



Doc. 13315

01 octobre 2013

La sécurité nationale et l'accès à l'information

Avis de commission¹

Commission de la culture, de la science, de l'éducation et des médias

Rapporteur: M. Hans FRANKEN, Pays-Bas, Groupe du Parti populaire européen

A. Les conclusions de la commission

Souscrivant au Principes de Tshwane, la commission de la culture, de la science, de l'éducation et des médias se félicite du rapport de la commission des questions juridiques et des droits de l'homme. Elle souhaite, néanmoins, proposer quelques amendements au projet de résolution qui visent à renforcer la protection des droits de l'homme et à préciser les modalités du maintien de l'équilibre entre la liberté d'information et la protection de la sécurité nationale ainsi que d'autres droits de l'homme, conformément à la jurisprudence de la Cour européenne des droits de l'homme.

B. Amendements proposés

Amendement A (au projet de résolution)

Après le paragraphe 3, ajouter le nouveau paragraphe suivant:

«Rappelant les Principes de Syracuse concernant les dispositions du Pacte international relatif aux droits civils et politiques qui autorisent des restrictions ou des dérogations, l'Assemblée confirme avec force que la violation systématique des droits de l'homme compromet la sécurité nationale et peut mettre en péril la paix et la sécurité internationales. L'Etat à qui la responsabilité en incombe n'invoquera pas la sécurité nationale comme justification.»

Note explicative: Comme l'article 10 de la Convention européenne des droits de l'homme (STE n° 5, «la Convention»), l'article 19 du Pacte international relatif aux droits civils et politiques précise que la sécurité nationale est un motif légitime pour restreindre la liberté d'information. Le droit à la protection de la vie privée et de la correspondance garanti par l'article 8 de la Convention européenne des droits de l'homme inclut également la sécurité nationale parmi les raisons légitimes de restreindre ce droit. Les Principes de Syracuse de 1984 concernant les dispositions du Pacte international relatif aux droits civils et politiques qui autorisent des restrictions ou des dérogations comprennent le paragraphe ci-dessus relatif à la violation systématique des droits de l'homme par les Etats qui, par conséquent, ne doivent pas invoquer la sécurité nationale pour justifier des mesures de lutte contre une opposition démocratique. Comme l'ont récemment illustré les affaires Manning et Snowden, des ingérences de grande ampleur dans la vie privée au nom de la sécurité nationale sont techniquement faisables et fréquentes aujourd'hui et l'on peut supposer que d'autres pays aux pratiques démocratiques moins solides utilisent les mêmes technologies pour porter atteinte à la vie privée, notamment celle des opposants politiques. Par conséquent, il est important de rappeler ici ce principe.

1. Renvoi à la commission: [Doc 12548](#), Renvoi 3762 du 15 avril 2011. Commission chargée du rapport: Commission des questions juridiques et des droits de l'homme. Voir [Doc. 13293](#). Avis approuvé par la commission le 1^{er} octobre 2013.



Amendement B (au projet de résolution)

Après le paragraphe 5, insérer le paragraphe suivant:

«Les pouvoirs publics ne peuvent avoir accès à des informations et communications privées ou à des données personnelles pour des raisons de sécurité nationale que si cet accès est prévu par la loi, qu'un impératif prépondérant quant à l'accès est établi et que cette mesure concrète s'impose dans une société démocratique afin de protéger l'existence de la nation, son intégrité territoriale ou son indépendance politique contre l'usage ou la menace de la force. Les pouvoirs publics ne doivent pas déléguer cette compétence à des personnes ou entreprises privées engagées pour assurer la protection de la sécurité nationale. Les mesures mises en œuvre dans ce contexte doivent être soumises à un contrôle administratif ou judiciaire.»

Note explicative: L'article 8 de la Convention européenne des droits de l'homme protège le droit au respect de la vie privée et de la correspondance. Il fixe également les conditions de toute ingérence dans la vie privée et la correspondance et cite la sauvegarde de la sécurité nationale comme motif possible d'une telle ingérence. Etant donné que les services de la sécurité nationale ne semblent pas toujours au fait de cette disposition, il est utile de rappeler les conditions justifiant l'ingérence au titre de la Convention. En outre, la définition établie par les Principes de Syracuse est assurément utile pour éviter de donner à la sécurité nationale un sens trop large.

