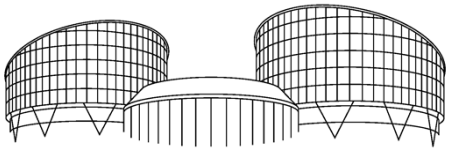

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

GRANDE CHAMBRE

AFFAIRE ROMAN ZAKHAROV c. RUSSIE

(Requête nº 47143/06)

ARRÊT

STRASBOURG

4 décembre 2015

Cet arrêt est définitif.

En l'affaire Roman Zakharov c. Russie,

La Cour européenne des droits de l'homme, siégeant en une Grande Chambre composée de :

Dean Spielmann, *président*,
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, *juges*,

et de Lawrence Early, *jurisconsulte*,

Après en avoir délibéré en chambre du conseil le 24 septembre 2014 et le 15 octobre 2015,

Rend l'arrêt que voici, adopté à cette dernière date :

PROCÉDURE

1. À l'origine de l'affaire se trouve une requête (n° 47143/06) dirigée contre la Fédération de Russie et dont un ressortissant de cet État, M. Roman Andreyevich Zakharov (« le requérant »), a saisi la Cour le 20 octobre 2006 en vertu de l'article 34 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (« la Convention »).

2. Le requérant a d'abord été représenté par M. B. Gruzd, avocat à Saint-Pétersbourg. Par la suite, il a été représenté par des avocats de l'organisation non gouvernementale Memorial Human Rights Centre/EHRAC, sise à Moscou. Le gouvernement russe (« le Gouvernement ») a été représenté par M. G. Matyushkin, représentant de la Fédération de Russie auprès de la Cour.

3. Le requérant alléguait que le système d'interception secrète des communications de téléphonie mobile en Russie avait emporté violation du son droit au respect de sa vie privée et de sa correspondance et qu'il n'avait pas disposé d'un recours effectif permettant de s'en plaindre.

4. Le 19 octobre 2009, la requête a été communiquée au Gouvernement.

5. Le 11 mars 2014, la chambre de la première section à laquelle la requête avait été attribuée (article 52 § 1 du règlement de la Cour – « le règlement »), composée de Isabelle Berro, présidente, Khanlar Hajiyev, Julia Laffranque, Linos-Alexandre Sicilianos, Erik Møse, Ksenija Turković, Dmitry Dedov, juges, ainsi que de Søren Nielsen, greffier de section, s'est dessaisie au profit de la Grande Chambre, aucune des parties ne s'y étant opposée (articles 30 de la Convention et 72 du règlement).

6. Une audience s'est déroulée en public au Palais des droits de l'homme, à Strasbourg, le 24 septembre 2014 (article 59 § 3 du règlement).

Ont comparu :

– *pour le Gouvernement*
M. G. MATYUSHKIN, représentant de la Fédération de Russie auprès de la Cour européenne des droits de l'homme, *agent*,
M^mes^ O. SIROTKINA,
I. KORIEVA,
O. IURCHENKO,
MM. O. AFANASEV,
A. LAKOV, *conseillers* ;

– *pour le requérant*
M. P. LEACH,
M^me^ K. LEVINE,
M. K. KOROTEEV,
M^mes^ A. RAZHIKOVA, *conseils*,
E. LEVCHISHINA, *conseiller*.

La Cour a entendu en leurs déclarations M. Matyushkin, M. Leach, M^me^ Levine, M^me^ Razhikova et M. Koroteev, ainsi que M. Matyushkin et M. Leach en leurs réponses aux questions posées par des juges.

EN FAIT

I. LES CIRCONSTANCES DE L'ESPÈCE

7. Le requérant est né en 1977 et réside à Saint-Pétersbourg.

8. Il est le rédacteur en chef d'une maison d'édition et d'un magazine d'aviation. Par ailleurs, il préside la branche pétersbourgeoise de la Fondation pour la défense de la glasnost, une organisation non gouvernementale (ONG) qui surveille la situation en matière de liberté des

médias dans les régions russes, défend l'indépendance des médias régionaux, la liberté d'expression et le respect des droits des journalistes, et offre à ceux-ci un soutien juridique, notamment par la voie procédurale.

9. Il était abonné aux services de plusieurs opérateurs de réseaux mobiles.

10. Le 23 décembre 2003, il engagea une procédure judiciaire contre trois opérateurs de réseaux mobiles, alléguant une atteinte à son droit au respect du caractère privé de ses communications téléphoniques. Il plaidait qu'en application de l'arrêté n° 70 (paragraphes 115-122 ci-dessous) pris par la Commission nationale des communications et des technologies de l'information – le prédécesseur du ministère des Communications et des Technologies de l'information (« le ministère des Communications ») –, les opérateurs de réseaux mobiles avaient mis en place un dispositif permettant au Service fédéral de sécurité (FSB) d'intercepter toute communication téléphonique sans autorisation judiciaire préalable. Il considérait que l'arrêté n° 70, qui n'avait jamais été publié, restreignait indûment le droit au respect de sa vie privée. Il pria le tribunal d'émettre une injonction ordonnant le retrait du dispositif installé en application de l'arrêté n° 70 et de veiller à ce que l'accès aux communications de téléphonie mobile ne fût donné qu'aux seules personnes autorisées. Le ministère des Communications et la section du FSB de Saint-Pétersbourg et de la région de Leningrad intervinrent dans la procédure en tant que tierce partie.

11. Le 5 décembre 2005, le tribunal du district Vassileostrovski de Saint-Pétersbourg (« le tribunal de district ») débouta le requérant au motif qu'il n'avait pas démontré que les opérateurs de réseaux mobiles avaient transmis la moindre information protégée à des personnes non autorisées ou permis l'interception illimitée ou non autorisée de communications. Le tribunal de district indiqua que le dispositif visé par l'intéressé avait été mis en place pour permettre aux organes d'application des lois de mener à bien des mesures opérationnelles d'investigation suivant la procédure prévue par la loi. Il estima que l'installation d'un tel dispositif ne constituait pas en soi une atteinte au caractère privé des communications du requérant, lequel, selon lui, n'avait établi aucun fait susceptible de justifier un constat de violation de son droit au respect du caractère privé de ses communications téléphoniques.

12. Le requérant interjeta appel. Il alléguait en particulier que le tribunal de district avait écarté des éléments de preuve de divers documents, dont deux décisions judiciaires autorisant rétroactivement l'interception de communications de téléphonie mobile ainsi qu'un addendum au contrat type de prestation de services émis par l'un des opérateurs de réseaux mobiles. La première décision de justice, rendue le 8 octobre 2002, avait autorisé l'interception des communications de téléphonie mobile de plusieurs personnes du 1er au 5 avril, du 19 au 23 juin, du 30 juin au 4 juillet, et du 16 au 20 octobre 2001. La seconde décision judiciaire, du 18 juillet 2003,

avait autorisé l'interception des communications de téléphonie mobile d'un certain M. E. du 11 avril au 11 octobre 2003. Quant à l'addendum, il informait l'abonné que si son numéro était utilisé pour lancer des menaces terroristes, l'opérateur de réseau mobile pouvait suspendre la prestation de services téléphoniques et transmettre les données recueillies aux organes d'application des lois. Selon le requérant, les décisions judiciaires et l'addendum en question prouvaient que les opérateurs de réseaux mobiles et les organes d'application des lois étaient techniquement capables d'intercepter toute communication téléphonique sans obtention préalable d'une autorisation judiciaire et qu'ils procédaient couramment à des interceptions non autorisées.

13. Le 26 avril 2006, le tribunal de Saint-Pétersbourg confirma en appel le jugement de première instance. Il réitéra le constat du tribunal de district selon lequel le requérant n'avait pas démontré que ses communications téléphoniques avaient été interceptées. Il ajouta que l'intéressé n'avait pas non plus établi le risque que son droit au respect du caractère privé de ses communications téléphoniques pût subir une atteinte illégale. Il indiqua qu'il aurait fallu, pour montrer l'existence d'un tel risque, que le requérant prouvât que les défendeurs avaient agi dans l'illégalité ; or, selon la juridiction d'appel, les opérateurs de réseaux mobiles étaient tenus en vertu de la loi d'installer un dispositif permettant aux organes d'application des lois de mettre en œuvre des mesures opérationnelles d'investigation, dispositif dont l'existence ne portait pas en soi atteinte au caractère privé des communications du requérant. Le tribunal de Saint-Pétersbourg estima légal le refus d'admettre comme éléments de preuve les décisions judiciaires du 8 octobre 2002 et du 18 juillet 2003, dès lors qu'elles avaient été prises à l'égard de tiers et ne concernaient pas le requérant. Par ailleurs, il admit comme élément de preuve et examina l'addendum au contrat du fournisseur de services, mais conclut que ce document ne contenait aucune information justifiant le réexamen du jugement rendu par le tribunal de district.

14. Il ressort d'un document soumis par le requérant qu'en janvier 2007 l'ONG Contrôle civil demanda au parquet général de procéder à l'examen des arrêtés pris par le ministère des Communications en matière d'interception de communications, en vue de vérifier leur compatibilité avec la législation fédérale. En février 2007, un membre du parquet général appela cette ONG pour lui demander des copies des annexes non publiées de l'arrêté n° 70, indiquant que le parquet n'avait pas pu en obtenir auprès du ministère des Communications. En avril 2007, le parquet général refusa de procéder à l'examen sollicité.

II. LE DROIT INTERNE PERTINENT

A. Le droit au respect de la vie privée et de la correspondance

15. La Constitution garantit à toute personne le droit au respect de sa vie privée, de ses secrets personnels et familiaux, ainsi que le droit de défendre son honneur et sa réputation (article 23 § 1). Elle garantit également le droit au respect de la correspondance et des communications téléphoniques, postales, télégraphiques et autres. Ce droit ne peut être restreint qu'en vertu d'une décision de justice (article 23 § 2).

16. Par ailleurs, la Constitution dispose qu'il est interdit de recueillir, conserver, utiliser ou diffuser des informations relatives à la vie privée d'une personne sans son consentement. Les services centraux et municipaux doivent veiller à ce que toute personne ait accès aux documents et pièces touchant à ses droits et libertés, sauf disposition contraire de la loi (article 24).

17. La loi sur les communications du 7 juillet 2003 (n° 126-FZ) garantit le caractère privé des communications postales, télégraphiques et autres passant par des réseaux de télécommunications ou des services de courrier. Les restrictions au caractère privé des communications ne sont permises que dans les cas prévus par la législation fédérale (article 63 § 1). L'interception de communications est subordonnée à une autorisation judiciaire préalable, sauf dans les cas indiqués par la législation fédérale (article 63 § 3).

18. Le 2 octobre 2003, dans sa décision n° 345-O, la Cour constitutionnelle a déclaré que le droit au respect du caractère privé des communications téléphoniques couvrait toutes les données transmises, conservées ou découvertes au moyen d'un dispositif téléphonique, y compris les métadonnées telles que les informations sur les connexions entrantes et sortantes d'un abonné spécifique. La haute juridiction a ajouté que la surveillance de telles données était elle aussi subordonnée à une autorisation judiciaire préalable.

B. La responsabilité pour atteinte à la vie privée

19. La collecte ou la diffusion non autorisées d'informations sur la vie privée ou familiale d'un individu sans son consentement, si elle est accomplie dans un intérêt mercantile ou un autre intérêt personnel et porte atteinte aux droits et aux intérêts légitimes du citoyen, est passible d'une amende, d'une peine de travail obligatoire ou d'une peine d'emprisonnement d'une durée maximale de quatre mois. Le même acte commis par un agent de l'État dans l'exercice de ses fonctions est passible d'une amende, de l'interdiction d'occuper certains postes ou d'une peine d'emprisonnement d'une durée maximale de six mois (article 137 du code pénal).

20. Toute atteinte au droit du citoyen au respect du caractère privé de ses communications postales, télégraphiques, téléphoniques ou autres est passible d'une amende ou d'une peine de travail obligatoire. Le même acte commis par un agent de l'État dans l'exercice de ses fonctions est passible d'une amende, de l'interdiction d'occuper certains postes ou d'une peine d'emprisonnement d'une durée maximale de quatre mois (article 138 du code pénal).

21. L'abus de pouvoir par un agent de l'État, s'il est commis dans un intérêt mercantile ou un autre intérêt personnel et porte gravement atteinte aux droits et aux intérêts légitimes d'une personne physique ou morale, est passible d'une amende, de l'interdiction d'occuper certains postes ou de prendre part à certaines activités pendant une période maximale de cinq ans, d'une peine de travail obligatoire d'une durée maximale de quatre ans ou d'une peine d'emprisonnement d'une durée comprise entre quatre mois et quatre ans (article 285 § 1 du code pénal).

22. Les actes par lesquels un agent de l'État, outrepassant manifestement le cadre de ses prérogatives, porte gravement atteinte aux droits et aux intérêts légitimes d'une personne physique ou morale, sont passibles d'une amende, de l'interdiction d'occuper certains postes ou de prendre part à certaines activités pendant une période maximale de cinq ans, d'une peine de travail obligatoire d'une durée maximale de quatre ans ou d'une peine d'emprisonnement d'une durée comprise entre quatre mois et quatre ans (article 286 § 1 du code pénal).

23. Dans son arrêt n° 19 du 16 octobre 2009, la formation plénière de la Cour suprême a dit qu'en vertu des articles 285 et 286 du code pénal « une atteinte grave aux droits et aux intérêts légitimes d'une personne physique ou morale » signifiait une violation des droits et libertés garantis par les principes généralement reconnus et les dispositions du droit international et de la Constitution russe – comme le droit d'une personne au respect de son honneur et de sa dignité, de sa vie privée ou familiale, de sa correspondance, de ses communications téléphoniques, postales, télégraphiques et autres, ou encore à l'inviolabilité de son domicile. Dans le cas d'une personne morale, pour déterminer si l'atteinte est « grave » il faut prendre en compte l'étendue du dommage subi en raison de l'acte illégal, la nature et le montant du préjudice matériel, le nombre de personnes touchées et la gravité du dommage corporel, matériel ou moral qui a été infligé à celles-ci (paragraphe 18.2 dudit arrêt).

24. Une procédure pénale est ouverte si des éléments factuels suffisants montrent qu'une infraction pénale a été commise (article 140 § 2 du code de procédure pénale).

C. Dispositions générales sur l'interception de communications

25. L'interception de communications est régie par la loi n° 144-FZ du 12 août 1995 sur les mesures opérationnelles d'investigation (« LMOI »), qui est applicable à l'interception de communications tant dans le cadre d'une procédure pénale qu'en dehors d'un tel cadre, et par le code de procédure pénale n° 174-FZ du 18 décembre 2001 (entré en vigueur le 1er juillet 2002 – « CPP »), qui s'applique uniquement à l'interception de communications dans le cadre d'une procédure pénale.

26. Les mesures opérationnelles d'investigation visent plusieurs buts : a) la détection, la prévention, la répression des infractions pénales et les investigations sur celles-ci, ainsi que l'identification des personnes qui se préparent à commettre une infraction pénale, qui en commettent ou qui en ont commis une ; b) la recherche des personnes qui tentent de se soustraire à la justice et des personnes portées disparues ; c) l'obtention d'informations sur des faits ou activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique de la Russie (article 2 de la LMOI). Le 25 décembre 2008, l'article 2 de la LMOI a été amendé par l'adjonction d'un nouvel objectif, à savoir l'obtention d'informations sur des biens faisant l'objet d'une mesure de confiscation**.**

27. Les agents et organes de l'État qui mettent en œuvre des mesures opérationnelles d'investigation doivent faire preuve de respect envers la vie privée et familiale, le domicile et la correspondance des citoyens. Il est interdit de recourir à de telles mesures pour atteindre des buts ou objectifs autres que ceux prévus par la loi (article 5 §§ 1 et 2 de la LMOI).

28. Il n'est pas permis aux agents et organes de l'État a) de procéder à des mesures opérationnelles d'investigation dans l'intérêt de partis politiques ou d'organisations à but non lucratif ou à caractère religieux ; b) de procéder en secret à des mesures opérationnelles d'investigation visant des services fédéraux, régionaux ou municipaux, des partis politiques ou des organisations à but non lucratif ou à caractère religieux dans le but d'influer sur leurs activités ou décisions ; c) de communiquer à quiconque les données recueillies au cours des mesures opérationnelles d'investigation si ces données concernent la vie privée ou familiale d'un citoyen ou nuisent à sa réputation ou à sa renommée, excepté dans les cas visés par la législation fédérale ; d) d'inciter ou d'induire quelqu'un à commettre une infraction pénale, ou de lui tendre un piège à cet effet ; e) de falsifier les résultats de mesures opérationnelles d'investigation (article 5 § 8 de la LMOI).

29. Les mesures opérationnelles d'investigation englobent notamment l'interception de communications postales, télégraphiques, téléphoniques ou autres et la collecte de données à partir de voies techniques de communication. La loi indique qu'il est possible, dans le cadre de telles mesures, de procéder à des enregistrements audio et vidéo, de photographier, de filmer et de recourir à d'autres moyens techniques, sous

réserve que cela ne soit pas préjudiciable à la vie ou à la santé des personnes concernées ou à l'environnement. Les mesures opérationnelles d'investigation entraînant l'interception de communications postales, télégraphiques, téléphoniques ou autres et la collecte de données à partir de voies techniques de communication par le biais d'un dispositif installé par les fournisseurs de services de communication sont mises en œuvre à l'aide de moyens techniques par le FSB et les services du ministère de l'Intérieur, conformément aux décisions et accords signés par les services concernés (article 6 de la LMOI).

30. Le décret présidentiel n° 891 du 1er septembre 1995 dispose que l'interception de communications postales, télégraphiques ou autres doit être réalisée par le FSB, dans l'intérêt et pour le compte de tous les organes d'application des lois (paragraphe 1). Dans les situations où le FSB ne dispose pas de l'équipement technique nécessaire, les interceptions peuvent être effectuées par les services du ministère de l'Intérieur, dans l'intérêt et pour le compte de tous les organes d'application des lois (paragraphe 2). Des dispositions similaires figurent aux paragraphes 2 et 3 de l'arrêté gouvernemental n° 538 du 27 août 2005.

D. Situations pouvant conduire à l'interception de communications

31. Des mesures opérationnelles d'investigation entraînant une atteinte au droit constitutionnel au respect du caractère privé des communications postales, télégraphiques et autres transmises au moyen d'un réseau de télécommunications ou de services de courrier, ou une atteinte à l'intimité du domicile, peuvent être mises en œuvre après réception d'informations : a) selon lesquelles une infraction pénale a été commise, est en train d'être commise ou est en préparation ; b) sur des personnes qui se préparent à commettre une infraction pénale, qui en commettent ou qui en ont commis une ; ou c) sur des faits ou activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique de la Russie (article 8 § 2 de la LMOI).

32. La LMOI dispose que l'interception de communications téléphoniques et autres ne peut être autorisée que dans les cas où une personne est soupçonnée ou inculpée d'une infraction pénale de gravité moyenne, d'une infraction grave ou d'une infraction pénale particulièrement grave, ou est susceptible de détenir des informations au sujet de pareille infraction (article 8 § 4 de la LMOI). Le CPP indique par ailleurs que l'interception des communications téléphoniques et autres d'un suspect, d'un prévenu ou d'une autre personne peut être autorisée s'il y a lieu de penser qu'elles peuvent contenir des informations pertinentes pour le dossier relatif à une infraction pénale de gravité moyenne, une infraction grave ou une infraction pénale particulièrement grave (article 186 § 1 du CPP).

33. L'article 15 du code pénal énonce que les « infractions de gravité moyenne » sont les infractions avec préméditation pour lesquelles le code pénal prévoit une peine maximale comprise entre trois et cinq ans d'emprisonnement, et les infractions sans préméditation pour lesquelles le code pénal prévoit une peine maximale supérieure à trois ans d'emprisonnement. Les « infractions graves » sont les infractions avec préméditation pour lesquelles le code pénal prévoit une peine maximale comprise entre cinq et dix ans d'emprisonnement. Les « infractions particulièrement graves » sont les infractions avec préméditation pour lesquelles le code prévoit une peine maximale supérieure à dix ans d'emprisonnement, voire une peine plus sévère.

E. Procédure d'autorisation et délais

1. La loi sur les mesures opérationnelles d'investigation

34. Les mesures opérationnelles d'investigation entraînant une atteinte au droit constitutionnel au respect du caractère privé des communications postales, télégraphiques et autres, transmises au moyen d'un réseau de télécommunications ou de services de courrier, ou une atteinte à l'intimité du domicile – comme l'inspection de locaux ou de bâtiments, l'interception de communications postales, télégraphiques, téléphoniques et autres, ou la collecte de données à partir de voies techniques de communication – exigent une autorisation judiciaire préalable (article 8 § 2 de la LMOI).

35. Dans les cas d'urgence où il existe un risque immédiat de commission d'une infraction grave ou particulièrement grave, ou en présence d'informations sur des faits ou activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique du pays, les mesures opérationnelles visées à l'article 8 § 2 peuvent être accomplies sans autorisation judiciaire préalable. En pareil cas, il convient, dans les vingt-quatre heures qui suivent le début des mesures opérationnelles d'investigation, d'en informer un juge. À défaut d'obtention d'une autorisation judiciaire dans un délai de quarante-huit heures à compter du début des mesures, celles-ci doivent cesser sur-le-champ (article 8 § 3 de la LMOI).

36. L'examen des demandes d'adoption de mesures entraînant une atteinte au droit constitutionnel au respect du caractère privé de la correspondance et des communications téléphoniques, postales, télégraphiques et autres transmises au moyen de réseaux de télécommunications ou de services de courrier, ou une atteinte à l'intimité du domicile, relève de la compétence d'un tribunal dans le ressort duquel se trouve le lieu où la mesure requise doit être mise en œuvre ou le lieu où est sis l'organe auteur de la demande. La demande doit être examinée sur-le-champ par un juge unique (article 9 § 1 de la LMOI).

37. Le juge statue en se fondant sur la demande motivée du chef de l'un des services compétents pour procéder à des mesures opérationnelles d'investigation. Les pièces justificatives pertinentes, excepté celles contenant des renseignements sur des agents infiltrés ou des informateurs de la police, ou sur l'organisation et la tactique afférentes aux mesures opérationnelles d'investigation, peuvent également être produites sur demande du juge (article 9 §§ 2 et 3 de la LMOI).

38. Le juge qui examine la demande décide s'il y a lieu d'autoriser des mesures impliquant une atteinte aux droits constitutionnels susmentionnés, ou au contraire de refuser l'autorisation ; il motive sa décision. Il doit préciser la période visée par l'autorisation, qui ne doit pas en principe excéder six mois. Si nécessaire, il peut prolonger la période en question après réexamen de l'ensemble des pièces pertinentes (article 9 §§ 4 et 5 de la LMOI).

39. La décision judiciaire autorisant les mesures opérationnelles d'investigation et les pièces sur lesquelles repose cette décision doivent rester en la possession exclusive de l'organe d'État qui accomplit les mesures opérationnelles d'investigation (article 12 § 3 de la LMOI).

40. Par sa décision n° 86-O du 14 juillet 1998, la Cour constitutionnelle a rejeté pour irrecevabilité une demande de contrôle de la constitutionnalité de certaines dispositions de la LMOI. Elle a notamment déclaré qu'un juge ne devait autoriser des mesures d'investigation entraînant une atteinte à des droits constitutionnels que s'il avait la conviction que pareilles mesures étaient légales, nécessaires et justifiées, c'est-à-dire compatibles avec l'ensemble des exigences de la LMOI. Elle a indiqué que la charge de la preuve incombait à l'organe d'État auteur de la demande, lequel devait établir la nécessité des mesures en question. Par ailleurs, elle a précisé que des pièces justificatives devaient être soumises au juge s'il en faisait la demande et que, dès lors que certaines d'entre elles étaient susceptibles de contenir des secrets d'État, seul un juge ayant le niveau requis d'habilitation de sécurité pouvait examiner les demandes d'autorisation. En outre, s'appuyant sur la nécessité de garder le secret sur les mesures de surveillance, la Cour constitutionnelle a estimé que les principes de publicité de l'audience et du contradictoire n'étaient pas applicables à la procédure d'autorisation. Partant, selon la haute juridiction, le fait que la personne concernée ne pût participer à la procédure d'autorisation, être informée de la décision prise ou interjeter appel auprès d'une juridiction supérieure n'emportait pas violation de ses droits constitutionnels.

41. Dans sa décision n° 345-O du 2 octobre 2003, la Cour constitutionnelle a déclaré que le juge était tenu d'examiner de manière attentive et approfondie les pièces qui lui étaient soumises à l'appui d'une demande d'interception, et qu'en cas de demande insuffisamment étayée il pouvait requérir des informations complémentaires.

42. En outre, par sa décision n° 1-O du 8 février 2007, la Cour constitutionnelle a rejeté pour irrecevabilité une demande de contrôle de la constitutionnalité de l'article 9 de la LMOI. La haute juridiction a estimé qu'avant d'autoriser la mise en œuvre de mesures opérationnelles d'investigation, le juge était tenu d'en vérifier le fondement. Elle a ajouté que la décision judiciaire autorisant de telles mesures devait être motivée et renvoyer à des raisons précises de penser qu'une infraction pénale avait été commise, était en train d'être commise ou était en préparation, ou que des activités mettant en péril la sécurité nationale, militaire, économique ou écologique du pays étaient menées, et que la personne visée par la demande de mesures opérationnelles d'investigation était impliquée dans ces activités criminelles ou, pour d'autres motifs, dangereuses.

43. Par sa décision n° 460-O-O du 15 juillet 2008, la Cour constitutionnelle a rejeté pour irrecevabilité une demande de contrôle de la constitutionnalité des articles 5, 11 et 12 de la LMOI. Elle a estimé qu'il était loisible à la personne dont les communications avaient été interceptées de déposer une requête en supervision contre la décision judiciaire ayant autorisé l'interception. Pour la Cour constitutionnelle, le fait que l'intéressé ne disposât pas d'une copie de cette décision ne l'empêchait pas de déposer sa requête en supervision dès lors que la juridiction saisie pouvait en demander une aux autorités compétentes.

2. Le code de procédure pénale

44. Les mesures d'enquête entraînant la perquisition du domicile d'une personne ou l'interception de ses appels téléphoniques et autres communications sont subordonnées à l'obtention d'une autorisation judiciaire préalable. Une demande aux fins de la perquisition du domicile d'une personne ou de l'interception de ses communications doit être soumise par un enquêteur avec l'approbation d'un procureur et être examinée par un juge unique dans un délai de vingt-quatre heures. Le procureur et l'enquêteur peuvent être présents. Le juge qui se penche sur la demande détermine s'il y a lieu d'autoriser la mesure requise ou au contraire de refuser l'autorisation ; il motive sa décision (article 165 du CPP).

45. Un tribunal peut accorder l'autorisation d'intercepter les communications d'un suspect, d'un prévenu ou d'une autre personne s'il y a lieu de penser que des informations pertinentes pour le dossier pénal en question pourraient être évoquées dans les échanges (article 186 § 1 du CPP).

46. Une demande d'autorisation d'interception de communications doit mentionner clairement a) le dossier pénal auquel se rattache la demande ; b) les raisons justifiant de procéder aux mesures requises ; c) le nom de famille, le patronyme et le prénom de la personne dont les communications doivent être interceptées ; d) la durée de la mesure requise ; et e) l'organe d'État qui effectuera l'interception (article 186 § 3 du CPP).

47. La décision judiciaire autorisant l'interception des communications doit être transmise par l'enquêteur à l'organe d'État chargé de sa mise en œuvre. L'interception de communications peut être autorisée pour une période n'excédant pas six mois, et l'enquêteur met un terme à cette mesure lorsqu'elle n'est plus nécessaire. En tout état de cause, elle doit cesser une fois l'enquête terminée (article 186 §§ 4 et 5 du CPP).

48. Un tribunal peut également autoriser la surveillance de données de communication relatives aux connexions téléphoniques ou sans fil d'une personne s'il existe des raisons suffisantes de penser que pareilles données peuvent être pertinentes pour un dossier pénal. Une demande d'autorisation doit contenir les éléments mentionnés au paragraphe 46 ci-dessus. Copie de la décision judiciaire ayant autorisé la surveillance des données relatives aux communications d'une personne est transmise par l'enquêteur au fournisseur de services de communication concerné ; celui-ci doit ensuite régulièrement, et au moins une fois par semaine, soumettre les données requises à l'enquêteur. La surveillance des données de communication peut être autorisée pour une durée n'excédant pas six mois, et l'enquêteur y met un terme lorsqu'elle n'est plus nécessaire. En tout état de cause, elle doit cesser une fois l'enquête terminée (article 186.1 du CPP, introduit le 1er juillet 2010).

F. La conservation, l'utilisation et la destruction des données recueillies

1. La conservation des données recueillies

49. L'article 10 de la LMOI dispose que les organes d'application des lois qui procèdent à des mesures opérationnelles d'investigation peuvent créer et utiliser des bases de données ou ouvrir des dossiers personnels. Un dossier personnel doit être clôturé lorsque les objectifs indiqués à l'article 2 de la loi ont été atteints ou s'il est établi qu'ils sont impossibles à atteindre.

50. Dans sa décision du 14 juillet 1998 (paragraphe 40 ci-dessus), la Cour constitutionnelle a relevé, concernant la possibilité – offerte par l'article 10 – pour les organes d'application des lois accomplissant des mesures opérationnelles d'investigation de créer des bases de données ou d'ouvrir des dossiers personnels, que seules les données touchant à la prévention des infractions pénales ou aux investigations sur celles-ci pouvaient être introduites dans ces bases de données ou ces dossiers personnels. Elle a ajouté que, dès lors que les activités criminelles ne relevaient pas de la sphère de la vie privée, la collecte d'informations sur de telles activités ne portait pas atteinte au droit au respect de la vie privée. Elle a enfin précisé que, si des informations sur les activités criminelles d'une personne introduites dans un dossier personnel n'étaient pas confirmées par la suite, ledit dossier devait être clôturé.

51. Les enregistrements des communications téléphoniques et autres interceptées doivent être scellés et conservés dans des conditions permettant d'écarter tout risque d'écoute ou de copie par des personnes non autorisées (article 8 § 4 de la LMOI).

52. Les informations relatives aux installations utilisées pour la mise en œuvre de mesures opérationnelles d'investigation, aux méthodes employées, aux agents qui interviennent et aux données recueillies constituent un secret d'État. Leur déclassification n'est possible qu'en vertu d'une décision spéciale du chef de l'organe d'État qui effectue les mesures opérationnelles d'investigation (article 12 § 1 de la LMOI et article 5 § 4 de la loi n° 5485-I du 21 juillet 1993 – « la loi sur les secrets d'État »).

53. Doivent être apposées en évidence sur les pièces renfermant des secrets d'État les informations suivantes : degré de confidentialité, organe d'État auteur de la décision de classification, numéro d'enregistrement et date ou conditions de déclassification (article 12 de la loi sur les secrets d'État).

