotriva interceptărilor neautorizate, reclamantul susține că dreptul intern nu obligă organele de aplicare a legii să prezinte o autorizație judiciară furnizorului de servicii de comunicații pentru a obține acces la comunicațiile unei persoane. Toate autorizațiile legale sunt documente clasificate, deținute exclusiv de organele de aplicare a legii. Obligația de a transmite o autorizație de interceptare furnizorului de servicii de comunicații este menționată o singură dată în dreptul rus, în legătură cu supravegherea datelor de comunicații exercitată în conformitate cu Codul de procedură penală (*supra*, pct. 48). Echipamentul instalat de furnizorii de servicii de comunicații în conformitate cu ordinele Ministerului Comunicațiilor, în special actele adiționale nepublicate ale Ordinului nr. 70, ar oferi organelor de aplicare a legii acces direct și nelimitat la toate comunicațiile de telefonie mobilă ale tuturor utilizatorilor. De asemenea, Ordinul nr. 538 impune furnizorilor de servicii de comunicații obligația de a crea baze de date pentru a putea păstra timp de 3 ani informații despre toți abonații și despre serviciile oferite acestora. Serviciile secrete ar avea astfel acces la distanță și direct la aceste baze de date. Astfel, modul de funcționare a sistemului de supraveghere secretă ar oferi serviciilor de securitate și poliției mijloace tehnice pentru a eluda procesul de autorizare și pentru a intercepta orice comunicare fără autorizare legală prealabilă. Prin urmare, necesitatea de a obține o astfel de autorizație va surveni numai în cauzele în care datele interceptate trebuie folosite ca probe în cadrul unei proceduri penale.

197. Reclamantul prezintă documente care, în opinia sa, arată că organele de aplicare a legii interceptează ilegal comunicațiile telefonice fără autorizație judiciară prealabilă și divulgă înregistrările acestora unor persoane neautorizate. Acesta dă, ca exemplu, versiunea tipărită a paginilor de internet care conțin stenogramele convorbirilor telefonice private ale unor politicieni. Acesta prezintă, de asemenea, articole din presă care menționează urmărirea penală îndreptată împotriva mai multor cadre superioare din serviciile tehnice ale poliției. Acești polițiști au fost suspectați de interceptarea ilegală a comunicațiilor private ale unor persoane din mediul politic și cel al afacerilor, în schimbul mitei plătite de oponenții politici sau comerciali ai persoanelor respective. Articolele respective menționează declarații ale martorilor care au afirmat că interceptarea comunicațiilor în schimbul mitei constituie o practică larg răspândită și că oricine poate cumpăra de la poliție stenograma convorbirilor telefonice ale altei persoane.

β) Guvernul

198. Guvernul declară că orice interceptare a comunicațiilor, telefonice sau de alt tip, trebuie să fie autorizată de o instanță. În opinia sa, instanța se pronunță în temeiul unei cereri motivate depuse de un organ de aplicare a legii. Sarcina probei revine organului solicitant, care este obligat să justifice necesitatea măsurilor de interceptare. Pentru a dovedi necesitatea, organul solicitant atașează cererii sale toate documentele justificative relevante, cu excepția celor care conțin informații despre investigatori sub acoperire sau informatori ai poliției ori despre tactica și organizarea corespunzătoare măsurilor operative de investigații. Derogarea se justifică prin necesitatea de a asigura securitatea și protecția investigatorilor sub acoperire și a informatorilor poliției, precum și a familiilor acestora, și este așadar compatibilă cu Convenția.

199. Guvernul menționează, de asemenea, hotărârea Plenului Curții Supreme din 27 iunie 2013, considerând că instanța a explicat aici instanțelor inferioare că orice restrângere a drepturilor și libertăților fundamentale trebuie să fie prevăzută de lege și să fie necesară într-o societate democratică, adică proporțională cu un scop legitim. Înalta instanță a cerut instanțelor să se bazeze pe fapte stabilite, să se asigure de existența unor motive pertinente și suficiente pentru a justifica o restrângere a drepturilor unei persoane și să creeze un echilibru între interesele persoanei ale cărei drepturi sunt restrânse și interesele altor persoane, ale statului și societății. LMOI obligă expres instanțele să motiveze decizia de autorizare a măsurii de interceptare. În urma deciziei Curții Constituționale din 8 februarie 2007 (*supra*, pct. 42), era necesar ca autorizația de interceptare să indice motivele exacte pentru care persoana vizată în cererea de măsuri operative de investigații este suspectată de o infracțiune sau de activități care pun în pericol securitatea națională, militară, economică sau ecologică a țării. În decizia din 2 octombrie 2003 (*supra*, pct. 41), Curtea Constituțională a mai declarat că judecătorul este obligat să examineze atent și amănunțit documentele care îi sunt prezentate.

200. În practică, orice autorizație de interceptare indică organul de stat responsabil pentru efectuarea interceptării, motivele care stau la baza aplicării măsurilor de supraveghere și motivele care justifică necesitatea acestora; în plus, se menționează prevederile legale aplicabile, numele persoanei ale cărei comunicații se interceptează, motivul pentru care aceasta este suspectată de implicare în comiterea unei anumite infracțiuni, numărul său de telefon sau codul IMEI, perioada pentru care se acordă autorizația, precum și orice alte informații necesare. În circumstanțe speciale, se permite autorizarea interceptării comunicațiilor unor persoane neidentificate. În acest caz, în principiu, judecătorul autorizează colectarea datelor provenite de la mijloace tehnice de comunicații pentru identificarea persoanelor prezente într-un anumit loc atunci când s-a comis o infracțiune acolo. Această practică este compatibilă cu principiile stabilite în jurisprudența Curții cu condiția ca, în astfel de situații, mandatul de interceptare să indice setul unic de spații (locuri) vizate de interceptarea autorizată în mandat (Guvernul se referă la cauza *Kennedy*, citată anterior).

201. În situații de urgență, dreptul rus încuviințează interceptarea comunicațiilor fără autorizație judiciară prealabilă. Judecătorul trebuie să fie informat despre existența unei astfel de situații în termen de 24 de ore, iar autorizația legală pentru prelungirea măsurii de interceptare trebui să fie obținută în termen de 48 de ore. Judecătorul este obligat să examineze legalitatea unei astfel de măsuri chiar dacă a fost deja ridicată. Guvernul face trimitere la o hotărâre pronunțată în apel de Curtea Supremă la 13 decembrie 2013 într-o cauză penală, hotărâre în care înalta instanță a declarat inadmisibile, ca mijloace de probă, înregistrările unor convorbiri telefonice realizate fără autorizație judiciară prealabilă în cadrul unei proceduri de urgență. Curtea Supremă a concluzionat că, și dacă un judecător a fost informat despre interceptare, nu s-a pronunțat nicio decizie judecătorească privind legalitatea sau necesitatea acesteia.

vi. Controlul aplicării măsurilor de supraveghere secretă

α) Reclamantul

202. Pentru început, reclamantul susține că, în Rusia, eficiența oricărui control asupra interceptărilor este compromis de lipsa unei obligații, pentru organele de interceptare, de a ține evidența interceptărilor pe care le efectuează. În plus, Ordinul nr. 70 prevede în mod expres că informațiile despre interceptări nu pot fi nici consemnate, nici înregistrate.

203. Reclamantul adaugă că, în Rusia, nici judecătorul care a emis autorizația de interceptare, nici alt funcționar independent având calificările necesare pentru a fi magistrat, nu are capacitatea de a controla punerea în aplicare a măsurii, inclusiv de a verifica dacă supravegherea a rămas în limitele stabilite de autorizație și a respectat diferitele condiții stabilite în dreptul intern.

204. Dreptul intern nu definește nicio procedură privind controlul asupra interceptărilor exercitat de Președinte, Parlament și Guvernul Federației Ruse. Aceștia nu au în mod evident nicio putere să controleze aplicarea măsurilor de interceptare în situații specifice.

205. În ceea ce privește controlul exercitat de Procurorul General și procurorii din subordine

competenți, reclamantul consideră că aceste persoane nu pot fi considerate independente, având în vedere poziția lor în sistemul de justiție penală și funcția lor constând în exercitarea urmăririi penale. Acesta susține în special că procurorii aprobă toate cererile de interceptare depuse de organele de anchetă în cursul procedurilor penale și participă la ședințele de judecată aferente. Acesta precizează că procurorii au, în cursul urmăririi penale, posibilitatea de a utiliza datele colectate prin interceptare, printre altele prezentându-le ca mijloace de probă în cursul procesului. Există așadar un conflict de interese deoarece procurorul exercită o funcție dublă, în sensul că este atât parte în procedura penală, cât și autoritatea de control asupra interceptărilor.

206. Reclamantul adaugă că funcțiile de control ale procurorilor sunt limitate ca urmare a faptului că unele elemente, în special cele care dezvăluie identitatea investigatorilor sub acoperire sau tacticile, metodele și mijloacele utilizate de serviciile de securitate, se situează în afara controlului lor. Competențele de control ale procurorilor sunt restrânse, de asemenea, în domeniul contra-informațiilor, unde verificările sunt posibile numai în urma unei plângeri individuale. Având în vedere caracterul secret al măsurilor de interceptare și lipsa informării persoanei vizate, este puțin probabilă depunerea unor astfel de plângeri individuale, astfel încât măsurile de supraveghere legate de contra-informații se află *de facto* în afara controlului procurorilor. În opinia reclamantului, este totodată de remarcat faptul că procurorii nu au competența de a anula o autorizație de interceptare, de a dispune încetarea unei interceptări ilegale sau de a dispune distrugerea datelor colectate în mod ilegal.

207. În plus, rapoartele semestriale întocmite de procurori nu sunt urmate nici de publicare, nici de dezbatere publică. Aceste rapoarte sunt documente clasificate și conțin doar informații statistice. Ele nu oferă nicio analiză pe fond cu privire la nivelul legalității care prevalează în domeniul măsurilor operative de investigații și nicio informație cu privire la încălcările depistate și la tipul de măsuri luate pentru a le remedia. În plus, aceste rapoarte contopesc toate tipurile de măsuri operative de investigații, fără a face distincție între interceptări și alte măsuri.

β) Guvernul

208. Potrivit Guvernului, controlul asupra măsurilor operative de investigații, inclusiv asupra interceptării comunicațiilor telefonice, este exercitat de Președintele, Parlamentul și Guvernul Federației Ruse. Mai exact, Președintele definește strategia de securitate națională și totodată numește și revocă persoanele responsabile de toate organele de aplicare a legii. De asemenea, administrația prezidențială include un serviciu însărcinat special cu controlarea activităților organelor de aplicare a legii, inclusiv a măsurilor operative de investigații. Acest serviciu este alcătuit din cadre ale Ministerului de Interne și ale FSB cu certificatul de securitate corespunzător. Parlamentul participă la procesul de control prin adoptarea și modificarea legislației care reglementează măsurile operative de investigații. Acesta are, de asemenea, posibilitatea de a înființa comitete și comisii și desfășoară ședințe parlamentare referitoare la o varietate de probleme, inclusiv cele legate de măsurile operative de investigații, și poate audia, după necesitate, persoanele responsabile din cadrul organelor de aplicare a legii. În ceea ce privește Guvernul, acesta emite decrete și ordine care reglementează măsurile operative de investigații și alocă resurse bugetare organelor de aplicare a legii.

209. Controlul este exercitat, de asemenea, de Procurorul General și procurorii din subordine competenți, care sunt independenți de autoritățile federale, regionale și locale. Procurorul General și adjuncții săi sunt numiți și eliberați din funcție de Consiliul Federației, camera superioară a Parlamentului. Procurorii nu au competența de a depune cereri de interceptare. Acestea pot fi depuse fie de organul de stat care pune în aplicare măsuri operative de investigații în temeiul LMOI, fie de organul de investigații în temeiul Codului de procedură penală. Procurorul nu este abilitat să dea dispoziții organului de investigații. În cadrul unui control efectuat de procuror, șeful organului de interceptare este obligat să prezinte procurorului orice material relevant la cererea acestuia din urmă; în caz de neîndeplinire, este posibil ca acesta să fie tras la răspundere. Procurorii care se ocupă de controlul măsurilor operative de investigații prezintă procurorului general rapoarte semestriale, care însă nu analizează interceptările separat de alte măsuri operative de investigații.

vii. Notificarea măsurilor de supraveghere secretă

α) Reclamantul

210. Reclamantul afirmă că dreptul rus nu prevede că persoana ale cărei comunicații sunt interceptate trebuie să primească notificare în acest sens anterior, în timpul sau ulterior operațiunii. Acesta consideră acceptabilă neinformarea persoanei vizate înaintea sau în timpul interceptării, din moment ce caracterul secret al măsurii este esențial pentru eficacitatea acesteia. Acesta susține însă că, odată încheiată interceptarea, notificarea este posibilă, „din moment ce [aceasta] poate fi realizată fără a pune în pericol scopul restrângerii” (reclamantul face trimitere la *Klass și alții*, citată anterior). În Rusia, persoana vizată nu primește notificare în niciun stadiu. Prin urmare, este posibil ca aceasta să nu aibă cunoștință de interceptare decât în cazul unei indiscreții sau al unei proceduri penale care a

fost declanșată împotriva sa și în cadrul căreia datele interceptate au fost folosite ca probe.

211. În ceea ce privește posibilitatea de a obține acces la datele colectate în timpul interceptării, reclamantul susține că aceasta există numai în circumstanțe foarte limitate. În opinia sa, dacă nu s-a declanșat nicio procedură penală sau dacă acuzațiile au fost retrase pentru alte motive decât cele enumerate în LMOI, persoana vizată nu poate avea acces la date. În plus, pentru a obține acest acces, reclamantul este obligat să demonstreze că a existat o interceptare a comunicațiilor sale. Având în vedere caracterul secret al măsurilor de supraveghere și lipsa notificării, această probă ar fi imposibil de prezentat în lipsa unei scurgeri de informații despre interceptare. Chiar și după ce a îndeplinit toate condiții prealabile, persoana vizată va putea primi doar „informații despre datele colectate”, dar nu va obține acces la datele propriu-zise. În cele din urmă, numai informațiile care nu conțin secrete de stat vor putea fi divulgate. Potrivit reclamantului, întrucât în temeiul LMOI toate datele colectate în cursul măsurilor operative de investigații constituie secrete de stat și decizia de clasificare aparține șefului serviciului de interceptare, accesul la documentele aferente interceptării este în totalitate la discreția serviciilor de interceptare.

212. Neacordarea accesului la datele colectate poate fi atacată în instanță, iar LMOI impune serviciilor de interceptare obligația de a prezenta, la cererea instanței, „materialul aferent măsurilor operaționale de investigații care conține informații despre datele la care s-a refuzat accesul”. Reclamantul consideră semnificativ faptul că serviciile de interceptare sunt obligate să furnizeze „informații despre date” și nu datele propriu-zise. Acesta a adăugat că materialul care conține informații despre investigatori sub acoperire sau informatori ai poliției nu poate fi prezentat instanței și se află, prin urmare, în afara domeniului de aplicare a controlului jurisdicțional.

β) Guvernul

213. Guvernul explică faptul că, în dreptul rus, nu se consideră că o persoană supusă unor măsuri de supraveghere secretă urmează să fie informată în acest sens. Acesta amintește că și Curtea Constituțională a declarat că, având în vedere necesitatea de a păstra secretul măsurilor de supraveghere, principiul publicității ședinței și cel al contradictorialității nu sunt aplicabile procedurii de autorizare (*supra*, pct. 40). Persoana vizată nu poate așadar nici să participe la procedura de autorizare, nici să fie informată despre decizia luată.