Le cas récent d'Edward Snowden a mis en lumière non seulement la question de la protection des donneurs d'alerte mais aussi le fait que des personnes et des entreprises privées sont engagées par les pouvoirs publics pour obtenir, par le biais d'internet et de la téléphonie mobile, une grande quantité d'informations secrètes susceptibles d'être utiles pour la sécurité nationale. Cette externalisation abaisse inévitablement le niveau de protection de la vie privée et de la correspondance des personnes surveillées et accroît le risque d'un abus de ces pouvoirs délégués. Par conséquent, le pouvoir d'investigation et de surveillance doit continuer d'être exercé par les autorités publiques compétentes et ne pas être délégué à des personnes ou entreprises privées.

Amendement C (au projet de résolution)

Au paragraphe 8.1, insérer, à la fin de la première phrase, les mots suivants:

«au public lorsque ces informations sont d'intérêt général ou à toute personne qui a le droit d'obtenir des informations telles que des données personnelles.»

Note explicative: L'article 10 de la Convention européenne des droits de l'homme établit le droit du public d'être informé des questions d'intérêt général, ce qui peut inclure le droit d'avoir accès aux informations détenues par des autorités publiques. Toutefois, les pouvoirs publics détiennent aussi un grand nombre d'informations relatives à la vie privée des citoyens, qui est protégée par l'article 8 de la Convention, comme les données concernant la santé ou la situation financière des citoyens en question. Bien évidemment, ces dernières ne doivent pas être librement accessibles au public mais les individus concernés peuvent avoir le droit d'accéder à ces données personnelles au titre de l'article 8 de la Convention. En outre, les autorités judiciaires détiennent des informations dont la divulgation pourrait compromettre le droit à un procès équitable au titre de l'article 6 de la Convention. Par conséquent, les informations détenues par les autorités publiques ne doivent pas toutes être, sans distinction, accessibles librement ou rendues publiques.

Amendement D (au projet de résolution)

Au paragraphe 8.2, supprimer les mots suivants: «tels que la protection des relations internationales, la santé et la sûreté ou l'environnement ou des intérêts privés».

Note explicative: L'article 10 de la Convention européenne des droits de l'homme énonce de manière exhaustive les dérogations au droit à la liberté d'information. Elles ne correspondent pas à celles énumérées au paragraphe 8.2 qui, dans sa formulation actuelle, s'en distingue et pourrait donner l'impression d'affaiblir l'article 10 de la Convention. La sécurité nationale et «la protection des relations internationales, la santé et la sûreté ou l'environnement» ne sont pas d'égale importance. Le texte ne devrait porter que sur le sujet du rapport, à savoir la sécurité nationale; il n'est pas nécessaire de mentionner d'autres exceptions comme «la protection des relations internationales» qui n'est pas un but légitime en vertu de la Convention européenne des droits de l'homme ou «des intérêts privés» qui se réfèrent à tort au droit à la protection de la vie privée au titre de la Convention.

Amendement E (au projet de résolution)

A la fin du paragraphe 8.3, ajouter la phrase suivante:

«La neutralité d'internet exige que les pouvoirs publics, les fournisseurs d'accès internet et d'autres s'abstiennent de recourir à des techniques d'écoute portant atteinte à la vie privée comme l'inspection des paquets en profondeur ou de s'immiscer dans le trafic de données des utilisateurs d'internet.»

Note explicative: La neutralité du réseau est un principe recommandé pour l'internet par le Conseil de l'Europe et l'Union européenne; ce principe vise à empêcher que les utilisateurs d'internet soient victimes d'une discrimination découlant de la possibilité offerte à certains fournisseurs de contenus, le plus souvent commerciaux, de transmettre plus rapidement des données. En outre, la neutralité d'internet peut être compromise par des inspections portant atteinte à la vie privée ou des ingérences dans le trafic des données sur internet. La brève référence à ce sujet au paragraphe 8.3 devrait donc être expliquée par une phrase supplémentaire à la fin dudit paragraphe.

Amendement F (au projet de résolution)

A la fin du paragraphe 8.4, ajouter la phrase suivante:

«Un réexamen des archives publiques contenant des informations secrètes devrait être effectué périodiquement afin de voir si la confidentialité reste légitime pour des raisons liées à la sécurité nationale.»

Note explicative: En matière de sécurité nationale, les règles sont très différentes d'un pays à l'autre concernant l'accès des particuliers aux archives publiques comme les archives militaires ou les archives constituées par les services de sécurité. Il peut s'avérer nécessaire, toutefois, d'avoir accès à ces archives pour établir des faits historiques, enquêter sur des actes illicites commis par des instances publiques ou obtenir des informations tenues secrètes sur sa propre vie ou celle d'un parent proche.