2. L'utilisation des données recueillies et les conditions de leur divulgation

54. Les informations contenant des secrets d'État ne peuvent être communiquées à un autre service de l'État, à une organisation ou à une personne qu'avec l'autorisation du service d'État auteur de la décision de classifier ces informations. Elles ne peuvent être communiquées qu'à des services d'État ou organisations spécialement habilités à cet effet ou à des personnes ayant le niveau requis d'habilitation de sécurité. Le service de l'État ou l'organisation auquel des informations classifiées sont communiquées doit veiller à ce qu'elles soient dûment protégées. Le chef du service de l'État ou de l'organisation en question est personnellement responsable de la protection des informations classifiées contre l'accès ou la divulgation non autorisés (articles 16 et 17 de la loi sur les secrets d'État).

55. Seules une organisation ou une entreprise dont il est confirmé qu'elles disposent de services internes spécifiquement chargés de la protection des données, que leurs employés sont qualifiés pour manier des informations classifiées et qu'elles utilisent des systèmes agréés de protection des données peuvent être autorisées à prendre connaissance de secrets d'État (article 27 de la loi sur les secrets d'État).

56. L'habilitation de sécurité n'est octroyée qu'aux agents de l'État qui en ont véritablement besoin pour s'acquitter de leurs tâches. Elle est également accordée aux juges pour la durée de leurs fonctions et aux avocats intervenant dans une affaire pénale si le dossier contient des pièces portant sur des secrets d'État. Quiconque s'est vu délivrer une habilitation de sécurité doit s'engager par écrit à s'abstenir de communiquer les informations classifiées qui lui sont confiées (paragraphes 7, 11 et 21 du règlement n° 63 pris le 6 février 2010 par le gouvernement russe).

57. Le chef du service de l'État ou de l'organisation qui est en possession d'informations renfermant des secrets d'État se charge de donner accès à ces informations aux agents de l'État et autres personnes autorisées. Il doit veiller à ce que seules soient communiquées les informations nécessaires au destinataire pour l'accomplissement de ses tâches (article 25 de la loi sur les secrets d'État).

58. Si les données recueillies au cours de mesures opérationnelles d'investigation contiennent des informations sur la commission d'une infraction pénale, ces informations ainsi que l'ensemble des pièces justificatives nécessaires (photographies et enregistrements audio ou vidéo, par exemple) doivent être adressés aux services d'enquête compétents ou à un tribunal. Si les informations ont été recueillies grâce à des mesures opérationnelles d'investigation entraînant une atteinte au droit au respect du caractère privé de communications postales, télégraphiques et autres transmises au moyen d'un réseau de télécommunications ou de services de courrier, ou une atteinte à l'intimité du domicile, elles doivent être adressées aux services d'enquête ou de poursuite, de même que la décision judiciaire ayant autorisé les mesures en question. Les informations doivent être transmises selon la procédure spécialement prévue pour le traitement des informations classifiées, sauf si l'organe d'État qui a mis en œuvre les mesures opérationnelles d'investigation a décidé de les déclassifier (paragraphes 1, 12, 14 et 16 de l'arrêté n° 776/703/509/507/1820/42/535/398/68 du ministère de l'Intérieur du 27 septembre 2013).

59. Si la personne dont les communications téléphoniques ou autres ont été interceptées est inculpée d'une infraction pénale, les enregistrements doivent être remis à l'enquêteur et versés au dossier pénal. Leur utilisation et leur conservation ultérieures sont régies par les règles de procédure pénale (article 8 § 5 de la LMOI).

60. Les données recueillies au moyen de mesures opérationnelles d'investigation peuvent être utilisées pour la préparation et la conduite d'une enquête et d'une procédure judiciaire et en tant qu'éléments de preuve dans le cadre d'une procédure pénale, conformément aux dispositions juridiques régissant la recherche, l'appréciation et l'examen des preuves. La décision de transmettre les données recueillies à d'autres organes d'application des lois ou à un tribunal appartient au chef de l'organe d'État ayant procédé aux mesures opérationnelles d'investigation (article 11 de la LMOI).

61. Si l'interception a été autorisée dans le cadre d'une procédure pénale, l'enquêteur peut, à tout moment pendant la période visée par l'autorisation d'interception, obtenir les enregistrements auprès de l'organe qui effectue l'interception. Les enregistrements doivent être scellés et accompagnés d'une lettre indiquant les dates et heures de début et de fin des communications enregistrées, ainsi que les moyens techniques employés pour les intercepter. Les enregistrements doivent être écoutés par

l'enquêteur en présence de témoins instrumentaires, le cas échéant d'un expert et des personnes dont les communications ont été interceptées. L'enquêteur doit dresser un procès-verbal contenant la transcription intégrale des parties des communications enregistrées qui sont pertinentes pour l'affaire pénale dont il s'agit (article 186 §§ 6 et 7 du CPP). Le 4 mars 2013, l'article 186 § 7 a été modifié par suppression de la prescription relative à la présence de témoins instrumentaires.

62. Les enregistrements et les données relatives aux communications qui ont été recueillies sont joints au dossier pénal. Ils doivent être scellés et conservés dans des conditions permettant d'écarter tout risque d'écoute ou de copie par des personnes non autorisées (article 186 § 8 du CPP et article 186.1, introduit le 1er juillet 2010).

63. Les résultats de mesures opérationnelles d'investigation entraînant une restriction au droit au respect de la correspondance ou des communications téléphoniques, postales, télégraphiques ou autres ne peuvent servir d'éléments de preuve dans une procédure pénale que s'ils ont été obtenus en vertu d'une décision judiciaire et si les mesures en question ont été mises en œuvre dans le respect des règles de procédure pénale (paragraphe 14 de l'arrêt no 8 rendu le 31 octobre 1995 par la formation plénière de la Cour russe).

64. Il est interdit d'utiliser comme éléments de preuve des données qui, recueillies au moyen de mesures opérationnelles d'investigation, ne satisfont pas aux règles du CPP sur la recevabilité des preuves (article 89 du CPP). Les éléments de preuve obtenus en infraction avec le CPP ne sont pas recevables. Des éléments de preuve irrecevables sont dénués de valeur juridique et ne peuvent servir de fondement à des accusations pénales ou pour établir l'une quelconque des circonstances pour lesquelles des preuves doivent être fournies dans le cadre d'une procédure pénale. Des éléments de preuve qui ont été écartés par un tribunal sont dépourvus de valeur juridique et ne peuvent ni être invoqués dans un jugement ou une autre décision judiciaire, ni être examinés ou utilisés pendant le procès (articles 75 et 235 du CPP).

3. La destruction des données recueillies

65. Les données recueillies au moyen de mesures opérationnelles d'investigation au sujet d'une personne dont la culpabilité n'a pas été établie selon les voies légales doivent être conservées pendant un an puis être détruites, sauf si elles sont nécessaires dans l'intérêt du service ou de la justice. Les enregistrements audio et autres éléments recueillis à la faveur de l'interception de communications téléphoniques ou autres doivent être conservés pendant six mois puis être détruits si la personne concernée n'a pas été inculpée d'une infraction pénale. Le juge ayant autorisé l'interception doit être informé trois mois à l'avance de la destruction prévue (article 5 § 7 de la LMOI).

66. Si la personne concernée a été inculpée d'une infraction pénale, à l'issue de la procédure pénale, le juge du fond décide de la conservation ou de la destruction des données utilisées comme éléments de preuve. La destruction doit être consignée dans un rapport à faire signer par le chef du service d'enquête et à verser au dossier de l'affaire (article 81 § 3 du CPP et paragraphe 49 de l'arrêté n° 142 du 30 septembre 2011 de la Commission des enquêtes).

G. Le contrôle de l'interception de communications

67. Les chefs des organes qui mettent en œuvre des mesures opérationnelles d'investigation sont personnellement responsables de la légalité de l'ensemble de ces mesures (article 22 de la LMOI).

68. Le contrôle général des mesures opérationnelles d'investigation est exercé par le président, le Parlement et le gouvernement russes, dans les limites de leurs compétences respectives (article 20 de la LMOI).

69. Le procureur général et les procureurs de rang inférieur compétents peuvent également contrôler des mesures opérationnelles d'investigation. Sur demande du procureur compétent, le chef de l'organe d'État qui procède à des mesures opérationnelles d'investigation doit produire le matériel afférent à ces mesures, notamment les dossiers personnels, les informations sur le dispositif technique employé, les registres et les instructions internes. Le matériel contenant des renseignements sur des agents infiltrés ou des informateurs de la police ne peut être communiqué au procureur qu'avec l'accord de l'agent ou de l'informateur concerné, sauf en cas de procédure pénale contre cet agent ou informateur. La responsabilité du chef d'un organe d'État peut être engagée en vertu de la loi s'il n'obtempère pas à la demande du procureur. Celui-ci doit veiller à la protection des données contenues dans le matériel produit (article 21 de la LMOI).

70. La loi sur le parquet (loi fédérale n° 2202-I du 17 janvier 1992) dispose que le procureur général est nommé et, le cas échéant, démis de ses fonctions par le Conseil de la Fédération (chambre haute du Parlement) sur proposition du président (article 12). Les procureurs de rang inférieur sont nommés par le procureur général après consultation des autorités exécutives régionales (article 13). Pour pouvoir être nommé procureur, il faut avoir la nationalité russe et être titulaire d'un diplôme de droit russe (article 40.1).

71. En sus de leurs fonctions de poursuite, les procureurs sont chargés de veiller à ce que l'administration des centres de détention, les activités des huissiers, les mesures opérationnelles d'investigation et les enquêtes pénales respectent la Constitution et la législation russes (article 1). Par ailleurs, ils coordonnent les activités de l'ensemble des services d'application des lois dans la lutte contre la criminalité (article 8).

72. Concernant le contrôle des mesures opérationnelles d'investigation, les procureurs peuvent vérifier si les actes accomplis pendant la mise en

œuvre de telles mesures ont été respectueux de la légalité et des droits de l'homme (article 29). Les instructions données par des procureurs dans le cadre de ce contrôle doivent être appliquées dans le délai fixé. Le défaut d'obtempération peut entraîner la mise en jeu de la responsabilité conformément à la loi (article 6).

73. Les procureurs peuvent également examiner les plaintes pour infraction à la loi ; ils statuent sur toute plainte par une décision motivée. Pareille décision n'empêche pas l'intéressé de porter une plainte identique devant un tribunal. Lorsqu'un procureur découvre une infraction à la loi, il doit prendre des mesures afin que soit engagée une action contre les auteurs de l'infraction (article 10).

74. La loi sur le FSB du 3 avril 1995 (n° 40-FZ) dispose que les informations sur les agents infiltrés des services de sécurité, de même que sur la tactique, les méthodes et les moyens employés par eux, ne relèvent pas du contrôle exercé par les procureurs (article 24).

75. Les procédures relatives au contrôle par les procureurs des mesures opérationnelles d'investigation sont définies par l'instruction du parquet général n° 33 du 15 février 2011.

76. Cette instruction énonce qu'un procureur peut soumettre les organes qui mettent en œuvre des mesures opérationnelles d'investigation à des inspections systématiques, mais aussi à des inspections *ad hoc* en cas de dépôt de plainte par un particulier ou de réception d'informations concernant d'éventuelles violations. Les mesures opérationnelles d'investigation accomplies par le FSB dans le contexte du contre-renseignement ne peuvent faire l'objet d'une inspection que sur plainte individuelle (paragraphe 5 de l'instruction n° 33).

77. Au cours de l'inspection, le procureur doit s'assurer qu'il est satisfait aux exigences suivantes :

– respect des droits constitutionnels des citoyens, tels le droit au respect de la vie privée et familiale, du domicile, de la correspondance, des communications téléphoniques, postales, télégraphiques et autres ;

– caractère légal et justifié des actes accomplis dans le cadre de mesures opérationnelles d'investigation, y compris ceux qui ont été autorisés par un tribunal (paragraphes 4 et 6 de l'instruction n° 33).

78. Lors de l'inspection, le procureur doit examiner le matériel original afférent aux mesures opérationnelles d'investigation, notamment les dossiers personnels, les informations sur le dispositif technique employé, les registres et les instructions internes ; il peut demander des explications aux agents compétents. Il est tenu de protéger les données sensibles qui lui sont confiées contre tout accès ou toute divulgation non autorisés (paragraphes 9 et 12 de l'instruction n° 33).

79. Si un procureur décèle une infraction à la loi, il doit demander à l'agent qui en est responsable d'y remédier. Il doit également prendre des mesures destinées à faire cesser et redresser les violations des droits des

citoyens et afin que soit engagée une action contre les auteurs de l'infraction (paragraphes 9 et 10 de l'instruction n° 33). Un agent de l'État qui refuse de se conformer aux instructions d'un procureur peut voir une action engagée contre lui en application de la loi (paragraphe 11).

80. Un procureur chargé du contrôle de mesures opérationnelles d'investigation doit soumettre au parquet général des rapports semestriels qui détaillent les résultats des inspections menées (paragraphe 15 de l'instruction n° 33). Le modèle de rapport à remplir par le procureur se trouve joint à l'instruction n° 33. Portant mention de son caractère confidentiel, ce document comporte deux parties se présentant toutes deux sous forme de tableau. La première partie concerne les inspections effectuées pendant la période de référence et doit fournir des informations sur le nombre d'inspections réalisées, de dossiers contrôlés et d'infractions découvertes. La seconde partie, qui a trait aux plaintes déposées par des particuliers, doit contenir des informations sur le nombre de plaintes examinées et accueillies.

H. Accès d'un particulier aux données recueillies à son sujet au moyen de l'interception de communications

81. Le droit russe ne prévoit pas l'obligation de notifier à une personne, à quelque stade que ce soit, le fait que ses communications sont interceptées. Toutefois, une personne qui a connaissance de faits touchant aux mesures opérationnelles d'investigation auxquelles elle a été soumise, et dont la culpabilité n'a pas été établie selon les voies légales – c'est-à-dire qu'elle n'a pas été inculpée ou que les chefs d'inculpation ont été abandonnés au motif que l'infraction alléguée n'avait pas été commise ou qu'un ou plusieurs des éléments constitutifs d'une infraction pénale faisaient défaut –, a droit à des informations sur les données recueillies dans le cadre des mesures en question, dans la mesure compatible avec les règles de confidentialité opérationnelle (*конспирации*) et à l'exclusion de données qui pourraient permettre la divulgation de secrets d'État (article 5 §§ 4, 5 et 6 de la LMOI).

82. Dans sa décision du 14 juillet 1998 (paragraphe 40 ci-dessus), la Cour constitutionnelle a relevé que toute personne ayant connaissance de faits relatifs aux mesures opérationnelles d'investigation auxquelles elle avait été soumise était en droit de recevoir des informations sur les données recueillies dans le cadre de ces mesures, sauf si ces données renfermaient des secrets d'État. La haute juridiction a indiqué qu'en vertu de l'article 12 de la LMOI les données recueillies à l'occasion de telles mesures – par exemple des informations sur des infractions pénales et les personnes impliquées dans leur commission – constituaient un secret d'État. Elle a toutefois précisé que les informations se rapportant à des atteintes aux droits des citoyens ou à des actes illégaux commis par les autorités ne pouvaient

être classées comme relevant du secret d'État et devaient être dévoilées. Elle a ajouté qu'en conséquence il n'était pas possible d'invoquer l'article 12 pour refuser l'accès à des informations touchant aux droits d'une personne, sauf si ces informations concernaient les buts ou motifs des mesures opérationnelles d'investigation. En conclusion, pour la haute juridiction, le fait qu'en application de la loi contestée une personne ne pût prétendre à l'accès à l'intégralité des données recueillies à son sujet n'emportait pas violation des droits constitutionnels de cette personne.

I. Le contrôle juridictionnel

1. Dispositions générales de la LMOI sur le contrôle juridictionnel de l'interception de communications

83. Une personne estimant que ses droits ont été ou sont violés par un agent de l'État à l'occasion de la mise en œuvre de mesures opérationnelles d'investigation peut adresser une plainte au supérieur hiérarchique de cet agent, à un procureur ou à un tribunal. Si les droits d'une personne ont été violés par un agent de l'État dans l'accomplissement de mesures opérationnelles d'investigation, le supérieur hiérarchique de celui-ci, le procureur ou le tribunal doit prendre des mesures afin que la violation soit réparée et la personne concernée indemnisée (article 5 §§ 3 et 9 de la LMOI).

84. Si une personne s'est vu refuser l'accès à des informations sur les données recueillies à son sujet au moyen de mesures opérationnelles d'investigation, elle a le droit de connaître les raisons de ce refus et peut faire appel de cette décision auprès d'un tribunal. La charge de la preuve incombe aux services d'application des lois, lesquels doivent montrer que ce refus est justifié. Pour que le contrôle soit complet et approfondi, l'organe d'application des lois qui est responsable des mesures opérationnelles d'investigation doit, sur demande du juge, produire le matériel afférent aux mesures opérationnelles d'investigation contenant des informations sur les données auxquelles l'accès a été refusé, à l'exclusion des pièces comportant des renseignements sur des agents infiltrés ou des informateurs de la police. Si le tribunal estime injustifié le refus d'octroyer l'accès, il peut obliger l'organe d'application des lois à communiquer le matériel à l'intéressé (article 5 §§ 4, 5 et 6 de la LMOI).

85. Dans sa décision du 14 juillet 1998 (paragraphe 40 ci-dessus), la Cour constitutionnelle a dit qu'une personne ayant découvert qu'elle avait fait l'objet de mesures opérationnelles d'investigation et estimant que les actes commis par des agents de l'État avaient emporté violation de ses droits pouvait, en vertu de l'article 5 de la LMOI, contester devant un tribunal les raisons de procéder aux mesures en question ainsi que les actes spécifiques

accomplis par les services compétents dans le cadre de ces mesures, y compris ceux qui avaient été autorisés par un tribunal.

86. Concernant les questions procédurales, la Cour constitutionnelle a déclaré que dans une procédure où étaient contestés les motifs des mesures opérationnelles d'investigation ou les actes commis par les autorités compétentes lors de la mise en œuvre de ces mesures, ainsi que dans une procédure visant le refus de donner accès aux données recueillies, les services d'application des lois devaient soumettre au juge, sur demande de celui-ci, tout matériel pertinent afférent aux mesures opérationnelles d'investigation, excepté les pièces contenant des renseignements sur des agents infiltrés ou des informateurs de la police.

87. Une personne qui souhaite se plaindre de l'interception de ses communications peut demander un contrôle juridictionnel en vertu de l'article 125 du CPP, demander un contrôle juridictionnel sur le fondement du chapitre 25 du code de procédure civile et de la loi n° 4866-1 du 27 avril 1993 sur le contrôle juridictionnel des décisions et actes violant les droits et libertés des citoyens (« la loi sur le contrôle juridictionnel »), remplacés depuis le 15 septembre 2015 par le code de procédure administrative, ou engager une action en responsabilité au titre de l'article 1069 du code civil.

2. La demande de contrôle juridictionnel fondée sur l'article 125 du CPP

88. Dans son arrêt n° 1 du 10 février 2009, la formation plénière de la Cour suprême a déclaré que les actes d'agents ou organes de l'État procédant à des mesures opérationnelles d'investigation à la demande d'un enquêteur pouvaient être contestés suivant la procédure prévue à l'article 125 du CPP (paragraphe 4). Les plaintes fondées sur cette disposition ne peuvent être examinées que dans le contexte d'une enquête pénale en cours. Si l'affaire a déjà été transmise à une juridiction de jugement, le juge déclare la plainte irrecevable et explique à l'intéressé qu'il pourra soumettre ses griefs au juge du fond compétent (paragraphe 9).

89. L'article 125 du CPP prévoit le contrôle juridictionnel des décisions et actes ou omissions d'un enquêteur ou d'un procureur qui sont susceptibles de porter atteinte aux droits ou libertés constitutionnels des participants à une procédure pénale. Sauf décision contraire de l'enquêteur, du procureur ou du tribunal, le dépôt d'une plainte n'a pas d'effet suspensif sur la décision ou l'acte contestés. Le tribunal examine la plainte dans un délai de cinq jours. L'auteur de la plainte, son conseil, l'enquêteur et le procureur peuvent assister à l'audience. Le demandeur doit étayer sa plainte (article 125 §§ 1, 2, 3 et 4 du CPP).

90. Les comparants peuvent étudier l'ensemble du matériel présenté au tribunal et soumettre des pièces complémentaires liées à la plainte. La divulgation d'éléments du dossier pénal n'est permise que si elle n'est pas contraire aux intérêts de l'enquête et ne porte pas atteinte aux droits des

participants à la procédure pénale. Le juge peut inviter les parties à produire les pièces sur lesquelles repose la décision contestée, ou toute autre pièce pertinente (paragraphe 12 de l'arrêt n° 1).

91. Après examen de la plainte, le tribunal soit rejette la plainte, soit constate le caractère illégal ou injustifié de la décision, de l'acte ou de l'omission litigieux et demande à l'agent responsable de remédier à la défaillance constatée (article 125 § 5 du CPP). Lorsqu'il prie l'agent de remédier à la défaillance signalée, le tribunal ne peut ni lui prescrire l'adoption de telle ou telle mesure, ni annuler ou ordonner à l'agent d'annuler la décision qui est jugée illégale ou injustifiée (paragraphe 21 de l'arrêt n° 1).

3. La demande de contrôle juridictionnel fondée sur le chapitre 25 du code de procédure civile, la loi sur le contrôle juridictionnel et le code de procédure administrative

92. Selon l'arrêt n° 2 rendu le 10 février 2009 par la formation plénière de la Cour suprême, les plaintes contre des décisions ou actes d'agents ou organes accomplissant des mesures opérationnelles d'investigation qui ne peuvent pas être contestés dans le cadre d'une procédure pénale, de même que les plaintes contre un refus de donner accès à des informations sur les données recueillies au moyen de mesures opérationnelles d'investigation, peuvent être examinées suivant la procédure établie au chapitre 25 du code de procédure civile (« CPC ») (paragraphe 7).

93. Le chapitre 25 du CPC, en vigueur jusqu'au 15 septembre 2015, définissait la procédure permettant d'examiner les plaintes contre des décisions et actes de fonctionnaires violant les droits et libertés des citoyens, procédure qui fut détaillée dans la loi sur le contrôle juridictionnel. Le 15 septembre 2015, le chapitre 25 du CPC et la loi sur le contrôle juridictionnel ont été abrogés et remplacés par la loi n° 21-FZ du 8 mars 2015 (code de procédure administrative – « CPA »), qui est entrée en vigueur à cette date. Le CPA a en substance confirmé et précisé les dispositions du chapitre 25 du CPC et de la loi sur le contrôle juridictionnel.

94. Le CPC, la loi sur le contrôle juridictionnel et le CPA disposent qu'un citoyen peut déposer une plainte auprès d'un tribunal au sujet d'un acte ou d'une décision d'un service ou agent de l'administration centrale ou municipale s'il estime que cet acte ou cette décision a violé ses droits et libertés (article 254 du CPC et article 1 de la loi sur le contrôle juridictionnel). La plainte peut porter sur toute décision, tout acte ou toute omission qui a violé les droits ou les libertés du citoyen, a entravé l'exercice par lui de ses droits ou libertés, ou lui a imposé une obligation ou une responsabilité (article 255 du CPC, article 2 de la loi sur le contrôle juridictionnel et article 218 § 1 du CPA).

95. La plainte doit être déposée auprès d'un tribunal de droit commun dans un délai de trois mois à compter de la date à laquelle son auteur a eu

connaissance de l'atteinte portée à ses droits. Ce délai peut être prolongé en cas de motifs valables (article 254 du CPC, articles 4 et 5 de la loi sur le contrôle juridictionnel et articles 218 § 5 et 219 §§ 1 et 7 du CPA). La plainte doit indiquer le numéro d'enregistrement et la date de la décision contestée ou la date et le lieu de commission de l'acte contesté (article 220 § 2 (3) du CPA). L'auteur de la plainte doit fournir des pièces justificatives ou expliquer pourquoi il n'est pas en mesure de le faire (article 220 §§ 2 (8) et 3 du CPA). Si l'auteur de la plainte ne s'acquitte pas des obligations ci-dessus, le juge déclare la plainte irrecevable (article 222 § 3 du CPA).

96. C'est au service ou à l'agent concerné qu'il revient de prouver la légalité de la décision, de l'acte ou de l'omission en cause. L'auteur de la plainte doit pour sa part établir que cette décision, cet acte ou cette omission a porté atteinte à ses droits et libertés (article 6 de la loi sur le contrôle juridictionnel et article 226 § 11 du CPA).

97. En vertu du CPC la plainte devait être examinée dans un délai de dix jours (article 257 du CPC), alors que le CPA prévoit aujourd'hui un délai de deux mois (article 226 § 1 du CPA). Si le tribunal estime la plainte justifiée, il rend une décision par laquelle il annule la décision ou l'acte contestés et impose au service ou à l'agent en cause de remédier pleinement à l'atteinte portée aux droits de l'intéressé (article 258 § 1 du CPC, article 7 de la loi sur le contrôle juridictionnel et article 227 §§ 2 et 3 du CPA). Le tribunal peut fixer le délai dans lequel il convient de remédier à la violation et/ou définir les mesures particulières à prendre pour réparer pleinement la violation (paragraphe 28 de l'arrêt n° 2 et article 227 § 3 du CPA). L'auteur de la plainte peut alors, dans le cadre d'une action civile distincte, demander réparation du préjudice matériel ou moral subi (article 7 de la loi sur le contrôle juridictionnel).

98. Le tribunal peut rejeter la plainte s'il estime que l'acte ou la décision en cause est le fait d'un service ou agent compétent, est légal et ne porte pas atteinte aux droits de l'intéressé (article 258 § 4 du CPC et articles 226 § 9 et 227 § 2 du CPA).

99. Une partie à la procédure peut interjeter appel auprès d'une juridiction supérieure (article 336 du CPC tel qu'en vigueur jusqu'au 1er janvier 2012, article 320 du CPC tel qu'en vigueur depuis cette date et article 228 du CPA). La décision rendue en appel prend effet dès le jour de son prononcé (article 367 du CPC tel qu'en vigueur jusqu'au 1er janvier 2012, article 329 § 5 tel qu'en vigueur depuis cette date et articles 186 et 227 § 5 du CPA).

100. Le CPC exigeait qu'une décision judiciaire accueillant une plainte et imposant à un service ou agent de remédier à l'atteinte portée aux droits d'un citoyen fût adressée au chef du service concerné, à l'agent concerné ou à leurs supérieurs dans un délai de trois jours à compter de sa prise d'effet (article 258 § 2 du CPC). La loi sur le contrôle juridictionnel prescrivait l'envoi de la décision judiciaire dans un délai de dix jours à compter de sa

prise d'effet (article 8). Le CPA exige que la décision judiciaire soit envoyée le jour de sa prise d'effet (article 227 § 7). Le tribunal et l'auteur de la plainte doivent se voir notifier l'exécution de la décision dans le mois qui suit sa réception (article 258 § 3 du CPC, article 8 de la loi sur le contrôle juridictionnel et article 227 § 9 du CPA).

4. L'action en responsabilité fondée sur l'article 1069 du code civil

101. Un dommage causé à une personne ou à ses biens donne lieu à une indemnisation intégrale par l'auteur du préjudice. Celui-ci n'est pas tenu à réparation s'il prouve que ce n'est pas par sa faute que le dommage est survenu (article 1064 §§ 1 et 2 du code civil).

102. Les organes et agents centraux et municipaux voient leur responsabilité engagée pour tout dommage causé à un citoyen par l'effet de leurs actions ou omissions entachées d'illégalité (article 1069 du code civil). Qu'il y ait ou non faute d'un agent de l'État, le Trésor public fédéral ou régional est tenu de réparer tout dommage subi par un citoyen à raison i) d'une condamnation ou de poursuites pénales irrégulières, ii) de l'application irrégulière d'une mesure préventive, ou iii) d'une sanction administrative irrégulière (article 1070 du code civil).

103. Un tribunal peut imposer à l'auteur du dommage l'obligation de réparer le préjudice moral (souffrance physique ou morale). L'indemnisation du préjudice moral n'est pas liée à une éventuelle réparation du préjudice matériel (articles 151 § 1 et 1099 du code civil). Le montant de l'indemnité est déterminé en fonction de la gravité de la faute commise par l'auteur du préjudice ainsi que selon d'autres éléments importants. Le tribunal tient compte également de l'ampleur de la souffrance physique ou morale, eu égard aux caractéristiques propres à la victime (articles 151 § 2 et 1101 du code civil).

104. Indépendamment de l'existence d'une faute de la part de l'auteur du dommage, le préjudice moral doit être réparé s'il a été causé i) par un dispositif dangereux, ii) en raison d'une condamnation ou de poursuites irrégulières ou de l'application irrégulière d'une mesure préventive ou d'une sanction administrative irrégulière, ou iii) par la diffusion d'informations ayant entaché l'honneur, la dignité ou la réputation d'une personne (article 1100 du code civil).

105. Dans une procédure civile, la charge de la preuve incombe à celui qui affirme, sauf disposition contraire de la législation fédérale (article 56 § 1 du CPC).

5. Le recours auprès de la Cour constitutionnelle

106. Selon la loi sur la Cour constitutionnelle (loi n° 1-FKZ du 21 juillet 1994), lorsque la juridiction constitutionnelle rend dans un arrêt un avis sur le point de savoir si l'interprétation donnée à une disposition législative

dans la pratique des organes judiciaires et d'application des lois est compatible avec la Constitution, cet avis doit être suivi par les juridictions et services d'application des lois dès le jour du prononcé de cet arrêt (article 79 § 5).

J. Les obligations des fournisseurs de services de communication

1. L'obligation de protéger les données personnelles et le caractère privé des communications

107. En vertu de la loi sur les communications, les fournisseurs de services de communication doivent veiller au respect du caractère privé des communications. Les informations sur les communications transmises au moyen de réseaux de télécommunications ou de services de courrier et le contenu de ces communications ne peuvent être révélés qu'à l'expéditeur et au destinataire ou à leurs représentants autorisés, sauf dans les cas visés par la législation fédérale (article 63 §§ 2 et 4 de la loi sur les communications).

108. Les informations sur les abonnés et les services qui leur sont fournis sont confidentielles. Les informations sur un abonné englobent ses nom de famille, patronyme, prénom et surnom, s'il s'agit d'une personne physique ; le nom de la société ainsi que les noms de famille, patronymes et prénoms du directeur et des employés, s'il s'agit d'une personne morale ; l'adresse et le numéro de l'abonné et autres informations permettant d'identifier l'intéressé ou son terminal ; les données contenues dans des bases de données de paiement, notamment les informations sur les communications, le trafic et les paiements de l'abonné. Les informations sur un abonné ne peuvent pas être révélées à des tiers sans l'accord de l'abonné, sauf dans les cas visés par la législation fédérale (article 53 de la loi sur les communications).

2. L'obligation de collaborer avec les services d'application des lois

109. La loi sur les communications impose aux fournisseurs de services de communication l'obligation de donner aux organes d'application des lois, dans les cas visés par la législation fédérale, des informations sur les abonnés et les prestations dont ils bénéficient, ainsi que tout autre renseignement nécessaire aux organes en question pour atteindre leurs buts et objectifs (article 64 § 1 de la loi sur les communications).