214. După încheierea urmăririi penale, este posibil ca persoana vizată să examineze toate probele depuse la dosar, inclusiv datele colectate în cursul măsurilor operative de investigații. De asemenea, în cazurile în care organul de cercetare a decis să nu declanșeze o procedură penală împotriva subiectului interceptării ori să renunțe la urmărirea penală pe motiv că presupusa infracțiune nu a fost comisă ori că unul sau mai multe dintre elementele constitutive ale unei infracțiuni lipsesc, persoana în cauză are posibilitatea de a primi, la cerere, informații despre datele colectate. Refuzul de a acorda aceste informații poate fi atacat în instanță, aceasta având competența de a dispune comunicarea lor în cazul în care consideră că refuzul este neîntemeiat. Guvernul a prezentat o copie a deciziei din 4 august 2009 a Judecătoriei Alexeievski (regiunea Belgorod), care a obligat poliția să ofere unei persoane supuse unei interceptări, în termen de o lună, informații despre datele colectate despre aceasta în timpul operațiunii, „în măsura în care normele de confidențialitate le authorizează și cu excepția datelor care ar putea permite divulgarea unor secrete de stat”.

215. Guvernul susține că dreptul rus diferă de dreptul bulgar, criticat de Curte în hotărârea *Asociația pentru Integritate Europeană și Drepturile Omului și Ekimdzhiev* (citată anterior, pct. 91), prin faptul că acesta prevede posibilitatea de a declassifica elementele interceptate și de a permite accesul persoanei vizate la aceste elemente. În susținerea acestei afirmații, acesta face trimitere la hotărârea din 11 iulie 2012, prin care Curtea Regională Zabaikalsk a pronunțat o condamnare penală. Această hotărâre – pe care Curtea nu a primit-o în copie – vizează, potrivit Guvernului, o decizie judecătorească de autorizare a interceptării comunicațiilor telefonice ale persoanei vizate, decizie care a fost declassificată și prezentată instanței de fond, la cererea acesteia. De asemenea, Guvernul se referă la alte două hotărâri - una a prezidiului Curții Regionale Krasnoyarsk, cealaltă a prezidiului Curții Supreme a Republicii Mari – care a anulat, pe calea revizuirii, hotărârile judecătorești care au autorizat interceptarea comunicațiilor. Guvernul nu a furnizat copii ale acestor hotărâri.

viii. Căile de atac disponibile

α) Reclamantul

216. Reclamantul consideră că problema notificării măsurilor de supraveghere și cea a eficienței căilor de atac sunt legate indisolubil între ele deoarece, dacă nu este informată despre măsurile luate fără știrea sa, persoana nu poate, în principiu, să conteste retroactiv legalitatea în instanță (reclamantul face trimitere la *Weber și Saravia*, decizie citată anterior).

217. Acesta susține că sunt ineficiente căile de atac disponibile în dreptul rus. În ceea ce privește posibilitatea persoanei supuse supravegherii de a solicita un control jurisdicțional asupra măsurilor

aplicate, reclamantul precizează că persoana respectivă este cea care trebuie să demonstreze că a fost supusă interceptării, dar că, întrucât persoana supusă supravegherii nu este informată despre această măsură decât în cazul în care este inculpată pentru o infracțiune, îi este imposibil să îndeplinească sarcina probei. Copiile hotărârilor interne prezentate de Guvern au ca obiect măsuri de percheziție și confiscare, adică măsuri operative de investigații cunoscute de persoanele vizate (*infra*, pct. 220, 221 și 223). Reclamantul a declarat că nu a avut cunoștință de deciziile judecătorești, accesibile publicului, prin care s-a admis plângerea unei persoane care a fost supusă unei interceptări și a denunțat caracterul ilegal al măsurii. De asemenea, acesta consideră semnificativ faptul că niciuna dintre hotărârile judecătorești prezentate de Guvern nu conținea o evaluare, de către instanțele interne, a proporționalității măsurilor operative de investigații în litigiu. Acesta adaugă că procedura internă pe care a inițiat-o arată totodată în mod clar că sunt ineficiente căile de atac oferite de dreptul intern. În plus, în cauza *Avanesyan împotriva Rusiei* (nr. 41152/06, 18 septembrie 2014), Curtea a hotărât deja că în dreptul rus nu existau căi de atac eficiente pentru a contesta măsurile operative de investigații.

218. În fine, reclamantul afirmă că, întrucât ordinele ministeriale privind interceptarea secretă a comunicațiilor erau considerate ca având caracter tehnic, nu juridic, și deci nu puteau face obiectul controlului jurisdicțional, nici persoana supusă interceptării și nici furnizorul de servicii de comunicații nu puteau să le conteste, așa cum s-a demonstrat deja (*supra*, pct. 161).

β) Guvernul

219. Guvernul afirmă că, în Rusia, o persoană care consideră că drepturile sale au fost ori sunt încălcate de un funcționar al statului în cadrul punerii în aplicare a măsurilor operative de investigații poate face plângere la superiorul ierarhic al funcționarului, la un procuror sau o instanță – în temeiul art. 5 din LMOI (*supra*, pct. 83).

220. Acesta precizează că, în conformitate cu explicațiile date de Plenul Curții Supreme, în cazul în care persoana vizată află că a existat interceptare, aceasta poate sesiza o instanță ordinară urmând procedura prevăzută în capitolul 25 C. proc. civ. (*supra*, pct. 92). Reclamantul nu este obligat să dovedească faptul că măsurile de interceptare au cauzat încălcarea drepturilor sale; serviciile de interceptare sunt cele cărora le revine sarcina de a demonstra că măsurile de interceptare au fost legale și justificate. Guvernul adaugă că, în dreptul rus, în cazul în care o instanță constată pe latura civilă încălcarea drepturilor reclamantului, aceasta trebuie să ia măsuri pentru remedierea încălcării și repararea prejudiciului (*supra*, pct. 97). Guvernul a furnizat copii după două decizii judecătorești întemeiate pe capitolul 25 C. proc. civ., decizii care au declarat ilegale anumite percheziții și confiscări de obiecte sau documente și au impus poliției să ia măsuri specifice pentru a remedia încălcarea.

221. În plus, este posibil în legătură cu interceptarea să se depună o cerere de revizuire împotriva hotărârii judecătorești de autorizare a interceptării, astfel cum a explicat Curtea Constituțională în decizia sa din 15 iulie 2008 (*supra*, pct. 43). De asemenea, persoana în cauză are posibilitatea de a declara apel sau recurs.

222. Guvernul precizează că, dacă interceptarea a avut loc în cadrul unei proceduri penale, persoana vizată poate depune o plângere și în temeiul art. 125 C. proc. pen. Acesta menționează hotărârea din 26 octombrie 2010, prin care Curtea Supremă a anulat, pe calea revizuirii, deciziile instanțelor de grad inferior prin care a fost declarată inadmisibilă plângerea formulată de K. În temeiul art. 125 C. proc. pen., cu privire la refuzul organului de cercetare de a-i furniza o copie a deciziei judecătorești de autorizare a interceptării comunicațiilor sale. Curtea Supremă a declarat că se impune examinarea plângerii în lumina art. 125 C. proc. pen., deși persoana în cauză fusese deja condamnată, și că aceasta avea dreptul la o copie a autorizației de interceptare. Guvernul a prezentat copii după 10 decizii judecătorești care au admis plângeri întemeiate pe art. 125 C. proc. pen., în materie de percheziții și confiscări ilegale de obiecte sau documente. Acesta a mai prezentat o copie a unei hotărâri de achitare a unei persoane, în apel, după ce s-a constatat că și condamnarea sa în primă instanță s-a bazat pe probe inadmisibile strânse în cursul unui flagrant de cumpărare de droguri desfășurat ilegal.

223. Guvernul adaugă că persoana în cauză poate solicita despăgubiri în temeiul art. 1069 C. civ. (*supra*, pct. 102). Acest articol prevede repararea prejudiciului material sau moral cauzat unei persoane fizice sau juridice printr-un act ilegal al unui organ sau funcționar al administrației centrale sau locale, cu condiția să fie dovedită culpa acelui organ sau funcționar. Chestiunea despăgubirii pentru prejudiciul moral este reglementată de principiile stabilite în art. 1099 - 1101 C. civ. (*supra*, pct. 103 și 104). Guvernul precizează în special că prejudiciul moral cauzat prin difuzarea de informații care aduc atingere onoarei, demnității sau reputației unei persoane poate duce la despăgubire, indiferent de existența sau absența unei abateri a autorului prejudiciului. Guvernul a prezentat o copie a deciziei din 9 decembrie 2013, în care Tribunalul Vichuga (regiunea Ivanovo) a acordat o despăgubire pentru repararea prejudiciului moral cauzat de interceptarea ilegală a convorbirilor telefonice ale unui suspect, instanța de fond declarând inadmisibile ca probe înregistrările obținute

prin interceptare. De asemenea, Guvernul a prezentat o decizie judecătorească prin care s-a acordat o despăgubire pentru percheziția ilegală și confiscarea ilegală de documente, precum și o decizie judecătorească prin care s-a dispus despăgubirea unei persoane achitate după ce a fost urmărită penal în mod ilegal.

224. Dreptul rus prevede, de asemenea, acțiuni penale în caz de abuz în serviciu (art. 285 și 286 din C. pen.), colectarea neautorizată sau difuzarea neautorizată de informații despre viața privată și de familie a unei persoane (art. 137 C. pen.) și încălcarea dreptului la caracterul privat al comunicațiilor (art. 138 C. pen. - *supra*, pct. 19 și 22). În acest sens, Guvernul menționează hotărârea din 24 octombrie 2002, prin care Curtea Supremă l-a condamnat pe E.S. pentru că era vinovat de încălcarea art. 138 C. pen. prin instigarea unui funcționar la furnizarea numelor titularilor unor numere de telefon, precum și a detaliilor apelurilor corespunzătoare acestor numere. Acesta mai face trimitere la hotărârea din 15 martie 2007, prin care Curtea Supremă a condamnat un vameș pentru încălcarea art. 138 C. pen. prin interceptarea convorbirilor telefonice ale unui anumit P. Guvernul a prezentat copii după alte două hotărâri de condamnare întemeiate pe art. 138 C. pen.: prima se referă la vânzarea de echipamente de spionaj, și anume stilouri și ceasuri cu cameră integrată; a doua se referă la accesarea ilegală a bazei de date a unui furnizor de servicii de comunicații în scopul obținerii de detalii ale apelurilor utilizatorilor.

225. În cele din urmă, Guvernul susține că dreptul rus prevede, de asemenea, căi de atac pentru a face plângere cu privire la pretinsa insuficiență a garanțiilor împotriva abuzului în cadrul interceptării comunicațiilor (*supra*, pct. 156).

226. Acesta susține că reclamantul nu a exercitat niciuna din căile de atac care sunt disponibile în dreptul rus și care sunt menționate mai sus. Mai precis, reclamantul a ales să declanșeze o acțiune în justiție împotriva operatorilor de rețele mobile, fără ca Ministerul Comunicațiilor să fi intervenit în procedură ca terț.

b) Motivarea Curții

i) Principii generale

227. Curtea reafirmă că o ingerință nu poate fi justificată în temeiul art. 8 decât în cazul în care este prevăzută de lege, urmărește unul sau mai multe dintre scopurile legitime enumerate în art. 8 § 2 și este necesară, într-o societate democratică, pentru atingerea acestui scop sau a acestor scopuri (*Kennedy*, citată anterior, pct. 130).

228. Curtea reamintește jurisprudența sa constantă, conform căreia termenii „prevăzută de lege” înseamnă că măsura trebuie să aibă temei în dreptul intern și să fie compatibilă cu statul de drept, menționat expres în preambulul Convenției și inerent obiectului și scopului art. 8. Prin urmare, legea trebuie să îndeplinească niște cerințe de calitate: trebuie să fie accesibilă persoanei interesate și previzibilă în privința efectelor ei [a se vedea, printre multe altele, *Rotaru împotriva României* (MC), nr. 28341/95, pct. 52, CEDO 2000-V; *S. și Marper împotriva Regatului Unit* (MC), nr. 30562/04 și 30566/04, pct. 95, CEDO 2008; și *Kennedy*, citată anterior, pct. 151].

229. Curtea a hotărât în repetate rânduri că, în domeniul interceptării comunicațiilor, „previzibilitatea” nu poate fi înțeleasă în același mod ca în multe alte domenii. În contextul special al măsurilor de supraveghere secretă, cum ar fi interceptarea comunicațiilor, previzibilitatea nu poate însemna că o persoană trebuie să fie pusă în posibilitatea de a prevedea când autoritățile pot intercepta comunicațiile sale astfel încât să-și poată adapta comportamentul în consecință. Riscul arbitrarului apare clar în cazul în care o competență a executivului este exercitată în secret. Existența unor norme clare și detaliate cu privire la interceptarea convorbirilor telefonice este așadar indispensabilă, mai ales că procedeele tehnice utilizabile evoluează în permanență. Legea trebuie să fie elaborată cu suficientă claritate pentru a indica tuturor în mod corespunzător în ce împrejurări și în ce condiții abilitază autoritățile publice să adopte astfel de măsuri secrete (*Malone*, citată anterior, pct. 67; *Leander împotriva Suediei*, 26 martie 1987, pct. 51, seria A, nr. 116; *Huvig împotriva Franței*, 24 aprilie 1990, pct. 29, seria A nr. 176-B; *Valenzuela Contreras împotriva Spaniei*, 30 iulie 1998, pct. 46, *Culegere* 1998-V; *Rotaru*, citată anterior, pct. 55; *Weber și Saravia*, citată anterior, pct. 93; și *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhev*, citată anterior, pct. 75).

230. În plus, întrucât aplicarea măsurilor de supraveghere secretă a comunicațiilor nu intră sub controlul persoanelor în cauză sau al publicului, „legea” ar fi contrară statului de drept dacă marja de apreciere acordată puterii executive sau judecătorești nu ar cunoaște limite. În consecință, legea trebuie să definească domeniul de aplicare și modul de exercitare a unei astfel de competențe cu suficientă claritate pentru a oferi persoanei o protecție adecvată împotriva arbitrarului (a se vedea, printre altele, *Malone*, citată anterior, pct. 68; *Leander*, citată anterior, pct. 51; *Huvig*, citată anterior, pct. 29; și *Weber și Saravia*, decizie citată anterior, pct. 94).

231. În jurisprudența referitoare la măsurile de supraveghere secretă, Curtea stabilește următoarele garanții minime împotriva abuzurilor de autoritate pe care legea trebuie să le conțină:

natura infracțiunilor care pot duce la un mandat de interceptare; definirea categoriilor de persoane care ar putea fi supuse interceptării; stabilirea unei limite a duratei executării măsurii; procedura de urmat pentru examinarea, utilizarea și păstrarea datelor colectate; măsurile de precauție ce trebuie luate pentru comunicarea datelor către alte părți; precum și circumstanțele în care este posibilă sau necesară ștergerea ori distrugerea înregistrărilor [Huvig, citată anterior, pct. 34; *Amann împotriva Elveției* (MC), nr. 27798/95, pct. 56-58, CEDO 2000-II; *Valenzuela Contreras*, citată anterior, pct. 46; *Prado Bugallo împotriva Spaniei*, nr. 58496/00, pct. 30, 18 februarie 2003; *Weber și Saravia*, citată anterior, pct. 95; și *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiev*, citată anterior, pct. 76].