110. Le 31 mars 2008, le conseil municipal de Moscou examina une proposition d'amendement de l'article 64 § 1 de la loi sur les communications visant à obliger les organes d'application des lois à présenter une autorisation judiciaire aux fournisseurs de services de communication auxquels ils demandent des informations sur des abonnés. Les représentants du FSB et du ministère de l'Intérieur indiquèrent aux personnes présentes qu'une décision judiciaire autorisant une interception

était un document classifié, donc non susceptible d'être montré aux fournisseurs de services de communication. La proposition d'amendement fut par la suite écartée.

111. Les fournisseurs de services de communication doivent veiller à ce que leurs réseaux et dispositifs soient conformes aux spécifications techniques établies par le ministère des Communications en collaboration avec les organes d'application des lois. Les fournisseurs de services de communication doivent également s'assurer que les méthodes et tactiques employées par lesdits organes demeurent confidentielles (article 64 § 2 de la loi sur les communications).

112. Dans les cas visés par la législation fédérale, un fournisseur de services de communication est tenu de suspendre ses prestations à un abonné dès réception d'un ordre écrit et motivé en ce sens émanant du chef d'un organe d'application des lois qui effectue des mesures opérationnelles d'investigation ou protège la sécurité nationale (article 64 § 3 de la loi sur les communications).

113. La loi sur le FSB oblige les fournisseurs de services de communication à installer un dispositif permettant au FSB de procéder à des mesures opérationnelles d'investigation (article 15).

3. Les spécifications techniques relatives au dispositif que les fournisseurs de services de communication doivent installer

114. Les principales caractéristiques du système d'installations techniques permettant la mise en œuvre de mesures opérationnelles d'investigation (*Система технических средств для обеспечения функций оперативно-разыскных мероприятий* – « SORM ») sont présentées dans un certain nombre d'arrêtés et de règlements pris par le ministère des Communications.

a) L'arrêté n° 70

115. L'arrêté n° 70 sur les spécifications techniques relatives au système d'installations techniques permettant la mise en œuvre de mesures opérationnelles d'investigation au moyen de réseaux de télécommunications, pris par le ministère des Communications le 20 avril 1999, indique que le dispositif installé par les fournisseurs de services de communication doit satisfaire à certaines spécifications présentées dans les addendums à l'arrêté. Cet arrêté, accompagné de ses addendums, a été publié dans le magazine officiel du ministère des Communications *SvyazInform*, diffusé par abonnement. Il peut aussi être consulté *via* une base de données Internet juridique privée, qui l'a repris à partir de *SvyazInform*.

116. Les addendums n^{os} 1 et 3 décrivent les spécifications techniques du SORM relatives aux réseaux de téléphonie mobile. Ils précisent que l'interception de communications est effectuée par un organe d'application

des lois à partir d'un terminal de contrôle à distance connecté au dispositif d'interception installé par l'opérateur de réseau mobile. Ce dispositif doit pouvoir notamment : a) créer des bases de données sur les sujets des interceptions, à gérer depuis le terminal de contrôle à distance ; b) intercepter des communications et transmettre les données ainsi recueillies au terminal de contrôle à distance ; c) protéger les données contre tout accès non autorisé, y compris par des employés de l'opérateur de réseau mobile ; d) assurer l'accès aux bases de données des adresses des abonnés (paragraphes 1.1 et 1.6 de l'addendum n° 1).

117. Plus spécifiquement, le dispositif doit permettre : a) l'interception de tous les appels entrants et sortants du sujet de l'interception ; b) l'accès aux informations sur sa localisation ; c) le maintien de la capacité d'interception lorsqu'une connexion en cours est transférée du réseau d'un opérateur de réseaux mobiles à celui d'un autre opérateur ; d) le maintien de la capacité d'interception en cas de recours à des prestations complémentaires telles que le renvoi d'appel, le transfert d'appel ou la conférence multiple, avec possibilité d'enregistrer le ou les numéros vers lesquels l'appel est acheminé ; e) la collecte de données de communication concernant tout type de connexion, que ce soit par télécopie, SMS ou autre ; f) l'accès aux informations sur les services fournis au sujet de l'interception (paragraphe 2.1.2 de l'addendum n° 1).

118. Il existe deux types d'interception : l'« interception totale » et la « surveillance statistique ». L'interception totale est l'interception en temps réel des données de communication et du contenu de toutes les communications entrantes ou sortantes du sujet de l'interception. La surveillance statistique est la surveillance en temps réel des seules données de communication, sans interception du contenu des communications. Les données de communication englobent le numéro de téléphone appelé, la date et l'heure correspondant au début et à la fin de la connexion, les prestations complémentaires utilisées, la localisation du sujet de l'interception et l'état de sa connexion (paragraphes 2.2 et 2.4 de l'addendum n° 1).

119. Le dispositif installé doit pouvoir lancer l'interception de communications dans les trente secondes qui suivent la réception d'un ordre émanant du terminal de contrôle à distance (paragraphe 2.5 de l'addendum n° 1).

120. Les informations sur les sujets des interceptions ou sur la transmission de toute donnée au terminal de contrôle à distance ne peuvent être ni consignées ni enregistrées (paragraphe 5.4 de l'addendum n° 1).

121. Le terminal de contrôle à distance reçoit de l'opérateur de réseau mobile un mot de passe lui donnant le plein accès au SORM. Le terminal change alors de mot de passe afin d'empêcher toute personne non autorisée d'avoir accès au SORM. À partir du terminal de contrôle à distance, il est possible d'activer le SORM afin notamment qu'il lance, suspende ou arrête

l'interception concernant un abonné, qu'il intercepte la communication en cours d'un abonné et qu'il soumette des informations spécifiques sur un abonné (paragraphe 3.1.2 de l'addendum n° 3).

122. Le centre de contrôle à distance reçoit les notifications automatiques suivantes concernant le sujet de l'interception : SMS envoyés ou reçus, avec leur contenu ; composition d'un numéro ; établissement d'une connexion ; interruption d'une connexion ; utilisation de prestations complémentaires ; changement dans l'état de la connexion ou de la localisation du sujet de l'interception (paragraphe 3.1.4 de l'addendum n° 3).

b) L'arrêté n° 130

123. L'arrêté n° 130 sur les procédures d'installation applicables au système technique permettant la mise en œuvre de mesures opérationnelles d'investigation, pris par le ministère des Communications le 25 juillet 2000, disposait que les fournisseurs de services de communication devaient installer un dispositif satisfaisant aux spécifications techniques énoncées par l'arrêté n° 70. La procédure et le programme d'installation devaient être approuvés par le FSB (paragraphe 1.4).

124. Les fournisseurs de services de communication devaient prendre des mesures aux fins de la protection des informations relatives aux méthodes et tactiques employées dans le cadre de mesures opérationnelles d'investigation (paragraphe 2.4).

125. Les fournisseurs de services de communication devaient veiller à ce que toute interception de communications ou tout accès à des données de communication fût accordé uniquement en vertu d'une décision judiciaire et suivant la procédure établie par la LMOI (paragraphe 2.5).

126. Il n'y avait pas lieu d'informer les fournisseurs de services de communication au sujet des interceptions concernant leurs abonnés. Il n'y avait pas lieu non plus de leur fournir les décisions judiciaires autorisant les interceptions (paragraphe 2.6).

127. Les interceptions étaient réalisées par le personnel et au moyen des installations techniques du FSB et des services du ministère de l'Intérieur (paragraphe 2.7).

128. Les paragraphes 1.4 et 2.6 de l'arrêté n° 130 furent contestés devant la Cour suprême par un certain M. N. Celui-ci plaidait le caractère illégal du renvoi à l'arrêté n° 70 contenu au paragraphe 1.4, alléguant que cet arrêté n'avait pas été publié et qu'il était dénué de validité. Quant au paragraphe 2.6, M. N. l'estimait incompatible avec la loi sur les communications, qui disposait que les fournisseurs de services de communication étaient tenus de veiller au respect du caractère privé des communications. Le 25 septembre 2000, la Cour suprême déclara que le renvoi à l'arrêté n° 70 contenu au paragraphe 1.4 était légal dès lors que cet arrêté revêtait un caractère technique et n'était donc pas censé figurer dans

une publication officielle accessible à tous, raison pour laquelle il n'avait été publié que dans une revue spécialisée. Concernant le paragraphe 2.6, la Cour suprême considéra qu'on pouvait l'interpréter comme faisant obligation aux fournisseurs de services de communication d'ouvrir aux organes d'application des lois, sans autorisation judiciaire, l'accès aux informations sur les abonnés. Jugeant qu'une telle exigence était incompatible avec la loi sur les communications, la haute juridiction parvint à la conclusion que le paragraphe 2.6 était entaché d'illégalité et inapplicable.

129. Le 25 octobre 2000, le ministère des Communications abrogea le paragraphe 2.6 de l'arrêté n° 130.

130. En réponse à une demande d'information de l'ONG Contrôle civil, le ministère des Communications déclara dans une lettre datée du 20 août 2006 que l'abrogation du paragraphe 2.6 de l'arrêté n° 130 ne signifiait pas que les fournisseurs de services de communication devaient être informés des mesures opérationnelles d'investigation visant un abonné ou recevoir copie de la décision pertinente accordant l'autorisation judiciaire en vue d'une telle surveillance.

131. L'arrêté n° 130 fut abrogé le 16 janvier 2008 (paragraphe 134 ci-dessous).

c) L'arrêté n° 538

132. Selon l'arrêté n° 538 sur la collaboration entre les fournisseurs de services de communication et les organes d'application des lois, pris par le gouvernement le 27 août 2005, les fournisseurs de services de communication doivent faire preuve de diligence dans la mise à jour des bases de données contenant les informations sur les abonnés et les prestations dont ils bénéficient. Ces renseignements doivent être conservés pendant trois ans. Les organes d'application des lois doivent avoir en permanence accès à distance à ces bases de données (paragraphe 12).

133. Les bases de données doivent comporter les informations suivantes au sujet des abonnés : a) prénom, patronyme et nom de famille, adresse du domicile et numéro de passeport, s'il s'agit d'une personne physique ; b) nom de la société, adresse et liste des personnes ayant accès à l'équipement terminal, ainsi que leurs prénom, patronyme, nom de famille, adresse du domicile et numéro de passeport, s'il s'agit d'une personne morale ; c) des informations relatives aux connexions, au trafic et aux paiements (paragraphe 14).

d) L'arrêté n° 6

134. L'arrêté n° 6 sur les spécifications relatives aux réseaux de télécommunications concernant la mise en œuvre de mesures opérationnelles d'investigation (première partie), pris par le ministère des Communications le 16 janvier 2008, a remplacé l'arrêté n° 130.

135. L'arrêté nº 6 a maintenu l'obligation pour les fournisseurs de services de communication d'assurer la transmission, vers le terminal de contrôle à distance de l'organe d'application des lois compétent, d'informations sur a) les numéros et codes d'identification des abonnés et b) le contenu de leurs communications. Ces informations doivent être transmises en temps réel sur demande provenant du terminal de contrôle à distance. Les fournisseurs de services de communication doivent également veiller à l'identification du lieu où se trouve un abonné (paragraphes 2, 3 et 5).

136. Le terminal de contrôle à distance doit avoir accès aux bases de données contenant les informations sur les abonnés, y compris leurs numéros et codes d'identification (paragraphes 7 et 8).

137. Les fournisseurs de services de communication doivent veiller à ce que le sujet de l'interception demeure dans l'ignorance de l'interception de ses communications. Les informations sur les interceptions passées ou en cours doivent être protégées contre tout accès non autorisé par les employés des fournisseurs de services de communication (paragraphe 9).

e) L'arrêté nº 73

138. L'arrêté nº 73 sur les spécifications relatives aux réseaux de télécommunications concernant la mise en œuvre de mesures opérationnelles d'investigation (deuxième partie), pris par le ministère des Communications le 27 mai 2010, donne des précisions sur certaines spécifications contenues dans l'arrêté nº 6. Il indique en particulier que le dispositif installé par les fournisseurs de services de communication doit permettre aux organes procédant à des mesures opérationnelles d'investigation d'avoir accès à l'ensemble des données transmises par le biais des réseaux de télécommunications et être capable de sélectionner les données et de transmettre les données sélectionnées à son terminal de contrôle (paragraphe 2).

III. INSTRUMENTS INTERNATIONAUX ET EUROPÉENS PERTINENTS

A. Nations unies

139. La Résolution nº 68/167 sur le droit à la vie privée à l'ère du numérique, adoptée par l'Assemblée générale le 18 décembre 2013, se lit comme suit :

« *L'Assemblée générale*,

(...)

4. *Invite* tous les États :

(...)

c) À revoir leurs procédures, leurs pratiques et leur législation relatives à la surveillance et à l'interception des communications, et à la collecte de données personnelles, notamment à grande échelle, afin de défendre le droit à la vie privée en veillant à respecter pleinement toutes leurs obligations au regard du droit international [des droits de l'homme] ;

d) À créer des mécanismes nationaux de contrôle indépendants efficaces qui puissent assurer la transparence de la surveillance et de l'interception des communications et de la collecte de données personnelles qu'ils effectuent, le cas échéant, et veiller à ce qu'ils en répondent, ou à les maintenir en place s'ils existent déjà ;

(...) »

B. Conseil de l'Europe

140. La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (STE n° 108) a établi des normes pour la protection des données dans le cadre du traitement automatisé de données à caractère personnel dans les secteurs public et privé. Elle énonce :

Article 8 – Garanties complémentaires pour la personne concernée

« Toute personne doit pouvoir :

a) connaître l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier ;

b) obtenir à des intervalles raisonnables et sans délais ou frais excessifs la confirmation de l'existence ou non dans le fichier automatisé, de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible ;

c) obtenir, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet aux principes de base énoncés dans les articles 5 et 6 de la présente Convention ;

d) disposer d'un recours s'il n'est pas donné suite à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'effacement, visée aux paragraphes b et c du présent article. »

Article 9 – Exceptions et restrictions

« 1. Aucune exception aux dispositions des articles 5, 6 et 8 de la présente Convention n'est admise, sauf dans les limites définies au présent article.

2. Il est possible de déroger aux dispositions des articles 5, 6 et 8 de la présente Convention lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique :

a) à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales ;

b) à la protection de la personne concernée et des droits et libertés d'autrui.

(...) »

Article 10 – Sanctions et recours

« Chaque Partie s'engage à établir des sanctions et recours appropriés visant les violations aux dispositions du droit interne donnant effet aux principes de base pour la protection des données énoncés dans le présent chapitre. »

141. La Convention n° 108 a été ratifiée par la Fédération de Russie le 15 mai 2013 et est entrée en vigueur à l'égard de cet État le 1er septembre 2013. L'instrument de ratification déposé le 15 mai 2013 par la Fédération de Russie contient les déclarations suivantes :

« La Fédération de Russie déclare que, conformément à l'article 3, paragraphe 2.a, de la Convention, elle n'appliquera pas la Convention aux données personnelles :

(...)

b) relevant du secret d'État en conformité avec la législation de la Fédération de Russie sur le secret d'État.

La Fédération de Russie déclare que, conformément à l'article 3, paragraphe 2.c, de la Convention, elle appliquera la Convention aux données personnelles qui ne sont pas traitées automatiquement, si l'application de la Convention correspond à la nature des actions effectuées avec les données à caractère personnel sans l'aide de moyens automatiques.

La Fédération de Russie déclare que, conformément à l'article 9, paragraphe 2.a, de la Convention, elle se réserve le droit de limiter l'accès d'une personne à ses propres données personnelles dans le but de protéger la sécurité de l'État et l'ordre public. »

142. Le Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données (STE n° 181), qui a été signé mais non ratifié par la Fédération de Russie, dispose :

Article 1 – Autorités de contrôle

« 1. Chaque Partie prévoit qu'une ou plusieurs autorités sont chargées de veiller au respect des mesures donnant effet, dans son droit interne, aux principes énoncés dans les chapitres II et III de la Convention et dans le présent Protocole.

2. a) À cet effet, ces autorités disposent notamment de pouvoirs d'investigation et d'intervention, ainsi que de celui d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente des violations aux dispositions du droit interne donnant effet aux principes visés au paragraphe 1 de l'article 1 du présent Protocole.

b) Chaque autorité de contrôle peut être saisie par toute personne d'une demande relative à la protection de ses droits et libertés fondamentales à l'égard des traitements de données à caractère personnel relevant de sa compétence.

3. Les autorités de contrôle exercent leurs fonctions en toute indépendance.

4. Les décisions des autorités de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel.

(...) »

143. La Recommandation nº R (87) 15 du Comité des Ministres aux États membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, adoptée le 17 septembre 1987, énonce ce qui suit :

« 1.1. Chaque État membre devrait disposer d'une autorité de contrôle indépendante et extérieure à la police, chargée de veiller au respect des principes énoncés dans la présente recommandation.

(...)

2.1. La collecte de données à caractère personnel à des fins de police devrait se limiter à ce qui est nécessaire à la prévention d'un danger concret ou à la répression d'une infraction pénale déterminée. Toute exception à cette disposition devrait faire l'objet d'une législation nationale spécifique.

2.2. Lorsque des données concernant une personne ont été collectées et enregistrées à son insu, elle devrait, si les données ne sont pas détruites, être informée, si cela est possible, que des informations sont détenues sur son compte, et ce, dès que l'objet des activités de police ne risque plus de subir un préjudice.

(...)

3.1. Dans la mesure du possible, l'enregistrement de données à caractère personnel à des fins de police ne devrait concerner que des données exactes et se limiter aux données nécessaires pour permettre aux organes de police d'accomplir leurs tâches légales dans le cadre du droit interne et des obligations découlant du droit international.

(...)

5.2.i. (...) La communication de données à des organes publics ne devrait être permise que, si dans un cas déterminé :

a) il y a obligation ou autorisation légales claires ou autorisation de l'autorité de contrôle, ou si

b) ces données sont indispensables au destinataire pour accomplir sa tâche légale propre et pour autant que le but de la collecte ou du traitement exécuté par ce destinataire n'est pas incompatible avec celui prévu à l'origine et que les obligations légales de l'organe communiquant ne s'y opposent pas.

5.2.ii. Une communication est, en outre, exceptionnellement permise si, dans un cas déterminé :

a) la communication est, sans aucun doute, dans l'intérêt de la personne concernée et si, soit celle-ci y a consenti, soit les circonstances permettent de présumer sans équivoque un tel consentement, ou si

b) la communication est nécessaire pour éviter un danger grave et imminent.

5.3.i. (...) La communication de données à des personnes privées ne devrait être permise que si, dans un cas déterminé, il y a obligation ou autorisation légales claires ou autorisation de l'autorité de contrôle.

(...)

6.4. L'exercice [par la personne concernée] des droits d'accès, de rectification ou d'effacement ne saurait faire l'objet d'une restriction que dans la mesure où une telle restriction serait indispensable pour l'accomplissement d'une tâche légale de la police ou nécessaire pour la protection de la personne concernée ou des droits et libertés d'autrui.

(...)

6.5. Un refus ou une restriction de ces droits devraient être motivés par écrit. La communication de la motivation ne pourrait être refusée que dans la mesure où cela serait indispensable pour l'accomplissement d'une tâche légale de la police ou nécessaire pour la protection des droits et libertés d'autrui.

6.6. Au cas où l'accès serait refusé, la personne concernée devrait disposer d'un recours auprès de l'autorité de contrôle ou d'un autre organe indépendant qui s'assurera que le refus est bien fondé.

(...)

7.1. Des mesures devraient être prises pour que les données à caractère personnel conservées à des fins de police soient effacées si elles ne sont plus nécessaires aux fins pour lesquelles elles avaient été enregistrées.

À cette fin, il convient notamment de prendre en considération les critères suivants : nécessité de garder des données à la lumière des conclusions d'une enquête pour un cas donné ; prononcé d'une décision définitive et notamment acquittement ; réhabilitation ; prescription ; amnistie ; âge de la personne concernée ; catégories particulières de données.

7.2. Des règles destinées à fixer des périodes de conservation pour les différentes catégories de données à caractère personnel ainsi que des contrôles périodiques sur leur qualité devraient être établis en accord avec l'autorité de contrôle ou conformément au droit interne.

8. L'organe responsable devrait prendre toutes les mesures nécessaires pour garantir aux données la sécurité physique et logique adéquate, et pour empêcher l'accès ou la communication non autorisés ou l'altération.

À cette fin, il faudrait tenir compte des différents contenus et caractéristiques des fichiers. »

144. La Recommandation n° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, adoptée le 7 février 1995, énonce ce qui suit en ses parties pertinentes :

« 2.4. Il ne peut y avoir ingérence des autorités publiques dans le contenu d'une communication, y compris l'utilisation de tables d'écoute ou d'autres moyens de surveillance ou d'interception des communications, que si cette ingérence est prévue par la loi et constitue une mesure nécessaire, dans une société démocratique :

a) à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales ;

b) à la protection de la personne concernée et des droits et libertés d'autrui.

2.5. En cas d'ingérence des autorités publiques dans le contenu d'une communication, le droit interne devrait réglementer :

a) l'exercice des droits d'accès et de rectification par la personne concernée ;

b) les conditions dans lesquelles les autorités publiques compétentes seront en droit de refuser de donner des renseignements à la personne concernée ou d'en différer la délivrance ;

c) la conservation ou la destruction de ces données.

Lorsqu'un exploitant de réseau ou un fournisseur de services est chargé par une autorité publique d'effectuer une ingérence, les données ainsi collectées ne devraient être communiquées qu'à l'organisme désigné dans l'autorisation pour cette ingérence. »

C. Union européenne

145. La Résolution du Conseil du 17 janvier 1995 relative à l'interception légale des télécommunications (96/C 329/01) dispose :

« La présente section expose les spécifications des services autorisés relatives à l'interception légale des télécommunications. Ces spécifications sont soumises à la loi nationale et doivent être interprétées conformément aux politiques nationales applicables.

(...)

1.3. Les télécommunications effectuées par le sujet de l'interception ou qui lui sont adressées doivent être accessibles aux services autorisés, à l'exclusion de toutes les télécommunications qui n'ont pas de rapport avec le service cible précisé dans l'autorisation d'interception.

(...)

2. Les services autorisés doivent avoir des possibilités de surveillance en temps réel et à temps plein pour les interceptions de transmissions de télécommunications. Des données suffisantes afférentes aux appels doivent également être fournies en temps réel. Si des données complémentaires afférentes à l'appel ne peuvent être fournies en temps réel, les services autorisés doivent disposer de ces données dans les meilleurs délais dès la fin de l'appel.

3. Les opérateurs de réseaux ou les fournisseurs de services doivent procurer aux services autorisés une ou plusieurs interfaces à partir desquelles les communications interceptées peuvent être transmises à leurs installations de surveillance. Ces interfaces doivent faire l'objet d'un accord entre les autorités qui interceptent les communications et les opérateurs de réseaux ou les fournisseurs de services. Les autres questions relatives à ces interfaces seront traitées selon les pratiques admises dans les différents pays.

(...)

5. L'interception doit être conçue et mise en œuvre de façon à empêcher toute utilisation non autorisée ou abusive et à sauvegarder les informations concernant l'interception.

(...)

5.2. Les opérateurs de réseaux ou les fournisseurs de services doivent veiller à ce que les communications interceptées soient exclusivement transmises au service de surveillance désigné dans l'autorisation d'interception.

(...) »

146. Les spécifications ci-dessus ont été confirmées et expliquées dans la Résolution nº 9194/01 du Conseil du 20 juin 2001 relative aux besoins opérationnels des services autorisés en matière de réseaux et services publics de télécommunication.

147. Dans son arrêt rendu le 8 avril 2014 dans les affaires jointes *Digital Rights Ireland et Seitlinger e.a.* (C-293/12 et C-594/12, EU:C:2014:238), la Cour de justice de l'Union européenne (CJUE) a déclaré invalide la Directive 2006/24/CE sur la conservation de données, qui imposait aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications l'obligation de conserver toutes les données relatives au trafic et à la localisation pendant une période comprise entre six mois et deux ans, pour que les données fussent disponibles à des fins de recherche, de détection et de poursuite d'infractions graves telles que définies par chaque État membre dans son droit interne. La CJUE a relevé que, même si la directive n'autorisait pas la conservation du contenu des communications, les données relatives au trafic et à la localisation visées par ce texte étaient susceptibles de permettre de tirer des conclusions très précises sur la vie privée des personnes dont les données avaient été conservées. En conséquence, selon la CJUE, l'obligation de conserver ces données constituait en soi une ingérence dans l'exercice du droit au respect de la vie privée et des communications garanti par l'article 7 de la Charte des droits fondamentaux de l'Union européenne, et du droit à la protection des données à caractère personnel tiré de l'article 8 de la Charte. En outre, pour la CJUE, l'accès des autorités nationales compétentes aux données constituait une ingérence supplémentaire dans l'exercice de ces droits fondamentaux. La CJUE a ajouté que l'ingérence était particulièrement grave et que la circonstance que des données étaient conservées et par la suite utilisées sans que l'abonné ou l'utilisateur inscrit en fussent informés était susceptible de faire naître dans l'esprit des personnes concernées le sentiment que leur vie privée faisait l'objet d'une surveillance constante. Elle a estimé que, si l'ingérence répondait à un objectif d'intérêt général, à savoir contribuer à la lutte contre les infractions graves et le terrorisme et ainsi, en fin de compte, à la sécurité publique, elle ne satisfaisait pas toutefois à l'exigence de proportionnalité. La CJUE a constaté en premier lieu que la directive couvrait de manière généralisée toute personne et tous moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception fussent opérées en fonction de l'objectif de lutte contre les infractions graves. Ainsi, selon la CJUE, le texte impliquait une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne et s'appliquait même à des personnes pour lesquelles il n'existait aucun indice de nature à laisser croire que leur comportement pût avoir un lien, même indirect ou lointain, avec des

infractions graves. La CJUE a dit qu'en deuxième lieu la directive ne contenait pas les conditions matérielles et procédurales relatives à l'accès des autorités nationales compétentes aux données et à leur utilisation ultérieure et qu'en se bornant à renvoyer de manière générale aux infractions graves telles que définies par chaque État membre dans son droit interne, le texte ne prévoyait aucun critère objectif permettant de déterminer quelles infractions pouvaient être considérées comme suffisamment graves pour justifier une ingérence d'une telle ampleur dans les droits fondamentaux consacrés par les articles 7 et 8 de la Charte. Surtout, pour la CJUE, l'accès par les autorités nationales compétentes aux données conservées n'était pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision aurait visé à limiter l'accès aux données et leur utilisation à ce qui était strictement nécessaire en vue d'atteindre l'objectif poursuivi. En troisième lieu, la CJUE a noté que la directive imposait la conservation de toutes les données pendant une période d'au moins six mois sans que fût opérée une quelconque distinction entre les catégories de données en fonction de leur utilité éventuelle en vue de l'objectif poursuivi ou selon les personnes concernées. La CJUE en a conclu que la directive entraînait une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux consacrés par les articles 7 et 8 de la Charte, sans qu'une telle ingérence fût précisément encadrée par des dispositions permettant de garantir qu'elle demeurât effectivement limitée au strict nécessaire. La CJUE a également fait observer que la directive ne prévoyait pas des garanties suffisantes – au moyen de mesures techniques et organisationnelles – permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès illicite à ces données et toute utilisation illicites de ces données.

EN DROIT

I. SUR LA VIOLATION ALLÉGUÉE DE L'ARTICLE 8 DE LA CONVENTION

148. Le requérant allègue que le système d'interception secrète des communications de téléphone mobile en Russie n'est pas conforme aux exigences de l'article 8 de la Convention, ainsi libellé :

> « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
>
> 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la

sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

A. Sur la recevabilité

149. Le Gouvernement soutient que le requérant ne peut se prétendre victime d'une violation du droit au respect de sa vie privée ou de sa correspondance (paragraphes 152-157 ci-dessous). Il estime par ailleurs que l'intéressé n'a pas épuisé les voies de recours internes (paragraphes 219-226 ci-dessous).

150. La Cour considère que les exceptions formulées par le Gouvernement sont si étroitement liées à la substance du grief du requérant qu'il y a lieu de les joindre au fond.

151. Constatant par ailleurs que ce grief n'est pas manifestement mal fondé au sens de l'article 35 § 3 a) de la Convention et qu'il ne se heurte à aucun autre motif d'irrecevabilité, la Cour le déclare recevable.

B. Sur le fond

1. Sur la qualité de victime du requérant et l'existence d'une « ingérence »

a) Thèses des parties

i. Le Gouvernement

152. Le Gouvernement estime que le requérant ne peut se prétendre victime d'une violation de l'article 8 de la Convention et qu'il n'y a pas eu ingérence dans l'exercice de ses droits. L'intéressé ne se serait pas plaint d'une interception de ses communications téléphoniques. Le grief soulevé par lui devant les juridictions internes et la Cour consisterait en substance à dire que les fournisseurs de services de communication ont installé un dispositif spécial permettant aux autorités de mettre en œuvre des mesures opérationnelles d'investigation. Or l'affaire *Orange Slovensko, a.s. c. Slovaquie* ((déc.), n° 43983/02, 24 octobre 2006) aurait confirmé que l'installation, voire le financement, d'un dispositif d'interception par des sociétés privées n'est pas en soi contraire à la Convention.

153. Le Gouvernement ajoute que l'article 34 ne peut pas être invoqué en vue de l'introduction d'une requête de type *actio popularis* ni servir de fondement à une plainte in abstracto selon laquelle une loi enfreint la Convention (*Aalmoes* et autres *c. Pays-Bas* (déc.), n° 16269/02, 25 novembre 2004). Il estime que la conception de la qualité de victime définie dans les arrêts *Klass et autres c. Allemagne* (6 septembre 1978, § 34, série A n° 28) et *Malone c. Royaume-Uni* (2 août 1984, § 64, série A n° 82)

– selon laquelle un individu peut, sous certaines conditions, se prétendre victime d'une violation entraînée par la simple existence de mesures secrètes ou d'une législation permettant de telles mesures, sans avoir besoin d'avancer qu'on les lui a réellement appliquées – ne doit pas recevoir une interprétation large au point d'englober toute personne qui dans l'État défendeur craint que les services de sécurité aient pu recueillir des informations à son sujet. Pour le Gouvernement, le requérant doit établir l'existence d'une « probabilité raisonnable » selon laquelle les services de sécurité ont recueilli et conservé des informations sur sa vie privée (*Esbester c. Royaume-Uni*, n° 18601/91, décision de la Commission du 2 avril 1993, non publiée, *Redgrave c. Royaume-Uni*, n° 20271/92, décision de la Commission du 1er septembre 1993, non publiée, *Matthews c. Royaume-Uni*, n° 28576/95, décision de la Commission du 16 octobre 1996, non publiée, *Halford c. Royaume-Uni*, 25 juin 1997, § 17, *Recueil des arrêts et décisions* 1997-III, *Weber et Saravia c. Allemagne* (déc.), n° 54934/00, §§ 4-6 et 78, CEDH 2006-XI, et *Kennedy c. Royaume-Uni*, n° 26839/05, §§ 122-123, 18 mai 2010).

154. Le Gouvernement considère que des dérogations au principe de la « probabilité raisonnable » ne sont acceptables qu'en vertu de raisons particulières. Selon lui, un individu ne peut se plaindre d'une ingérence due à la simple existence d'une législation autorisant des mesures de surveillance secrète que, dans des circonstances exceptionnelles, et il faut tenir compte de la disponibilité d'un éventuel recours au niveau interne et du risque que des mesures de surveillance secrète soient appliquées à l'intéressé (*Kennedy*, précité, § 124). Or, pour le Gouvernement, aucune raison particulière de cette nature ne peut être établie en l'espèce.

155. Premièrement, selon le Gouvernement, dès lors que le requérant n'a été soupçonné d'aucune infraction pénale, il n'existe aucune « probabilité raisonnable », ni même le moindre risque, qu'il ait fait l'objet de mesures de surveillance. Sa profession – rédacteur en chef d'une maison d'édition – ne serait pas de nature à justifier une mesure d'interception en vertu du droit russe. Le Gouvernement assure que les conversations téléphoniques du requérant n'ont jamais été interceptées et que l'intéressé n'a fourni aucune preuve du contraire. Les documents soumis par lui dans le cadre de la procédure interne concerneraient des tiers et ne contiendraient aucune preuve de sa mise sur écoute.

156. Deuxièmement, il existerait des voies de recours internes permettant de dénoncer aussi bien l'insuffisance alléguée des garanties contre les abus offertes par le droit russe que toute mesure de surveillance particulière appliquée à un individu. Il serait possible de demander à la Cour constitutionnelle de vérifier la constitutionnalité de la loi n° 144-FZ du 12 août 1995 sur les mesures opérationnelles d'investigation (« LMOI »), et également de saisir la Cour suprême, comme l'aurait fait avec succès un certain M. N., lequel aurait ainsi obtenu un constat d'illégalité relatif à une

disposition de l'arrêté n° 130 du ministère des Communications (paragraphe 128 ci-dessus). Concernant l'arrêté n° 70, contrairement aux dires du requérant, il aurait été dûment publié (paragraphe 181 ci-dessous) et serait dès lors susceptible d'être contesté devant les tribunaux. Une personne dont les communications ont été interceptées illégalement en l'absence d'autorisation judiciaire préalable pourrait également obtenir réparation devant une juridiction civile. Le Gouvernement évoque l'arrêt du 15 juillet 2009 dans lequel la Cour suprême aurait estimé que l'installation d'une caméra vidéo dans le bureau du demandeur et la mise sur écoute de son téléphone professionnel avaient été illégales, ces mesures de surveillance ayant été mises en œuvre sans autorisation préalable d'un juge (paragraphes 219-224 ci-dessous). Enfin, le Gouvernement indique qu'en droit russe les mesures d'interception sont contrôlées par un organe indépendant, le parquet.

157. Le Gouvernement en conclut que la présente espèce se distingue de l'affaire *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev c. Bulgarie* (n° 62540/00, 28 juin 2007), dans laquelle la Cour aurait refusé d'appliquer le critère de la « probabilité raisonnable » en raison de l'absence de garanties contre les interceptions illégales en Bulgarie. Pour le Gouvernement, dès lors que le droit russe offre des garanties adéquates et suffisantes – y compris des voies de recours – contre les abus en matière d'interception de communications, le requérant ne peut se plaindre d'une ingérence à cause de la simple existence d'une législation permettant la surveillance secrète. Faute de « probabilité raisonnable » que ses communications téléphoniques aient été interceptées, il ne pourrait se prétendre victime de la violation de l'article 8 de la Convention qu'il allègue.

ii. Le requérant

158. Le requérant estime pouvoir se prétendre victime d'une violation de l'article 8 causée par la simple existence d'une législation autorisant un système d'interceptions secrètes de communications, sans avoir à démontrer que pareilles mesures secrètes lui ont effectivement été appliquées. Pour lui, l'existence d'une telle législation implique une menace de surveillance pour tout usager des services de télécommunications et s'analyse donc en soi en une ingérence dans l'exercice de ses droits découlant de l'article 8. Le requérant étaye sa position en invoquant les arrêts *Klass et autres* (précité, §§ 34 et 37), *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev* (précité, § 58) et *Kennedy* (précité, § 123).

159. Il soutient que la Cour n'a employé le critère de la « probabilité raisonnable » que dans des affaires où le requérant se plaignait d'interceptions qui avaient réellement eu lieu, tandis que dans les affaires portant sur un grief général relatif à une législation et à une pratique autorisant des mesures de surveillance secrète, la Cour a selon lui appliqué

le critère de la « simple existence » établi dans l'arrêt *Klass et autres* (*Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, § 59, et *Kennedy*, précité, §§ 122-123, avec d'autres références). Il ajoute que, dans l'affaire *Liberty et autres c. Royaume-Uni* (n° 58243/00, §§ 56-57, 1er juillet 2008), la Cour a considéré que l'existence de pouvoirs permettant aux autorités d'intercepter des communications s'analysait en une ingérence dans les droits des requérantes au titre de l'article 8 dès lors que celles-ci étaient susceptibles de se voir appliquer les pouvoirs en question. Il indique aussi que, dans l'arrêt *Kennedy* (précité, § 124), la Cour a complété ce critère en y ajoutant une appréciation de la disponibilité de tout recours au niveau interne et du risque que des mesures de surveillance secrète fussent appliquées à l'intéressé. Enfin, dans l'affaire *Mersch et autres c. Luxembourg* (nos 10439/83 et 5 autres, décision de la Commission du 10 mai 1985, Décisions et rapports 43), la Commission aurait estimé que dans les situations où les autorités n'étaient pas tenues de notifier aux intéressés les mesures de surveillance dont ils avaient fait l'objet, ceux-ci pouvaient se prétendre « victimes » d'une violation de la Convention à raison de la simple existence d'une législation sur la surveillance secrète, et ce même s'ils ne pouvaient alléguer à l'appui de leurs requêtes avoir été réellement soumis à une mesure de surveillance.

160. Le requérant considère qu'il peut se prétendre victime d'une violation de l'article 8, en raison à la fois de la simple existence d'une législation sur la surveillance secrète et de sa situation personnelle. Il allègue que la LMOI, combinée avec la loi sur le FSB, la loi sur les communications et les arrêtés pris par le ministère des Communications – notamment l'arrêté n° 70 –, permet aux services de sécurité d'intercepter par des moyens techniques les communications de toute personne sans avoir à obtenir d'autorisation judiciaire préalable à cet effet. Plus particulièrement, les services de sécurité n'auraient aucune obligation de présenter une autorisation d'interception à quiconque, pas même au fournisseur de services de communication. Le requérant en conclut que la législation litigieuse permet l'interception généralisée des communications.

161. Le droit russe n'offrirait aucun recours qui permette de contester la législation en question. Ainsi, concernant la possibilité de mettre en cause l'arrêté n° 70, le requérant renvoie à l'arrêt de la Cour suprême du 25 septembre 2000 relatif à la plainte d'un certain M. N. (paragraphe 128 ci-dessus), dans lequel la haute juridiction aurait déclaré que l'arrêté litigieux présentait un caractère davantage technique que juridique et était donc insusceptible de figurer dans une publication officielle. Le requérant a par ailleurs produit copie d'une décision rendue le 24 mai 2010 par le Tribunal supérieur de commerce, dans laquelle celui-ci aurait constaté que les arrêtés du ministère des Communications imposant aux fournisseurs de services de communication l'obligation d'installer un dispositif permettant aux autorités de mettre en œuvre des mesures opérationnelles

d'investigation ne relevaient pas du contrôle des juridictions commerciales. Il ajoute que la procédure interne engagée par lui a montré que l'arrêté n° 70 ne pouvait pas être contesté de manière effective devant les juridictions russes. Quant à la LMOI, la Cour constitutionnelle se serait déjà penchée plusieurs fois sur sa constitutionnalité et aurait conclu que cette loi était compatible avec la Constitution. S'agissant pour finir de la possibilité d'attaquer des mesures de surveillance individuelle, le requérant soutient que la personne concernée n'est pas informée de la mesure d'interception, sauf si les informations interceptées sont produites comme preuves dans le cadre d'une procédure pénale dirigée contre elle. Faute de notification, les voies de recours internes seraient ineffectives (paragraphe 217 ci-dessous).

162. Concernant sa situation personnelle, le requérant indique qu'il est journaliste et qu'il préside la branche pétersbourgeoise de la Fondation pour la défense de la glasnost, qui surveille la situation en matière de liberté des médias et offre un soutien juridique aux journalistes dont les droits professionnels ont été bafoués (paragraphe 8 ci-dessus). Le risque d'interception de ses communications s'en trouverait donc accru. Il évoque à cet égard l'importance cruciale que revêt la protection des sources journalistiques, que la Grande Chambre aurait soulignée dans l'arrêt *Sanoma Uitgevers B.V. c. Pays-Bas* ([GC], n° 38224/03, § 50, 14 septembre 2010).

b) Appréciation de la Cour

163. La Cour observe que le requérant en l'espèce allègue une ingérence dans l'exercice de ses droits, laquelle ingérence découlerait non pas de mesures spécifiques d'interception qui lui auraient été appliquées mais de la simple existence d'une législation autorisant l'interception secrète de communications de téléphonie mobile ainsi que d'un risque de faire lui-même l'objet de mesures d'interception.

i. Résumé de la jurisprudence de la Cour

164. Selon la jurisprudence constante de la Cour, la Convention ne reconnaît pas l'*actio popularis* et la Cour n'a pas normalement pour tâche d'examiner dans l'abstrait la législation et la pratique pertinentes, mais de rechercher si la manière dont elles ont été appliquées au requérant ou l'ont touché a donné lieu à une violation de la Convention (voir, entre autres, *N.C. c. Italie* [GC], n° 24952/94, § 56, CEDH 2002-X, *Krone Verlag GmbH & Co. KG c. Autriche (n° 4)*, n° 72331/01, § 26, 9 novembre 2006, et *Centre de ressources juridiques au nom de Valentin Câmpeanu c. Roumanie* [GC], n° 47848/08, § 101, CEDH 2014). Il s'ensuit que pour pouvoir introduire une requête en vertu de l'article 34, une personne doit pouvoir démontrer qu'elle a « subi directement les effets » de la mesure litigieuse. Cette condition est nécessaire pour que soit enclenché le mécanisme de protection prévu par la Convention, même si ce critère ne doit pas s'appliquer de façon

rigide, mécanique et inflexible tout au long de la procédure (*Centre de ressources juridiques au nom de Valentin Câmpeanu*, précité, § 96).

165. Ainsi, compte tenu des particularités des mesures de surveillance secrète et de l'importance qu'il y a à veiller à ce qu'elles fassent l'objet d'un contrôle et d'un encadrement effectifs, la Cour admet les recours généraux dirigés contre la législation qui régit cette matière. Dans l'affaire *Klass et autres*, elle a dit qu'un individu pouvait, sous certaines conditions, se prétendre victime d'une violation entraînée par la simple existence de mesures secrètes ou d'une législation permettant de telles mesures, sans avoir besoin d'avancer qu'on les lui avait réellement appliquées. Elle a ajouté que les conditions requises devaient être définies dans chaque cause selon le ou les droits de la Convention dont on alléguait la violation, le caractère secret des mesures incriminées et la relation entre l'intéressé et ces mesures (*Klass et autres*, précité, § 34). La Cour a justifié son approche comme suit :

> « 36. La Cour relève que quand un État instaure une surveillance secrète dont les personnes contrôlées ignorent l'existence et qui demeure dès lors inattaquable, l'article 8 pourrait dans une large mesure être réduit à néant. Dans une telle situation, il se peut qu'un individu soit traité d'une façon contraire à l'article 8, voire privé du droit garanti par cet article, sans le savoir et partant sans être à même d'exercer un recours au niveau national ou devant les organes de la Convention.
>
> (...)
>
> La Cour ne saurait admettre que l'assurance de bénéficier d'un droit garanti par la Convention puisse être ainsi supprimée du simple fait de maintenir l'intéressé dans l'ignorance de sa violation. Un droit de recours à la Commission pour les personnes potentiellement touchées par une surveillance secrète découle de l'article 25 [article 34 actuel], faute de quoi l'article 8 risquerait de perdre toute portée.
>
> 37. Quant aux faits de l'espèce, la Cour note que la législation incriminée institue un système de surveillance exposant chacun, en République fédérale d'Allemagne, au contrôle de sa correspondance, de ses envois postaux et de ses télécommunications, sans qu'il le sache jamais à moins d'une indiscrétion ou d'une notification ultérieure dans les circonstances indiquées par l'arrêt de la Cour constitutionnelle fédérale (...) Ladite législation frappe par là directement tout usager ou usager virtuel des services des postes et télécommunications de la République fédérale d'Allemagne. En outre, les délégués l'ont relevé à juste titre, on peut dénoncer cette menace de surveillance comme restreignant par elle-même la liberté de communiquer au moyen de ces services et comme constituant donc, pour chaque usager ou usager virtuel, une atteinte directe au droit garanti par l'article 8.
>
> (...)
>
> 38. Eu égard aux particularités de la cause, la Cour décide que les requérants sont chacun en droit de « se prétend(re) victime(s) d'une violation » de la Convention bien qu'ils ne puissent alléguer à l'appui de leur requête avoir subi une mesure concrète de surveillance. Pour savoir s'ils ont réellement été victimes d'une telle violation, il faut rechercher si la législation contestée cadre en elle-même avec les clauses de la Convention.
>
> (...) »

166. À la suite de l'affaire *Klass et autres*, deux conceptions de la qualité de victime dans les affaires de surveillance secrète se sont développées en parallèle dans la jurisprudence des organes de la Convention.

167. Dans plusieurs affaires, la Commission et la Cour ont dit que les critères énoncés dans l'arrêt *Klass et autres* ne devaient pas recevoir une interprétation large au point d'englober toute personne craignant dans l'État défendeur que les services de sécurité eussent recueilli des informations à son sujet. Elles ont toutefois estimé que l'on ne pouvait raisonnablement attendre d'un requérant qu'il démontrât que des informations concernant sa vie privée avaient été recueillies et conservées. Elles ont ajouté qu'en matière de mesures secrètes il suffisait que l'existence de pratiques permettant une surveillance secrète fût établie et qu'il y eût une probabilité raisonnable que les services de sécurité eussent recueilli et conservé des informations sur la vie privée de l'intéressé (*Esbester*, décision précitée, *Redgrave*, décision précitée, *Christie c. Royaume-Uni*, n° 21482/93, décision de la Commission du 27 juin 1994, Décisions et rapports 78-B, *Matthews*, décision précitée, *Halford*, précité, §§ 47 et 55-57, et *Iliya Stefanov c. Bulgarie*, n° 65755/01, §§ 49-50, 22 mai 2008). Dans toutes ces affaires, les requérants alléguaient que leurs communications avaient réellement été interceptées. Dans certaines d'entre elles, ils se plaignaient aussi de façon générale d'une législation et d'une pratique autorisant des mesures de surveillance secrète (*Esbester*, *Redgrave*, *Matthews* et *Christie*, décisions précitées).

168. Dans d'autres affaires, la Cour a réitéré l'approche adoptée dans l'arrêt *Klass et autres* selon laquelle les lois et pratiques autorisant et instaurant un système de surveillance secrète des communications créaient par leur simple existence, pour tous ceux auxquels on pourrait appliquer la législation, une menace de surveillance entravant forcément la liberté de communication entre usagers des services de télécommunications et constituant en soi une ingérence dans l'exercice par les requérants de leurs droits découlant de l'article 8, quelles que soient les mesures prises dans les faits à leur égard (*Malone*, précité, § 64, *Weber et Saravia*, décision précitée, § 78, *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, §§ 58-59 et 69, *Liberty et autres*, précité, §§ 56-57, et *Iordachi et autres c. Moldova*, n° 25198/02, §§ 30-35, 10 février 2009). Dans toutes ces affaires, les requérants formulaient des plaintes générales au sujet de la législation et de la pratique autorisant les mesures de surveillance secrète. Dans certaines d'entre elles, ils alléguaient aussi une interception effective de leurs communications (*Malone*, précité, § 62, et *Liberty et autres*, précité, §§ 41-42).

169. Enfin, dans l'affaire *Kennedy*, la plus récente en la matière, la Cour a déclaré qu'il convenait de garder à l'esprit les considérations particulières justifiant qu'elle dérogeât, dans les affaires où étaient en cause des mesures

de surveillance secrète, à son approche générale déniant aux particuliers le droit de se plaindre *in abstracto* d'une loi. Elle a précisé que la principale d'entre elles tenait à ce qu'il importait de s'assurer que le caractère secret de pareilles mesures ne conduisît pas à ce qu'elles fussent en pratique inattaquables et qu'elles échappassent au contrôle des autorités judiciaires nationales et de la Cour. Elle a estimé que, pour se prononcer dans une affaire donnée sur la question de savoir si un particulier peut se plaindre d'une ingérence du seul fait qu'il existe une législation autorisant des mesures de surveillance secrète, elle devait avoir égard à la disponibilité de recours au niveau interne et au risque que des mesures de surveillance secrète fussent appliquées à l'intéressé. Elle a ajouté que lorsqu'il n'existait aucune possibilité de contester l'application de mesures de surveillance secrète au niveau interne, les soupçons et les craintes de la population quant à l'usage abusif qui pourrait être fait des pouvoirs de surveillance secrète n'étaient pas injustifiés. Elle a conclu qu'en pareil cas, un contrôle accru par la Cour s'avérait nécessaire même si, en pratique, le risque de surveillance n'était guère élevé (*Kennedy*, précité, § 124).

ii. Harmonisation des approches

170. Vu ce contexte, la Cour estime qu'il convient de préciser les conditions dans lesquelles un requérant peut se prétendre victime d'une violation de l'article 8 sans avoir à démontrer que des mesures de surveillance secrète lui ont bien été appliquées, de manière à permettre l'adoption d'une approche uniforme et prévisible.

171. Pour la Cour, l'approche *Kennedy* est la mieux adaptée à la nécessité de veiller à ce que le caractère secret des mesures de surveillance ne conduise pas à ce qu'elles soient en pratique inattaquables et qu'elles échappent au contrôle des autorités judiciaires nationales et de la Cour. Dès lors, la Cour admet qu'un requérant peut se prétendre victime d'une violation entraînée par la simple existence de mesures de surveillance secrète ou d'une législation permettant de telles mesures si les conditions suivantes sont remplies. Premièrement, la Cour prendra en considération la portée de la législation autorisant les mesures de surveillance secrète et recherchera pour cela si le requérant peut éventuellement être touché par la législation litigieuse, soit parce qu'il appartient à un groupe de personnes visées par elle, soit parce qu'elle concerne directement l'ensemble des usagers des services de communication en instaurant un système dans lequel tout un chacun peut voir intercepter ses communications. Deuxièmement, la Cour tiendra compte de la disponibilité de recours au niveau national et ajustera le niveau de son contrôle en fonction de l'effectivité de ces recours. Comme elle l'a souligné dans l'arrêt *Kennedy*, lorsque l'ordre interne n'offre pas de recours effectif à la personne qui pense avoir fait l'objet d'une surveillance secrète, les soupçons et les craintes de la population quant à l'usage abusif qui pourrait être fait des pouvoirs de surveillance

secrète ne sont pas injustifiés (*Kennedy*, précité, § 124). Dans ces circonstances, on est fondé à alléguer que la menace de surveillance restreint par elle-même la liberté de communiquer au moyen des services des postes et télécommunications et constitue donc, pour chaque usager ou usager potentiel, une atteinte directe au droit garanti par l'article 8. Un contrôle accru par la Cour s'avère donc nécessaire, et il se justifie de déroger à la règle selon laquelle les particuliers n'ont pas le droit de se plaindre d'une loi *in abstracto*. En pareil cas, la personne concernée n'a pas besoin d'établir l'existence d'un risque que des mesures de surveillance secrète lui aient été appliquées. Si en revanche l'ordre interne comporte des recours effectifs, des soupçons généralisés d'abus sont plus difficiles à justifier. Dans ce cas de figure, l'intéressé peut se prétendre victime d'une violation entraînée par la simple existence de mesures secrètes ou d'une législation permettant de telles mesures uniquement s'il est à même de montrer qu'en raison de sa situation personnelle il est potentiellement exposé au risque de subir pareilles mesures.

172. L'approche définie dans l'arrêt *Kennedy* offre donc à la Cour la souplesse nécessaire pour traiter tous les types de situations qui peuvent se présenter en matière de surveillance secrète eu égard aux spécificités des ordres juridiques des États membres, c'est-à-dire les recours existants, ainsi qu'à la situation personnelle de chaque requérant.

iii. Application à la présente affaire

173. Nul ne conteste que les communications de téléphonie mobile relèvent des notions de « vie privée » et de « correspondance » au sens de l'article 8 § 1 (voir, par exemple, *Liberty et autres*, précité, § 56).

174. La Cour observe que le requérant allègue en l'espèce une ingérence dans l'exercice de ses droits, qui découlerait non pas de mesures spécifiques de surveillance qui lui auraient été appliquées mais de la simple existence d'une législation autorisant les mesures de surveillance secrète ainsi que d'un risque de faire lui-même l'objet de telles mesures.

175. La Cour note que la législation incriminée a instauré un système de surveillance secrète dans le cadre duquel tout usager de services de téléphonie mobile proposés par des fournisseurs russes peut voir intercepter ses communications de téléphonie mobile, sans jamais être informé de cette surveillance. À ce titre, la législation en question frappe directement tout usager de ces services de téléphonie mobile.

176. En outre, pour les motifs exposés ci-dessous (paragraphes 286-300), le droit russe n'offre pas de recours effectifs à une personne qui pense avoir fait l'objet d'une surveillance secrète.

177. Partant, le requérant n'a pas à établir qu'il est exposé au risque de faire l'objet d'une surveillance secrète en raison de sa situation personnelle.

178. Eu égard au caractère secret des mesures de surveillance prévues par la législation litigieuse, à leur large application, puisqu'elles touchent

tous les usagers des services de communications de téléphonie mobile, et à l'absence de moyens effectifs qui permettraient de contester au niveau interne l'application alléguée de telles mesures, la Cour estime justifié l'examen *in abstracto* de cette législation.

179. Dès lors, elle considère que le requérant est en droit de se prétendre victime d'une violation de la Convention bien qu'il ne puisse alléguer à l'appui de sa requête avoir fait l'objet d'une mesure concrète de surveillance. Pour les mêmes raisons, la simple existence de la législation incriminée constitue en soi une ingérence dans l'exercice par l'intéressé des droits découlant de l'article 8. En conséquence, la Cour rejette l'exception du Gouvernement tirée du défaut de qualité de victime du requérant.

2. Sur la justification de l'ingérence

a) Thèses des parties

i. Accessibilité du droit interne

180. Le requérant soutient que les addendums à l'arrêté n° 70 exposant les spécifications techniques relatives au dispositif devant être installé par les fournisseurs de services de communication n'ont jamais été officiellement publiés et qu'ils ne sont pas accessibles aux citoyens. À son avis, dans la mesure où ils déterminent les pouvoirs des services d'application des lois en matière de surveillance secrète, ces addendums ont une incidence sur les droits des citoyens et auraient donc dû être publiés. Selon lui, ce n'est pas parce qu'il a finalement pu les consulter lors de la procédure interne que cela a remédié à l'absence de publication officielle (le requérant se réfère à *Kasymakhunov et Saybatalov c. Russie*, nos 26261/05 et 26377/06, § 92, 14 mars 2013). À ses yeux, les citoyens ne doivent pas être contraints d'entamer une procédure judiciaire pour avoir accès à la réglementation qui leur est applicable. La Cour aurait déjà conclu qu'il était essentiel de fixer des règles claires, détaillées et accessibles sur l'application de mesures de surveillance secrète (*Shimovolos c. Russie*, n° 30194/09, § 68, 21 juin 2011).

181. Selon le Gouvernement, l'arrêté n° 70 revêt un caractère technique et ne se prête donc pas à une publication officielle. Il aurait été publié dans un magazine spécialisé, *SvyazInform* (numéro 6 de 1999) et figurerait également dans la base de données juridique sur Internet *ConsultantPlus*, où il serait consultable gratuitement. Le Gouvernement remarque que le requérant a soumis à la Cour une copie de l'arrêté accompagné de ses addendums, ce qui montrerait qu'il a pu y accéder. Le droit interne serait dès lors accessible.

ii. Champ d'application des mesures de surveillance secrète

182. Le requérant soutient que la Cour a déjà constaté que la LMOI ne respectait pas l'exigence de « prévisibilité » au motif que le pouvoir discrétionnaire légal dont jouissaient les autorités pour prescrire une « opération test » impliquant l'enregistrement de communications privées au moyen d'un appareil de radiotransmission n'était subordonné à aucune condition et que l'étendue ainsi que les modalités d'exercice de ce pouvoir n'étaient pas définies (*Bykov c. Russie* [GC], n° 4378/02, § 80, 10 mars 2009). Or, pour le requérant, la présente espèce est similaire à l'affaire *Bykov*. En particulier, le droit russe n'indiquerait pas clairement les catégories de personnes susceptibles d'être soumises à des mesures d'interception. Ainsi, les mesures de surveillance ne se limiteraient pas aux personnes soupçonnées ou accusées d'infractions pénales : toute personne détentrice d'informations sur une infraction pénale pourrait être mise sur écoute. En outre, les mesures d'interception ne se borneraient pas aux infractions graves ou particulièrement graves. Le droit russe autoriserait aussi de telles mesures dans le contexte d'infractions de gravité moyenne, comme le vol à la tire.

183. Le Gouvernement arguë que les interceptions de communications ne peuvent être effectuées qu'après réception d'informations selon lesquelles une infraction pénale a été commise, est en train d'être commise ou est en cours de préparation, d'informations sur des personnes qui se préparent à commettre une infraction pénale, qui en commettent ou en ont commis une, ou d'informations sur des faits ou activités mettant en péril la sécurité nationale, militaire, économique ou écologique de la Russie. Dans sa décision du 14 juillet 1998, la Cour constitutionnelle aurait déclaré que recueillir des informations sur la vie privée d'une personne était autorisé uniquement en vue de la prévention ou de la détection des infractions pénales, ou des enquêtes sur celles-ci, ou pour atteindre d'autres buts légitimes énumérés dans la LMOI.

184. Le Gouvernement ajoute que seules les infractions de gravité moyenne, les infractions graves et les infractions particulièrement graves peuvent donner lieu à une décision d'interception, et que seules les personnes soupçonnées de telles infractions ou susceptibles de détenir des informations sur de telles infractions peuvent faire l'objet de mesures d'interception. À cet égard, la Cour aurait déjà conclu que des mesures de surveillance à l'égard d'une personne non soupçonnée d'une infraction peuvent être justifiées au regard de la Convention (*Greuter c. Pays-Bas* (déc.), n° 40045/98, 19 mars 2002).

185. Concernant en outre les interceptions visant à la protection de la sécurité nationale, le Gouvernement avance que l'exigence de « prévisibilité » de la loi ne va pas jusqu'à imposer aux États l'obligation d'édicter des dispositions juridiques énumérant dans le détail tous les comportements pouvant conduire à la décision de soumettre un individu à

une surveillance pour des motifs de « sécurité nationale » (le Gouvernement se réfère à *Kennedy*, précité, § 159).

iii. Durée des mesures de surveillance secrète

186. Le requérant plaide que la LMOI ne précise pas les circonstances dans lesquelles une interception peut être prorogée au-delà de six mois, et que la loi n'établit pas non plus la durée maximale d'une mesure d'interception.

187. Le Gouvernement déclare qu'en droit russe une interception peut être autorisée par un juge pour une période maximale de six mois et être prorogée si nécessaire. Il ajoute que la mesure doit être levée si l'enquête est achevée. Il estime raisonnable de laisser la durée des interceptions à la discrétion des autorités internes, eu égard à la complexité et à la durée de l'enquête dans une affaire donnée (*Kennedy*, précité). Le Gouvernement mentionne également l'affaire *Van Pelt c. Pays-Bas* (nº 20555/92, décision de la Commission du 6 avril 1994, non publiée), dans laquelle la Commission aurait conclu que les écoutes téléphoniques dont le requérant avait fait l'objet pendant près de deux ans n'avaient pas emporté violation de la Convention.

iv. Procédures à suivre pour la conservation, la consultation, l'examen, l'utilisation, la transmission et la destruction des données interceptées

188. Le requérant indique que la LMOI ne fixe ni les procédures à suivre pour l'examen, la conservation, la consultation ou l'utilisation des données interceptées, ni les précautions à prendre quant à leur transmission à d'autres parties. La loi disposerait qu'elles doivent être détruites dans les six mois, sauf si elles sont nécessaires aux intérêts du service ou de la justice. Or il n'y aurait aucune définition de la notion d'« intérêts du service ou de la justice ». Le droit russe laisserait par ailleurs une liberté complète au juge du fond pour décider après la fin du procès s'il y a lieu de conserver ou de détruire les données utilisées comme éléments de preuve.

189. Le Gouvernement soutient que la LMOI exige que les enregistrements des communications interceptées soient conservés dans des conditions écartant tout risque qu'ils soient écoutés ou copiés par des personnes non autorisées. Il ajoute que la décision judiciaire autorisant l'interception de communications, les pièces sur lesquelles repose cette décision et les données collectées au moyen de l'interception constituent un secret d'État et qu'elles doivent rester en la possession exclusive de l'organe d'État effectuant les interceptions. En cas de nécessité de les transmettre à un enquêteur, un procureur ou une juridiction, ces éléments seraient susceptibles d'être déclassifiés par les chefs des organes réalisant les mesures opérationnelles d'investigation. Les autorisations d'interception seraient déclassifiées par les tribunaux qui les ont délivrées. La procédure à suivre pour transmettre les données collectées lors de mesures

opérationnelles d'investigation aux organes d'enquête compétents ou à une juridiction serait définie par l'arrêté du ministère de l'Intérieur du 27 septembre 2013 (paragraphe 58 ci-dessus).

190. Selon le Gouvernement, les données recueillies lors de mesures opérationnelles d'investigation doivent être conservées pendant un an puis détruites, sauf si elles sont nécessaires aux intérêts du service ou de la justice, et les enregistrements doivent être conservés pendant six mois puis détruits. Dès lors, le droit russe serait prévisible et offrirait des garanties suffisantes.

v. Autorisation des mesures de surveillance secrète

α) Le requérant

191. Le requérant soutient que, même si le droit interne exige pour toute interception une autorisation judiciaire préalable, la procédure d'autorisation n'offre pas de garanties suffisantes contre les abus. Premièrement, dans les cas urgents il serait possible d'intercepter des communications sans autorisation judiciaire pendant une durée maximale de quarante-huit heures. Deuxièmement, contrairement au CPP, la LMOI ne poserait aucune condition relative au contenu de l'autorisation d'interception. En particulier, la loi ne prescrirait pas que le sujet de l'interception soit clairement désigné dans l'autorisation par son nom, son numéro de téléphone ou son adresse (voir, *a contrario*, les législations britannique et bulgare citées dans *Kennedy*, précité, §§ 41 et 160 ; voir aussi *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, § 13). Le droit interne n'exigerait pas non plus que l'autorisation précise quelles communications ou quels types de communications doivent être enregistrés, de sorte à restreindre le pouvoir discrétionnaire dont jouissent les services d'application des lois pour déterminer la portée des mesures de surveillance. Le droit russe n'établirait pas davantage de règles particulières pour la surveillance dans les situations sensibles, par exemple lorsqu'est en jeu la confidentialité des sources journalistiques ou lorsque la surveillance porte sur des communications entre un avocat et son client couvertes par le secret professionnel.