232. În ceea ce privește întrebarea dacă o ingerință este „necesară într-o societate democratică” pentru atingerea unui scop legitim, Curtea a recunoscut că, atunci când autoritățile naționale pun în balanță interesele statului pârât pentru a proteja securitatea națională prin măsuri secrete de supraveghere, pe de o parte, și gravitatea ingerinței în exercitarea de către reclamant a dreptului la respectarea vieții private, pe de altă parte, aceste autorități dispun de o anumită marjă de apreciere în alegerea mijloacelor corespunzătoare pentru atingerea scopului legitim de protejare a securității naționale. Însă această marjă de apreciere se corelează cu un control european care vizează atât legislația, cât și deciziile de aplicare a acesteia. Curtea trebuie să se convingă de existența unor garanții corespunzătoare și eficiente împotriva abuzurilor deoarece un sistem de supraveghere secretă conceput pentru a proteja securitatea națională riscă să submineze democrația, ba chiar să o distrugă, pe motivul apărării acesteia. Evaluarea acestei chestiuni depinde de toate circumstanțele cauzei, precum natura, domeniul de aplicare și durata măsurilor posibile; motivele necesare pentru dispunerea lor; autoritățile competente să le permită, să le efectueze și să le controleze; precum și tipul de căi de atac prevăzute de dreptul intern. Curtea trebuie să verifice dacă procedurile de control asupra inițierii și aplicării măsurilor restrictive sunt susceptibile de a circumscrie „ingerința” în ceea ce constituie o măsură „necesară într-o societate democratică” (*Klass și alții*, citată anterior, pct. 49, 50 și 59; *Weber și Saravia*, citată anterior, pct. 106; *Kvasnica împotriva Slovaciei*, nr. 72094/01, pct. 80, 9 iunie 2009; și *Kennedy*, citată anterior, pct. 153-154).

233. Examinarea și controlul măsurilor de supraveghere secretă pot interveni în trei etape: în momentul dispunerii supravegherii, în cursul desfășurării ei sau după încetarea ei. În ceea ce privește primele două etape, însăși natura și logica supravegherii secrete impun exercitarea, fără cunoștința persoanei vizate, nu doar a supravegherii ca atare, ci și a controlului aferent. Prin urmare, întrucât în mod necesar persoana vizată este împiedicată să recurgă la o cale de atac eficientă ori să ia parte direct la un control, este indispensabil ca procedurile existente să ofere ele însele garanții corespunzătoare și echivalente în apărarea drepturilor persoanei. În plus, pentru a nu depăși limitele necesității în sensul art. 8 § 2, trebuie respectate cât mai fidel posibil, în procedurile de control, valorile unei societăți democratice. Într-un domeniu în care abuzurile sunt, potențial, destul de ușoare în cazuri individuale și ar putea avea consecințe negative pentru societatea democratică în ansamblu, este dezirabil în principiu să se încredințeze acest control unei instanțe deoarece puterea judecătorească oferă cele mai bune garanții de independență, imparțialitate și procedură legală (*Klass și alții*, citată anterior, pct. 55-56).

234. În ceea ce privește a treia etapă, respectiv încetarea supravegherii, chestiunea notificării a posteriori a măsurilor de supraveghere este indisolubil legată de cea a eficacității căilor de atac și deci de existența unor garanții efective împotriva folosirii abuzive a competențelor de supraveghere. Persoana vizată cu greu poate, în principiu, să conteste retroactiv în instanță legalitatea măsurilor întreprinse fără știrea sa, dacă nu este informată despre acestea (*Klass și alții*, citată anterior, pct. 57; și *Weber și Saravia*, decizia citată anterior, pct. 135), sau dacă – în altă ipoteză –, bănuind că îi sunt ori i-au fost interceptate comunicațiile, persoana are posibilitatea de a sesiza instanțele, acestea având competență chiar dacă subiectul interceptării nu a fost informat despre această măsură (*Kennedy*, citată anterior, pct. 167).

ii. Aplicarea, în prezenta cauză, a principiilor generale sus-menționate

235. Curtea reamintește concluzia sa, conform căreia legislația rusă privind interceptarea secretă a comunicațiilor de telefonie mobilă, denunțată de reclamant într-un capăt de cerere general, constituie o ingerință în exercitarea dreptului garantat de art. 8. În consecință, pentru a decide dacă această ingerință a fost justificată în temeiul art. 8 § 2, Curtea va examina dacă legislația în litigiu este în sine conformă cu Convenția.

236. În cauzele în care legislația prin care se autorizează supravegherea secretă este contestată în fața Curții, problema legalității ingerinței este strâns legată de chestiunea dacă s-a respectat criteriul de „necesitate”, motiv pentru care Curtea trebuie să examineze în solidar criteriile conform cărora măsura trebuie să fie „prevăzută de lege” și „necesară” (*Kennedy*, citată anterior, pct. 155; a se vedea, de asemenea, *Kvasnica*, citată anterior, pct. 84). „Calitatea legii”, în acest sens, implică faptul că dreptul intern trebuie să fie nu doar accesibil și previzibil în aplicarea lui, ci și că trebuie să garanteze

că măsurile de supraveghere secretă sunt aplicate numai atunci când sunt „necesare într-o societate democratică”, în special oferind garanții suficiente și efective împotriva abuzurilor.

237. Părțile nu contestă faptul că interceptarea comunicațiilor de telefonie mobilă are un temei în dreptul intern. Acestea sunt reglementate, în special, de Codul de procedură penală și Legea privind măsurile operative de investigații, precum și Legea privind comunicațiile și ordinele Ministerului Comunicațiilor. De asemenea, Curții îi este clar că măsurile de supraveghere autorizate în dreptul rus urmăresc scopurile legitime de apărare a securității naționale și a siguranței publice, prevenirea infracțiunilor și protejarea bunăstării economice a țării (*supra*, pct. 26). Rămâne așadar de verificat dacă dreptul intern este accesibil și dacă acesta conține garanții suficiente și efective pentru a îndeplini cerințele de „previzibilitate” și „necesitate într-o societate democratică”.

238. Curtea va examina așadar, pe rând, accesibilitatea dreptului intern; domeniul de aplicare și durata măsurilor de supraveghere secretă; procedurile aplicabile pentru păstrarea, consultarea, examinarea, utilizarea, comunicarea și distrugerea datelor interceptate; procedurile de autorizare; procedurile de control asupra aplicării măsurilor de supraveghere secretă; existența eventuală a unui mecanism de notificare și căile de atac prevăzute în dreptul intern.

α) Accesibilitatea dreptului intern

239. Părțile sunt de acord asupra faptului că aproape toate prevederile legale privind supravegherea secretă – inclusiv Codul de procedură penală și Legea privind măsurile operative de investigații, Legea privind comunicațiile și majoritatea ordinelor emise de Ministerul Comunicațiilor – au fost publicate oficial și sunt accesibile cetățenilor. Părțile au opinii diferite asupra chestiunii dacă anexele Ordinului nr. 70 al Ministerului Comunicațiilor îndeplinesc cerința de accesibilitate.

240. Curtea observă că aceste anexe nu au apărut niciodată într-o publicație oficială disponibilă tuturor deoarece au fost considerate a fi de natură tehnică (*supra*, pct. 128).

241. Curtea admite că, în esență, anexele Ordinului nr. 70 conțin specificațiile tehnice pentru echipamentul de interceptare pe care furnizorii de servicii de comunicații trebuie să îl instaleze. Totodată, prin faptul că impune ca echipamentul respectiv să asigure serviciilor de aplicare a legii acces direct la toate comunicațiile de telefonie mobilă ale tuturor utilizatorilor, deși interzice informațiile privind consemnarea sau înregistrarea interceptărilor efectuate de astfel de servicii (*supra*, pct. 115 și 122), anexele Ordinului nr. 70 sunt de natură să aducă atingere dreptului utilizatorilor la respectarea vieții lor private și a corespondenței lor. Prin urmare, Curtea consideră că anexele trebuie să fie accesibile cetățenilor.

242. Publicat în revista oficială a Ministerului Comunicațiilor *SvyazInform*, care este distribuit pe bază de abonament, ordinul a fost accesibil doar experților în comunicații, nu și publicului larg. Cu toate acestea, Curtea observă că textul ordinului alături de anexele aferente poate fi consultat printr-o bază de date juridică și privată disponibilă pe internet, care l-a preluat din *SvyazInform* (*supra*, pct. 115). Curtea regretă lipsa unei publicări oficiale a Ordinului nr. 70 care să îl facă accesibil tuturor. Cu toate acestea, ținând seama de faptul că acesta a fost publicat într-o revistă ministerială oficială, precum și de posibilitatea ca publicul să îl consulte printr-o bază de date juridică și privată disponibilă pe internet, Curtea consideră că nu este necesar să continue examinarea problemei accesibilității în dreptul intern. Se va concentra în schimb pe cerințele de „previzibilitate” și „necesitate”.

β) Domeniul de aplicare a măsurilor de supraveghere secretă

243. Curtea reamintește că dreptul intern trebuie să definească domeniul de aplicare a supravegherii secrete punând la dispoziția cetățenilor indicații corespunzătoare cu privire la circumstanțele în care autoritățile publice pot recurge la astfel de măsuri – în special, indicând clar natura infracțiunilor care pot duce la un mandat de interceptare și definind categoriile de persoane care pot fi supuse interceptării (*supra*, pct. 231).

244. În ceea ce privește natura infracțiunilor, Curtea subliniază că prin criteriul previzibilității nu se impune statelor să facă o listă exhaustivă în care să menționeze pe cele care pot duce la o măsură de interceptare. Cu toate acestea, ele trebuie să furnizeze suficiente detalii despre natura infracțiunilor respective (*Kennedy*, citată anterior, pct. 159). Atât Legea privind măsurile operative de investigații, cât și Codul de procedură penală precizează că se pot intercepta comunicațiile, telefonice și de alt tip, în contextul unei infracțiuni de gravitate medie, al unei infracțiuni grave sau al unei infracțiuni deosebit de grave – respectiv, o infracțiune pentru care Codul penal prevede o pedeapsă maximă mai mare de 3 ani de închisoare – care a fost comisă deja, este în curs de comitere sau în curs de pregătire (*supra*, pct. 31 și 33). Curtea consideră că natura infracțiunilor care pot duce la un mandat de interceptare este suficient de clară. Cu toate acestea, este preocupată de constatarea că dreptul rus autorizează interceptarea secretă a comunicațiilor pentru un mare număr de infracțiuni, inclusiv, de exemplu, după cum semnalează reclamantul, furtul din buzunare (*supra*, pct. 182; pentru un raționament similar, a se vedea de asemenea *lordachi și alții*, citată anterior, pct. 43 și 44).

245. De asemenea, Curtea observă că interceptarea poate fi dispusă nu doar în privința unui

suspect sau acuzat, ci și în privința unei persoane care ar putea avea informații despre o infracțiune sau alte informații relevante pentru un dosar penal (*supra*, pct. 32). Curtea a hotărât în trecut că măsurile de interceptare ce vizează o persoană care nu este bănuită de o infracțiune dar ar putea avea informații despre o astfel de infracțiune pot fi justificate în temeiul art. 8 din Convenție (*Greuter*, decizie citată anterior). Curtea constată însă absența oricărei precizări, în legislația rusă sau în jurisprudența consacrată a instanțelor ruse, cu privire la modul în care se interpretează în practică formularea „persoană care poate avea informații despre o infracțiune” și „persoană care poate avea informații relevante într-un dosar penal” (pentru un raționament similar, a se vedea *Lordachi și alții*, citată anterior, pct. 44).

246. De asemenea, Curtea observă că, pe lângă interceptările având ca obiect prevenirea sau depistarea infracțiunilor, LMOI prevede posibilitatea de a intercepta comunicațiile, telefonice sau de alt tip, ulterior primirii de informații despre fapte sau activități care pun în pericol securitatea națională, militară, economică sau ecologică a Federației Ruse (*supra*, pct. 31). Or, natura faptelor sau activităților care pot fi considerate ca punând în pericol aceste tipuri de interese în materie de securitate nu este definită nicăieri în dreptul rus.

247. Curtea a avut deja ocazia să declare că cerința de „previzibilitate” a legii nu ajunge până la a impune statelor obligația de a adopta dispoziții legale care enumeră în detaliu toate comportamentele care pot duce la decizia de a supune o persoană unei supravegheri secrete pentru motive de „securitate națională”. Prin forța împrejurărilor, amenințările la adresa securității naționale pot fi de diferite tipuri și pot fi neprevăzute sau greu de definit în prealabil (*Kennedy*, citată anterior, pct. 159). Cu toate acestea, Curtea subliniază totodată că, în ceea ce privește aspectele legate de drepturile fundamentale, legea ar fi contrară statului de drept, unul dintre principiile de bază ale unei societăți democratice pe care îl consacră Convenția, dacă marja de apreciere acordată executivului în materie de securitate națională nu ar avea nicio limită. În consecință, legea trebuie să definească domeniul de aplicare și modul de exercitare a unei astfel de marje cu suficientă claritate – având în vedere scopul legitim urmărit – pentru a oferi persoanei o protecție adecvată împotriva arbitrarului (*Liou împotriva Rusiei*, nr. 42086/05, pct. 56, 6 decembrie 2007, cu alte trimiteri).

248. Este important de remarcat faptul că LMOI nu oferă nicio indicație cu privire la împrejurările în care comunicațiile unei persoane pot fi interceptate din cauza unor acțiuni sau activități care pun în pericol securitatea națională, militară, economică sau ecologică a Federației Ruse. Această absență conferă autorităților o latitudine aproape nelimitată atunci când este vorba de a stabili ce fapte sau acte constituie o astfel de amenințare și dacă aceasta este suficient de gravă pentru a justifica o supraveghere secretă; rezultă de aici riscuri de abuz (pentru un raționament similar, a se vedea *Lordachi și alții*, citată anterior, pct. 46).

249. Cu toate acestea, Curtea nu pierde din vedere faptul că, în Rusia, o măsură de interceptare necesită o autorizație judiciară prealabilă. Acest lucru poate contribui la limitarea latitudinii organelor de aplicare a legii în lectura formulărilor generale precum „persoană care poate avea informații despre o infracțiune”, „persoană care poate avea informații relevante pentru un dosar penal” și „fapte sau activități care pun în pericol securitatea națională, militară, economică sau ecologică a Federației Ruse”, grație unei interpretări judiciare consacrate a acestor termeni sau a unei practici consacrate constând în a verifica, de la caz la caz, dacă există motive suficiente pentru a intercepta comunicațiile unei anumite persoane. Curtea admite că această cerință de autorizare legală prealabilă constituie o importantă garanție împotriva arbitrarului. Mai jos, Curtea va examina eficacitatea acestei garanții.

y) Durata măsurilor de supraveghere secretă

250. Curtea a hotărât că nu este nerezonabil ca problema duratei totale a unei măsuri de interceptare să fie lăsată la aprecierea autorităților interne competente pentru emiterea și reînnoirea unui mandat de interceptare, cu condiția să existe garanții suficiente – ca de exemplu precizări clare în dreptul intern – cu privire la data expirării autorizației de interceptare, condițiile în care aceasta poate fi reînnoită și circumstanțele în care ar trebui să fie anulată (*Kennedy, supra*, pct. 161; a se vedea totodată *Klass și alții*, citată anterior, pct. 52; și *Weber și Saravia*, decizie citată anterior, pct. 98).