192. En outre, le requérant indique que le droit interne n'impose nullement au juge l'obligation de vérifier l'existence d'un « soupçon raisonnable » à l'égard de la personne concernée ou d'appliquer les critères de « nécessité » et de « proportionnalité ». Les services demandeurs ne seraient pas tenus de joindre des pièces justificatives aux demandes d'interception. De plus, la LMOI interdirait expressément de présenter au juge certaines pièces – celles contenant des renseignements sur des agents infiltrés ou des informateurs de la police, ou sur l'organisation et la tactique afférentes aux mesures opérationnelles d'investigation –, ce qui empêcherait le juge de vérifier réellement l'existence d'un « soupçon raisonnable ». Le

droit russe n'exigerait pas que le juge limite l'autorisation aux seuls cas où les buts légitimes poursuivis ne peuvent être atteints par d'autres moyens moins intrusifs.

193. À l'appui de son allégation selon laquelle les juges ne vérifient pas si un « soupçon raisonnable » pèse sur la personne concernée et n'appliquent pas les critères de « nécessité » et de « proportionnalité », le requérant a soumis copie des notes analytiques produites par trois tribunaux de district situés dans différentes régions russes (région de Tambov, région de Toula et république du Daguestan). Selon le requérant, ces tribunaux y résument pour la période 2010-2013 leur propre jurisprudence relative aux mesures opérationnelles d'investigation impliquant des atteintes au caractère privé des communications ou à l'intimité du domicile. L'un d'eux déclarerait refuser l'autorisation de procéder à une mesure opérationnelle d'investigation si celle-ci ne relève pas de la liste de mesures figurant dans la LMOI, si la demande d'autorisation n'est pas signée par un agent compétent ou n'est pas motivée, ou si l'affaire relève d'une restriction légale empêchant le recours à une telle mesure (du fait par exemple de la situation de la personne concernée ou de la nature de l'infraction). Ce même tribunal dirait accorder l'autorisation lorsque toutes les conditions précitées sont réunies. Un autre tribunal indiquerait que l'autorisation peut aussi être refusée si la demande est insuffisamment motivée, c'est-à-dire si elle ne contient pas assez d'informations pour permettre au juge de s'assurer que la mesure est légale et justifiée. Le troisième tribunal déclarerait qu'il accorde l'autorisation lorsqu'un service d'application des lois le demande. Il dirait n'avoir jamais rejeté pareille demande. Les trois tribunaux estimeraient que la demande est suffisamment motivée dès lors qu'elle renvoie à l'existence d'informations visées à l'article 8 § 2 de la LMOI (paragraphe 31 ci-dessus). L'un d'eux relèverait que les demandes d'autorisation ne sont jamais accompagnées de pièces justificatives ; un autre observerait que certaines demandes en comportent, mais pas toutes ; le troisième déclarerait que toutes les demandes sont accompagnées de telles pièces. Les trois tribunaux déclareraient ne jamais demander aux services d'application des lois de fournir des pièces justificatives complémentaires, confirmant par exemple les motifs de l'interception ou prouvant que les numéros de téléphone à mettre sur écoute appartiennent à la personne concernée. Deux tribunaux diraient délivrer des autorisations d'interception visant des personnes non identifiées ; l'un d'eux préciserait que ces autorisations portent uniquement sur la collecte de données à partir de voies techniques de communication. Pareilles autorisations ne mentionneraient pas une personne précise ou un numéro de téléphone à mettre sur écoute, mais permettraient l'interception de toutes les communications téléphoniques dans la zone où une infraction pénale a été commise. L'un des tribunaux dirait ne jamais accorder ce genre d'autorisation. Deux tribunaux déclareraient que les autorisations indiquent toujours la durée pendant

laquelle l'interception est permise ; le troisième dirait que la durée de l'opération n'est jamais précisée dans les autorisations qu'il délivre. Enfin, aucun des trois tribunaux n'aurait examiné de griefs formulés par des personnes dont les communications avaient été interceptées.

194. Le requérant produit également des statistiques officielles établies par la Cour suprême pour la période 2009-2013. Il en ressort qu'en 2009 les tribunaux russes ont accueilli 130 083 demandes d'interception formées en vertu du CPP sur un total de 132 821 et 245 645 demandes présentées au titre de la LMOI sur 246 228 (soit 99 %). En 2010, ils ont fait droit à 136 953 demandes d'interception soumises en vertu du CPP sur 140 372 et à 276 682 demandes introduites au titre de la LMOI sur 284 137. En 2011, ils ont accueilli 140 047 demandes d'interception fondées sur le CPP sur 144 762 et 326 105 demandes basées sur la LMOI sur 329 415. En 2012, ils ont fait droit à 156 751 demandes d'interception formées en vertu du CPP sur 163 469 (soit 95 %) et à 372 744 demandes présentées au titre de la LMOI sur 376 368 (soit 99 %). En 2013, ils ont accueilli 178 149 demandes d'interception soumises en vertu du CPP sur 189 741 (soit 93 %) et 416 045 demandes introduites au titre de la LMOI sur 420 242 (soit 99 %). Le requérant souligne que le nombre d'autorisations d'interception a quasiment doublé de 2009 à 2013. Il soutient en outre que le pourcentage fort élevé d'autorisations délivrées montre que les juges ne vérifient pas si un « soupçon raisonnable » pèse sur le sujet de l'interception et n'exercent pas non plus un contrôle attentif et rigoureux. En conséquence, selon le requérant, des mesures d'interception sont ordonnées à l'égard de très nombreuses personnes dans des situations où les informations auraient pu être recueillies par des moyens moins intrusifs.

195. Le requérant en conclut que la procédure d'autorisation est viciée et donc impropre à limiter l'utilisation des mesures de surveillance secrète à ce qui est nécessaire dans une société démocratique.

196. Concernant les garanties contre les interceptions non autorisées, le requérant arguë que le droit interne n'oblige pas les services d'application des lois à présenter une autorisation judiciaire au fournisseur de services de communication pour obtenir l'accès aux communications d'une personne. Toutes les autorisations judiciaires seraient des documents classifiés, détenus exclusivement par les services d'application des lois. L'obligation de transmettre une autorisation d'interception au fournisseur de services de communication ne serait mentionnée qu'une seule fois dans le droit russe, au sujet de la surveillance des données relatives aux communications exercée en vertu du CPP (paragraphe 48 ci-dessus). Le dispositif installé par les fournisseurs de services de communication en application des arrêtés du ministère des Communications, en particulier les addendums non publiés à l'arrêté n° 70, offrirait aux services d'application des lois un accès direct et illimité à l'ensemble des communications de téléphonie mobile de tous les usagers. L'arrêté n° 538 imposerait également aux fournisseurs de services

de communication l'obligation de créer des bases de données permettant de conserver pendant trois ans des informations sur tous les abonnés et sur les services fournis à ceux-ci. Les services secrets jouiraient d'un accès à distance direct à ces bases de données. Ainsi, le mode de fonctionnement du système de surveillance secrète donnerait aux services de sécurité et à la police les moyens techniques de contourner la procédure d'autorisation et d'intercepter toute communication sans autorisation judiciaire préalable. La nécessité d'obtenir pareille autorisation n'interviendrait donc que dans les affaires où les données interceptées doivent être utilisées comme éléments de preuve dans le cadre d'une procédure pénale.

197. Le requérant produit des documents montrant selon lui que les autorités d'application des lois interceptent de manière illicite des communications téléphoniques sans autorisation judiciaire préalable et en divulguent les enregistrements à des personnes non habilitées. Il fournit par exemple la version imprimée de pages Internet contenant des transcriptions de conversations téléphoniques privées de personnalités politiques. Il soumet également des articles de presse faisant état de poursuites pénales contre plusieurs hauts responsables des services techniques de la police. Ces policiers auraient été soupçonnés d'avoir intercepté illégalement les communications privées de personnes du monde politique et du monde des affaires en échange de pots-de-vin versés par des adversaires politiques ou commerciaux des individus concernés. Les articles en question évoquent des dépositions de témoins qui attesteraient que l'interception de communications en contrepartie de pots-de-vin est une pratique répandue et que n'importe qui peut acheter à la police la transcription de conversations téléphoniques d'une autre personne.

β) Le Gouvernement

198. Le Gouvernement déclare que toute interception de communications, téléphoniques ou autres, doit être autorisée par un tribunal. Selon lui, le tribunal se prononce à partir d'une demande motivée formée par un service d'application des lois. La charge de la preuve incomberait au service demandeur, qui serait tenu de justifier la nécessité des mesures d'interception. Pour apporter cette preuve, le service demandeur joindrait à sa demande toutes pièces justificatives pertinentes, excepté celles contenant des renseignements sur des agents infiltrés ou des informateurs de la police, ou sur l'organisation et la tactique afférentes aux mesures opérationnelles d'investigation. Cette dérogation se justifierait par la nécessité d'assurer la sécurité et la protection des agents infiltrés et des informateurs de la police ainsi que de leurs proches, et serait donc compatible avec la Convention.

199. Le Gouvernement évoque par ailleurs l'arrêt de la formation plénière de la Cour suprême du 27 juin 2013, dans lequel celle-ci a selon lui expliqué aux juridictions inférieures que toute restriction aux droits et libertés fondamentaux devait être prévue par la loi et être nécessaire dans

une société démocratique, c'est-à-dire proportionnée à un but légitime. La haute juridiction aurait invité les tribunaux à s'appuyer sur des faits établis, à s'assurer de l'existence de motifs pertinents et suffisants pour justifier une restriction aux droits d'un individu et à mettre en balance les intérêts de l'individu dont les droits sont restreints et les intérêts d'autres personnes, de l'État et de la société. La LMOI obligerait expressément les tribunaux à motiver la décision d'autoriser la mesure d'interception. Suivant la décision de la Cour constitutionnelle du 8 février 2007 (paragraphe 42 ci-dessus), il serait nécessaire que l'autorisation d'interception indique les raisons précises pour lesquelles la personne visée par la demande de mesures opérationnelles d'investigation est soupçonnée d'une infraction pénale ou d'activités mettant en péril la sécurité nationale, militaire, économique ou écologique du pays. Dans sa décision du 2 octobre 2003 (paragraphe 41 ci-dessus), la Cour constitutionnelle aurait également déclaré que le juge était tenu d'examiner de manière attentive et approfondie les pièces qui lui sont soumises.

200. En pratique, toute autorisation d'interception indiquerait l'organe d'État chargé de la réalisation de l'interception, les motifs sous-tendant l'application de mesures de surveillance et les raisons justifiant leur nécessité ; de plus, elle mentionnerait les dispositions juridiques applicables, le nom de la personne dont les communications doivent être interceptées, les raisons de soupçonner celle-ci d'être impliquée dans la commission de telle ou telle infraction pénale, son numéro de téléphone ou code IMEI, la période pour laquelle l'autorisation est accordée et toute autre information nécessaire. Dans des circonstances exceptionnelles, il serait possible d'autoriser l'interception des communications de personnes non identifiées. Dans ce cas, en principe, le juge autoriserait la collecte de données à partir de voies techniques de communication en vue de l'identification des personnes qui étaient présentes en un lieu donné au moment où une infraction pénale y a été commise. Cette pratique serait compatible avec les principes qui se dégagent de la jurisprudence de la Cour, dès lors qu'en pareille situation le mandat d'interception indiquerait l'unique ensemble de locaux (lieux) visé par l'interception autorisée par le mandat (*Kennedy*, précité).

201. Dans les cas d'urgence, le droit russe autoriserait l'interception de communications sans autorisation judiciaire préalable. Le juge devrait être informé de l'existence d'une telle situation dans un délai de vingt-quatre heures et une autorisation judiciaire prorogeant la mesure d'interception devrait être obtenue dans les quarante-huit heures. Le juge serait tenu d'examiner la légalité d'une telle mesure même si elle a déjà été levée. Le Gouvernement renvoie à un arrêt rendu en appel par la Cour suprême le 13 décembre 2013 dans une affaire pénale, dans lequel la haute juridiction aurait déclaré irrecevables comme éléments de preuve des enregistrements de conversations téléphoniques réalisés sans autorisation judiciaire préalable

dans le cadre d'une procédure d'urgence. La Cour suprême aurait conclu que même si un juge avait été informé de l'interception, aucune décision judiciaire sur la légalité ou la nécessité de celle-ci n'avait jamais été rendue.

vi. Contrôle de l'application de mesures de surveillance secrète

α) Le requérant

202. Le requérant allègue d'emblée qu'en Russie l'effectivité de tout contrôle exercé sur les interceptions est compromise par l'absence d'obligation pour les services d'interception de garder une trace des interceptions effectuées par eux. De plus, l'arrêté n° 70 prévoirait explicitement que les informations sur les interceptions ne peuvent être ni consignées ni enregistrées.

203. Le requérant ajoute qu'en Russie ni le juge ayant délivré l'autorisation d'interception ni aucun autre agent indépendant possédant les qualifications requises pour être magistrat n'a le pouvoir de contrôler la mise en œuvre de la mesure, notamment de vérifier si la surveillance est restée dans les limites fixées par l'autorisation et a respecté les diverses conditions établies par le droit interne.

204. Le droit interne ne définirait aucune procédure s'agissant du contrôle des interceptions par le président, le Parlement et le gouvernement. Ceux-ci n'auraient à l'évidence aucun pouvoir de contrôler l'application des mesures d'interception dans des situations précises.

205. Quant au contrôle exercé par le procureur général et les procureurs de rang inférieur compétents, le requérant estime que ces personnes ne peuvent pas être considérées comme indépendantes, compte tenu de leur position au sein du système de justice pénale et de leur fonction consistant à exercer les poursuites. Il arguë en particulier que les procureurs approuvent toutes les demandes d'interception déposées par des enquêteurs dans le contexte de procédures pénales et participent aux audiences judiciaires afférentes. Il précise qu'ils ont ensuite, lorsqu'ils exercent les poursuites, la possibilité d'utiliser les données recueillies au moyen de l'interception, notamment en les présentant comme éléments de preuve lors du procès. Il y aurait donc un conflit d'intérêts dès lors que le procureur exercerait une fonction double en ce qu'il serait à la fois partie à la procédure pénale et l'autorité contrôlant les interceptions.

206. Le requérant ajoute que les fonctions de contrôle des procureurs sont limitées du fait que certains éléments, en particulier ceux révélant l'identité d'agents infiltrés ou les tactiques, méthodes et moyens employés par les services de sécurité, échappent à leur contrôle. Les pouvoirs de contrôle des procureurs seraient également restreints dans le domaine du contre-renseignement, où les inspections ne seraient possibles que sur plainte individuelle. Eu égard au caractère secret des mesures d'interception et à l'absence de notification à la personne concernée, il serait peu probable

que de telles plaintes individuelles soient déposées, de sorte que les mesures de surveillance liées au contre-renseignement échapperaient *de facto* au contrôle des procureurs. Pour le requérant, il est notable également que les procureurs ne sont pas habilités à annuler une autorisation d'interception, à faire cesser une interception illégale ou à ordonner la destruction de données recueillies de manière illégale.

207. En outre, les rapports semestriels établis par les procureurs ne donneraient lieu ni à publication ni à débat public. Ces rapports seraient des documents classifiés et ne contiendraient que des informations statistiques. Ils ne fourniraient aucune analyse de fond sur le niveau de légalité régnant dans le domaine des mesures opérationnelles d'investigation, ni aucune information sur la nature des infractions à la loi décelées et le genre de mesures adoptées pour y remédier. En outre, ces rapports amalgameraient tous les types de mesures opérationnelles d'investigation, sans faire de distinction entre les interceptions et les autres mesures.

β) Le Gouvernement

208. Le Gouvernement indique que le contrôle des mesures opérationnelles d'investigation, y compris les interceptions de communications téléphoniques, est exercé par le président, le Parlement et le gouvernement. Plus particulièrement, le président définirait la stratégie en matière de sécurité nationale et désignerait et révoquerait les responsables de l'ensemble des organes d'application des lois. L'administration présidentielle comporterait par ailleurs un service spécialement chargé de contrôler les activités des organes d'application des lois, notamment les mesures opérationnelles d'investigation. Ce service serait composé d'agents du ministère de l'Intérieur et du FSB ayant le niveau approprié d'habilitation de sécurité. Le Parlement participerait au processus de contrôle en adoptant et en modifiant la législation qui régit les mesures opérationnelles d'investigation. Il aurait également la possibilité de former des comités et des commissions et organiserait des auditions parlementaires sur toutes sortes de questions, y compris celles relatives aux mesures opérationnelles d'investigation, et pourrait auditionner, en tant que de besoin, les responsables des organes d'application des lois. Quant au gouvernement, il prendrait des décrets et des arrêtés régissant les mesures opérationnelles d'investigation et attribuerait les ressources budgétaires aux organes d'application des lois.

209. Un contrôle serait également exercé par le procureur général et les procureurs de rang inférieur compétents, qui seraient indépendants des autorités fédérales, régionales et locales. Le procureur général et ses adjoints seraient désignés et révoqués par le Conseil de la Fédération, la chambre haute du Parlement. Les procureurs n'auraient pas le pouvoir de déposer des demandes d'interception. Celles-ci pourraient être formées soit par l'organe d'État mettant en œuvre des mesures opérationnelles d'investigation en

vertu de la LMOI, soit par l'enquêteur au titre du CPP. Le procureur ne serait pas habilité à donner des instructions à l'enquêteur. Dans le cadre d'une inspection effectuée par le procureur, le responsable de l'organe d'interception serait tenu de soumettre au procureur tout matériel pertinent sur demande de celui-ci ; en cas de non-obtempération, il risquerait de devoir rendre des comptes. Les procureurs chargés du contrôle des mesures opérationnelles d'investigation soumettraient au procureur général des rapports semestriels, lesquels n'analyseraient cependant pas les interceptions séparément des autres mesures opérationnelles d'investigation.

vii. Notification des mesures de surveillance secrète

α) Le requérant

210. Le requérant indique que le droit russe ne prévoit pas que la personne dont les communications sont interceptées se le voie notifier, que ce soit avant, pendant ou après l'opération. Il estime acceptable de ne pas informer l'intéressé avant ou pendant l'interception, dès lors que le caractère secret de la mesure est essentiel à son efficacité. Il arguë toutefois qu'une fois l'interception terminée la notification est possible, « dès [qu'elle] peut être donnée sans compromettre le but de la restriction » (*Klass et autres*, précité). En Russie, la personne concernée ne recevrait notification à aucun stade. Elle ne serait donc susceptible d'avoir connaissance de l'interception qu'en cas d'indiscrétion ou si une procédure pénale a été engagée contre elle et que les données interceptées ont servi d'éléments de preuve.

211. Concernant la possibilité d'obtenir l'accès aux données recueillies lors de l'interception, le requérant soutient qu'elle n'existe que dans des circonstances très limitées. À son avis, si aucune procédure pénale n'a été ouverte ou si les accusations ont été abandonnées pour des motifs autres que ceux énumérés dans la LMOI, la personne concernée ne peut pas avoir accès aux données. En outre, pour obtenir cet accès, le demandeur serait tenu d'établir qu'il y a eu interception de ses communications. Compte tenu du caractère secret des mesures de surveillance et de l'absence de notification, cette preuve serait impossible à apporter, sauf fuite d'informations sur l'interception. Même en ayant rempli toutes ces conditions préalables, l'intéressé ne pourrait recevoir que des « informations sur les données recueillies » et non obtenir l'accès aux données elles-mêmes. Enfin, seules des informations ne contenant pas de secrets d'État pourraient être divulguées. D'après le requérant, dès lors qu'en vertu de la LMOI toutes les données recueillies au cours de mesures opérationnelles d'investigation constituent des secrets d'État et que la décision de les déclassifier appartient au responsable du service d'interception, l'accès aux documents relatifs à une interception est entièrement soumis au pouvoir discrétionnaire des services d'interception.

212. Le refus d'accorder l'accès aux données recueillies serait susceptible de recours auprès d'un tribunal, et la LMOI imposerait aux services d'interception l'obligation de produire, sur demande du juge, « le matériel afférent aux mesures opérationnelles d'investigation contenant des informations sur les données auxquelles l'accès a été refusé ». Le requérant estime révélateur que les services d'interception soient tenus de fournir des « informations sur les données » et non les données elles-mêmes. Il ajoute que le matériel contenant des informations sur des agents infiltrés ou des informateurs de la police ne peut pas être soumis au tribunal et se trouve ainsi soustrait au champ couvert par le contrôle juridictionnel.

β) Le Gouvernement

213. Le Gouvernement explique qu'en droit russe une personne visée par des mesures de surveillance secrète n'est à aucun stade censée en être informée. Il rappelle que la Cour constitutionnelle a déclaré qu'eu égard à la nécessité de garder le secret sur les mesures de surveillance, les principes de publicité de l'audience et du contradictoire n'étaient pas applicables à la procédure d'autorisation (paragraphe 40 ci-dessus). La personne concernée ne pourrait donc ni participer à la procédure d'autorisation ni être informée de la décision prise.

214. Après clôture de l'enquête pénale, il serait loisible à la personne mise en cause d'examiner tous les éléments versés au dossier, y compris les données recueillies au cours de mesures opérationnelles d'investigation. Par ailleurs, dans les cas où l'enquêteur a décidé de ne pas entamer de procédure pénale contre le sujet de l'interception ou d'abandonner les poursuites au motif que l'infraction alléguée n'a pas été commise ou qu'un ou plusieurs des éléments constitutifs d'une infraction pénale font défaut, l'intéressé aurait la possibilité de recevoir à sa demande des informations sur les données recueillies. Le refus de fournir pareilles informations serait susceptible de recours auprès d'un tribunal, lequel aurait le pouvoir d'en ordonner la communication s'il juge le refus infondé. Le Gouvernement a soumis copie de la décision rendue le 4 août 2009 par le tribunal du district Alexeïevski (région de Belgorod), qui aurait ordonné à la police de fournir à une personne visée par une interception, dans un délai de un mois, des informations sur les données recueillies à son sujet au cours de l'opération, « pour autant que les règles de confidentialité l'autorisaient et à l'exclusion de données qui pourraient permettre la divulgation de secrets d'État ».

215. Le Gouvernement soutient que le droit russe diffère du droit bulgare critiqué par la Cour dans l'arrêt *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev* (précité, § 91), en ce qu'il prévoit selon lui la possibilité de déclassifier les éléments interceptés et de donner à la personne concernée accès à ces éléments. À l'appui de cette affirmation, il renvoie au jugement du 11 juillet 2012 par lequel la cour régionale de Zabaïkalsk aurait prononcé une condamnation pénale. Ce

jugement – dont la Cour n'a pas reçu copie – porte selon le Gouvernement sur une décision judiciaire ayant autorisé l'interception des communications téléphoniques de l'intéressé, décision qui aurait été déclassifiée et soumise au juge du fond à la demande de celui-ci. Le Gouvernement se réfère également à deux autres arrêts – l'un du présidium de la cour régionale de Krasnoïarsk et l'autre du présidium de la Cour suprême de la République des Maris – qui auraient annulé, par voie de supervision, des décisions judiciaires ayant autorisé l'interception de communications. Le Gouvernement n'a pas fourni copie de ces arrêts.

viii. Les recours disponibles

α) Le requérant

216. Le requérant considère que la question de la notification des mesures de surveillance et celle de l'effectivité des recours judiciaires sont indissolublement liées dès lors que, si on ne l'avise pas des mesures prises à son insu, l'intéressé ne peut guère, en principe, en contester rétrospectivement la légalité en justice (*Weber et Saravia*, décision précitée).

217. Il arguë que les recours disponibles en droit russe sont ineffectifs. Concernant la possibilité pour la personne objet de la surveillance de demander un contrôle juridictionnel des mesures appliquées, il indique que c'est à elle d'établir qu'elle a été mise sur écoute mais que, la personne placée sous surveillance n'étant pas informée de cette mesure sauf si elle est inculpée d'une infraction pénale, il lui est impossible de s'acquitter de la charge de la preuve. Les copies de jugements internes fournies par le Gouvernement porteraient sur des mesures de perquisition et de saisie, à savoir des mesures opérationnelles d'investigation connues des intéressés (paragraphes 220-221 et 223 ci-dessous). Le requérant dit ne pas avoir connaissance de décisions judiciaires accessibles au public qui auraient accueilli la plainte d'une personne ayant fait l'objet d'une interception dénonçant le caractère illégal de cette mesure. Par ailleurs, il estime révélateur qu'aucun des jugements produits par le Gouvernement n'ait renfermé une appréciation par les juridictions internes de la proportionnalité des mesures opérationnelles d'investigation incriminées. Il ajoute que la procédure interne engagée par lui démontre aussi clairement que les voies de recours offertes par le droit interne étaient ineffectives. En outre, dans l'affaire *Avanesyan c. Russie* (n° 41152/06, 18 septembre 2014), la Cour aurait déjà jugé qu'il n'y avait pas en droit russe de recours effectifs permettant de contester des mesures opérationnelles d'investigation.

218. Le requérant indique enfin que, les arrêtés ministériels régissant les interceptions secrètes de communication étant considérés comme ayant un caractère technique et non juridique et n'étant donc pas susceptibles de faire l'objet d'un contrôle juridictionnel, ni le sujet de l'interception ni le

fournisseur de services de communication ne peuvent les contester, ainsi qu'il l'aurait déjà démontré (paragraphe 161 ci-dessus).

β) Le Gouvernement

219. Le Gouvernement affirme qu'en Russie une personne estimant que ses droits ont été ou sont violés par un agent de l'État à l'occasion de la mise en œuvre de mesures opérationnelles d'investigation peut adresser une plainte au supérieur hiérarchique de cet agent, à un procureur ou à un tribunal, et ce en vertu de l'article 5 de la LMOI (paragraphe 83 ci-dessus).

220. Il indique que, comme la formation plénière de la Cour suprême l'a selon lui expliqué, si la personne concernée apprend qu'il y a eu interception, elle peut saisir une juridiction de droit commun suivant la procédure définie au chapitre 25 du CPC (paragraphe 92 ci-dessus). Le demandeur ne serait pas tenu de prouver que les mesures d'interception ont emporté violation de ses droits ; ce serait aux services d'interception qu'il incomberait d'établir que les mesures d'interception étaient légales et justifiées. Le Gouvernement ajoute qu'en droit russe si un tribunal conclut au civil qu'il y a eu atteinte aux droits du demandeur, il doit prendre des mesures aux fins du redressement de la violation et de la réparation du dommage (paragraphe 97 ci-dessus). Le Gouvernement a fourni copie de deux décisions judiciaires fondées sur le chapitre 25 du CPC, décisions ayant déclaré illégales des perquisitions et saisies d'objets ou de documents et ordonné à la police de prendre des mesures spécifiques destinées à réparer la violation.

221. En outre, il serait loisible au sujet de l'interception de former une requête en supervision contre la décision judiciaire ayant autorisé l'interception, comme l'aurait expliqué la Cour constitutionnelle dans sa décision du 15 juillet 2008 (paragraphe 43 ci-dessus). De même, l'intéressé aurait la possibilité de former un appel ou un pourvoi en cassation.

222. Le Gouvernement indique que si l'interception a eu lieu dans le cadre d'une procédure pénale, la personne concernée peut aussi déposer une plainte sur le fondement de l'article 125 du CPP. Il évoque l'arrêt du 26 octobre 2010 par lequel la Cour suprême aurait annulé, par voie de supervision, les décisions de juridictions inférieures de déclarer irrecevable la plainte formée par K. en vertu de l'article 125 du CPP, relativement au refus de l'enquêteur de lui délivrer copie de la décision judiciaire ayant autorisé l'interception de ses communications. La Cour suprême aurait déclaré qu'il fallait examiner la plainte sous l'angle de l'article 125 du CPP bien que l'intéressée eût déjà été condamnée, et que celle-ci avait droit à une copie de l'autorisation d'interception. Le Gouvernement a soumis copie de dix décisions judiciaires ayant accueilli des plaintes fondées sur l'article 125 du CPP, relatives à des perquisitions et saisies illégales d'objets ou de documents. Il a également produit copie d'un jugement ayant acquitté une personne en appel après constat que sa condamnation en première instance

reposait sur des éléments de preuve irrecevables recueillis au moyen d'un « achat test » illégal de stupéfiants.

223. Le Gouvernement ajoute que la personne concernée peut demander une indemnisation sur le fondement de l'article 1069 du code civil (paragraphe 102 ci-dessus). Cet article prévoirait la réparation du préjudice matériel ou moral causé à une personne physique ou morale par un acte illégal d'un organe ou d'un agent de l'administration centrale ou municipale, dès lors que la faute de cet organe ou agent se trouve établie. La question de l'indemnisation pour préjudice moral serait régie par les principes énoncés dans les articles 1099 à 1101 du code civil (paragraphes 103-104 ci-dessus). Le Gouvernement indique en particulier que le préjudice moral causé par la diffusion d'informations portant atteinte à l'honneur, à la dignité ou à la réputation d'une personne peut donner lieu à indemnisation, et ce que l'auteur du préjudice ait ou non commis une faute. Le Gouvernement a soumis copie de la décision du 9 décembre 2013 par laquelle le tribunal de Vitchouga (région d'Ivanovo) a alloué une indemnité au titre du préjudice moral dû à l'interception illégale des conversations téléphoniques d'un suspect, le juge du fond ayant déclaré irrecevables comme éléments de preuve les enregistrements obtenus par cette interception. Le Gouvernement a également présenté une décision judiciaire ayant alloué une indemnité pour perquisition et saisie illégales de documents, et une décision judiciaire ayant ordonné l'indemnisation d'une personne acquittée qui avait fait l'objet de poursuites illégales.

224. Le droit russe prévoirait aussi des recours à caractère pénal en cas d'abus de pouvoir (articles 285 et 286 du code pénal), de collecte ou de diffusion non autorisées d'informations sur la vie privée et familiale d'une personne (article 137 du code pénal) et de violation du droit au caractère privé des communications (article 138 du code pénal – paragraphes 19-22 ci-dessus). À cet égard, le Gouvernement évoque l'arrêt du 24 octobre 2002 par lequel la Cour suprême aurait condamné un certain E.S. pour s'être rendu coupable d'une infraction à l'article 138 du code pénal en incitant un fonctionnaire à lui fournir les noms des titulaires de plusieurs numéros de téléphone ainsi que les relevés d'appels correspondant à ces numéros. Il renvoie aussi à l'arrêt du 15 mars 2007 par lequel la Cour suprême aurait condamné un douanier pour infraction à l'article 138 du code pénal en raison de l'interception des communications téléphoniques d'un certain P. Le Gouvernement a soumis copie de deux autres jugements de condamnation fondés sur l'article 138 du code pénal : le premier concerne la vente de matériel d'espionnage, à savoir des stylos et des montres avec caméra intégrée ; le second porte sur le piratage secret de la base de données d'un fournisseur de services de communication aux fins de l'obtention de relevés d'appels d'usagers.

225. Pour finir, le Gouvernement arguë que le droit russe comporte aussi des recours permettant de se plaindre de l'insuffisance alléguée des

garanties contre les abus dans le cadre de l'interception de communications (paragraphe 156 ci-dessus).

226. Il maintient que le requérant n'a exercé aucun des recours que lui offrait le droit russe et qui sont évoqués ci-dessus. Plus particulièrement, l'intéressé aurait choisi d'engager une procédure judiciaire contre des opérateurs de réseaux mobiles, le ministère des Communications n'étant intervenu dans la procédure que comme tierce partie.

b) Appréciation de la Cour

i. Principes généraux

227. La Cour réaffirme qu'une ingérence ne peut se justifier au regard de l'article 8 § 2 que si elle est prévue par la loi, vise un ou plusieurs des buts légitimes énumérés au paragraphe 2 de l'article 8 et est nécessaire, dans une société démocratique, pour atteindre ce ou ces buts (*Kennedy*, précité, § 130).

228. La Cour rappelle sa jurisprudence constante selon laquelle les termes « prévue par la loi » signifient que la mesure litigieuse doit avoir une base en droit interne et être compatible avec la prééminence du droit, expressément mentionnée dans le préambule de la Convention et inhérente à l'objet et au but de l'article 8. La loi doit donc satisfaire à des exigences de qualité : elle doit être accessible à la personne concernée et prévisible quant à ses effets (voir, parmi bien d'autres, *Rotaru c. Roumanie* [GC], n° 28341/95, § 52, CEDH 2000-V, *S. et Marper c. Royaume-Uni* [GC], n^os^ 30562/04 et 30566/04, § 95, CEDH 2008, et *Kennedy*, précité, § 151).

229. La Cour a jugé à plusieurs reprises que, en matière d'interception de communications, la « prévisibilité » ne pouvait se comprendre de la même façon que dans beaucoup d'autres domaines. Dans le contexte particulier des mesures de surveillance secrète, telle l'interception de communications, la prévisibilité ne saurait signifier qu'un individu doit se trouver à même de prévoir quand les autorités sont susceptibles d'intercepter ses communications de manière qu'il puisse adapter sa conduite en conséquence. Or le risque d'arbitraire apparaît avec netteté là où un pouvoir de l'exécutif s'exerce en secret. L'existence de règles claires et détaillées en matière d'interception de conversations téléphoniques apparaît donc indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner. La loi doit être rédigée avec suffisamment de clarté pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes (*Malone*, précité, § 67, *Leander c. Suède*, 26 mars 1987, § 51, série A n° 116, *Huvig c. France*, 24 avril 1990, § 29, série A n° 176-B, *Valenzuela Contreras c. Espagne*, 30 juillet 1998, § 46, *Recueil* 1998-V, *Rotaru*, précité, § 55, *Weber et Saravia*, décision précitée, § 93, et

Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev, précité, § 75).

230. En outre, puisque l'application de mesures de surveillance secrète des communications échappe au contrôle des intéressés comme du public, la « loi » irait à l'encontre de la prééminence du droit si le pouvoir d'appréciation accordé à l'exécutif ou à un juge ne connaissait pas de limites. En conséquence, elle doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une clarté suffisante pour fournir à l'individu une protection adéquate contre l'arbitraire (voir, entre autres, *Malone*, précité, § 68, *Leander*, précité, § 51, *Huvig*, précité, § 29, et *Weber et Saravia*, décision précitée, § 94).

231. Dans sa jurisprudence relative aux mesures de surveillance secrète, la Cour énonce les garanties minimales suivantes contre les abus de pouvoir que la loi doit renfermer : la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée d'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements (*Huvig*, précité, § 34, *Amann c. Suisse* [GC], n° 27798/95, §§ 56-58, CEDH 2000-II, *Valenzuela Contreras*, précité, § 46, *Prado Bugallo c. Espagne*, n° 58496/00, § 30, 18 février 2003, *Weber* etSaravia, décision précitée, § 95, et *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, § 76).

232. En ce qui concerne la question de savoir si une ingérence est « nécessaire dans une société démocratique » à la réalisation d'un but légitime, la Cour a reconnu que, lorsqu'elles mettent en balance l'intérêt de l'État défendeur à protéger la sécurité nationale au moyen de mesures de surveillance secrète, d'une part, et la gravité de l'ingérence dans l'exercice par un requérant du droit au respect de la vie privée, d'autre part, les autorités nationales disposent d'une certaine marge d'appréciation dans le choix des moyens propres à atteindre le but légitime que constitue la protection de la sécurité nationale. Cette marge d'appréciation va toutefois de pair avec un contrôle européen portant à la fois sur la loi et sur les décisions qui l'appliquent. La Cour doit se convaincre de l'existence de garanties adéquates et effectives contre les abus, car un système de surveillance secrète destiné à protéger la sécurité nationale risque de saper, voire de détruire, la démocratie au motif de la défendre. L'appréciation de cette question est fonction de toutes les circonstances de la cause, par exemple la nature, la portée et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, les exécuter et les contrôler, et le type de recours fourni par le droit interne. La Cour doit rechercher si les procédures de contrôle du déclenchement et de la

mise en œuvre de mesures restrictives sont de nature à circonscrire « l'ingérence » à ce qui est « nécessaire dans une société démocratique » (*Klass et autres*, précité, §§ 49-50 et 59, *Weber et Saravia*, décision précitée, § 106, *Kvasnica c. Slovaquie*, nº 72094/01, § 80, 9 juin 2009, et *Kennedy*, précité, §§ 153-154).

233. L'examen et le contrôle des mesures de surveillance secrète peuvent intervenir à trois stades : lorsqu'on ordonne la surveillance, pendant qu'on la mène ou après qu'elle a cessé. Concernant les deux premières phases, la nature et la logique mêmes de la surveillance secrète commandent d'exercer à l'insu de l'intéressé non seulement la surveillance comme telle, mais aussi le contrôle qui l'accompagne. Puisque l'on empêchera donc forcément l'intéressé d'introduire un recours effectif ou de prendre une part directe à un contrôle quelconque, il se révèle indispensable que les procédures existantes procurent en elles-mêmes des garanties appropriées et équivalentes sauvegardant les droits de l'individu. Il faut de surcroît, pour ne pas dépasser les bornes de la nécessité au sens de l'article 8 § 2, respecter aussi fidèlement que possible, dans les procédures de contrôle, les valeurs d'une société démocratique. En un domaine où les abus sont potentiellement si aisés dans des cas individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique tout entière, il est en principe souhaitable que le contrôle soit confié à un juge, car le pouvoir judiciaire offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière (*Klass et autres*, précité, §§ 55-56).

234. Quant au troisième stade, c'est-à-dire lorsque la surveillance a cessé, la question de la notification *a posteriori* de mesures de surveillance est indissolublement liée à celle de l'effectivité des recours judiciaires et donc à l'existence de garanties effectives contre les abus des pouvoirs de surveillance. La personne concernée ne peut guère, en principe, contester rétrospectivement devant la justice la légalité des mesures prises à son insu, sauf si on l'avise de celles-ci (*Klass et autres*, précité, § 57, et *Weber et Saravia*, décision précitée, § 135) ou si – autre cas de figure –, soupçonnant que ses communications font ou ont fait l'objet d'interceptions, la personne a la faculté de saisir les tribunaux, ceux-ci étant compétents même si le sujet de l'interception n'a pas été informé de cette mesure (*Kennedy*, précité, § 167).

ii. Application en l'espèce des principes généraux précités

235. La Cour rappelle avoir conclu que la législation russe sur l'interception secrète de communications de téléphonie mobile, dénoncée par le requérant dans un grief général, constitue une ingérence dans l'exercice du droit garanti par l'article 8 § 1. Dès lors, pour trancher la question de savoir si cette ingérence se justifie sous l'angle de l'article 8 § 2, elle devra rechercher si en soi la législation litigieuse est conforme à la Convention.

236. Dans les affaires où la législation autorisant la surveillance secrète est contestée devant la Cour, la question de la légalité de l'ingérence est étroitement liée à celle de savoir s'il a été satisfait au critère de la « nécessité », raison pour laquelle la Cour doit examiner conjointement les critères selon lesquels la mesure doit être « prévue par la loi » et « nécessaire » (*Kennedy*, précité, § 155 ; voir aussi *Kvasnica*, précité, § 84). La « qualité de la loi » en ce sens implique que le droit interne doit non seulement être accessible et prévisible dans son application, mais aussi garantir que les mesures de surveillance secrète soient appliquées uniquement lorsqu'elles sont « nécessaires dans une société démocratique », notamment en offrant des garanties et des garde-fous suffisants et effectifs contre les abus.

237. Les parties ne contestent pas que les interceptions des communications de téléphonie mobile ont une base en droit interne. Celles-ci sont régies en particulier par le CPP et la LMOI, ainsi que par la loi sur les communications et les arrêtés du ministère des Communications. Par ailleurs, il est clair pour la Cour que les mesures de surveillance autorisées en droit russe poursuivent les buts légitimes que sont la protection de la sécurité nationale et de la sûreté publique, la prévention des infractions pénales et la protection du bien-être économique du pays (paragraphe 26 ci-dessus). Il reste donc à vérifier si le droit interne est accessible et s'il contient des garanties et des garde-fous suffisants et effectifs propres à satisfaire aux exigences de « prévisibilité » et de « nécessité dans une société démocratique ».

238. La Cour appréciera donc successivement l'accessibilité du droit interne, la portée et la durée des mesures de surveillance secrète, les procédures à suivre pour la conservation, la consultation, l'examen, l'utilisation, la communication et la destruction des données interceptées, les procédures d'autorisation, les modalités du contrôle de l'application de mesures de surveillance secrète, l'existence éventuelle d'un mécanisme de notification et les recours prévus en droit interne.

α) Accessibilité du droit interne

239. Les parties s'accordent à dire que la quasi-totalité des dispositions juridiques régissant la surveillance secrète – notamment le CPP, la LMOI, la loi sur les communications et la plupart des arrêtés pris par le ministère des Communications – ont fait l'objet d'une publication officielle et sont accessibles aux citoyens. En revanche, elles divergent sur le point de savoir si les addendums à l'arrêté n° 70 du ministère des Communications satisfont à l'exigence d'accessibilité.

240. La Cour observe que ces addendums n'ont jamais figuré dans une publication officielle accessible à tous, car ils ont été considérés comme présentant un caractère technique (paragraphe 128 ci-dessus).

241. La Cour admet que pour l'essentiel les addendums à l'arrêté n° 70 exposent les spécifications techniques relatives au dispositif d'interception que les fournisseurs de services de communication doivent installer. En même temps, en exigeant que le dispositif en question confère aux services d'application des lois un accès direct à toutes les communications de téléphonie mobile de tous les usagers, tout en prohibant la consignation ou l'enregistrement d'informations sur les interceptions effectuées par lesdits services (paragraphes 115-122 ci-dessus), les addendums à l'arrêté n° 70 sont susceptibles de porter atteinte au droit des usagers au respect de leur vie privée et de leur correspondance. La Cour considère dès lors qu'ils doivent être accessibles aux citoyens.

242. Publié dans le magazine officiel du ministère des Communications *SvyazInform*, qui est diffusé par abonnement, l'arrêté n'a été rendu accessible qu'aux spécialistes des communications et non au grand public. La Cour note toutefois que le texte de l'arrêté accompagné de ses addendums peut être consulté *via* une base de données Internet juridique privée, qui l'a repris à partir de *SvyazInform* (paragraphe 115 ci-dessus). Elle juge regrettable l'absence de publication officielle de l'arrêté n° 70 le rendant accessible à tous. Cependant, prenant en compte le fait qu'il a été publié dans un magazine ministériel officiel, auquel s'ajoute la possibilité pour le grand public de le consulter par le biais d'une base de données juridique sur Internet, la Cour estime qu'il n'y a pas lieu d'examiner plus avant la question de l'accessibilité du droit interne. Elle se concentrera plutôt sur les exigences de « prévisibilité » et de « nécessité ».

β) Champ d'application des mesures de surveillance secrète

243. La Cour rappelle que le droit national doit définir le champ d'application des mesures de surveillance secrète en fournissant aux citoyens des indications appropriées sur les circonstances dans lesquelles les pouvoirs publics peuvent recourir à de telles mesures – en particulier en énonçant clairement la nature des infractions susceptibles de donner lieu à un mandat d'interception et en définissant les catégories de personnes susceptibles d'être mises sur écoute (paragraphe 231 ci-dessus).

244. En ce qui concerne la nature des infractions, la Cour souligne que le critère de la prévisibilité n'exige pas des États qu'ils énumèrent exhaustivement en les nommant celles qui peuvent donner lieu à une mesure d'interception. En revanche, ils doivent fournir des précisions suffisantes sur la nature des infractions en question (*Kennedy*, précité, § 159). Tant la LMOI que le CPP indiquent que les communications, téléphoniques et autres, peuvent être interceptées dans le contexte d'une infraction de gravité moyenne, d'une infraction grave ou d'une infraction pénale particulièrement grave – c'est-à-dire une infraction pour laquelle le code pénal prescrit une peine maximale supérieure à trois ans d'emprisonnement – qui a déjà été commise, est en train d'être commise ou est en préparation

(paragraphes 31-33 ci-dessus). La Cour est d'avis que la nature des infractions pouvant donner lieu à un mandat d'interception est suffisamment claire. Elle n'en est pas moins préoccupée de constater que le droit russe autorise l'interception secrète des communications pour un très large éventail d'infractions pénales, y compris par exemple, comme le signale le requérant, le vol à la tire (paragraphe 182 ci-dessus ; voir aussi, pour un raisonnement similaire, *Iordachi et autres*, précité, §§ 43-44).

245. La Cour note par ailleurs qu'une interception peut être ordonnée non seulement à l'égard d'un suspect ou d'un prévenu, mais aussi d'une personne susceptible de détenir des informations sur une infraction ou d'autres informations pertinentes pour un dossier pénal (paragraphe 32 ci-dessus). Elle a déjà dit par le passé que les mesures d'interception visant une personne non soupçonnée d'une infraction mais susceptible de détenir des informations sur une telle infraction pouvaient être justifiées au regard de l'article 8 de la Convention (*Greuter*, décision précitée). Elle relève cependant l'absence de toute précision, dans la législation russe ou la jurisprudence constante des juridictions russes, sur la manière dont il convient d'interpréter en pratique les termes « personne susceptible de détenir des informations sur une infraction pénale » et « personne susceptible de détenir des informations pertinentes pour un dossier pénal » (voir, pour un raisonnement similaire, *Iordachi et autres*, précité, § 44).

246. La Cour observe également que, outre les interceptions visant à la prévention ou à la détection des infractions pénales, la LMOI prévoit aussi la possibilité d'intercepter les communications, téléphoniques ou autres, après réception d'informations sur des faits ou activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique de la Russie (paragraphe 31 ci-dessus). Or la nature des faits ou activités pouvant passer pour mettre en péril ces types d'intérêts en matière de sécurité n'est définie nulle part dans le droit russe.

247. La Cour a déjà eu l'occasion de dire que l'exigence de « prévisibilité » de la loi n'allait pas jusqu'à imposer aux États l'obligation d'édicter des dispositions juridiques énumérant dans le détail tous les comportements pouvant conduire à la décision de soumettre un individu à une surveillance secrète pour des motifs de « sécurité nationale ». Par la force des choses, des menaces dirigées contre la sécurité nationale peuvent être de différentes natures et peuvent être imprévues ou difficiles à définir à l'avance (*Kennedy*, précité, § 159). La Cour, cependant, a également souligné que, s'agissant de questions touchant aux droits fondamentaux, la loi irait à l'encontre de la prééminence du droit, l'un des principes de base d'une société démocratique consacrés par la Convention, si le pouvoir d'appréciation accordé à l'exécutif en matière de sécurité nationale ne connaissait pas de limite. En conséquence, elle doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une clarté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection

adéquate contre l'arbitraire (*Liou c. Russie*, nº 42086/05, § 56, 6 décembre 2007, avec d'autres références).

248. Il importe de noter que la LMOI ne donne aucune indication sur les circonstances dans lesquelles les communications d'une personne peuvent être interceptées en raison de faits ou d'activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique de la Russie. Cette absence confère aux autorités une latitude quasi illimitée lorsqu'il s'agit de déterminer quels faits ou actes représentent pareille menace, et si celle-ci est grave au point de justifier une surveillance secrète ; il en résulte des risques d'abus (voir, pour un raisonnement similaire, *Iordachi et autres*, précité, § 46).

249. Cela étant, la Cour ne perd pas de vue le fait qu'en Russie une mesure d'interception requiert au préalable une autorisation judiciaire. Celle-ci peut contribuer à limiter la latitude des services d'application des lois dans la lecture des formules générales que sont « personne susceptible de détenir des informations sur une infraction pénale », « personne susceptible de détenir des informations pertinentes pour un dossier pénal » et « faits ou activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique de la Russie », grâce à une interprétation judiciaire établie de ces termes ou à une pratique consacrée consistant à vérifier au cas par cas s'il existe des raisons suffisantes d'intercepter les communications d'une personne donnée. La Cour admet que la condition de l'autorisation judiciaire préalable constitue une importante garantie contre l'arbitraire. Elle se penchera ci-dessous sur l'effectivité de cette garantie.

γ) La durée des mesures de surveillance secrète

250. La Cour a dit qu'il n'était pas déraisonnable de laisser la question de la durée totale d'une mesure d'interception à l'appréciation des autorités internes compétentes pour délivrer et renouveler un mandat d'interception, pourvu qu'il existe des garanties suffisantes telles que des indications claires dans le droit interne sur le délai d'expiration de l'autorisation d'interception, les conditions dans lesquelles elle peut être renouvelée et les circonstances dans lesquelles elle doit être annulée (*Kennedy*, précité, § 161 ; voir aussi *Klass et autres*, précité, § 52, et *Weber et Saravia*, décision précitée, § 98).

251. Pour ce qui est de la première garantie, tant le CPP que la LMOI disposent qu'un juge peut autoriser une mesure d'interception pour une durée n'excédant pas six mois (paragraphes 38 et 47 ci-dessus). Le droit interne indique donc avec clarté la période maximale au terme de laquelle une autorisation d'interception parvient à expiration. Deuxièmement, les conditions dans lesquelles pareille autorisation peut être renouvelée sont elles aussi précisées clairement dans la loi. En particulier, le CPP comme la LMOI disposent qu'un juge peut proroger la mesure d'interception de six mois en six mois, après réexamen de l'ensemble des éléments pertinents (*ibidem*). Concernant la troisième garantie, relative aux circonstances dans

lesquelles la mesure d'interception doit être levée, la Cour remarque en revanche que l'obligation de mettre un terme à cette mesure lorsqu'elle n'est plus nécessaire est mentionnée uniquement dans le CPP, mais non, hélas, dans la LMOI (*ibidem*). Cela signifie en pratique que les interceptions intervenant dans le contexte de poursuites pénales sont entourées de plus de garanties que celles qui n'entrent pas dans ce cadre, en particulier pour ce qui touche aux « faits ou activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique » du pays.

252. Partant, la Cour conclut que le droit russe comporte, au sujet de la durée et de la prorogation d'une mesure d'interception, des règles claires qui offrent des garde-fous adéquats contre les abus, mais qu'en revanche les dispositions de la LMOI sur la levée de mesures de surveillance ne fournissent pas des garanties suffisantes contre les ingérences arbitraires.

δ) Procédures à suivre pour la conservation, la consultation, l'examen, l'utilisation, la communication et la destruction des données interceptées

253. Le droit russe dispose que les données recueillies au moyen de mesures de surveillance secrète constituent des secrets d'État et doivent être scellées et conservées dans des conditions permettant d'écarter tout risque d'accès non autorisé ; ces données peuvent être transmises aux agents de l'État qui en ont véritablement besoin pour s'acquitter de leurs tâches et possèdent le niveau approprié d'habilitation de sécurité. Il prévoit que des mesures soient prises pour veiller à ce que seules soient communiquées les informations nécessaires au destinataire pour l'accomplissement de ses fonctions. L'agent chargé de veiller à ce que les données soient conservées de manière sûre et soient rendues inaccessibles aux personnes non titulaires de l'habilitation de sécurité requise est clairement désigné (paragraphes 51-57 ci-dessus). Le droit interne expose également les conditions et procédures de transmission aux services de poursuite de données interceptées contenant des informations sur une infraction pénale. Il indique en particulier les règles relatives à la conservation sécurisée de ces données et les conditions de leur utilisation comme éléments de preuve lors de poursuites pénales (paragraphes 58-64 ci-dessus). La Cour constate que le droit russe comporte en matière de conservation, d'utilisation et de communication de données interceptées des règles claires qui permettent de réduire au minimum le risque d'accès ou de divulgation non autorisés (voir, pour un raisonnement similaire, *Kennedy*, précité, §§ 162-163).

254. Selon le droit interne, la destruction des éléments interceptés doit intervenir au terme des six mois de conservation si la personne concernée n'a pas été inculpée d'une infraction pénale ; si elle a été inculpée d'une telle infraction, le juge du fond doit décider, à l'issue de la procédure pénale, si les éléments interceptés ayant servi de preuves doivent être conservés ou détruits (paragraphes 65-66 ci-dessus).

255. Pour ce qui est du cas où la personne concernée n'a pas été inculpée d'une infraction pénale, la Cour n'est pas convaincue par l'argument du requérant selon lequel le droit russe permet la conservation des éléments interceptés au-delà du délai légal (paragraphe 188 ci-dessus). En effet, la disposition visée par le requérant ne s'applique pas au cas spécifique de la conservation de données recueillies au moyen de l'interception de communications. La Cour juge raisonnable la durée maximale de conservation, à savoir six mois, fixée par le droit russe pour de telles données. Elle déplore toutefois l'absence d'obligation de détruire sur-le-champ les données qui n'ont pas de rapport avec le but pour lequel elles ont été recueillies (comparer avec *Klass et autres*, précité, § 52, et *Kennedy*, précité, § 162). La conservation automatique, six mois durant, de données manifestement dénuées d'intérêt ne saurait passer pour justifiée au regard de l'article 8.

256. Concernant enfin le cas où l'intéressé a été inculpé d'une infraction pénale, la Cour observe avec préoccupation que le droit russe laisse au juge du fond une latitude illimitée pour décider de la conservation ou de la destruction, à l'issue du procès, des données qui ont servi de preuves (paragraphe 66 ci-dessus). Le droit russe ne donne aux citoyens aucune indication sur les circonstances dans lesquelles les éléments interceptés peuvent être conservés au-delà du procès. La Cour estime dès lors qu'il manque de clarté sur ce point.

ε) Autorisation des interceptions

– *Procédures d'autorisation*

257. Pour déterminer si les procédures d'autorisation sont à même de garantir que la surveillance secrète n'est pas ordonnée au hasard, irrégulièrement ou sans examen approprié et convenable, la Cour prendra en compte un certain nombre de facteurs, parmi lesquels, notamment, le service compétent pour autoriser la surveillance, la portée de l'examen qu'il effectue et le contenu de l'autorisation d'interception.

258. En ce qui concerne le service compétent pour autoriser la surveillance, la Cour note que la délivrance d'autorisations d'effectuer des écoutes téléphoniques par un service non judiciaire peut être compatible avec la Convention (voir, par exemple, *Klass et autres*, précité, § 51, *Weber et Saravia*, décision précitée, § 115, et *Kennedy*, précité, § 31), à condition que cet organe soit suffisamment indépendant à l'égard de l'exécutif (*Dumitru Popescu c. Roumanie (n° 2)*, n° 71525/01, § 71, 26 avril 2007).

259. Le droit russe contient une importante garantie contre la surveillance secrète arbitraire ou systématique, puisqu'il prévoit que toute interception de communications, téléphoniques ou autres, doit faire l'objet d'une autorisation judiciaire (paragraphes 34 et 44 ci-dessus). L'organe d'application des lois qui souhaite obtenir une autorisation d'interception

doit à cet effet présenter une demande motivée au juge, lequel peut le prier de produire des pièces justificatives (paragraphes 37 et 46 ci-dessus). Le juge doit motiver sa décision d'autoriser une mesure d'interception (paragraphes 38 et 44 ci-dessus).

260. Pour ce qui est de la portée de l'examen effectué par le service délivrant l'autorisation, la Cour rappelle que celui-ci doit être à même de vérifier l'existence d'un soupçon raisonnable à l'égard de la personne concernée, en particulier de rechercher s'il existe des indices permettant de la soupçonner de projeter, de commettre ou d'avoir commis des actes délictueux ou d'autres actes susceptibles de donner lieu à des mesures de surveillance secrète, comme des actes mettant en péril la sécurité nationale. Il doit également s'assurer que l'interception requise satisfait au critère de « nécessité dans une société démocratique » prévu à l'article 8 § 2 de la Convention, notamment qu'elle est proportionnée aux buts légitimes poursuivis, en vérifiant par exemple s'il est possible d'atteindre les buts recherchés par des moyens moins restrictifs (*Klass et autres*, précité, § 51, *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, §§ 79-80, *Iordachi et autres*, précité, § 51, et *Kennedy*, précité, §§ 31-32).

261. La Cour note qu'en Russie le contrôle juridictionnel a une portée limitée. Ainsi, le matériel contenant des renseignements sur des agents infiltrés ou des informateurs de la police, ou sur l'organisation et la tactique afférentes aux mesures opérationnelles d'investigation, ne peut pas être soumis au juge et est donc exclu de l'examen effectué par le tribunal (paragraphe 37 ci-dessus). La Cour considère que la non-divulgation aux tribunaux des informations pertinentes ôte à ceux-ci le pouvoir de vérifier s'il existe une base factuelle suffisante pour soupçonner la personne visée par la demande de mesures d'être l'auteur d'une infraction pénale ou d'activités mettant en péril la sécurité nationale, militaire, économique ou écologique du pays (voir, *mutatis mutandis*, *Liou*, précité, §§ 59-63). La Cour a déjà déclaré par le passé qu'il existait des techniques permettant de concilier, d'une part, les soucis légitimes de sécurité quant à la nature et aux sources de renseignements et, de l'autre, la nécessité d'accorder en suffisance au justiciable le bénéfice des règles de procédure (voir, *mutatis mutandis*, *Chahal c. Royaume-Uni*, 15 novembre 1996, § 131, *Recueil* 1996-V).

262. En outre, la Cour observe qu'en Russie ni le CPP ni la LMOI n'imposent aux juges de vérifier l'existence d'un « soupçon raisonnable » à l'égard de la personne concernée ou d'appliquer les critères de « nécessité » et de « proportionnalité ». Elle note cependant que la Cour constitutionnelle a expliqué dans ses décisions que la charge de la preuve incombait à l'organe demandeur, lequel devait établir la nécessité de l'interception, et que le juge qui examinait une demande d'interception devait vérifier les motifs de cette mesure et n'accorder l'autorisation que s'il était convaincu

que l'interception était légale, nécessaire et justifiée. La Cour constitutionnelle a également déclaré que la décision judiciaire autorisant l'interception devait être motivée et indiquer des raisons spécifiques de penser qu'une infraction pénale a été commise, est en train d'être commise ou est en préparation ou que des activités mettant en péril la sécurité nationale, militaire, économique ou écologique du pays sont déployées, et que la personne visée par la demande d'interception est impliquée dans ces activités criminelles ou dangereuses (paragraphes 40-42 ci-dessus). La Cour constitutionnelle a ainsi recommandé, en substance, qu'au moment d'examiner les demandes d'autorisation d'interception les juridictions russes vérifient l'existence d'un « soupçon raisonnable » à l'égard de la personne concernée et n'autorisent la mesure que si elle satisfait aux critères de nécessité et de proportionnalité.

263. Toutefois, la Cour constate que le droit interne n'oblige pas expressément les juridictions de droit commun à se conformer à un avis de la Cour constitutionnelle sur la manière d'interpréter une disposition législative lorsque cet avis a été formulé dans une décision et non dans un arrêt (paragraphe 106 ci-dessus). De fait, les documents soumis par le requérant montrent que les juridictions internes ne suivent pas toujours les recommandations susmentionnées de la Cour constitutionnelle, qui sont toutes contenues dans des décisions et non dans des arrêts. Ainsi, il ressort des notes analytiques produites par des tribunaux de district que souvent les demandes d'interception ne sont pas accompagnées de pièces justificatives, que les juges de ces tribunaux ne demandent jamais à l'organe d'interception de leur soumettre de telles pièces et qu'une simple référence à l'existence d'informations sur une infraction pénale ou sur des activités mettant en péril la sécurité nationale, militaire, économique ou écologique du pays est considérée comme suffisante pour la délivrance d'une autorisation. Une demande d'interception n'est rejetée que si elle ne porte pas la signature d'une personne compétente, ne contient pas de référence à l'infraction en rapport avec laquelle une interception doit être ordonnée ou concerne une infraction pénale pour laquelle une interception n'est pas autorisée en droit interne (paragraphe 193 ci-dessus). Ainsi, les notes analytiques établies par les tribunaux de district, combinées avec les statistiques fournies par le requérant pour la période 2009-2013 (paragraphe 194 ci-dessus), font apparaître que dans leur pratique quotidienne les juridictions russes ne vérifient pas s'il existe un « soupçon raisonnable » à l'égard de la personne concernée et n'appliquent pas les critères de « nécessité » et de « proportionnalité ».

264. Enfin, le contenu du mandat d'interception doit désigner clairement la personne précise à placer sous surveillance ou l'unique ensemble de locaux (lieux) visé par l'interception autorisée par le mandat. Cette désignation peut être faite au moyen des noms, adresses, numéros de téléphone ou d'autres informations pertinentes (*Klass et autres*, précité,

§ 51, *Liberty et autres*, précité, §§ 64-65, *Dumitru Popescu*, précité, § 78, *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, § 80, et *Kennedy*, précité, § 160).

265. La Cour observe que le CPP exige que la demande d'autorisation d'interception indique de façon claire qui est la personne précise dont les communications doivent être interceptées et quelle est la durée de la mesure en question (paragraphe 46 ci-dessus). La LMOI, en revanche, ne renferme aucune prescription quant au contenu de la demande ou de l'autorisation d'interception. En conséquence, il arrive que les tribunaux délivrent une autorisation qui ne mentionne pas une personne précise ou un numéro de téléphone particulier à placer sur écoute, mais autorise l'interception de toutes les communications téléphoniques dans le secteur où une infraction pénale a été commise. Certaines autorisations n'indiquent pas la période pendant laquelle l'interception est permise (paragraphe 193 ci-dessus). La Cour estime que de telles autorisations, qui ne sont pas clairement prohibées par la LMOI, confèrent une très grande latitude aux services d'application des lois quant au type de communications à intercepter et à la durée de la mesure.