251. În ceea ce privește prima garanție, atât Codul de procedură penală, cât și LMOI prevăd că un judecător poate autoriza o măsură de interceptare pentru o perioadă de cel mult 6 luni (*supra*, pct. 38 și 47). Prin urmare, dreptul intern indică în mod clar perioada maximă la finalul căreia o autorizație de interceptare expiră. În al doilea rând, condițiile în care o astfel de autorizație poate fi reînnoită sunt, de asemenea, specificate clar în legislație. În special, atât Codul de procedură penală, cât și LMOI prevăd că un judecător poate prelungi măsura de interceptare din 6 în 6 luni, în urma unei reexaminări a tuturor elementelor relevante (*idem*). În ceea ce privește a treia garanție, referitoare la circumstanțele în care măsura de interceptare trebuie să fie anulată, Curtea observă totuși că obligația de a pune capăt acestei măsuri atunci când nu mai este necesară este menționată numai în Codul de procedură penală, nu și în LMOI din păcate (*idem*). Aceasta înseamnă că, în practică, interceptările care survin în cadrul unei urmăriri penale sunt înconjurate de mai multe garanții decât cele care nu

aparțin acestui cadru, în special în ceea ce privește „fapte sau activități care pun în pericol securitatea națională, militară, economică sau ecologică” a țării.

252. Prin urmare, Curtea concluzionează că dreptul rus include, cu privire la durata și prelungirea unei măsuri de interceptare, norme clare care oferă garanții adecvate împotriva abuzurilor, dar că în schimb dispozițiile din LMOI cu privire la anularea măsurilor de supraveghere nu oferă garanții suficiente împotriva ingerințelor arbitrare.

δ) Proceduri de urmat pentru păstrarea, consultarea, examinarea, folosirea, transmiterea și distrugerea datelor interceptate

253. Dreptul rus prevede că datele colectate în cadrul unor măsuri de supraveghere secretă constituie secrete de stat și trebuie să fie sigilate și păstrate în condiții de natură să excludă orice risc de acces neautorizat; aceste date pot fi transmise către funcționarii statului care au nevoie reală de ele pentru a-și îndeplini sarcinile și au certificatul de securitate corespunzător. Acesta prevede luarea de măsuri pentru a garanta că se comunică numai informațiile necesare destinatarului pentru îndeplinirea atribuțiilor sale. Funcționarul responsabil pentru asigurarea faptului că datele sunt păstrate în siguranță și sunt inaccesibile persoanelor care nu dețin certificatul de securitate necesar este identificată în mod clar (*supra*, pct. 51 și 57). De asemenea, dreptul intern prezintă condițiile și procedurile pentru transmiterea, către organele de urmărire penală, a datelor interceptate care conțin informații despre o infracțiune. Acesta indică, în special, normele privind păstrarea în siguranță a acestor date și condițiile de utilizare a acestora ca probe în cursul urmăririi penale (*supra*, pct. 58-64). Curtea constată că dreptul rus include – în materie de conservare, utilizare și comunicare a datelor interceptate – norme clare care permit minimizarea riscului de acces neautorizat sau de dezvăluire neautorizată (pentru un raționament similar, a se vedea *Kennedy*, citată anterior, pct. 62 și 63).

254. În conformitate cu dreptul intern, distrugerea elementelor interceptate trebuie să intervină după 6 luni de păstrare dacă persoana nu a fost inculpată pentru o infracțiune; dacă acesta a fost inculpată pentru o infracțiune, instanța de fond trebuie să decidă, la încheierea procedurii penale, dacă elementele interceptate utilizate ca probe trebuie să fie păstrate ori distruse (*supra*, pct. 65 și 66).

255. În cazul în care persoana vizată nu a fost inculpată pentru o infracțiune, Curtea nu este convinsă de argumentul reclamantului conform căruia dreptul rus permite păstrarea elementelor interceptate după expirarea termenului legal (*supra*, pct. 188). Într-adevăr, dispoziția vizată de reclamant nu se aplică în cazul specific al păstrării datelor colectate în cadrul interceptării comunicațiilor. Curtea consideră rezonabilă termenul maxim de păstrare, respectiv 6 luni, stabilit în dreptul rus pentru astfel de date. Cu toate acestea, Curtea regretă absența obligației de a distruge imediat datele care nu au nicio legătură cu scopul pentru care au fost colectate (a se compara cu *Klass și alții*, citată anterior, pct. 52; și *Kennedy*, citată anterior, pct. 162). Păstrarea automată, timp de 6 luni, a unor date vădit lipsite de interes nu poate fi considerată justificată în temeiul art. 8.

256. În fine, în ceea ce privește cazul în care persoana a fost inculpată pentru o infracțiune, Curtea constată cu îngrijorare că dreptul rus permite instanței de fond o marjă de apreciere nelimitată pentru a decide păstrarea sau distrugerea, la soluționarea procesului, a datelor care au servit ca probe (*supra*, pct. 66). Dreptul rus nu oferă cetățenilor nicio informație cu privire la împrejurările în care elementele interceptate pot fi păstrate după terminarea procesului. Prin urmare, Curtea consideră că există o lipsă de claritate în această privință în legislație.

ε) Autorizarea interceptărilor

Procedurile de autorizare

257. Pentru a stabili dacă procedurile de autorizare sunt în măsură să garanteze că supravegherea secretă nu este dispusă la întâmplare, contrar legii sau fără o examinare corespunzătoare, Curtea va lua în considerare o serie de factori, incluzând, în special, autoritatea competentă să autorizeze supravegherea, domeniul de aplicare a examinării pe care o efectuează și conținutul autorizației de interceptare.

258. În ceea ce privește organul competent pentru a autoriza supravegherea, Curtea constată că emiterea de autorizații pentru interceptarea convorbirilor telefonice de către un organ nejudiciar poate fi compatibilă cu Convenția (a se vedea, de exemplu, *Klass și alții*, citată anterior, pct. 51; *Weber și Saravia*, citată anterior, pct. 115; și *Kennedy*, citată anterior, pct. 31), cu condiția ca acest organ să fie suficient de independent față de puterea executivă [*Dumitru Popescu împotriva României* (nr. 2), nr. 71525/01, pct. 71, 26 aprilie 2007].

259. Dreptul rus conține o importantă garanție împotriva supravegherii secrete arbitrare ori sistematice, dispunând că orice interceptare a comunicațiilor, telefonice sau de alt tip, necesită o autorizație judiciară (*supra*, pct. 34 și 44). Organul de aplicare a legii care dorește să obțină o autorizație de interceptare trebuie, în acest scop, să adreseze o cerere motivată instanței, care poate

solicita prezentarea unor documente justificative (*supra*, pct. 37 și 46). Judecătorul trebuie să motiveze decizia de autorizare a unei măsuri de interceptare (*supra*, pct. 38 și 44).

260. În ceea ce privește domeniul de aplicare a examinării efectuate de organul care emite autorizația, Curtea amintește că acesta trebuie să fie în măsură să verifice existența unei suspiciuni întemeiate față de persoana vizată, în special să verifice dacă există indicii pentru a o suspecta că plănuiește, săvârșește ori a săvârșit infracțiuni sau alte fapte care pot conduce la măsuri de supraveghere secretă, ca de exemplu fapte care pun în pericol securitatea națională. De asemenea, acesta trebuie să se asigure că interceptarea solicitată îndeplinește criteriul de măsură „necesară într-o societate democratică” prevăzut la art. 8 § 2 din Convenție, în special, că aceasta este proporțională cu scopurile legitime urmărite, verificând – de exemplu – dacă este posibilă atingerea scopurilor urmărite prin mijloace mai puțin restrictive (*Klass și alții*, citată anterior, pct. 51; *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiev*, citată anterior, pct. 79 și 80; *Iordachi și alții*, citată anterior, pct. 51; și *Kennedy*, citată anterior, pct. 31 și 32).

261. Curtea observă că, în Rusia, controlul jurisdicțional are o sferă de aplicare limitată. Astfel, materialul care conține informații despre investigatori sub acoperire sau informatori ai poliției, ori despre organizarea și tacticile aferente măsurilor operative de investigații, nu poate fi prezentat judecătorului și este exclus așadar din examinarea efectuată de instanță (*supra*, pct. 37). Curtea consideră că nedivulgarea informațiilor relevante privează instanțele de capacitatea de a verifica dacă există un temei faptic suficient pentru a suspecta persoana, vizată în cererea de măsuri, că ar fi săvârșit o infracțiune sau activități care pun în pericol securitatea națională, militară, economică sau ecologică a țării (a se vedea, *mutatis mutandis*, *Liou*, citată anterior, pct. 59-63). Curtea a declarat deja în trecut că există tehnici care permit concilierea între, pe de o parte, preocupările de securitate legitime legate de natura și sursele informațiilor, iar pe de altă parte, necesitatea de a acorda justițiabililor posibilitatea de a beneficia de normele de procedură (a se vedea, *mutatis mutandis*, *Chahal împotriva Regatului Unit*, 15 noiembrie 1996, pct. 131, *Culegere* 1996-V).

262. În plus, Curtea observă că, în Rusia, nici Codul de procedură penală, nici LMOI nu impun judecătorilor să verifice existența unei „suspiciuni întemeiate” în privința persoanei vizate ori să aplice criteriile de „necesitate” și „proporționalitate”. Curtea constată însă că, în deciziile sale, Curtea Constituțională a explicat că sarcina probei revine organului solicitant, care trebuie să demonstreze necesitatea interceptării, iar judecătorul care examinează o cerere de interceptare trebuie să verifice motivele pentru această măsură și să acorde autorizația numai în cazul în care consideră că interceptarea este legală, necesară și justificată. De asemenea, Curtea Constituțională a declarat că decizia judecătorească de autorizare a interceptării trebuie să fie motivată și să indice motive specifice pentru a crede că o infracțiune a fost săvârșită, este în curs de săvârșire sau de pregătire sau că alte activități care pun în pericol securitatea națională, militară, economică sau ecologică a țării sunt în desfășurare și că persoana vizată în cererea de interceptare este implicată în aceste activități infracționale sau periculoase (*supra*, pct. 40-42). Astfel, Curtea Constituțională a recomandat instanțelor ruse, în esență, ca în momentul examinării cererilor de autorizare a interceptării să verifice existența unei „suspiciuni întemeiate” privind persoana vizată și să autorizeze măsura doar dacă îndeplinește criteriile de necesitate și proporționalitate.

263. Cu toate acestea, Curtea constată că dreptul intern nu obligă expres instanțele de drept comun să se conformeze opiniei Curții Constituționale cu privire la modalitatea de interpretare a unei dispoziții legislative atunci când opinia a fost formulată într-o decizie, nu într-o hotărâre (*supra*, pct. 106). De fapt, documentele prezentate de reclamant arată că instanțele naționale nu respectă întotdeauna sus-menționatele recomandări ale Curții Constituționale, toate fiind cuprinse în decizii, nu în hotărâri. Astfel, rezultă din notele analitice prezentate de instanțele districtuale că, deseori, cererile de interceptare nu sunt însoțite de documente justificative, că judecătorii de la aceste instanțe nu solicită niciodată organului de interceptare să le prezinte aceste documente și că o simplă referire la existența unor informații despre infracțiuni sau despre activități care pun în pericol securitatea națională, militară, economică sau ecologică a țării este considerată suficientă pentru emiterea unei autorizații. O cerere de interceptare este respinsă doar în cazul în care nu poartă semnătura unei persoane competente, nu conține nicio referire la infracțiunea în legătură cu care trebuie să fie dispusă interceptarea sau vizează o infracțiune pentru care interceptarea nu este permisă în dreptul intern (*supra*, pct. 193). Astfel, notele analitice întocmite de instanțele districtuale, combinate cu statisticile prezentate de reclamant pentru perioada 2009-2013 (*supra*, pct. 194), arată că, în practica lor curentă, instanțele ruse nu verifică dacă există o „suspiciune întemeiată” în privința persoanei vizate și nu aplică criteriile de „necesitate” și „proporționalitate”.

264. În fine, conținutul mandatului de interceptare trebuie să identifice în mod clar persoana exactă care urmează să fie pusă sub supraveghere sau setul unic de zone (locuri) vizat de interceptarea autorizată prin mandat. Această identificare se poate face prin intermediul unor nume, adrese, numere de telefon sau alte informații relevante [*Klass și alții*, citată anterior, pct. 51; *Liberty și alții*, citată anterior, pct. 64 și 65; *Dumitru Popescu (nr. 2)*, citată anterior, pct. 78; *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiev*, pct. 80; și *Kennedy*, citată anterior, pct. 160].

265. Curtea observă că în Codul de procedură penală se prevede obligativitatea ca în cererea pentru autorizația de interceptare să se indice în mod clar persoana exactă ale cărei comunicații trebuie interceptate și care este durata măsurii respective (*supra*, pct. 46). În schimb, LMOI nu prevede nicio obligație pentru conținutul cererii sau al autorizației de interceptare. În consecință, în unele cazuri instanțele emit o autorizație care nu menționează o anumită persoană sau un anumit număr de telefon de interceptat, ci permite interceptarea tuturor comunicațiilor telefonice din zona în care s-a comis o infracțiune. Unele autorizații nu indică perioada pentru care se permite interceptarea (*supra*, pct. 193). Curtea consideră că astfel de autorizații, care nu sunt în mod clar interzise de LMOI, conferă o foarte largă marjă de apreciere organelor de aplicare a legii cu privire la tipul de comunicații de interceptat și durata măsurii.

266. În plus, Curtea constată că, în caz de urgență, este posibilă interceptarea comunicațiilor fără autorizație judiciară prealabilă, și asta pe o perioadă de cel mult 48 de ore. Judecătorul trebuie să fie informat despre un astfel de caz în termen de 24 de ore de la începutul interceptării. În cazul în care în termen de 48 de ore nu se eliberează nicio autorizație judiciară, interceptarea trebuie să înceteze imediat (*supra*, pct. 35). Curtea a avut ocazia de studiere „procedura de urgență” prevăzută în legislația bulgară și a considerat-o compatibilă cu Convenția (*Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiiev*, citată anterior, pct. 16 și 82). Cu toate acestea, spre deosebire de sistemul bulgar, „procedura de urgență” din Rusia nu conține garanții suficiente pentru a asigura o utilizare atentă și limitată la cazuri justificate corespunzător. Într-adevăr, deși în materie penală LMOI restrânge utilizarea procedurii de urgență la cazurile de pericol imediat de comitere a unei infracțiuni grave sau deosebit de grave, legea nu conține nicio restricție similară pentru supravegherea secretă legată de fapte sau activități care pun în pericol securitatea națională, militară, economică sau ecologică a țării. Dreptul intern nu restrânge utilizarea procedurii de urgență la cazurile care implică un pericol grav și iminent la adresa securității naționale, militare, economice sau ecologice a țării; ci lasă autorităților o marjă nelimitată pentru a determina situațiile în care se justifică utilizarea procedurii de urgență nejudiciare, ceea ce creează riscuri de abuz în folosirea acestei proceduri (a se vedea, *a contrario*, *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiiev*, citată anterior, pct. 16). În plus, deși dreptul rus prevede că un judecător trebuie să fie informat imediat despre fiecare caz de interceptare de urgență, competența judecătorului este limitată la eliberarea unei autorizații de prelungire a măsurii de interceptare peste cele 48 de ore. Judecătorul nu are autoritate să examineze dacă utilizarea procedurii de urgență a fost justificată ori să se pronunțe dacă materialul colectat în cursul celor 48 de ore anterioare ar trebui să fie păstrat sau distrus (a se vedea, *a contrario*, *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiiev*, citată anterior, pct. 16). Prin urmare, dreptul rus nu prevede un control jurisdicțional efectiv asupra procedurii de urgență.

267. Având în vedere cele de mai sus, Curtea consideră că procedurile de autorizare existente în dreptul rus nu sunt capabile să garanteze că măsurile de supraveghere secretă nu sunt dispuse la întâmplare, contrar legii sau fără o examinare corespunzătoare.

Accesul autorităților la comunicații

268. Curtea ia act de argumentul reclamantului potrivit căruia serviciile de securitate și poliția dispun de mijloacele tehnice pentru a intercepta comunicațiile de telefonie mobilă fără să trebuiască să obțină autorizație judiciară, întrucât beneficiază de acces direct la toate comunicațiile și capacitatea lor de a intercepta comunicațiile unei persoane sau ale mai multora nu este condiționată de obligația de a prezenta autorizația de interceptare furnizorului de servicii de comunicații.

269. Pentru Curte, obligația de a prezenta o autorizație de interceptare furnizorului de servicii de comunicații pentru a dobândi acces la comunicațiile unei persoane este una dintre garanțiile importante împotriva abuzurilor din partea organelor de aplicare a legii în sensul că permite garanția că se obține o autorizație corespunzătoare înainte de orice interceptare. În Rusia, serviciile de aplicare a legii nu sunt obligate de dreptul intern să prezinte o autorizație judiciară furnizorului de servicii de comunicații pentru a avea acces la comunicațiile unei persoane (a se vedea, *a contrario*, Rezoluția Consiliului UE citată la pct. 145 *supra*), cu excepția supravegherii datelor de comunicații în temeiul Codului de procedură penală (*supra*, pct. 48). Într-adevăr, în conformitate cu ordinele Ministerului Comunicațiilor, în special anexele la Decretul nr. 70, furnizorii de servicii de comunicații sunt obligați să instaleze un echipament care acordă organelor de aplicare a legii acces direct la toate comunicațiile de telefonie mobilă ale tuturor utilizatorilor (*supra*, pct. 115-122). Ordinul nr. 538 impune totodată furnizorilor de servicii de comunicații obligația de a crea baze de date pentru a stoca timp de 3 ani informații despre toți abonații și serviciile pe care le primesc, baze de date la care serviciile secrete au acces direct la distanță (*supra*, pct. 132 și 133). Prin urmare, organele de aplicare a legii au acces direct la toate comunicațiile de telefonie mobilă și datele aferente acestora.

270. Curtea consideră că modul de funcționare a sistemului de supraveghere secretă din Rusia oferă organelor de securitate și poliției mijloace tehnice pentru a ocoli procedura de autorizare și a intercepta orice comunicație fără autorizație judiciară prealabilă. Deși, indiferent de sistem, este

imposibil să se excludă complet posibilitatea ca un funcționar necinstit, neglijent sau excesiv de zelos să comită fapte ilegale (*Klass și alții*, citată anterior, pct. 59), Curtea consideră totuși că un sistem precum cel din Rusia, care permite serviciilor secrete și poliției să intercepteze direct comunicațiile oricărui cetățean, fără a le impune obligația de a prezenta o autorizație de interceptare furnizorului de servicii de comunicații sau altcuiva, este deosebit de vulnerabil la abuzuri. Necesitatea unor garanții împotriva arbitrarului și abuzului pare așadar deosebit de mare.

271. Prin urmare, Curtea va examina cu atenție specială dacă metoda de control prevăzută în dreptul rus poate să ofere garanția că orice interceptare se efectuează în mod legal, în baza unei autorizații legale corespunzătoare.

ζ) Controlul aplicării măsurilor de supraveghere secretă

272. Pentru început, Curtea constată că, în conformitate cu Ordinul nr. 70, echipamentul instalat de furnizorii de servicii de comunicații nu trebuie nici să înregistreze, nici să consemneze informații despre interceptări (*supra*, pct. 120). Curtea a declarat deja, în trecut, că obligația impusă organelor de interceptare de a păstra arhive despre interceptări este deosebit de importantă pentru a garanta organului de control un acces efectiv la detaliile operațiunilor de supraveghere întreprinse (*Kennedy*, citată anterior, pct. 165). Interdicția, prevăzută în dreptul rus, asupra consemnării sau înregistrării interceptărilor împiedică autoritatea de control să identifice interceptările efectuate fără autorizație judiciară corespunzătoare. Combinată cu capacitatea tehnică acordată organelor de aplicare a legii prin acest ordin, de a intercepta direct orice comunicație, această normă face ca orice sistem de control să fie inadecvat pentru a depista interceptările ilegale și, prin urmare, inefficient.

273. Referitor la controlul interceptărilor efectuate în temeiul unei autorizații legale corespunzătoare, Curtea va examina dacă sistemul de control existent în Rusia este capabil să garanteze că cerințele legale privind punerea în aplicare a măsurilor de supraveghere, precum și păstrarea, consultarea, utilizarea, prelucrarea, comunicarea și distrugerea elementelor interceptate sunt respectate în mod sistematic.

274. Instanța care a emis o autorizație de interceptare nu este competentă să controleze punerea în aplicare a acesteia. Aceasta nu este informată despre rezultatul interceptărilor și nu are competența de a verifica dacă au fost respectate condițiile aferente deciziei de acordare a autorizației. Instanțele ruse, în general, nu sunt competente nici să exercite un control general asupra interceptărilor. Controlul exercitat de instanțe este limitat la etapa inițială a autorizației. În ceea ce privește controlul ulterior, acesta este încredințat Președintelui, Parlamentului, Guvernului, Procurorului general și procurorilor din subordine competenți.

275. După cum a declarat Curtea în trecut, deși în principiu este de dorit ca funcția de control să fie încredințată unui judecător, controlul exercitat de un organ nejudiciar poate fi considerat compatibil cu Convenția dacă acest organ este independent față de autoritățile care desfășoară supravegherea și este investit cu competențe și atribuții suficiente pentru a exercita un control eficace și permanent (*Klass și alții*, citată anterior, pct. 56).

276. Cu privire la Președinte, Parlament și Guvern, dreptul rus nu definește modul în care aceștia pot exercita controlul asupra interceptărilor. Nu există reglementări sau instrucțiuni accesibile publicului care descriu întinderea examinării realizate de aceștia, condițiile în care aceasta poate avea loc, sau procedurile de control aplicabile măsurilor de supraveghere sau repararea infracțiunilor constatate (pentru un raționament similar, a se vedea *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhev*, citată anterior, pct. 88).

277. Cu privire la procurori, Curtea observă că dreptul intern definește domeniul de aplicare a controlului și procedurile de control exercitat de aceștia asupra măsurilor operative de investigații (*supra*, pct. 69-80). Într-adevăr, dreptul rus precizează că procurorii pot supune unor inspecții sistematice și *ad-hoc* organele de aplicare a măsurilor operative de investigații și sunt abilitați să examineze documentele relevante, chiar și cele confidențiale. Aceștia pot lua măsuri pentru a stopa sau a repara încălcările care au fost depistate și pentru a declanșa acțiuni împotriva autorilor acestora. Aceștia trebuie să prezinte Parchetului general rapoarte semestriale detaliind rezultatele inspecțiilor efectuate. Curtea admite că există un cadru legal care se ocupă, cel puțin teoretic, de un oarecare control al procurorilor asupra măsurilor de supraveghere secretă. Următorul pas este de a examina dacă procurorii sunt independenți față de serviciile care efectuează supravegherea și dacă sunt investiți cu competențe și atribuții suficiente pentru a exercita un control eficace și permanent.

278. În ceea ce privește cerința de independență, Curtea a luat în considerare, în cauze anterioare, metoda de numire și statutul juridic al membrilor organului de control. În special, Curtea a considerat suficient de independente organele alcătuite din deputați – ai majorității dar și ai opoziției – sau din persoane cu calificările necesare pentru accesul la magistratură și numite fie de Parlament, fie de Prim-ministru (a se vedea, exemplu, *Klass și alții*, citată anterior, pct. 21 și 56; *Weber și Saravia*, citată anterior, pct. 24, 25 și 117; *Leander*, citată anterior, pct. 65; *L. împotriva Norvegiei*, nr. 13564/88, decizia Comisiei din 8 iunie 1990; și *Kennedy*, citată anterior, pct. 57 și 166). În schimb, Curtea a

considerat insuficient de independent un ministru de Interne care nu doar că era numit de puterea politică și membru al executivului, ci mai era și direct implicat în conducerea mijloacelor speciale de supraveghere (*Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhev*, citată anterior, pct. 85 și 87); la fel a concluzionat în privința Procurorului general și a procurorilor din subordine competenți (*Iordachi și alții*, citată anterior, pct. 47).

279. Contrar organelor de control sus-menționate, în Rusia procurorii sunt numiți și eliberați din funcție de Procurorul general după consultarea cu autoritățile executive regionale (*supra*, pct. 70). Acest simplu fapt este de natură să ridice îndoieli cu privire la independența lor față de executiv.

280. În plus, este esențial ca rolul procurorilor în apărarea drepturilor omului să nu ducă la niciun conflict de interese (*Mentchinskaya împotriva Rusiei*, nr. 42454/02, pct. 19 și 38, 15 ianuarie 2009). Curtea observă că parchetele nu sunt specializate în controlul asupra interceptărilor (*supra*, pct. 71). Acest control este doar o parte a atribuțiilor lor, care, extinse și diversificate, includ urmărirea penală și controlul cercetării penale. În cadrul atribuțiilor de urmărire penală, procurorii aprobă toate cererile de interceptare depuse de investigatori în cursul procedurilor penale (*supra*, pct. 44). Acest cumul de atribuții în cadrul unui parchet, în care același serviciu aprobă cererile de interceptare și apoi controlează punerea în aplicare a operațiunii, este de asemenea de natură să ridice îndoieli cu privire la independența procurorilor (a se vedea, *a contrario*, *Ananiev și alții împotriva Rusiei*, nr. 42525/07 și 60800/08, pct. 215, 10 ianuarie 2012, cauză care a avut ca obiect controlul exercitat de procurori asupra locurilor de deținere și în care Curtea a hotărât că procurorii îndeplinesc cerința de independență față de organele sistemului penitenciar).

281. Referitor la competențele și atribuțiile procurorilor, este esențial - potrivit Curții - ca organul de control să aibă acces la toate documentele relevante, inclusiv la informații confidențiale, și ca toate persoanele implicate în operațiuni de interceptare să fie obligate să îi comunice toate informațiile pe care le solicită (*Kennedy*, citată anterior, pct. 166). Dreptul rus prevede că procurorii pot examina orice document relevant, chiar și confidențial. Trebuie totuși remarcat că informațiile despre investigatorii sub acoperire ai serviciilor de securitate, precum și cele despre tacticile, metodele și mijloacele folosite de acestea, sunt exceptate de la controlul exercitat de procurori (*supra*, pct. 74). Domeniul de aplicare a controlului lor este limitat așadar. În plus, interceptările făcute de FSB în contextul contra-informațiilor nu pot fi inspectate decât în urma plângerii unei persoane (*supra*, pct. 76). Dar, întrucât persoanele nu primesc notificări despre interceptări (*supra*, pct. 81 și 289 *infra*), este puțin probabil ca o astfel de plângere să fie depusă vreodată. În consecință, măsurile de supraveghere legate de contra-informații eludează *de facto* controlul exercitat de procurori.

282. Competențele organului de control cu privire la infracțiuni pe care le poate depista constituie totodată un aspect important pentru evaluarea eficacității controlului pe care îl exercită (a se vedea, de exemplu, *Klass și alții*, citată anterior, pct. 53, cauză în care organul de interceptare trebuia să înceteze imediat interceptarea în cazul în care Comisia G 10 considera că măsura este ilegală sau inutilă; precum și *Kennedy*, citată anterior, pct. 168, cauză în care toate elementele interceptate au trebuit să fie distruse imediat după ce comisarul pentru interceptarea comunicațiilor a constatat ilegalitatea interceptării). Curtea constată că procurorii au anumite competențe în ceea ce privește încălcările legii pe care le depistează. Astfel, aceștia pot lua măsuri pentru sistarea sau repararea acestor încălcări și luarea de măsuri împotriva autorilor acestora (*supra*, pct. 79). Cu toate acestea, nicio prevedere specifică nu dispune distrugerea elementelor interceptate ilegal (*Kennedy*, citat mai sus, pct. 168).

283. De asemenea, Curtea trebuie să verifice dacă activitățile organului de control sunt deschise controlului public (a se vedea, de exemplu, *L. împotriva Norvegiei*, citată anterior, cauză în care verificarea a fost exercitată de Comisia de control, care prezenta rapoarte anuale Guvernului și ale cărei rapoarte erau publicate și examinate de Parlament; *Kennedy*, citată anterior, pct. 166, cauză în care controlul interceptărilor era exercitat de comisarul responsabil de interceptarea comunicațiilor, care anual prezenta Prim-ministrului un raport, document public prezentat Parlamentului; a se vedea, *a contrario*, *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhev*, pct. 88, cauză în care Curtea a criticat un sistem în care nici ministrul de Interne nici alți responsabili nu erau obligați să raporteze periodic unui organism independent sau cetățenilor cu privire la funcționarea generală a sistemului sau la măsurile aplicate în cazuri individuale). În Rusia, procurorii trebuie să prezinte Procurorului general rapoarte semestriale în care detaliază rezultatele controalelor efectuate. Dar, aceste rapoarte acoperă toate tipurile de măsuri operative de investigații, fără deosebire, interceptările nefiind prezentate separat de alte măsuri. În plus, aceste rapoarte conțin doar informații statistice cu privire la numărul de inspecții realizate cu privire la măsuri operative de investigații și numărul de încălcări depistate, fără să precizeze natura infracțiunilor sau măsurile luate pentru remedierea lor. De asemenea, trebuie remarcat că aceste rapoarte sunt documente confidențiale, care nu sunt făcute publice și nici puse la dispoziția publicului (*supra*, pct. 80). Rezultă de aici că, în Rusia, controlul exercitat de procurori nu permite dreptul la controlul public și la informarea cetățenilor.

284. În cele din urmă, Curtea observă că Guvernul este cel care trebuie să illustreze, cu exemple adecvate, eficiența concretă a sistemului de control (a se vedea, *mutatis mutandis*, *Ananiev și alții*,

citată anterior, pct. 109 și 110). Dar Guvernul rus nu a prezentat niciun raport de inspecție și nicio rezoluție a procurorilor prin care s-a dispus adoptarea de măsuri pentru stoparea sau repararea unei încălcări a legii care a fost depistată. Prin urmare, Guvernul nu a demonstrat eficacitatea, în practică, a controlului exercitat de procurori cu privire la măsurile de supraveghere secretă. În această privință, Curtea ia notă totodată de documentele prezentate de reclamant, care arată imposibilitatea procurorilor de a avea acces la materiale clasificate cu privire la interceptări (*supra*, pct. 14). Acest exemplu ridică totodată îndoieli cu privire la eficacitatea, în practică, a controlului exercitat de procurori.

285. Având în vedere deficiențele de mai sus și importanța deosebită a controlului într-un sistem în care organele de aplicare a legii au acces direct la toate comunicațiile, Curtea consideră că, așa cum este organizat în prezent, controlul exercitat de procurori cu privire la interceptări nu poate să ofere garanții adecvate și eficiente împotriva abuzurilor.

η) Notificarea privind interceptarea comunicațiilor și căile de atac disponibile

286. Curtea va aborda acum problema notificării privind interceptarea comunicațiilor, care este indisolubil legată de cea a eficacității căilor de atac (a se vedea jurisprudența citată la pct. 234 *supra*).