266. La Cour note en outre que, dans les cas d'urgence, il est possible d'intercepter des communications sans autorisation judiciaire préalable, et ce pendant une durée maximale de quarante-huit heures. Le juge doit être informé d'un tel cas dans un délai de vingt-quatre heures à compter du début de l'interception. Si aucune autorisation judiciaire n'est délivrée dans les quarante-huit heures, l'interception doit cesser sur-le-champ (paragraphe 35 ci-dessus). La Cour a eu l'occasion de se pencher sur la procédure « d'urgence » prévue par le droit bulgare et l'a jugée compatible avec la Convention (*Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, §§ 16 et 82). Cependant, contrairement au système bulgare, la « procédure d'urgence » russe ne comporte pas de garanties suffisantes pour en assurer une utilisation parcimonieuse et limitée aux cas dûment justifiés. En effet, bien qu'en matière pénale la LMOI restreigne le recours à la procédure d'urgence aux cas de danger immédiat de commission d'une infraction grave ou particulièrement grave, elle ne contient pas de limitation similaire pour la surveillance secrète liée à des faits ou activités mettant en péril la sécurité nationale, militaire, économique ou écologique du pays. Le droit interne ne restreint pas l'utilisation de la procédure d'urgence aux cas impliquant un péril grave et imminent pour la sécurité nationale, militaire, économique ou écologique du pays ; il laisse aux autorités une latitude illimitée pour déterminer dans quelles situations il se justifie de recourir à la procédure d'urgence non judiciaire, ce qui engendre des risques de recours abusif à cette procédure (voir, *a contrario*, *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, § 16). En outre, bien que le droit russe exige qu'un juge soit informé sur-le-champ de chaque cas d'interception d'urgence, le

pouvoir du juge se borne à la délivrance d'une autorisation de proroger la mesure d'interception au-delà de quarante-huit heures. Le juge n'a pas le pouvoir d'apprécier si le recours à la procédure d'urgence était justifié ou de décider si le matériel recueilli au cours des quarante-huit heures précédentes doit être conservé ou détruit (voir, *a contrario*, *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, § 16). Dès lors, le droit russe ne prévoit pas un contrôle juridictionnel effectif de la procédure d'urgence.

267. Eu égard aux considérations qui précèdent, la Cour estime que les procédures d'autorisation existant en droit russe ne sont pas aptes à garantir que les mesures de surveillance secrète ne soient pas ordonnées au hasard, irrégulièrement ou sans examen approprié et convenable.

– *L'accès des autorités aux communications*

268. La Cour prend note de l'argument du requérant selon lequel les services de sécurité et la police ont les moyens techniques d'intercepter des communications de téléphonie mobile sans avoir à obtenir d'autorisation judiciaire dès lors qu'ils jouissent d'un accès direct à toutes les communications et que leur capacité à intercepter les communications d'un ou plusieurs individus précis n'est pas subordonnée à la présentation d'une autorisation d'interception au fournisseur de services de communication.

269. Pour la Cour, l'obligation de présenter une autorisation d'interception au fournisseur de services de communication pour pouvoir accéder aux communications d'une personne constitue l'une des garanties importantes contre les abus de la part des services d'application des lois en ce qu'elle permet d'assurer qu'une autorisation en bonne et due forme soit obtenue avant toute interception. En Russie, les services d'application des lois ne sont pas contraints par le droit interne à présenter une autorisation judiciaire au fournisseur de services de communication pour avoir accès aux communications d'une personne (voir, *a contrario*, la Résolution du Conseil de l'Union européenne, paragraphe 145 ci-dessus), excepté dans le cadre de la surveillance des données relatives aux communications en vertu du CPP (paragraphe 48 ci-dessus). En effet, en application des arrêtés du ministère des Communications, en particulier les addendums à l'arrêté n° 70, les fournisseurs de services de communication sont tenus d'installer un dispositif offrant aux services d'application des lois un accès direct à toutes les communications de téléphonie mobile de tous les usagers (paragraphes 115-122 ci-dessus). L'arrêté n° 538 impose également aux fournisseurs de services de communication l'obligation de créer des bases de données permettant de stocker pendant trois ans des informations sur tous les abonnés et les prestations dont ils bénéficient, bases de données auxquelles les services secrets ont un accès direct à distance (paragraphes 132-133 ci-dessus). Les services d'application des lois ont

donc un accès direct à toutes les communications de téléphonie mobile et aux données y afférentes.

270. La Cour estime que le mode de fonctionnement du système de surveillance secrète en Russie donne aux services de sécurité et à la police les moyens techniques de contourner la procédure d'autorisation et d'intercepter n'importe quelle communication sans mandat judiciaire préalable. Si l'on ne peut jamais, quel que soit le système, écarter complètement l'éventualité qu'un fonctionnaire malhonnête, négligent ou trop zélé commette des actes irréguliers (*Klass et autres*, précité, § 59), la Cour considère néanmoins qu'un système tel que le système russe, qui permet aux services secrets et à la police d'intercepter directement les communications de n'importe quel citoyen sans leur imposer l'obligation de présenter une autorisation d'interception au fournisseur de services de communication ou à quiconque, est particulièrement exposé aux abus. La nécessité de disposer de garanties contre l'arbitraire et les abus apparaît donc particulièrement forte.

271. Dès lors, la Cour recherchera avec une attention particulière si le mode de contrôle prévu par le droit russe est à même de garantir que toute interception est effectuée légalement, en vertu d'une autorisation judiciaire en bonne et due forme.

ζ) Contrôle de l'application de mesures de surveillance secrète

272. La Cour note d'emblée que, suivant l'arrêté n° 70, le dispositif installé par les fournisseurs de services de communication ne doit ni consigner ni enregistrer des informations sur les interceptions (paragraphe 120 ci-dessus). La Cour a déjà dit par le passé que l'obligation faite aux organes d'interception de tenir des archives sur les interceptions était particulièrement importante pour garantir à l'organe de contrôle un accès effectif aux détails des opérations de surveillance entreprises (*Kennedy*, précité, § 165). L'interdiction prévue par le droit russe de consigner ou d'enregistrer les interceptions empêche l'autorité de contrôle de repérer les interceptions réalisées sans autorisation judiciaire en bonne et due forme. Combinée à la capacité technique conférée aux services d'application des lois, par ce même arrêté, d'intercepter directement toute communication, cette règle rend tout système de contrôle impropre à détecter les interceptions irrégulières, et donc ineffectif.

273. Concernant le contrôle des interceptions effectuées en vertu d'une autorisation judiciaire en bonne et due forme, la Cour recherchera si le système de contrôle existant en Russie est apte à garantir que les prescriptions légales concernant la mise en œuvre de mesures de surveillance ainsi que la conservation, la consultation, l'utilisation, le traitement, la communication et la destruction des éléments interceptés sont systématiquement respectées.

274. Le tribunal qui a délivré une autorisation d'interception n'est pas compétent pour en contrôler la mise en œuvre. Il n'est pas informé du résultat des interceptions et n'a pas le pouvoir de vérifier si les conditions associées à la décision d'octroyer l'autorisation ont été respectées. Les juridictions russes en général ne sont pas elles non plus compétentes pour exercer un contrôle global sur les interceptions. Le contrôle par les juridictions se limite au stade initial de l'autorisation. Quant au contrôle ultérieur, il est confié au président, au Parlement, au gouvernement, au procureur général et aux procureurs de rang inférieur compétents.

275. Comme la Cour l'a dit par le passé, s'il est en principe souhaitable que la fonction de contrôle soit confiée à un juge, le contrôle par un organe non judiciaire peut passer pour compatible avec la Convention dès lors que cet organe est indépendant des autorités qui procèdent à la surveillance et est investi de pouvoirs et attributions suffisants pour exercer un contrôle efficace et permanent (*Klass et autres*, précité, § 56).

276. En ce qui concerne le président, le Parlement et le gouvernement, le droit russe ne définit pas la manière dont ils peuvent contrôler les interceptions. Il n'y a pas de règlements ou d'instructions accessibles au public qui décrivent la portée de leur examen, les conditions dans lesquelles il peut avoir lieu, ou les procédures applicables pour le contrôle des mesures de surveillance ou la réparation des infractions décelées (voir, pour un raisonnement similaire, *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, § 88).

277. Pour ce qui est des procureurs, la Cour observe que le droit national définit la portée et les procédures du contrôle exercé par eux sur les mesures opérationnelles d'investigation (paragraphes 69-80 ci-dessus). Le droit russe indique en effet que les procureurs peuvent soumettre à des inspections systématiques et *ad hoc* les organes mettant en œuvre des mesures opérationnelles d'investigation et qu'ils sont habilités à examiner les documents pertinents, même confidentiels. Ils peuvent prendre des mesures afin de faire cesser ou réparer les infractions à la loi qui ont été décelées et afin qu'une action soit engagée contre leurs auteurs. Ils doivent soumettre au parquet général des rapports semestriels détaillant les résultats des inspections menées. La Cour admet qu'il existe un cadre légal ménageant, en théorie au moins, un certain contrôle des procureurs sur les mesures de surveillance secrète. Il convient ensuite de rechercher si les procureurs sont indépendants des services qui effectuent la surveillance et s'ils sont investis de pouvoirs et attributions suffisants pour exercer un contrôle efficace et permanent.

278. Concernant l'exigence d'indépendance, la Cour a pris en compte dans de précédentes affaires le mode de désignation et le statut juridique des membres de l'organe de contrôle. En particulier, elle a jugé suffisamment indépendants les organes composés de députés – de la majorité comme de l'opposition – ou de personnes possédant les qualifications requises pour

accéder à la magistrature et nommées soit par le parlement soit par le Premier ministre (voir, par exemple, *Klass et autres*, précité, §§ 21 et 56, *Weber et Saravia*, décision précitée, §§ 24-25 et 117, *Leander*, précité, § 65, *L. c. Norvège*, nº 13564/88, décision de la Commission du 8 juin 1990, et *Kennedy*, précité, §§ 57 et 166). En revanche, elle a jugé insuffisamment indépendant un ministre de l'Intérieur qui non seulement était nommé par le pouvoir politique et membre de l'exécutif, mais de plus était directement impliqué dans la commande de moyens spéciaux de surveillance (*Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, §§ 85 et 87) ; elle a conclu de même pour un procureur général et des procureurs de rang inférieur compétents (*Iordachi et autres*, précité, § 47).

279. Contrairement aux organes de contrôle évoqués ci-dessus, les procureurs en Russie sont nommés et révoqués par le procureur général après consultation des autorités exécutives régionales (paragraphe 70 ci-dessus). Ce simple fait est de nature à susciter des doutes quant à leur indépendance à l'égard de l'exécutif.

280. En outre, il est essentiel que le rôle que jouent les procureurs dans la protection des droits de l'homme ne donne lieu à aucun conflit d'intérêts (*Mentchinskaïa c. Russie*, nº 42454/02, §§ 19 et 38, 15 janvier 2009). La Cour observe que les parquets ne sont pas spécialisés dans le contrôle des interceptions (paragraphe 71 ci-dessus). Ce contrôle ne représente qu'une partie de leurs fonctions, lesquelles, étendues et diversifiées, englobent les poursuites et le contrôle des enquêtes pénales. Dans le cadre de leurs fonctions de poursuite, les procureurs approuvent toutes les demandes d'interception déposées par des enquêteurs lors de procédures pénales (paragraphe 44 ci-dessus). Ce mélange de fonctions au sein d'un parquet, où le même service approuve les demandes d'interception puis contrôle la mise en œuvre de l'opération, est lui aussi de nature à faire naître des doutes quant à l'indépendance des procureurs (voir, *a contrario*, *Ananyev et autres c. Russie*, nos 42525/07 et 60800/08, § 215, 10 janvier 2012, affaire concernant le contrôle exercé par les procureurs sur les lieux de détention, dans laquelle la Cour a jugé que les procureurs satisfaisaient à l'exigence d'indépendance à l'égard des organes du système pénitentiaire).

281. S'agissant des pouvoirs et attributions des procureurs, il est essentiel selon la Cour que l'organe de contrôle ait accès à tous les documents pertinents, y compris à des informations confidentielles, et que toutes les personnes participant à des opérations d'interception soient tenues de lui communiquer tous les renseignements qu'il demande (*Kennedy*, précité, § 166). Le droit russe dispose que les procureurs peuvent examiner tout document pertinent, même confidentiel. Il est néanmoins important de noter que les informations sur les agents infiltrés des services de sécurité, de même que sur les tactiques, méthodes et moyens employés par eux, ne relèvent pas du contrôle exercé par les procureurs (paragraphe 74 ci-dessus).

La portée de leur contrôle est donc limitée. De plus, les interceptions opérées par le FSB dans le contexte du contre-renseignement ne peuvent faire l'objet d'une inspection que sur plainte individuelle (paragraphe 76 ci-dessus). Or les particuliers ne se voyant pas notifier les interceptions (paragraphes 81 ci-dessus et 289 ci-dessous), il est peu probable que pareil type de plainte soit jamais déposé. En conséquence, les mesures de surveillance liées au contre-renseignement échappent *de facto* au contrôle des procureurs.

282. Les pouvoirs de l'organe de contrôle relativement aux infractions qu'il peut déceler constituent aussi un aspect important pour l'appréciation de l'effectivité du contrôle qu'il exerce (voir, par exemple, *Klass et autres*, précité, § 53, affaire dans laquelle l'organe d'interception devait cesser immédiatement l'interception si la commission G 10 jugeait cette mesure illégale ou inutile, et *Kennedy*, précité, § 168, affaire où tous les éléments interceptés devaient être détruits dès la découverte du caractère illégal d'une interception par le commissaire chargé des interceptions de communications). La Cour constate que les procureurs disposent de certains pouvoirs en ce qui concerne les infractions à la loi décelées par eux. Ainsi, ils peuvent prendre des mesures afin de faire cesser ou réparer ces infractions et afin qu'une action soit engagée contre leurs auteurs (paragraphe 79 ci-dessus). Toutefois, aucune disposition particulière n'exige la destruction des éléments interceptés de manière illégale (*Kennedy*, précité, § 168).

283. La Cour doit rechercher par ailleurs si les activités de l'organe de contrôle sont ouvertes à un droit de regard du public (voir, par exemple, *L. c. Norvège*, décision précitée, affaire dans laquelle la supervision était exercée par la commission de contrôle, qui rendait compte annuellement au gouvernement et dont les rapports étaient publiés et examinés par le Parlement ; *Kennedy*, précité, § 166, où le contrôle des interceptions était effectué par le commissaire chargé des interceptions de communications, qui chaque année soumettait au Premier ministre un rapport, document public présenté au Parlement ; voir, *a contrario*, *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, § 88, affaire dans laquelle la Cour a critiqué un système en vertu duquel ni le ministre de l'Intérieur ni aucun autre responsable n'étaient tenus de rendre compte régulièrement à un organe indépendant ou aux citoyens au sujet du fonctionnement général du système ou des mesures appliquées dans tel ou tel cas). En Russie, les procureurs doivent soumettre au parquet général des rapports semestriels détaillant les résultats des inspections menées. Or ces rapports concernent tous les types de mesures opérationnelles d'investigation sans distinction, les interceptions n'étant pas traitées séparément des autres mesures. De plus, ces rapports ne contiennent que des informations statistiques sur le nombre d'inspections de mesures opérationnelles d'investigation effectuées et le nombre d'infractions

découvertes, et ils ne précisent pas la nature des infractions ou des mesures prises pour y remédier. Il convient par ailleurs de noter que ces rapports sont des documents confidentiels qui ne sont ni publiés ni d'une autre manière rendus accessibles au public (paragraphe 80 ci-dessus). Il s'ensuit qu'en Russie le contrôle des procureurs n'est pas exercé de façon à permettre droit de regard et information des citoyens.

284. Enfin, la Cour observe que c'est au Gouvernement d'illustrer à l'aide d'exemples appropriés l'effectivité concrète du système de contrôle (voir, *mutatis mutandis*, *Ananyev et autres*, précité, §§ 109-110). Or celui-ci n'a soumis aucun rapport d'inspection ni aucune décision du parquet ayant ordonné l'adoption de mesures destinées à faire cesser ou à réparer une infraction à la loi qui a été décelée. Le Gouvernement n'a donc pas démontré que le contrôle exercé par les procureurs sur les mesures de surveillance secrète était effectif en pratique. À cet égard, la Cour prend acte également des documents soumis par le requérant montrant l'impossibilité pour les procureurs d'avoir accès au matériel classifié relatif à des interceptions (paragraphe 14 ci-dessus). Cet exemple suscite également des doutes quant à l'effectivité en pratique du contrôle exercé par les procureurs.

285. Eu égard aux défaillances susmentionnées et à l'importance particulière que revêt le contrôle dans un système où les services d'application des lois jouissent d'un accès direct à l'ensemble des communications, la Cour estime que, tel qu'il est organisé à l'heure actuelle, le contrôle exercé par les procureurs sur les interceptions n'est pas à même d'offrir des garanties adéquates et effectives contre les abus.

η) Notification de l'interception de communications et recours disponibles

286. La Cour va à présent se pencher sur la question de la notification de l'interception de communications, qui est indissolublement liée à celle de l'effectivité des recours judiciaires (voir la jurisprudence citée au paragraphe 234 ci-dessus).

287. Il peut ne pas être possible en pratique d'exiger une notification *a posteriori* dans tous les cas. L'activité ou le danger qu'un ensemble de mesures de surveillance vise à combattre peut subsister pendant des années, voire des décennies, après la levée de ces mesures. Une notification *a posteriori* à chaque individu touché par une mesure désormais levée risquerait de compromettre le but à long terme qui motivait à l'origine la surveillance. En outre, pareille notification risquerait de contribuer à révéler les méthodes de travail des services de renseignement, leurs champs d'activité et même, le cas échéant, l'identité de leurs agents. Dès lors, l'absence de notification *a posteriori* aux personnes touchées par des mesures de surveillance secrète, dès la levée de celles-ci, ne saurait en soi justifier la conclusion que l'ingérence n'était pas « nécessaire dans une société démocratique », car c'est précisément cette absence d'information

qui assure l'efficacité de la mesure constitutive de l'ingérence. Cependant, il est souhaitable d'aviser la personne concernée après la levée des mesures de surveillance dès que la notification peut être donnée sans compromettre le but de la restriction (*Klass et autres*, précité, § 58, et *Weber et Saravia*, décision précitée, § 135). Par ailleurs, la Cour prend acte de la recommandation du Comité des Ministres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, laquelle dispose que lorsque des données concernant une personne ont été collectées et enregistrées à son insu, elle doit, si les données ne sont pas détruites, être informée, si cela est possible, que des informations sont détenues sur son compte, et ce dès que l'objet des activités de police ne risque plus d'en pâtir (point 2.2, paragraphe 143 ci-dessus).

288. Dans les affaires *Klass et autres* et *Weber et Saravia*, la Cour s'est penchée sur la législation allemande, qui prévoyait que la surveillance soit notifiée dès que possible après sa levée sans que cela en compromette le but. La Cour a tenu compte du fait que c'était une autorité indépendante, la commission G 10, qui avait le pouvoir de décider si une personne faisant l'objet d'une surveillance devait être avisée de cette mesure. Elle a estimé que la disposition pertinente garantissait un système effectif de notification qui contribuait à maintenir l'atteinte au secret des télécommunications dans les limites de ce qui était nécessaire pour atteindre les buts légitimes poursuivis (*Klass et autres*, précité, § 58, et *Weber et Saravia*, décision précitée, § 136). Dans les affaires *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev* et *Dumitru Popescu*, précitées, la Cour a jugé incompatible avec la Convention l'absence d'obligation de donner notification à un stade quelconque à la personne visée par l'interception, au motif que cette absence ôtait à l'intéressé toute possibilité de demander réparation d'une atteinte illégale à ses droits tirés de l'article 8, et rendait les recours offerts par le droit interne théoriques et illusoires et non concrets et effectifs. Elle a ainsi conclu que la législation nationale négligeait d'offrir une garantie importante contre l'utilisation indue de mesures spéciales de surveillance (*Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, §§ 90-91, et *Dumitru Popescu*, précité, § 77). Dans l'affaire *Kennedy*, au contraire, elle a dit que l'absence d'obligation de donner notification à un stade quelconque à la personne visée par l'interception était compatible avec la Convention du fait qu'au Royaume-Uni toute personne soupçonnant que ses communications faisaient ou avaient fait l'objet d'interceptions pouvait saisir la commission des pouvoirs d'enquête puisque la compétence de celle-ci n'était pas subordonnée à une notification de l'interception (*Kennedy*, précité, § 167).

289. Pour en venir aux circonstances de l'espèce, la Cour observe qu'en Russie les personnes dont les communications ont été interceptées ne reçoivent à aucun moment ni en aucune circonstance notification de cette

mesure. Il s'ensuit que, à moins qu'une procédure pénale ait été déclenchée contre le sujet de l'interception et que les données interceptées aient servi d'éléments de preuve, ou à moins d'une indiscrétion, il est peu probable que la personne concernée apprenne un jour qu'il y a eu interception de ses communications.

290. La Cour prend acte du fait qu'une personne ayant appris d'une manière ou d'une autre que ses communications ont été interceptées peut demander des informations sur les données correspondantes (paragraphe 81 ci-dessus). À cet égard, il convient de noter que pour pouvoir former pareille demande la personne concernée doit avoir connaissance de faits touchant aux mesures opérationnelles d'investigation dont elle a été l'objet. L'accès aux informations est donc subordonné à la capacité de l'intéressé à prouver qu'il y a eu interception de ses communications. En outre, le sujet de l'interception n'a pas de droit d'accès aux documents relatifs à l'interception de ses communications ; il peut, au mieux, recevoir « des informations » sur les données recueillies. Ces informations ne sont fournies que dans des cas très limités, à savoir lorsque la culpabilité de l'intéressé n'a pas été établie selon les voies légales, c'est-à-dire qu'il n'a pas été inculpé ou que les accusations ont été abandonnées au motif que l'infraction alléguée n'avait pas été commise ou qu'un ou plusieurs éléments constitutifs d'une infraction pénale faisaient défaut. Il convient également de noter que seules des informations ne contenant pas de secrets d'État peuvent être divulguées à la personne visée par l'interception et qu'en droit russe les informations relatives aux installations utilisées pour la mise en œuvre de mesures opérationnelles d'investigation, aux méthodes employées, aux agents qui sont intervenus et aux données recueillies constituent un secret d'État (paragraphe 52 ci-dessus). Eu égard à ces particularités du droit russe, la possibilité d'obtenir des informations sur des interceptions apparaît ineffective.

291. Pour apprécier l'effectivité des voies de recours offertes par le droit russe, la Cour gardera à l'esprit les éléments ci-dessus, à savoir l'absence de notification et le défaut de possibilité effective de demander et d'obtenir auprès des autorités des informations sur les interceptions.

292. Selon le droit russe, une personne estimant que ses droits ont été ou sont violés par un agent de l'État à l'occasion de la mise en œuvre de mesures opérationnelles d'investigation peut adresser une plainte au supérieur hiérarchique de cet agent, à un procureur ou à un tribunal (paragraphe 83 ci-dessus). La Cour rappelle qu'un recours hiérarchique auprès d'un supérieur direct de l'autorité dont les actes sont contestés ne répond pas aux critères d'indépendance requis pour pouvoir constituer une protection suffisante contre l'abus de pouvoir (voir, pour un raisonnement similaire, *Khan c. Royaume-Uni*, n° 35394/97, §§ 45-47, CEDH 2000-V, *Dumitru Popescu*, précité, § 72, et *Avanesyan*, précité, § 32). Par ailleurs, un procureur manque d'indépendance et la portée de son contrôle est limitée,

comme cela a été établi précédemment (paragraphes 277-285 ci-dessus). Il reste à déterminer si une plainte auprès d'un tribunal peut passer pour un recours effectif.

293. Une personne qui souhaite se plaindre de l'interception de ses communications dispose selon le Gouvernement de quatre types d'actions judiciaires : l'appel, le pourvoi en cassation ou la requête en supervision contre la décision judiciaire ayant autorisé l'interception des communications ; la demande de contrôle juridictionnel fondée sur l'article 125 du CPP ; la demande de contrôle juridictionnel basée sur la loi sur le contrôle juridictionnel et le chapitre 25 du CPC ; l'action en responsabilité fondée sur l'article 1069 du code civil. La Cour examinera ces recours l'un après l'autre.

294. La première voie de droit évoquée par le Gouvernement est celle de l'appel, du pourvoi en cassation ou de la requête en supervision contre la décision judiciaire ayant autorisé l'interception de communications. Or la Cour constitutionnelle a indiqué clairement que la personne objet d'une interception de communications ne pouvait pas interjeter appel de l'autorisation judiciaire en question (paragraphe 40 ci-dessus ; voir aussi *Avanesyan*, précité, § 30). Par ailleurs, le droit interne ne dit rien de la possibilité de former un pourvoi en cassation. Le Gouvernement n'ayant pas fourni d'exemple de la pratique interne en matière d'examen de pourvois en cassation, la Cour a de sérieux doutes quant à l'existence d'un droit de former un tel pourvoi contre une décision judiciaire autorisant l'interception de communications. En revanche, il est manifestement loisible au sujet de l'interception de déposer une requête en supervision (paragraphe 43 ci-dessus). Encore faut-il, pour pouvoir attaquer par ce biais l'autorisation judiciaire d'intercepter ses communications, que l'intéressé connaisse l'existence d'une telle décision. Bien que la Cour constitutionnelle ait dit qu'il n'était pas nécessaire de joindre à la requête en supervision une copie de la décision judiciaire contestée (*ibidem*), on voit mal comment une personne pourrait former un tel recours sans disposer d'un minimum d'informations sur la décision qu'elle conteste, par exemple sa date d'adoption et la juridiction dont elle émane. Sachant que le droit russe ne prévoit pas la notification des mesures de surveillance, un particulier ne pourra quasiment jamais être en mesure d'obtenir ces informations ; il ne le pourra que si elles sont révélées dans le cadre d'une procédure pénale dirigée contre lui ou si une indiscrétion a abouti à leur divulgation.

295. En outre, seule une personne participant à une procédure pénale alors que l'instruction est en cours peut former une plainte fondée sur l'article 125 du CPP (paragraphes 88-89 ci-dessus). Ce recours n'est donc ouvert qu'à une personne ayant découvert dans le cadre de poursuites contre elle qu'il y avait eu interception de ses communications. Il ne peut pas être exercé par une personne contre laquelle aucune procédure pénale n'a été déclenchée après interception de ses communications et qui ignore si ses

communications ont fait l'objet d'une telle mesure. Il est à noter également que le Gouvernement n'a présenté aucune décision judiciaire relative à l'examen d'une plainte fondée sur l'article 125 du CPP pour dénoncer l'interception de communications. Il n'a donc pas démontré, à l'aide d'exemples tirés de la jurisprudence interne, l'effectivité concrète du recours évoqué par lui (voir, pour un raisonnement similaire, *Rotaru*, précité, § 70, et *Ananyev et autres*, précité, §§ 109-110).

296. Pour ce qui est de la demande de contrôle juridictionnel fondée sur la loi sur le contrôle juridictionnel, le chapitre 25 du CPC et le nouveau code de procédure administrative, et de l'action en responsabilité basée sur l'article 1069 du code civil, il convient de noter que c'est au demandeur de prouver que l'interception a eu lieu et qu'il y a eu à cette occasion violation de ses droits (paragraphes 85, 95-96 et 105 ci-dessus). En l'absence de notification ou d'une forme quelconque d'accès aux documents officiels concernant les interceptions, cette preuve est quasiment impossible à apporter. Du reste, le requérant a en l'espèce été débouté de son action par les juridictions internes pour n'avoir pas démontré que ses communications téléphoniques avaient été interceptées (paragraphes 11 et 13 ci-dessus). La Cour relève que le Gouvernement a présenté diverses décisions judiciaires rendues sur le fondement du chapitre 25 du CPC ou de l'article 1069 du code civil (paragraphes 220-223 ci-dessus). Or toutes ces décisions, sauf une, portent sur des perquisitions ou des saisies de documents ou d'objets, c'est-à-dire des mesures opérationnelles d'investigation effectuées au su de la personne concernée. Seule l'une de ces décisions a trait à l'interception de communications : dans l'affaire en question, la personne visée avait pu apporter la preuve voulue parce qu'elle avait eu connaissance de la mesure d'interception au cours de la procédure pénale dirigée contre elle.

297. La Cour prend note également de l'argument du Gouvernement selon lequel le droit russe comporte des voies de droit pénal permettant de se plaindre d'un abus de pouvoir, de la collecte ou de la diffusion non autorisées d'informations sur la vie privée et familiale d'une personne, ou d'une atteinte au droit du citoyen au respect du caractère privé de ses communications. Pour les raisons exposées dans les paragraphes qui précèdent, ces recours sont également ouverts uniquement aux personnes qui sont à même de soumettre aux services de poursuite au moins quelques informations factuelles sur l'interception de leurs communications (paragraphe 24 ci-dessus).

298. La Cour déduit de ce qui précède que les recours évoqués par le Gouvernement sont ouverts uniquement aux personnes qui disposent d'informations relatives à l'interception de leurs communications. L'effectivité de ces recours est donc compromise par l'absence d'obligation de donner notification à un stade quelconque à la personne visée par l'interception, et par l'inexistence d'une possibilité satisfaisante de demander et d'obtenir auprès des autorités des informations sur les

interceptions. La Cour estime en conséquence que le droit russe n'offre pas de recours judiciaire effectif contre les mesures de surveillance secrète dans les cas où une procédure pénale n'a pas été engagée contre le sujet de l'interception. Il ne lui appartient pas en l'espèce de déterminer si les recours en question peuvent être effectifs dans la situation où un particulier apprend lors d'une procédure pénale dirigée contre lui qu'il y a eu interception de ses communications (voir, cependant, *Avanesyan*, précité, affaire dans laquelle certains de ces recours ont été jugés ineffectifs alors qu'il s'agissait pour le requérant de se plaindre de l'« inspection » de son appartement).

299. Concernant pour finir les recours judiciaires permettant de se plaindre d'une insuffisance des garanties prévues en droit russe contre les abus, la Cour n'est pas convaincue par l'argument du Gouvernement selon lequel ces recours sont effectifs (paragraphes 156 et 225 ci-dessus). S'agissant de la possibilité de mettre en cause la LMOI devant la Cour constitutionnelle, la Cour observe que la haute juridiction a maintes fois examiné la constitutionnalité de cette loi, qu'elle a jugée compatible avec la Constitution (paragraphes 40-43, 50, 82 et 85-87 ci-dessus). Dans ces conditions, la Cour estime peu probable qu'une plainte du requérant auprès de la Cour constitutionnelle soulevant des points identiques à ceux déjà examinés par elle aurait des chances d'aboutir. Elle n'est pas convaincue non plus qu'une mise en cause de l'arrêté n° 70 devant la Cour suprême ou les juridictions inférieures constituerait un recours effectif. En effet, le requérant a bien attaqué l'arrêté n° 70 dans le cadre de la procédure interne ; or, tant le tribunal de district que le tribunal de Saint-Pétersbourg ont conclu que l'intéressé n'avait pas qualité pour contester cet arrêté, au motif que le dispositif installé en application de ce texte ne portait pas en soi atteinte au caractère privé de ses communications (paragraphes 10-11 et 13 ci-dessus). Il est à noter également que la Cour suprême a estimé que l'arrêté n° 70 avait un caractère technique et non juridique (paragraphe 128 ci-dessus).