287. Se poate să nu existe posibilitatea practică de a solicita o notificare *a posteriori* în toate cazurile. Activitatea sau pericolul pe care un set de măsuri de supraveghere urmărește să le combată poate dura ani de zile, chiar zeci de ani, după ridicarea acestor măsuri. O notificare *a posteriori* adresată fiecărei persoane afectate de o măsură acum ridicată ar risca să submineze obiectivul pe termen lung care a motivat inițial supravegherea. În plus, o astfel de notificare ar risca să ajute la dezvăluirea metodelor de lucru ale serviciilor de informații, a domeniilor lor de activitate și chiar, după caz, a identității agenților acestora. Prin urmare, lipsa unei notificări *a posteriori* adresate persoanelor afectate de măsuri de supraveghere secretă, imediat după ridicarea acestora, nu poate justifica în sine concluzia că ingerința nu a fost „necesară într-o societate democratică” pentru că tocmai această lipsă de informații este cea care asigură eficacitatea măsurii constitutive a ingerinței. Cu toate acestea, este dezirabilă informarea persoanei vizate după ridicarea măsurilor de supraveghere de îndată ce notificarea poate fi emisă fără a pune în pericol scopul restrângerii (*Klass și alții*, citată anterior, pct. 58; și *Weber și Saravia*, citată anterior, pct. 135). În plus, Curtea ia notă de recomandarea Comitetului de Miniștri referitoare la reglementarea utilizării datelor cu caracter personal în domeniul polițienesc, care prevede că, atunci când datele referitoare la o persoană au fost colectate și înregistrate fără știrea sa, aceasta trebuie, dacă datele nu sunt distruse, să fie informată, dacă este posibil, că se dețin informații despre aceasta, și aceasta de îndată ce nu mai există riscul ca obiectul activităților de poliție să fie afectate (2.2, pct. 143 *supra*).

288. În cauzele *Klass și alții* și *Weber și Saravia*, Curtea a examinat legislația germană, care prevedea că supravegherea trebuie să fie notificată cât mai curând posibil după încetarea măsurii fără a compromite scopul ei. Curtea a luat în considerare faptul că exista o autoritate independentă, Comisia G 10, care avea competența de a decide dacă o persoană supusă unei supravegheri trebuie să fie informată despre măsură. Curtea a considerat că dispoziția relevantă garantează un sistem de notificare efectiv, care contribuia la menținerea ingerinței în caracterul secret al telecomunicațiilor în limitele a ceea ce era necesar pentru atingerea scopurilor legitime urmărite (*Klass și alții*, citată anterior, pct. 58; și *Weber și Saravia*, decizie citată anterior, pct. 136). În cauza *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiev* și cauza *Dumitru Popescu (nr. 2)*, Curtea a declarat incompatibilă cu Convenția absența obligației de a transmite, în orice stadiu, o notificare persoanei vizate de interceptare, pe motiv că această absență privează persoana respectivă de orice posibilitate de a solicita despăgubiri pentru ingerința ilegală în drepturile sale prevăzute la art. 8 și că făcea căile de atac prevăzute de dreptul intern să pară teoretice și iluzorii, nu concrete și efective. Astfel, Curtea a concluzionat că legislația națională a neglijat să ofere o garanție importantă împotriva utilizării necorespunzătoare a măsurilor speciale de supraveghere [*Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiev*, citată anterior, pct. 90 și 91; și *Dumitru Popescu (nr. 2)*, pct. 77]. În cauza *Kennedy*, din contră, Curtea a declarat că absența obligației de a notifica, în orice stadiu, persoana vizată de interceptare era compatibilă cu Convenția pentru faptul că, în Marea Britanie, orice persoană care suspectează că îi sunt ori i-au fost interceptate comunicațiile putea sesiza comisia cu atribuții de investigare deoarece competența acesteia din urmă nu era condiționată de notificarea privind interceptarea (*Kennedy*, citată anterior, pct. 167).

289. Revenind la circumstanțele cauzei, Curtea observă că, în Rusia, persoanele ale căror comunicații au fost interceptate nu primesc în niciun moment și în nicio împrejurare o notificare despre această măsură. Rezultă de aici că – dacă nu se pune în mișcare o acțiune penală împotriva persoanei supuse interceptării și dacă datele interceptate nu servesc ca probe, sau dacă nu există o indiscreție – este puțin probabil ca persoana vizată să afle vreodată despre interceptarea comunicațiilor sale.

290. Curtea ia notă de faptul că o persoană care a aflat într-un fel sau altul despre interceptarea

comunicațiilor sale poate solicita informații despre datele corespunzătoare (*supra*, pct. 81). În această privință, trebuie remarcat faptul că, pentru a putea formula o astfel de cerere, persoana trebuie să aibă cunoștință de fapte legate de măsurile operative de investigații care i-au fost aplicate. Accesul la informații este așadar condiționat de capacitatea persoanei respective de a dovedi că a avut loc interceptarea comunicațiilor. În plus, persoana supusă interceptării nu are drept de acces la documente referitoare la interceptarea comunicațiilor; aceasta poate primi, cel mult, „informații” despre datele colectate. Aceste informații sunt furnizate numai în împrejurări foarte limitate, și anume în cazul în care vinovăția persoanei vizate nu a fost stabilită conform legii, cu alte cuvinte – persoana nu a fost inculpată sau acuzațiile au fost retrase pe motiv că presupusa infracțiune nu a fost comisă ori că unul ori mai multe dintre elementele constitutive ale unei infracțiuni lipsesc. De asemenea, trebuie remarcat faptul că numai informațiile care nu conțin secrete de stat pot fi divulgate persoanei supuse interceptării și că, în dreptul rus, informațiile privind echipamentele utilizate pentru punerea în aplicare a măsurilor operative de investigații, metodele utilizate, funcționarii implicați și datele colectate constituie secret de stat (*supra*, pct. 52). Având în vedere aceste particularități ale dreptului rus, posibilitatea de a obține informații despre interceptări pare inefficientă.

291. Pentru a evalua eficacitatea căilor de atac oferite de dreptul rus, Curtea va ține seama de factorii de mai sus, și anume absența notificării și absența posibilității efective de a solicita și a obține, de la autorități, informații despre interceptări.

292. Conform dreptului rus, o persoană care consideră că drepturile sale au fost ori sunt încălcate de un funcționar al statului în cadrul punerii în aplicare a măsurilor operative de investigații poate depune plângere la superiorul ierarhic al funcționarului, la un procuror sau o instanță (*supra*, pct. 83). Curtea reamintește că o procedură ierarhică pe lângă superiorul direct al funcționarului ale cărui acte sunt contestate nu îndeplinește criteriile de independență necesare pentru a constitui o protecție suficientă împotriva abuzului de autoritate (pentru un raționament similar, a se vedea *Khan împotriva Regatului Unit*, nr. 35394/97, pct. 45-47, CEDO 2000-V; *Dumitru Popescu (nr. 2)*, citată anterior, pct. 72; și *Avanesyan*, citată anterior, pct. 32). De asemenea, unui procuror îi lipsește independența și îi este limitată sfera de control, astfel cum s-a stabilit mai sus (*supra*, pct. 277-285). Rămâne de stabilit dacă o plângere depusă la o instanță poate fi considerată o cale de atac efectivă.

293. Potrivit Guvernului, o persoană care dorește să facă plângere privind interceptarea comunicațiilor sale are la dispoziție patru tipuri de acțiuni în justiție: apel, recurs sau cerere de revizuire împotriva deciziei instanței care a autorizat interceptarea comunicațiilor; cerere de control jurisdicțional întemeiată pe art. 125 C. proc. pen.; cerere de control jurisdicțional în temeiul Legii privind controlul jurisdicțional și capitolul 25 C. proc. civ.; o acțiune în răspundere întemeiată pe art. 1069 C. civ. Curtea va examina aceste căi de atac una după alta.

294. Prima cale de atac menționată de Guvern este constituită de apel, recurs sau cerere de revizuire împotriva deciziei instanței care a autorizat interceptarea comunicațiilor. Însă Curtea Constituțională a precizat clar că persoana căreia i-au fost interceptate comunicațiile nu poate declara apel împotriva autorizației judiciare respective (*supra*, pct. 40; a se vedea, de asemenea, *Avanesyan*, citată anterior, pct. 30). De asemenea, dreptul intern nu menționează nimic despre posibilitatea de a declara recurs. Întrucât Guvernul nu a oferit exemple din practica internă în materie de examinare a recursurilor, Curtea are îndoieli serioase cu privire la existența unui drept de a declara un astfel de recurs împotriva unei decizii judecătorești de autorizare a interceptării comunicațiilor. În schimb, în cazul interceptării, există posibilitatea evidentă de a depune o cerere de revizuire (*supra*, pct. 43). De asemenea, pentru a putea să atace, pe această cale, autorizația legală de interceptare a comunicațiilor, este necesar ca persoana vizată să aibă cunoștință de existența unei astfel de decizii. Deși Curtea Constituțională a declarat că nu este necesar să se atașeze la cererea de revizuire o copie a deciziei judecătorești în litigiu (*supra*, pct. 42), nu ne este clar modul în care o persoană ar putea declara recurs fără a avea un minim de informații despre decizia pe care o contestă, ca de exemplu data adoptării și instanța emitentă. Știind că dreptul rus nu prevede notificarea măsurilor de supraveghere, o persoană nu va putea aproape niciodată să obțină astfel de informații; nu va avea această posibilitate decât în cazul în care acestea îi sunt dezvăluite în cursul unei acțiuni penale îndreptate împotriva sa ori în cazul în care o indiscreție a dus la divulgarea lor.

295. În plus, doar o persoană implicată într-o acțiune penală în care cercetarea judecătorească este în curs poate depune plângere în temeiul art. 125 C. proc. pen. (*supra*, pct. 88 și 89). Prin urmare, această cale de atac nu este disponibilă decât pentru o persoană care a aflat, în cadrul urmăririi penale îndreptate împotriva sa, că i-au fost interceptate comunicațiile. Aceasta nu poate fi folosită de o persoană împotriva căreia nu s-a declanșat nicio acțiune penală ulterior interceptării comunicațiilor sale și care nu știe dacă comunicațiile sale au făcut obiectul unei astfel de măsuri. De asemenea, trebuie remarcat faptul că Guvernul nu a prezentat nicio decizie judecătorească referitoare la examinarea unei plângeri întemeiate pe art. 125 C. proc. pen. pentru a denunța interceptarea comunicațiilor. Prin urmare, Guvernul nu a demonstrat, folosind exemple din jurisprudența internă, eficacitatea concretă a căii de atac menționate de acesta (pentru un raționament similar, a se vedea *Rotaru*, citată anterior, pct. 70; și *Ananyev și alții*, citată anterior, pct. 109 și 110).

296. În ceea ce privește cererea de control jurisdicțional, întemeiată pe Legea privind controlul jurisdicțional, capitolul 25 C. proc. civ. și noul Cod de procedură administrativă, precum și acțiunea în răspundere întemeiată pe art. 1069 C. civ., trebuie remarcat că petentul este cel care trebuie să demonstreze că interceptarea a avut loc și că astfel a existat o încălcare a drepturilor sale (*supra*, pct. 85, 95, 96 și 105). În lipsa unei notificări sau a oricărei forme de acces la documente oficiale privind interceptările, această dovadă este aproape imposibil de prezentat. În plus, în prezenta cauză, instanțele naționale au respins acțiunea reclamantului pe motiv că acesta nu a demonstrat că i-au fost interceptate comunicațiile telefonice (*supra*, pct. 11 și 13). Curtea constată că Guvernul a prezentat diverse decizii judecătorești pronunțate în temeiul capitolului 25 C. proc. civ. sau al art. 1069 C. civ. (*supra*, pct. 220-223). Însă toate aceste decizii, cu o singură excepție, se referă la percheziții ori confiscarea documentelor sau obiectelor, adică măsuri operative de investigații efectuate cu știrea persoanei în cauză. Numai una dintre aceste decizii se referă la interceptarea comunicațiilor: în respectiva cauză, persoana vizată putea să furnizeze dovada necesară deoarece a avut cunoștință de măsura de interceptare în cursul acțiunii penale îndreptate împotriva sa.

297. Curtea reține, de asemenea, argumentul Guvernului potrivit căruia dreptul rus prevede căi de drept penal care permit depunerea de plângeri privind abuzul de autoritate, colectarea sau difuzarea neautorizată de informații despre viața privată și de familie a unei persoane, sau încălcarea dreptului cetățeanului la respectarea caracterului privat al comunicațiilor sale. Pentru motivele menționate în paragrafele precedente, aceste căi de atac sunt de asemenea disponibile numai persoanelor care au posibilitatea de a prezenta serviciilor de urmărire penală cel puțin câteva informații concrete despre interceptarea propriilor comunicații (*supra*, pct. 24).

298. Curtea deduce de aici că acele căi de atac menționate de Guvern sunt disponibile numai persoanelor care dețin informații despre interceptarea comunicațiilor lor. Eficacitatea acestor căi de atac este așadar compromisă de lipsa obligației de a notifica într-o etapă oarecare persoana supusă interceptării, precum și lipsa unei posibilități corespunzătoare de a solicita și a obține, de la autorități, informații despre interceptări. În consecință, Curtea consideră că dreptul rus nu prevede o cale de atac efectivă împotriva măsurilor de supraveghere secretă în cazurile în care nu se declanșează o acțiune penală împotriva subiectului interceptării. În speță, nu este sarcina Curții să se pronunțe dacă respectivele căi de atac pot fi efective în situația în care o persoană află în cursul acțiunii penale îndreptate împotriva sa că i-au fost interceptate comunicațiile (a se vedea, totuși, *Avanesyan*, citată anterior, cauză în care unele dintre aceste căi de atac au fost considerate inefficiente în legătură cu plângerea reclamantului referitoare la „inspecția” efectuată la apartamentul său).

299. În fine, în ceea ce privește căile de atac în fața instanțelor pentru a face plângere privind insuficiența garanțiilor prevăzute în dreptul rus împotriva abuzurilor, Curtea nu este convinsă de argumentul Guvernului potrivit căruia aceste căi de atac sunt efective (*supra*, pct. 156 și 225). În ceea ce privește posibilitatea de a contesta LMOI la Curtea Constituțională, Curtea observă că această instanță a examinat în mod repetat constituționalitatea acestei legi, pe care a declarat-o compatibilă cu Constituția (*supra*, pct. 40–43, 50, 82 și 85–87). În aceste condiții, Curtea consideră puțin probabil ca plângerea reclamantului la Curtea Constituțională invocând probleme identice cu cele pe care le-a examinat deja să aibă șansă de reușită. De asemenea, Curtea nu este convinsă că atacarea Ordinului nr. 70 la Curtea Supremă sau la instanțe de grad inferior ar constitui o cale de atac efectivă. Într-adevăr, reclamantul a atacat Ordinul nr. 70 conform procedurii interne; însă, atât judecătoria, cât și Tribunalul Sankt Petersburg au concluzionat că reclamantul nu avea calitatea necesară să conteste acest ordin, motivând că echipamentul instalat conform acestui act nu aduce atingere în sine caracterului privat al comunicațiilor sale (*supra*, pct. 10, 11 și 13). Trebuie reținut faptul că, de asemenea, Curtea Supremă a considerat că Ordinul nr. 70 avea caracter tehnic, nu juridic (*supra*, pct. 128).