300. Eu égard aux considérations qui précèdent, la Cour conclut que le droit russe n'offre pas de recours effectif à une personne qui pense avoir fait l'objet d'une surveillance secrète. En privant la personne visée par l'interception de la possibilité effective de contester rétrospectivement des mesures d'interception, le droit russe néglige d'offrir une importante garantie contre l'utilisation indue de mesures de surveillance secrète.

301. Pour les raisons exposées ci-dessus, la Cour rejette également l'exception de non-épuisement des voies de recours internes formulée par le Gouvernement.

θ) Conclusion

302. La Cour conclut que les dispositions du droit russe régissant l'interception de communications ne comportent pas de garanties adéquates et effectives contre l'arbitraire et le risque d'abus inhérent à tout système de

surveillance secrète, risque qui est particulièrement élevé dans un système où les services secrets et la police jouissent grâce à des moyens techniques d'un accès direct à l'ensemble des communications de téléphonie mobile. Plus particulièrement, les circonstances dans lesquelles les pouvoirs publics sont habilités à recourir à des mesures de surveillance secrète ne sont pas définies de façon suffisamment claire. Les dispositions sur la levée des mesures de surveillance secrète ne fournissent pas de garanties suffisantes contre les ingérences arbitraires. Le droit interne autorise la conservation automatique de données manifestement dénuées de pertinence et manque de clarté quant aux circonstances dans lesquelles les éléments interceptés doivent être conservés ou détruits après le procès. Les procédures d'autorisation ne sont pas à même de garantir que les mesures de surveillance secrète ne soient ordonnées que lorsque cela est « nécessaire dans une société démocratique ». Le contrôle des interceptions tel qu'il est organisé à l'heure actuelle ne satisfait pas aux exigences relatives à l'indépendance, à l'existence de pouvoirs et attributions suffisants pour exercer un contrôle efficace et permanent, au droit de regard du public et à l'effectivité en pratique. L'effectivité des recours est compromise par l'absence de notification des interceptions à un stade quelconque, ou d'un accès approprié aux documents relatifs aux interceptions.

303. Il est important d'observer que les défaillances du cadre juridique relevées ci-dessus paraissent avoir un impact sur la mise en œuvre concrète du système de surveillance secrète en place en Russie. La Cour n'est pas convaincue par l'affirmation du Gouvernement selon laquelle toutes les interceptions qui sont opérées en Russie le sont en toute légalité et en vertu d'une autorisation judiciaire en bonne et due forme. Les exemples présentés par le requérant lors de la procédure interne (paragraphe 12 ci-dessus) et de la procédure menée devant la Cour (paragraphe 197 ci-dessus) indiquent l'existence de pratiques de surveillance arbitraires et abusives, lesquelles paraissent dues à l'insuffisance des garanties offertes par la loi (voir, pour un raisonnement similaire, *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, § 92 ; voir aussi, *a contrario*, *Klass et autres*, précité, § 59, et *Kennedy*, précité, §§ 168-169).

304. Eu égard aux défaillances relevées ci-dessus, la Cour juge que le droit russe ne satisfait pas à l'exigence relative à la « qualité de la loi » et n'est pas à même de limiter l'« ingérence » à ce qui est « nécessaire dans une société démocratique ».

305. Dès lors, il y a eu violation de l'article 8 de la Convention.

II. SUR LA VIOLATION ALLÉGUÉE DE L'ARTICLE 13 DE LA CONVENTION

306. Le requérant se plaint de ne pas disposer d'un recours effectif qui lui permettrait de faire valoir son grief fondé sur l'article 8. Il invoque l'article 13 de la Convention, ainsi libellé :

> « Toute personne dont les droits et libertés reconnus dans la (...) Convention ont été violés, a droit à l'octroi d'un recours effectif devant une instance nationale, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles. »

307. Compte tenu de la conclusion à laquelle elle est parvenue au sujet de l'article 8 de la Convention (paragraphes 286-300 ci-dessus), la Cour estime qu'il n'y a pas lieu d'examiner séparément le grief tiré de l'article 13, bien qu'il soit étroitement lié à celui fondé sur l'article 8 et doive donc être déclaré recevable (*Liberty et autres*, précité, § 73).

III. SUR L'APPLICATION DE L'ARTICLE 41 DE LA CONVENTION

308. Aux termes de l'article 41 de la Convention,

> « Si la Cour déclare qu'il y a eu violation de la Convention ou de ses Protocoles, et si le droit interne de la Haute Partie contractante ne permet d'effacer qu'imparfaitement les conséquences de cette violation, la Cour accorde à la partie lésée, s'il y a lieu, une satisfaction équitable. »

A. Dommage

309. Le requérant demande 9 000 euros (EUR) pour préjudice moral.

310. Le Gouvernement estime cette demande excessive dès lors que, selon lui, le requérant a contesté le droit russe *in abstracto*, sans être aucunement touché par celui-ci à titre personnel. À son avis, le constat d'une violation fournirait donc une satisfaction équitable suffisante.

311. La Cour rappelle que, dans le cadre de l'exécution d'un arrêt en application de l'article 46 de la Convention, un arrêt constatant une violation de la Convention ou de ses Protocoles entraîne pour l'État défendeur l'obligation juridique non seulement de verser aux intéressés les sommes allouées à titre de satisfaction équitable, mais aussi de choisir, sous le contrôle du Comité des Ministres, les mesures générales et/ou, le cas échéant, individuelles à adopter dans son ordre juridique interne afin de mettre un terme à la violation constatée par la Cour et d'en effacer dans la mesure du possible les conséquences de manière à rétablir autant que faire se peut la situation antérieure à celle-ci. En outre, en ratifiant la Convention les États contractants s'engagent à faire en sorte que leur droit interne soit compatible avec celle-ci (*Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, précité, § 111, avec d'autres références).

312. La Cour considère que le constat de violation représente une satisfaction équitable suffisante pour tout préjudice moral causé au requérant.

B. Frais et dépens

313. Devant la chambre, le requérant a demandé 26 579 roubles russes (RUB) (environ 670 EUR à la date du dépôt de la demande) pour frais de poste et de traduction. À l'appui il a fourni des factures relatives à des services de poste et de télécopie ainsi qu'un contrat de traduction.

314. Devant la Grande Chambre, l'intéressé réclame 22 800 livres sterling (GBP) (environ 29 000 EUR à la date du dépôt de la demande) et 13 800 EUR au titre des honoraires d'avocats. Il se fonde sur des relevés d'heures de travail de ses avocats. Se référant à des factures, il demande également 6 833,24 GBP (environ 8 700 EUR à la date du dépôt de la demande) en remboursement de frais de traduction et de voyage ainsi que d'autres frais administratifs.

315. Le Gouvernement accepte la demande relative aux frais et dépens présentée devant la chambre dès lors qu'elle est étayée par des justificatifs. Concernant les prétentions pour frais et dépens soumises à la Grande Chambre, il avance qu'elles ont été présentées plus de un mois après l'audience. Pour ce qui est des honoraires d'avocats, une partie de ceux-ci recouvriraient le travail effectué par les représentants avant signature par le requérant d'un formulaire de pouvoir et il n'y aurait aucun pouvoir établi au nom de M^me^ Levine. En outre, le nombre de représentants et le nombre d'heures consacrées par eux à la préparation du dossier seraient excessifs. Du reste, rien ne prouverait que le requérant ait payé ou soit tenu de payer les honoraires en question en vertu d'une obligation légale ou contractuelle. Quant aux frais de traduction et autres frais administratifs, le Gouvernement soutient que le requérant n'a soumis aucun document montrant qu'il aurait versé les montants indiqués. Il n'aurait pas non plus établi la nécessité des frais de traduction, certains de ses avocats parlant russe d'après le Gouvernement. Enfin, les tarifs demandés par les traducteurs seraient exagérés, de même que les frais de voyage.

316. Selon la jurisprudence de la Cour, un requérant ne peut obtenir le remboursement de ses frais et dépens que dans la mesure où se trouvent établis leur réalité, leur nécessité et le caractère raisonnable de leur taux. En l'espèce, compte tenu des pièces en sa possession et des critères ci-dessus, la Cour juge raisonnable d'accorder au requérant la somme de 40 000 EUR, tous frais confondus, plus tout montant pouvant être dû par lui à titre d'impôt.

C. Intérêts moratoires

317. La Cour juge approprié de calquer le taux des intérêts moratoires sur le taux d'intérêt de la facilité de prêt marginal de la Banque centrale européenne majoré de trois points de pourcentage.

PAR CES MOTIFS, LA COUR

1. *Joint au fond*, à l'unanimité, les exceptions préliminaires de défaut de qualité de victime et de non-épuisement des voies de recours internes formulées par le Gouvernement, et *déclare* la requête recevable ;

2. *Dit*, à l'unanimité, qu'il y a eu violation de l'article 8 de la Convention, et *rejette* les exceptions du Gouvernement susmentionnées ;

3. *Dit*, à l'unanimité, qu'il n'y a pas lieu d'examiner le grief tiré de l'article 13 de la Convention ;

4. *Dit*, par seize voix contre une, que le constat d'une violation représente en soi une satisfaction équitable suffisante pour tout dommage moral pouvant avoir été subi par le requérant ;

5. *Dit*, à l'unanimité,
   a) que l'État défendeur doit verser au requérant, dans les trois mois, 40 000 EUR (quarante mille euros), plus tout montant pouvant être dû à titre d'impôt par le requérant, pour frais et dépens ;
   b) qu'à compter de l'expiration dudit délai et jusqu'au versement, ce montant sera à majorer d'un intérêt simple à un taux égal à celui de la facilité de prêt marginal de la Banque centrale européenne applicable pendant cette période, augmenté de trois points de pourcentage ;

6. *Rejette*, à l'unanimité, la demande de satisfaction équitable pour le surplus.

Fait en français et en anglais, puis prononcé en audience publique au Palais des droits de l'homme, à Strasbourg, le 4 décembre 2015.

Lawrence Early Jurisconsulte	Dean Spielmann Président

Au présent arrêt se trouve joint, conformément aux articles 45 § 2 de la Convention et 74 § 2 du règlement, l'exposé des opinions séparées suivantes :

– opinion concordante du juge Dedov ;
– opinion en partie dissidente de la juge Ziemele.

D.S.
T.L.E.

OPINION CONCORDANTE DU JUGE DEDOV

(Traduction)

1. Compétence de la Cour pour examiner le droit interne *in abstracto*

Comme le souligne le Gouvernement, il peut y avoir des doutes quant à la compétence de la Cour pour examiner la qualité et l'effectivité du droit interne *in abstracto* sans qu'ait été établie la qualité de victime du requérant ni vérifiée l'existence d'une atteinte à son droit au respect de sa vie privée en pratique, et non pas simplement en théorie.

La Cour a déjà suivi cette approche dans des affaires d'interception, en vue de la prévention d'éventuels abus de pouvoir. Dans deux affaires importantes, *Kennedy c. Royaume-Uni* (nº 26839/05, §§ 122-123, 18 mai 2010) et *Klass et autres c. Allemagne* (6 septembre 1978, § 34, série A nº 28), qui étaient dirigées contre deux grands États démocratiques – le Royaume-Uni et la République fédérale d'Allemagne –, la Cour a confirmé l'effectivité des systèmes nationaux en cause pour lutter contre l'arbitraire. Cependant, et c'est regrettable, nous ne pouvons ignorer le fait que ces deux États ont été touchés récemment par des scandales retentissants liés à la surveillance : dans un cas, les conversations de téléphonie mobile de la chancelière fédérale allemande avaient été interceptées illégalement par les services secrets nationaux ; dans l'autre, les autorités du Royaume-Uni avaient fourni aux services secrets américains des informations et accès relatifs à toute la base de données des communications du premier État, permettant ainsi aux autorités américaines d'intercepter les communications de tout citoyen britannique sans être soumis à aucune garantie interne adéquate.

Cela montre que, dès le départ, quelque chose était vicié dans l'approche de la Cour. Peut-être serait-il plus efficace de traiter les requêtes au cas par cas, de sorte que la Cour ait la possibilité d'établir l'existence d'une ingérence et de conclure – comme elle le fait régulièrement au sujet de fouilles injustifiées dans les locaux de requérants – à la violation de la Convention. De manière générale, le problème dans ces affaires ne concerne pas les pouvoirs des juridictions internes en matière d'autorisation, mais la façon dont les juges autorisent les fouilles à des fins d'enquête.

L'approche de la Cour peut facilement glisser de l'application effective de la loi à l'ingérence potentielle. En témoignent l'affaire *Kennedy* :

> « 119. Selon la jurisprudence constante de la Cour, celle-ci n'a pas pour tâche d'examiner *in abstracto* la législation et la pratique pertinentes, mais de rechercher si la manière dont elles ont été appliquées au requérant ou l'ont touché a enfreint la Convention (voir, entre autres, *Klass et autres*, précité, § 33 ; *N.C. c. Italie* [GC], nº 24952/94, § 56, CEDH 2002-X ; et *Krone Verlag GmbH & Co. KG c. Autriche (nº 4)*, nº 72331/01, § 26, 9 novembre 2006) » ;

et l'affaire *Klass et autres* :

> « 36. (...) La Cour ne saurait admettre que l'assurance de bénéficier d'un droit garanti par la Convention puisse être ainsi supprimée du simple fait de maintenir l'intéressé dans l'ignorance de sa violation. Un droit de recours à la Commission pour les personnes potentiellement touchées par une surveillance secrète découle de l'article 25, faute de quoi l'article 8 risquerait de perdre toute portée. »

Les scandales allemand et anglais évoqués ci-dessus confirment cependant que tôt ou tard la personne concernée découvre l'interception. On trouve des exemples en ce sens dans le contexte russe (*Shimovolos c. Russie*, nº 30194/09, 21 juin 2011). Le requérant dans la présente affaire n'a pas connaissance d'une quelconque interception de ses communications, et c'est là un fait que la Cour ne saurait ignorer.

La Cour a maintes fois évité d'examiner des affaires *in abstracto* (*Silver et autres c. Royaume-Uni*, 25 mars 1983, § 79, série A nº 61, *Nikolova c. Bulgarie* [GC], nº 31195/96, § 60, CEDH 1999-II, *Nejdet Şahin et Perihan Şahin c. Turquie* [GC], nº 13279/05, §§ 68-70, 20 octobre 2011, *Sabanchiyeva et autres c. Russie*, nº 38450/05, § 137, CEDH 2013, et *Monnat c. Suisse*, nº 73604/01, §§ 31-32, CEDH 2006-X). On peut donc présumer que les affaires d'interception sont singulières. Il nous faut alors connaître les raisons pour lesquelles la Cour devrait changer d'approche générale dans l'examen de telles affaires. Nous n'avons cependant aucune idée de ce que peuvent être ces raisons. Si la législation crée un risque d'arbitraire, alors il nous faut voir le résultat de cet arbitraire. Je ne suis pas sûr que quelques exemples (sans rapport avec la cause du requérant) suffisent à établir que l'ensemble du système de garanties doit être révisé et renforcé. J'accepterais pareille approche si la Cour avait un énorme arriéré de requêtes individuelles répétitives montrant que l'arrêté nº 70 (sur la connexion d'un dispositif d'interception aux réseaux d'opérateurs) n'est pas à caractère technique mais qu'il crée un problème structurel en Russie. Si tel était le cas, nous aurions toutefois besoin d'une procédure et d'un arrêt pilotes.

Toutes les affaires où la Cour a formulé un constat de violation (plus de 15 000 arrêts) reposent sur l'abus de pouvoir, même lorsque la législation interne est de bonne qualité. Tout abus de pouvoir est une question d'éthique, et on ne peut l'éliminer au moyen des seules mesures législatives.

Selon la jurisprudence constante de la Cour, celle-ci n'a pas pour tâche d'examiner dans l'abstrait la législation et la pratique internes ou d'exprimer un point de vue sur la compatibilité des dispositions législatives avec la Convention, mais de rechercher si la manière dont elles ont été appliquées au requérant ou l'ont touché a donné lieu à une violation de la Convention (voir, notamment, dans le contexte de l'article 14, *Religionsgemeinschaft der Zeugen Jehovas et autres c. Autriche*, nº 40825/98, § 90, 31 juillet 2008).

L'article 34 de la Convention n'institue pas au profit des particuliers une sorte d'*actio popularis* pour l'interprétation de la Convention ; il ne les autorise pas à se plaindre *in abstracto* d'une loi par cela seul qu'elle leur semble enfreindre la Convention. En principe, il ne suffit pas à un individu requérant de soutenir qu'une loi viole par sa simple existence les droits dont il jouit aux termes de la Convention ; elle doit avoir été appliquée à son détriment (*Klass et autres*, précité, § 33). Ces principes ne devraient pas être appliqués de façon arbitraire.

2. Organe parlementaire et organe judiciaire : la Cour doit respecter les différences

Cette affaire est très importante du point de vue de la séparation des fonctions entre la Cour et l'Assemblée parlementaire du Conseil de l'Europe ; il faut en effet séparer les pouvoirs de l'organe parlementaire et de l'organe judiciaire. L'Assemblée parlementaire adopte des recommandations, des résolutions et des avis qui font office de lignes directrices pour le Comité des Ministres, les gouvernements nationaux, les parlements et les partis politiques. En définitive, par le biais des conventions, de la législation et de la pratique, le Conseil de l'Europe agit en faveur des droits de l'homme, de la démocratie et de la prééminence du droit. Il suit les progrès des États membres dans ces domaines et formule des recommandations par l'intermédiaire d'organes de surveillance spécialisés et indépendants. La Cour européenne des droits de l'homme statue sur les requêtes individuelles ou étatiques dans lesquelles on allègue la violation de droits civils et politiques consacrés par la Convention européenne des droits de l'homme. Compte tenu de cette séparation des fonctions, l'examen d'une affaire *in abstracto* s'apparente à une expertise et non à un arrêt.

Morten Kjaerum, directeur de l'Agence des droits fondamentaux de l'Union européenne, s'est exprimé comme suit lors d'un débat conjoint sur les droits fondamentaux qui a eu lieu le 4 septembre 2014 au sein de la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen (traduction du greffe) :

> « Les révélations de Snowden sur la surveillance de masse ont mis en exergue le fait que la protection des données personnelles se trouve menacée. La protection du droit à la vie privée est loin d'être suffisante si l'on examine l'ensemble de l'Europe aujourd'hui. À la suite des débats de l'année dernière, nous accueillons de manière très favorable la demande du Parlement européen adressée à l'Agence des droits fondamentaux afin que celle-ci continue à se pencher sur les droits fondamentaux et les garanties en place dans le cadre des vastes programmes de surveillance. Bien sûr vous serez informés, probablement vers la fin de l'année, des conclusions de cette demande particulière.
>
> Mais il ne s'agit pas uniquement des grands programmes de surveillance. Il y a aussi une suspicion à l'égard des mécanismes de surveillance dans le domaine de la

> protection générale des données. [En effet,] nous confions des données aux services de santé, à l'administration fiscale ou à d'autres organes, publics ou privés. Les travaux de l'Agence des droits fondamentaux montrent qu'à l'heure actuelle les structures nationales de surveillance au sein de l'Union européenne sont trop faibles pour remplir leur mission. Les autorités chargées de la protection des données qui sont en place dans chaque État membre ont un rôle important à jouer dans la mise en œuvre du système global de protection des données, mais il faut d'urgence renforcer les pouvoirs et ressources des autorités nationales de protection des données, et également garantir l'indépendance de ces autorités.
>
> Enfin, je tiens à souligner que les entités chargées de la conservation des données – publiques ou privées –, les institutions, doivent être tenues de rendre des comptes, et ce de manière bien plus forte que ce que nous voyons aujourd'hui, si les garanties qu'elles créent ne sont pas suffisantes. »

Ces remarques s'adressaient aux membres nouvellement élus du Parlement européen (et non aux juges) et soulevaient des questions qui préoccupent toute l'Europe et exigent un système de protection des données plus sophistiqué. L'objet du discours était de lancer un débat public en vue de définir des mesures effectives et d'œuvrer en faveur de véritables normes éthiques pour la société ; or une enceinte judiciaire n'est pas un lieu adéquat pour un tel débat.

J'ai tendance à penser que la Cour ferait mieux de se concentrer sur telle ou telle ingérence et sur l'effectivité de la mesure en place afin de prévenir la violation en question (comme elle le fait d'habitude dans toute autre catégorie d'affaires). La tâche essentielle de la Cour est d'établir qu'une ingérence s'est produite puis de rechercher si cette ingérence était prévue par la loi et nécessaire dans une société démocratique. Sur le plan éthique, il est inacceptable que des juges, sans connaître les faits, présument que tout citoyen d'un pays donné pourrait être soumis à une surveillance secrète illégale. Un arrêt ne saurait être bâti sur des allégations.

La Cour a utilisé de nombreux outils pour combattre les violations. L'un d'eux a consisté à conclure à la violation de l'article 10 en raison du refus d'un service de renseignement de fournir à l'organisation requérante des informations sur des personnes placées sous surveillance électronique pendant une période donnée (*Youth Initiative for Human Rights c. Serbie*, n° 48135/06, 25 juin 2013). Dans le dispositif de l'arrêt en question, la Cour a invité le Gouvernement à veiller à ce que les informations réclamées fussent mises à la disposition de l'organisation requérante (sans attendre que des mesures fussent proposées par le Comité des Ministres). Je vois dans cette démarche une mesure effective en même temps qu'une réussite judiciaire.

3. L'approche de la « probabilité raisonnable » doit être développée

Établir la qualité de victime du requérant fait partie intégrante du processus judiciaire. L'article 34 de la Convention dispose que « [l]a Cour

peut être saisie d'une requête par toute personne physique, toute organisation non gouvernementale ou tout groupe de particuliers qui se prétend victime d'une violation par l'une des Hautes Parties contractantes des droits reconnus dans la Convention ou ses Protocoles ». La notion de « victime » n'implique pas l'existence d'un préjudice (*Brumărescu c. Roumanie* [GC], nº 28342/95, § 50, CEDH 1999-VII).

La Cour a déjà jugé que, si l'existence d'un régime de surveillance peut porter atteinte à la vie privée, une plainte selon laquelle cela a engendré la violation de droits ne peut être portée en justice que s'il y a une « probabilité raisonnable » qu'une personne a effectivement fait l'objet d'une surveillance illégale (*Esbester c. Royaume-Uni*, nº 18601/91, décision de la Commission du 2 avril 1993, non publiée, *Redgrave c. Royaume-Uni*, nº 20271/92, décision de la Commission du 1er septembre 1993, non publiée, et *Matthews c. Royaume-Uni*, nº 28576/95, décision de la Commission du 16 octobre 1996, non publiée). Ces références concernent des décisions déclarées irrecevables, toutes les allégations d'interception ayant été jugées manifestement dénuées de fondement.

Toutefois, la Cour a totalement modifié son approche dans l'affaire *Kennedy* : « l'on ne peut exclure que des mesures de surveillance secrète (...) ont été appliquées [au requérant] ou qu'il courait (...) le risque de subir pareilles mesures » (*Kennedy*, précité, §§ 125-129). Nous voyons aujourd'hui que ce changement dans la jurisprudence n'a pas été effectif.

La formule « probabilité raisonnable » implique l'existence de conséquences négatives pour un requérant qui est potentiellement exposé à une surveillance secrète, en raison de certaines informations qui sont mises à la disposition des autorités par le biais de l'interception, et exclut la possibilité que ces informations puissent être découvertes par d'autres moyens. La Cour a rendu cette approche dangereusement simple pour examiner ces affaires au fond, présumant que, puisque des personnes soumises à une surveillance secrète des autorités ne sont pas toujours informées par la suite de ces mesures prises à leur égard, il est donc impossible pour les requérants de montrer qu'il y a eu atteinte à l'un quelconque de leurs droits. La Cour a dès lors conclu qu'il fallait considérer que les requérants étaient en droit d'introduire une requête même s'ils ne pouvaient établir leur qualité de victime. Les requérants dans les affaires *Klass et autres* et *Liberty et autres c. Royaume-Uni* (nº 58243/00, 1er juillet 2008) étaient avocats et il n'était pas exclu qu'ils eussent fait « l'objet d'une surveillance secrète à raison des contacts qu'ils [pouvaient] avoir avec des clients soupçonnés d'activités [illégales] » (*Klass et autres*, précité, § 27).

Dans l'affaire *Kennedy*, le requérant alléguait la non-réception d'appels locaux et la réception d'appels qui ne lui étaient pas destinés et qui lui faisaient perdre du temps. D'après l'intéressé, ces dysfonctionnements étaient dus à des interceptions de sa correspondance ainsi que de ses communications téléphoniques et électroniques ; la Cour a pris cela au

sérieux, rejetant les objections du Gouvernement selon lesquelles le requérant n'avait pas démontré qu'il y avait eu ingérence au sens de l'article 8, ni établi l'existence d'une probabilité raisonnable. La Cour a également rejeté les arguments relatifs au non-épuisement des voies de recours internes, en dépit du fait que le requérant n'avait pas vérifié auprès de son opérateur la qualité des services de télécommunication mais avait adressé au MI5 et au GCHQ – les services de renseignement britanniques chargés de la sûreté nationale – une demande de communication de ses données personnelles fondée sur la loi de 1998 sur la protection des données.

Pour en revenir aux circonstances de l'espèce, on peut raisonnablement conclure que l'interconnexion entre les équipements de télécommunication et le dispositif d'interception ne signifie pas nécessairement qu'il y a réellement eu interception des conversations téléphoniques du requérant. La Cour ne peut pas non plus fonder ses conclusions sur la présomption de « l'éventualité de l'action irrégulière d'un fonctionnaire malhonnête, négligent ou trop zélé » (*Klass et autres*, §§ 49-50 et 59, *Weber et Saravia c. Allemagne* (déc.), nº 54934/00, § 106, CEDH 2006-XI, et *Kennedy*, précité, §§ 153-154). De même, elle ne peut pas présumer de façon générale (pour examiner l'affaire *in abstracto*) l'existence d'une violence étatique visant les mouvements d'opposition et d'autres institutions démocratiques de l'État défendeur, même si l'Assemblée parlementaire a adopté des résolutions à ce sujet. La Cour doit rester impartiale et neutre.

4. Le rôle du pouvoir judiciaire dans la société civile

J'ai néanmoins voté en faveur de la recevabilité et du constat de violation de l'article 8 de la Convention, parce que l'importance fondamentale des garanties protégeant les communications privées contre la surveillance arbitraire, en particulier dans un contexte non pénal, n'a jamais été prise en compte dans la procédure interne. Les tribunaux russes ont refusé d'examiner au fond les allégations du requérant, évoquant à tort le caractère technique des arrêtés ministériels litigieux. En ma qualité de juge national, je ne puis ignorer qu'il existe au sein de la société russe des soupçons généralisés selon lesquels une surveillance s'exerce sur les personnalités politiques et économiques, notamment les défenseurs des droits de l'homme, les militants et responsables de l'opposition, les journalistes, les fonctionnaires, les gestionnaires de biens de l'État – autrement dit tous ceux qui interviennent dans les affaires publiques. Ces soupçons découlent de l'expérience du régime totalitaire de l'ère soviétique, et même de la longue histoire de l'empire russe.

Cet arrêt pourrait servir de base à une amélioration de la législation en matière de mesures opérationnelles d'investigation et à l'établissement d'un système effectif de contrôle public sur la surveillance. En outre, cet arrêt

montre que s'il existe des soupçons généralisés dans la société, et s'il n'y a aucune autre possibilité pour celle-ci de lever ces soupçons en l'absence d'un contrat social et de changements adéquats dans la législation et la pratique nationales, alors, si le problème n'est pas décelé par les autres branches du pouvoir, c'est le pouvoir judiciaire qui doit être actif pour faciliter ces changements. C'est d'autant plus évident qu'il n'y a pas d'autres moyens disponibles pour protéger la démocratie et la prééminence du droit. C'est là un rôle important que le pouvoir judiciaire se doit de jouer dans la société civile.

Il se peut que la Cour soit critiquée pour n'avoir pas fourni de raisons plus précises à l'appui de son examen *in abstracto* dans le contexte social, et que d'aucuns fassent observer qu'elle s'est bornée à suivre la jurisprudence de ses chambres. L'arrêt rendu en l'espèce est cependant un arrêt délicat, car avant de parvenir à leur conclusion les juges ont dû prendre soin d'établir si tous les autres moyens étaient ou non inutiles. À l'inverse, dans l'affaire *Clapper v. Amnesty International USA* (568 US 398 (2013), la Cour suprême des États-Unis d'Amérique s'est abstenue de faire un pas en avant, malgré l'existence d'un programme de surveillance de masse et les « soupçons généralisés » à ce sujet (ou, pour reprendre les termes employés par le juge Breyer dans son opinion dissidente : « [le préjudice] est aussi susceptible de se produire que la plupart des événements futurs que nous prédisent les conclusions dérivées du bon sens et la connaissance ordinaire de la nature humaine »). La juridiction suprême a préféré juger insuffisant l'argument des auteurs du recours (des organisations œuvrant dans le domaine des droits de l'homme et du droit, ainsi que des médias), argument selon lequel ils risquaient de faire l'objet d'une surveillance en raison de la nature de leur travail.

Je m'arrêterai là, pour laisser aux universitaires les discussions sur l'agressivité, l'activisme ou la modération judiciaire. J'aimerais simplement conclure mon opinion en citant Edward Snowden : « Avec chaque victoire judiciaire, chaque modification du droit, nous démontrons que les faits sont plus convaincants que la peur. En tant que société, nous redécouvrons que la valeur du droit n'est pas dans ce qu'il cache, mais dans ce qu'il protège. »

OPINION EN PARTIE DISSIDENTE DE LA JUGE ZIEMELE

(Traduction)

1. Je souscris pleinement au constat de violation formulé dans cette affaire. La Cour rend ici un arrêt fort important sur une question de principe, la surveillance secrète qui s'exerce comme décrit dans les faits de l'espèce étant, par son essence même, incompatible avec l'état de droit et les principes de la démocratie.

2. Eu égard précisément à ce contexte, je ne puis approuver la décision de la Cour de ne pas allouer de somme au titre du préjudice moral subi. À mes yeux, la demande de réparation du requérant était très raisonnable (paragraphe 309 du présent arrêt) et un constat de violation, quoique très important par principe dans cette affaire, ne représente pas une satisfaction appropriée pour la situation spécifique du requérant. C'est pourquoi j'ai voté contre le point 4 du dispositif de l'arrêt.