300. Având în vedere considerentele de mai sus, Curtea concluzionează că dreptul rus nu asigură o cale de atac efectivă unei persoane care crede că a fost supusă unei supravegheri secrete. Lipsind persoana supusă interceptării de posibilitatea efectivă de a contesta retroactiv măsurile de interceptare, dreptul rus nu reușește să ofere o garanție importantă împotriva folosirii necorespunzătoare a măsurilor de supraveghere secretă.

301. Pentru motivele expuse mai sus, Curtea respinge excepția de neepuizare a căilor de atac interne, ridicată de Guvern.

θ) Concluzie

302. Curtea concluzionează că dispozițiile din dreptul rus privind interceptarea comunicațiilor nu conțin garanții corespunzătoare și efective împotriva arbitrarului și a riscului de abuz inerent oricărui sistem de supraveghere secretă, risc care este deosebit de mare într-un sistem în care serviciile secrete și poliția beneficiază, prin mijloace tehnice, de acces direct la toate comunicațiile de telefonie mobilă. În special, circumstanțele în care autoritățile publice sunt abilitate să recurgă la măsuri de supraveghere secretă nu sunt definite suficient de clar. Dispozițiile privind ridicarea măsurilor de

supraveghere secretă nu oferă garanții suficiente împotriva ingerințelor arbitrare. Dreptul intern autorizează păstrarea automată a unor date evident irelevante și nu este suficient de clar cu privire la circumstanțele în care elementele interceptate trebuie păstrate sau distruse după proces. Procedurile de autorizare nu sunt apte să garanteze că o măsură de supraveghere secretă este dispusă numai atunci când este „necesară într-o societate democratică”. Controlul asupra interceptărilor, așa cum este organizat în prezent, nu îndeplinește cerințele privind independența, existența unor competențe și atribuții suficiente pentru a exercita un control efectiv și permanent, dreptul de control public și eficacitatea în practică. Eficacitatea măsurilor este compromisă de lipsa de notificare, în orice stadiu, cu privire la interceptare sau lipsa de acces corespunzător la documente referitoare la interceptări.

303. Este important de remarcat faptul că deficiențele cadrului legal, identificate mai sus, par să afecteze aplicarea concretă a sistemului de supraveghere secretă existent în Rusia. Curtea nu este convinsă de afirmația Guvernului, potrivit căreia toate interceptările care se efectuează în Rusia sunt perfect legale și bazate pe o autorizație judiciară corespunzătoare. Exemplele prezentate de reclamant în cadrul procedurii interne (*supra*, pct. 12) și al procedurii în fața Curții (*supra*, pct. 197) indică existența unor practici de supraveghere arbitrară și abuzive, care par a fi cauzate de insuficiența garanțiilor oferite de lege (pentru un raționament similar, a se vedea *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiev*, citată anterior, pct. 92; a se vedea, a contrario, *Klass și alții*, citată anterior, pct. 59 și *Kennedy*, citată anterior, pct. 168 și 169).

304. Având în vedere deficiențele sus-menționate, Curtea consideră că dreptul rus nu îndeplinește cerința privind „calitatea legii” și nu poate să limiteze „ingerința” la ceea ce constituie o măsură „necesară într-o societate democratică”.

305. Prin urmare, a fost încălcat art. 8 din Convenție.

II. Cu privire la pretinsa încălcare a art. 13 din Convenție

306. Reclamantul s-a plâns că nu a avut la dispoziție o cale de atac efectivă pentru capătul său de cerere întemeiat pe art. 8. Acesta invocă art. 13 din Convenție, care prevede:

„Orice persoană, ale cărei drepturi și libertăți recunoscute de prezenta Convenție au fost încălcate, are dreptul să se adreseze efectiv unei instanțe naționale, chiar și atunci când încălcarea s-ar datora unor persoane care au acționat în exercitarea atribuțiilor lor oficiale.”

307. Având în vedere concluzia la care a ajuns cu privire la art. 8 din Convenție (*supra*, pct. 286-300), Curtea consideră că nu este necesar să examineze separat capătul de cerere întemeiat pe art. 13, deși acesta este strâns legat de cel întemeiat pe art. 8 și, prin urmare, trebuie să fie declarat admisibil (*Liberty și alții*, citată anterior, pct. 73).

III. Cu privire la aplicarea art. 41 din Convenție

308. În conformitate cu art. 41 din Convenție,

„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

309. Reclamantul solicită 9 000 euro (EUR) pentru prejudiciul moral.

310. Guvernul consideră această cerere excesivă deoarece, în opinia sa, reclamantul a contestat dreptul rus *in abstracto*, fără să fie afectat personal de acesta. În opinia sa, constatarea unei încălcări ar constitui așadar o reparație echitabilă suficientă.

311. Curtea reamintește că, în cadrul executării unei hotărâri în temeiul art. 46 din Convenție, o hotărâre de constatare a încălcării Convenției sau a protocoalelor sale impune statului pârât obligația legală nu doar de a plăti reclamanților sumele acordate cu titlu de reparație echitabilă, ci și de a alege, sub supravegherea Comitetului de Miniștri, măsurile generale și/sau, după caz, măsurile individuale care trebuie adoptate în ordinea juridică internă pentru a pune capăt încălcării constatate de Curte și a remedia pe cât posibil efectele acesteia astfel încât să se restabilească cât mai mult posibil situația anterioară acesteia. De asemenea, prin ratificarea Convenției, statele contractante se angajează să asigure faptul că dreptul lor intern este în concordanță cu aceasta (*Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiev*, citată anterior, pct. 111, cu alte trimiteri).

312. În opinia Curții, constatarea încălcării constituie o reparație echitabilă suficientă pentru orice prejudiciu moral cauzat reclamantului.

B. Cheltuieli de judecată

313. În fața Camerei, reclamantul a solicitat 26 579 de ruble rusești (RUB) [aproximativ 670 de euro (EUR) la data depunerii cererii] pentru cheltuielile poștale și de traducere. Pentru justificare, a prezentat facturi pentru servicii de poștă și de fax, precum și un contract de traducere.

314. În fața Marii Camere, reclamantul solicită 22 800 de lire sterline (GBP) (aproximativ 29 000 EUR la data depunerii cererii) și 13 800 EUR cu titlu de onorarii ale avocaților. Acesta se bazează pe centralizatorul cu orele lucrate de avocații săi. Referitor la facturi, acesta mai solicită 6 833,24 GBP (aproximativ 8 700 EUR la data depunerii cererii) pentru rambursarea cheltuielilor de traducere și de călătorie, precum și alte cheltuieli administrative.

315. Guvernul acceptă cererea privind cheltuielile de judecată prezentată Camerei întrucât este susținută de documente justificative. În ceea ce privește pretențiile privind cheltuielile de judecată prezentate Marii Camere, Guvernul susține că acestea au fost formulate la mai mult de o lună după ședință. În ceea ce privește onorariile avocaților, unele dintre acestea corespund muncii efectuate de reprezentanți înainte ca reclamantul să semneze un formular de împuternicire și nu există nicio împuternicire pe numele doamnei Levine. În plus, numărul reprezentanților și numărul de ore dedicate de aceștia pregătirii dosarului sunt excesive. De asemenea, nu există nicio dovadă că reclamantul a plătit sau este obligat să plătească onorariile respective în temeiul unei obligații legale sau contractuale. În ceea ce privește cheltuielile de traducere și alte cheltuieli administrative, Guvernul susține că reclamantul nu a prezentat niciun document care să ateste că a plătit sumele indicate. De asemenea, acesta nu a demonstrat necesitatea cheltuielilor de traducere, unii dintre avocații săi fiind vorbitori de limbă rusă – potrivit Guvernului. În fine, tarifele practicate de traducători sunt exagerate, ca și cheltuielile de călătorie.

316. Conform jurisprudenței Curții, un reclamant nu poate obține rambursarea cheltuielilor de judecată decât în măsura în care se stabilește caracterul real, necesar și rezonabil al acestora. În prezenta cauză, având în vedere documentele de care dispune și criteriile de mai sus, Curtea consideră că este rezonabil să acorde reclamantului suma de 40 000 EUR pentru toate cheltuielile, plus orice sumă ce poate fi datorată cu titlu de impozit.

C. Dobânzi moratorii

317. 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. unește cu fondul, în unanimitate, excepțiile preliminare ridicate de Guvern cu privire la lipsa calității de victimă și la neepuizarea căilor de atac interne și declară cererea admisibilă;
2. hotărăște, în unanimitate, că a fost încălcat art. 8 din Convenție și respinge excepțiile ridicate de Guvern, sus-menționate;
3. hotărăște, în unanimitate, că nu este necesar să examineze capătul de cerere întemeiat pe art. 13 din Convenție;
4. hotărăște, cu 16 voturi la 1, că această constatare a unei încălcări constituie în sine o reparație echitabilă suficientă pentru orice prejudiciu moral pe care l-ar fi putut suferi reclamantul;
5. hotărăște, în unanimitate:
 - a) că statul pârât trebuie să plătească reclamantului în termen de 3 luni suma de 40 000 EUR (patruzeci de mii de euro) pentru cheltuielile de judecată, plus orice sumă ce poate fi datorată de reclamant cu titlu de impozit;
 - b) că, de la expirarea termenului menționat și până la efectuarea plății, această sumă trebuie majorată cu o dobândă simplă, la o rată egală cu rata dobânzii facilității de împrumut marginal practică de Banca Centrală Europeană, aplicabilă pe parcursul acestei perioade și majorată cu trei puncte procentuale;
6. respinge, în unanimitate, cererea de acordare a unei reparații echitabile pentru celelalte capete de cerere.

Redactată în limbile franceză și engleză, apoi pronunțată în ședință publică la Palatul Drepturilor Omului din Strasbourg, la 4 decembrie 2015.

PREȘEDINTE,
DEAN SPIELMANN

Jurisconsult,
Lawrence Early

În conformitate cu art. 45 § 2 din Convenție și art. 74 § 2 din Regulament, la prezenta hotărâre se anexează următoarele opinii separate:

- opinia concordantă a domnului judecător Dedov;
- opinia parțial dizidentă a doamnei judecător Ziemele.

D.S.
T.L.E.

1. Competența Curții de a examina dreptul intern *in abstracto*

Așa cum subliniază Guvernul, pot exista îndoieli cu privire la competența Curții de a examina calitatea și eficacitatea dreptului intern *in abstracto*, fără să se fi stabilit calitatea de victimă a reclamantului ori să se fi verificat existența unei ingerințe în dreptul său la respectarea vieții sale private în practică, nu doar în teorie.

Curtea a urmat această abordare în cauze referitoare la interceptări pentru a preveni eventualele abuzuri de autoritate. În două cauze importante, *Kennedy împotriva Regatului Unit* (nr. 26839/05, 18 mai 2010, pct. 122-123) și *Klass și alții împotriva Germaniei* (6 septembrie 1978, pct. 34, seria A nr. 28), care au fost îndreptate împotriva a două state democratice mari – Regatul Unit și Republica Federală Germania –, Curtea a confirmat eficacitatea sistemelor naționale respective pentru combaterea arbitrarului. Cu toate acestea, în mod regretabil, nu putem ignora faptul că acele două state au fost implicate recent în scandaluri răsunătoare legate de supraveghere: într-un caz, convorbirile de telefonie mobilă ale Cancelarului federal german au fost interceptate ilegal de serviciile secrete naționale; în celălalt, autoritățile britanice au furnizat serviciilor secrete americane acces și informații referitoare la întreaga bază de date privind comunicațiile din primul stat, permițând astfel autorităților americane să intercepteze comunicațiile oricărui cetățean britanic fără a fi supuse niciunei garanții interne adecvate.

Asta arată că, încă de la început, ceva a fost greșit în abordarea Curții. Poate că ar fi mai eficient să se ocupe de cereri de la caz la caz, astfel încât Curtea să aibă posibilitatea de a stabili existența unei ingerințe și de a constata încălcarea Convenției – așa cum face de regulă în materie de percheziții nejustificate la adresele reclamantilor. În general, problema în aceste cauze nu vizează competențele instanțelor naționale în materie de autorizare, ci modul în care judecătorii autorizează perchezițiile în vederea cercetărilor penale.

Abordarea Curții poate trece ușor de la aplicarea efectivă a legii la o potențială ingerință. Există exemple în cauza *Kennedy*:

„119. Conform jurisprudenței constante a Curții, aceasta nu are sarcina de a examina *in abstracto* legislația și practica relevante, ci de a verifica dacă modul, în care acestea au fost aplicate reclamantului ori l-au afectat, a încălcat Convenția [a se vedea, printre altele, *Klass și alții*, citată anterior, pct. 33; *N.C. împotriva Italiei* (MC), nr. 24952/94, pct. 56, CEDO 2002-X; și *Krone Verlag GmbH & Co. KG împotriva Austriei* (nr. 4), nr. 72331/01, pct. 26, 9 noiembrie 2006]”

și cauza *Klass*:

„36. [...] Curtea nu poate admite faptul că asigurarea exercitării unui drept garantat de Convenție poate fi astfel eliminată prin simplul fapt de a menține persoana respectivă neinformată despre încălcarea acestuia. Dreptul de a sesiza Comisia, care le aparține persoanelor eventual afectate de supravegherea secretă, decurge de la art. 25; în caz contrar, art. 8 ar risca să devină nul.”

Scandalul german și cel englez, menționate mai sus, confirmă însă că, mai devreme sau mai târziu, persoana vizată află despre interceptare. Există exemple în acest sens în contextul rus (*Shimovolos împotriva Rusiei*, nr. 30194/09, 21 iunie 2011). În prezenta cauză, reclamantul nu are cunoștință de vreo interceptare a comunicațiilor sale, acesta fiind un fapt pe care Curtea nu îl poate ignora.

Curtea a evitat, în mod repetat, să examineze cauzele *in abstracto* [*Silver și alții împotriva Regatului Unit*, 25 martie 1983, pct. 79, seria A nr. 61; *Nikolova împotriva Bulgariei* (MC), nr. 31195/96, pct. 60, CEDO 1999-II; *Nejdet Şahin și Perihan Şahin împotriva Turciei* (MC), nr. 13279/05, pct. 68-70, 20 octombrie 2011; *Sabanchiyeva și alții împotriva Rusiei*, nr. 38450/05, pct. 137, CEDO 2013; și *Monnat împotriva Elveției*, nr. 73604/01, pct. 31-32, CEDO 2006-X]. Putem presupune așadar că fiecare cauză referitoare la interceptări este unică. Astfel, trebuie să cunoaștem motivele pentru care Curtea ar trebui să își modifice abordarea generală în examinarea unor astfel de cauze. Nu avem însă nicio idee în privința motivelor. Dacă legislația creează riscul arbitrarului, atunci trebuie să vedem rezultatul acestui arbitrar. Nu sunt sigur că sunt suficiente câteva exemple (fără legătură cu cazul reclamantului) pentru a dovedi că întregul sistem de garanții trebuie să fie revizuit și consolidat. Aș accepta o astfel de abordare în cazul în care Curtea ar avea o întârziere enormă în materie de cereri individuale repetitive care arată că Ordinul nr. 70 (privind conectarea unui echipament de interceptare a rețelelor operatorilor) nu are caracter tehnic, dar creează o problemă structurală în Rusia. Într-un astfel de caz, am avea totuși nevoie de o procedură-pilot și o hotărâre-

pilot.

Toate cauzele în care Curtea a constatat o încălcare (mai mult de 15 000 de hotărâri) se bazează pe abuzul de autoritate, chiar și atunci când legislația internă este de bună calitate. Orice abuz de autoritate este o chestiune de etică și nu îl putem elimina doar prin măsuri legislative.

Conform jurisprudenței constante a Curții, aceasta nu are sarcina de a examina *in abstracto* legile și practicile interne sau de a exprima o opinie privind compatibilitatea prevederilor legale cu Convenția, ci de a verifica dacă modul în care acestea i-au fost aplicate reclamantului sau l-au afectat constituie o încălcare a Convenției (a se vedea, în special, în contextul art. 14, *Religionsgemeinschaft der Zeugen Jehovas și alții împotriva Austriei*, nr. 40825/98, 31 iulie 2008, pct. 90).

Art. 34 din Convenție nu instituie, pentru folosul persoanelor, un fel de *actio popularis* pentru interpretarea Convenției; acesta nu le autorizează să facă plângere *in abstracto* împotriva unei legi pentru simplul motiv că li se pare că aceasta contravine Convenției. În principiu, nu este suficient ca un reclamant individual să susțină că o lege îi încalcă prin simpla ei existență drepturile prevăzute de Convenție; legea trebuie să fi fost aplicată în detrimentul său (a se vedea *Klass*, citată anterior, pct. 33). Aceste principii nu ar trebui să fie aplicate în mod arbitrar.

2. Organul parlamentar și organul judecătoresc: Curtea trebuie să respecte diferențele

Prezenta cauză este foarte importantă din perspectiva separării funcțiilor între Curte și Adunarea Parlamentară a Consiliului Europei; într-adevăr, este necesar să se separe competențele organului parlamentar și cele ale organului judecătoresc. Adunarea Parlamentară adoptă recomandări, rezoluții și avize care servesc ca linii directoare pentru Comitetul Miniștrilor, precum și pentru guvernele, parlamentele și partidele politice naționale. În cele din urmă, prin intermediul convențiilor, legilor și practicilor, Consiliul Europei promovează drepturile omului, democrația și statul de drept. Acesta urmărește progresele înregistrate de statele membre în aceste domenii și emite recomandări prin intermediul organelor de supraveghere specializate și independente. Curtea Europeană a Drepturilor Omului se pronunță cu privire la cererile persoanelor sau statelor în care se invocă încălcarea drepturilor civile și politice consacrate în Convenția europeană a drepturilor omului. Având în vedere această separare a funcțiilor, examinarea unei cauze *in abstracto* seamănă cu o expertiză, nu cu o hotărâre.

Morten Kjaerum, directorul Agenției pentru Drepturi Fundamentale a Uniunii Europene (FRA), a declarat următoarele într-o dezbatere comună cu privire la drepturile omului care a avut loc la 4 septembrie 2014 în cadrul Comisiei pentru libertăți civile, justiție și afaceri interne a Parlamentului European (LIBE) [traducerea Grefei]:

„Dezvăluirile lui Snowden despre supravegherea în masă au scos în evidență faptul că protecția datelor cu caracter personal este amenințată. Protecția dreptului la viață privată este departe de a fi suficientă dacă examinăm toată Europa contemporană în ansamblu. În urma dezbatelor de anul trecut, primim foarte favorabil solicitarea adresată de Parlamentul European Agenției pentru Drepturi Fundamentale ca aceasta să abordeze în continuare drepturile fundamentale și garanțiile existente în cadrul unor ample programe de supraveghere. Desigur, veți fi informați, probabil spre sfârșitul anului, despre concluziile acestei solicitări deosebite.

Dar nu este vorba numai despre programele majore de supraveghere. Există, de asemenea, suspiciune față de mecanismele de supraveghere în domeniul protecției generale a datelor. [Într-adevăr,] încredințăm date serviciilor de sănătate, administrației fiscale sau altor instituții, publice sau private. Activitatea Agenției pentru Drepturi Fundamentale arată că, în prezent, structurile naționale de supraveghere din cadrul UE sunt prea slabe pentru a-și îndeplini misiunea. Autoritățile responsabile de protecția datelor din fiecare stat membru trebuie să joace un rol important în punerea în aplicare a sistemului general de protecție a datelor, dar este urgent să se consolideze atribuțiile și resursele autorităților naționale de protecție a datelor și să se asigure totodată independența acestor autorități.

În fine, doresc să subliniez faptul că entitățile responsabile de păstrarea datelor – publice sau private –, instituțiile, trebuie să fie considerate răspunzătoare, și încă mult mai mult față de ceea ce observăm în prezent, dacă garanțiile pe care acestea le creează nu sunt suficiente.”

Aceste observații au fost adresate noilor membri ai Parlamentului European (nu judecătorilor) și au ridicat probleme care preocupă întreaga Europă și care necesită un sistem de protecție a datelor mai sofisticat. Scopul discursului a fost de a lansa o dezbatere publică în vederea definirii unor măsuri eficiente și a depunerii de eforturi pentru standarde etice reale în societate; o sală de judecată nu este un loc potrivit pentru o astfel de dezbatere.

Aș considera că, astfel, Curtea ar face bine să se concentreze asupra unei anumite ingerințe și asupra eficienței măsurilor în vigoare pentru a preveni încălcarea respectivă (așa cum Curtea

procedează de obicei în orice altă categorie de cauze). Sarcina principală a Curții este de a stabili că a avut loc o ingerință, apoi de a verifica dacă această ingerință a fost prevăzută de lege și necesară într-o societate democratică. În plan etic, este inacceptabil ca judecătorii, fără să cunoască faptele, să presupună că orice cetățean al unui stat ar putea fi supus unei supravegheri secrete ilegale. O hotărâre nu se poate baza pe alegații.

Curtea a folosit mai multe instrumente pentru a combate încălcările. Unul dintre ele a fost de a constata încălcarea art. 10 pe fondul refuzului unui serviciu de informații de a furniza organizației reclamante informații despre persoanele aflate sub supraveghere electronică într-o anumită perioadă de timp (*Youth Initiative for Human Rights împotriva Serbiei*, nr. 48135/06, 25 iunie 2013). În dispozitivul hotărârii respective, Curtea a invitat Guvernul să se asigure că informațiile solicitate sunt puse la dispoziția organizației reclamante (fără a aștepta ca anumite măsuri să fie propuse de Comitetul de Miniștri). Eu văd în această abordare o măsură eficientă și totodată un succes judiciar.

3. Ar trebui dezvoltată abordarea privind „probabilitatea rezonabilă”

Stabilirea calității de victimă a reclamantului face parte din procesul judiciar. Art. 34 din Convenție prevede următoarele „Curtea poate fi sesizată printr-o cerere de către orice persoană fizică, orice organizație neguvernamentală sau de orice grup de particulari care se pretinde victimă a unei încălcări de către una dintre înaltele părți contractante a drepturilor recunoscute în Convenție sau în protocoalele sale”. Noțiunea de „victimă” nu presupune existența unui prejudiciu [*Brumărescu împotriva României* (MC), nr. 28342/95, pct. 50, CEDO 1999-VII].

Curtea a hotărât anterior că, deși existența unui sistem de supraveghere poate aduce atingere vieții private, o plângere conform căreia acest fapt a generat încălcarea drepturilor nu poate fi adresată instanței decât în cazul în care există o „probabilitate rezonabilă” ca o persoană să fi fost supusă unei supravegheri ilegale (*Esbester împotriva Regatului Unit*, nr. 18601/91, decizia Comisiei din 2 aprilie 1993; *Redgrave împotriva Regatului Unit*, nr. 202711/92, decizia Comisiei din 1 septembrie 1993; și *Matthews împotriva Regatului Unit*, nr. 28576/95, decizia Comisiei din 16 octombrie 1996). Aceste trimiteri vizează decizii declarate inadmisibile, toate acuzațiile în materie de interceptare fiind considerate ca vădit nefondate.

Cu toate acestea, Curtea și-a modificat în totalitate abordarea în cauza *Kennedy*: „[...] nu se poate exclude faptul că măsuri de supraveghere secretă [...] au fost aplicate [reclamantului] sau că acesta [...] risca să fie supus unor astfel de măsuri” (*Kennedy*, citată anterior, pct. 125-129). În prezent, vedem că această modificare a jurisprudenței nu a fost eficientă.

Expresia „probabilitate rezonabilă” implică existența unor consecințe negative pentru un reclamant care este potențial expus unei supravegheri secrete ca urmare a anumitor informații care sunt puse la dispoziția autorităților prin interceptare, și exclude posibilitatea ca aceste informații să poată fi aflate prin alte mijloace. Curtea a făcut această abordare periculos de simplă pentru examinarea acestor cauze pe fond, presupunând că persoanele supuse supravegherii secrete de către autorități nu sunt întotdeauna informate ulterior despre măsurile aplicate lor și astfel este imposibil pentru reclamant să demonstreze că a existat o ingerință în oricare dintre drepturile lor. Prin urmare, Curtea a ajuns la concluzia că trebuie să se considere că reclamantii aveau dreptul să introducă o cerere chiar dacă nu puteau dovedi calitatea lor de victimă. Reclamantii din cauza *Klass* și cauza *Liberty și alții împotriva Regatului Unit* (nr. 58243/00, 1 iulie 2008) erau avocați și nu era exclus ca aceștia să fi fost „supuși unei supravegheri secrete din cauza contactelor pe care le [pot] avea cu clienții suspecți de activități [ilegale]” (*Klass*, pct. 27).

În cauza *Kennedy*, reclamantul a invocat neprimirea unor apeluri locale și primirea unor apeluri care nu îi erau adresate și care i-au cauzat pierdere de timp. Reclamantul a bănuț că problemele au fost cauzate de interceptarea corespondenței sale, dar și a comunicațiilor sale telefonice și electronice; Curtea a luat în serios acest lucru, a respins excepțiile Guvernului pârât conform cărora reclamantul nu a demonstrat că a existat o ingerință în sensul art. 8 sau nu a stabilit existența unei probabilități rezonabile. Curtea a respins și argumentele referitoare la neputința de atac interne, cu toate că reclamantul nu a verificat la operatorul său calitatea serviciilor de telecomunicații, ci a transmis la MI5 și GCHQ – serviciile britanice de informații responsabile cu securitatea națională – o cerere de comunicare a datelor sale cu caracter personal în baza Legii din 1998 privind protecția datelor.

Revenind la circumstanțele cauzei, se poate concluziona în mod justificat că interconexiunea dintre echipamentele de telecomunicații și echipamentele de interceptare nu înseamnă neapărat că ar fi avut loc într-adevăr interceptarea convorbirilor telefonice ale reclamantului. De asemenea, Curtea nu își poate întemeia concluziile nici pe prezumția legată de „posibilitatea ca un funcționar necinstit, neglijent sau excesiv de zelos să comită fapte ilegale” [*Klass*, pct. 49, 50, 59; *Weber și Saravia împotriva Germaniei* (dec.), nr. 54934/00, pct. 106, CEDO 2006-XI; și *Kennedy*, pct. 153-154]. În mod similar, nu se poate presupune cu titlu general (pentru a examina cauza *in abstracto*) existența unei măsuri

violente a statului împotriva mișcărilor de opoziție și a altor instituții democratice din statul pârât, chiar dacă Adunarea Parlamentară a adoptat rezoluții pe această temă. Curtea trebuie să rămână imparțială și neutră.

4. Rolul puterii judecătorești în societatea civilă

Cu toate acestea, am votat pentru admisibilitate și pentru constatarea încălcării art. 8 din Convenție, deoarece importanța fundamentală a garanțiilor care protejează comunicațiile private împotriva supravegherii arbitrare, mai ales într-un context non-penal, nu a fost niciodată luată în considerare în procedura internă. Instanțele ruse au refuzat să examineze fondul acuzațiilor reclamantului, invocând în mod eronat caracterul tehnic al ordinelor ministeriale în litigiu. În calitatea mea de judecător național, nu pot ignora faptul că în societatea rusă există suspiciuni generalizate că se exercită supravegherea personalităților politice și economice, inclusiv a activiștilor pentru drepturile omului, a activiștilor și liderilor din opoziție, a jurnaliștilor, a funcționarilor, a administratorilor bunurilor statului – altfel spus, a tuturor celor implicați în afacerile publice. Aceste suspiciuni decurg din experiența regimului totalitar al erei sovietice, și chiar din lunga istorie a Imperiului Rus.

Această hotărâre ar putea servi ca bază pentru îmbunătățirea legislației privind măsurile operative de investigații și pentru stabilirea unui sistem eficient de control public asupra supravegherii. În plus, această hotărâre arată că, dacă există suspiciuni generalizate în societate și dacă nu există nicio altă posibilitate ca societatea să înlăture suspiciunile în lipsa unui contract social și a unor modificări adecvate în legislația și practica națională, atunci - în cazul în care problema nu este depistată de celelalte ramuri ale puterii - sistemul judiciar este cel care trebuie să fie activ pentru a facilita aceste modificări. Acest lucru este cu atât mai evident dacă nu există alte mijloace disponibile pentru a proteja democrația și statul de drept. Acesta este un rol important pe care puterea judecătorească trebuie să îl joace în societatea civilă.

Curtea ar putea fi criticată pentru că nu a oferit motive mai clare în susținerea examinării sale *in abstracto* în contextul social, cu precizarea că aceasta s-a limitat la respectarea jurisprudenței camerelor sale. Hotărârea pronunțată în prezenta cauză este totuși una delicată deoarece, înainte de a ajunge la o concluzie, judecătorii au fost nevoiți să se asigure dacă toate celelalte mijloace au fost inutile sau nu. În schimb, în cauza *Clapper împotriva Amnesty International USA* (568 U.S. __ (2013), Curtea Supremă a Statelor Unite s-a abținut să facă un pas înainte, în pofida existenței unui program de supraveghere în masă și a unor „suspiciuni generalizate” referitoare la acesta (sau, în cuvintele judecătorului Breyer în opinia sa dizidentă: „[prejudiciul] este la fel de probabil să se întâmple ca și majoritatea evenimentelor viitoare pe care ni le anticipează inferențele derivate din bunul simț și cunoștințele comune despre natura umană”). Curtea Supremă a preferat să considere insuficient argumentul petenților (printre care organizații care activează în domeniul drepturilor omului și al legii, precum și al mass-media), potrivit căruia aceștia riscau să fie supuși supravegherii ca urmare a naturii muncii lor.

Mă voi opri aici, lăsând academicienilor discuțiile despre agresivitate, activism sau moderație judiciară. Aș dori doar să-mi închei opinia citându-l pe Edward Snowden: „Cu fiecare victorie în instanță, cu fiecare modificare a legii, demonstrăm că faptele sunt mai convingătoare decât frica. Ca societate, redescoperim că valoarea dreptului nu constă în ceea ce se ascunde, ci în ceea ce protejează”.

OPINIA PARȚIAL DIZIDENTĂ A DOAMNEI JUDECĂTOR ZIEMELE

1. Subscriu în totalitate la constatarea unei încălcări în prezenta cauză. Curtea pronunță astfel o hotărâre foarte importantă într-o problemă de principiu, supravegherea secretă realizată așa cum s-a menționat în faptele cauzei fiind, în esența ei, incompatibilă cu statul de drept și cu principiile democrației.

2. Având în vedere tocmai acest context, nu pot fi de acord cu decizia Curții de a nu acorda nicio sumă de bani pentru prejudiciul moral suferit. În opinia mea, cererea de reparație formulată de reclamant este foarte justificată (pct. 309 din hotărâre), iar constatarea încălcării, deși foarte importantă în principiu în prezenta cauză, nu constituie o reparație corespunzătoare în situația specifică a reclamantului. Din acest motiv, am votat împotriva pct. 4 din dispozitivul hotărârii.