A titre d'exemples, on peut citer l'organisme public créé après la chute du Mur de Berlin pour donner accès aux archives du ministère de la Sécurité d'Etat de l'ex-Allemagne de l'Est («Stasi») ainsi que les cas d'accès individuel accordé par les autorités russes à des chercheurs concernant les archives du KGB de l'ex-URSS.

Amendement G (au projet de résolution)

Supprimer les alinéas 8.5.1 et 8.5.2.

Note explicative: La deuxième phrase du paragraphe 8.5 va bien au-delà des Principes de Tshwane correspondants, à savoir les principes 9 et 10. En fait, ces derniers recensent les raisons légitimes de retenir l'information ainsi que des catégories d'informations entraînant une «forte présomption» en faveur de la divulgation. Ils n'affirment pas que l'apport «d'importants éléments de réflexion à un débat public en cours» (paragraphe 8.5.1) ou la promotion de «la participation des citoyens au débat politique» (paragraphe 8.5.2) devraient par nature primer la sécurité nationale. Les préoccupations en matière de sécurité nationale sont fréquemment au centre des débats publics ou politiques. Si de tels débats étaient considérés comme relevant par essence d'un intérêt général primordial, les intérêts de la sécurité nationale seraient vidés de leur sens. Outre qu'ils sont très vagues et abstraits, de tels postulats ne seraient pas couverts par l'article 10 de la Convention européenne des droits de l'homme.

Amendement H (au projet de résolution)

Après le paragraphe 8.7, insérer le paragraphe suivant:

«Rappelant la Recommandation N° R (2000) 7 du Comité des Ministres, l'Assemblée réaffirme que les mesures ci-après ne devraient pas être appliquées si elles visent à contourner le droit des journalistes de ne pas divulguer des informations identifiant leurs sources: i) les décisions ou mesures d'interception concernant les communications ou la correspondance des journalistes ou de leurs employeurs; ii) les décisions ou mesures de surveillance concernant les journalistes, leurs contacts ou leurs employeurs; ou iii) les décisions ou mesures de perquisition ou de saisie concernant le domicile ou le lieu de travail, les effets personnels ou la correspondance des journalistes ou de leurs employeurs, ou des données personnelles ayant un lien avec leurs activités professionnelles.»

Note explicative: Les mesures d'interception, de surveillance et de perquisition appliquées pour des raisons liées à la sécurité nationale risquent de compromettre le droit des journalistes de ne pas divulguer leurs sources d'information au titre de l'article 10 de la Convention européenne des droits de l'homme. Cette

question a été soulevée lors de la perquisition récente des locaux du journal *The Guardian* à Londres. Il est donc utile de rappeler la Recommandation pertinente N° R (2000) 7 du Comité des Ministres sur le droit des journalistes de ne pas révéler leurs sources d'information.

Amendement I (au projet de résolution)

A la fin du paragraphe 8.8, deuxième phrase, remplacer les mots «un organisme indépendant» par les mots «une instance nationale».

Note explicative: L'expression «organisme indépendant» ne précise pas si cet organisme doit être une autorité publique ou un organisme privé. Comme le droit d'avoir accès aux informations d'intérêt général se fonde sur l'article 10 de la Convention européenne des droits de l'homme, le déni et l'éventuelle violation d'un tel droit nécessitent un recours effectif devant une «instance nationale» au titre de l'article 13 de cette Convention. L'«instance nationale» mentionnée à l'article 13 ne doit pas nécessairement être une institution judiciaire mais alors, ses pouvoirs et les garanties qu'elle présente entrent en ligne de compte pour apprécier l'effectivité du recours s'exerçant devant elle (voir l'arrêt de la Cour européenne des droits de l'homme dans l'affaire *Kudla c. Pologne*, Requête n° 30210/96, paragraphe 157).

C. Exposé des motifs, par M. Franken, rapporteur pour avis

1. Bien que l'article 10 de la Convention européenne des droits de l'homme protège le droit à la liberté d'information et son article 8 le droit au respect de la vie privée, ces droits peuvent être soumis, au titre de la Convention, à certaines restrictions pour des raisons de sécurité nationale. Le maintien d'un équilibre entre ces droits et la sécurité nationale est au cœur même du rapport de la commission des questions juridiques et des droits de l'homme.

2. La commission de la culture, de la science, de l'éducation et des médias rappelle l'échange de vues sur cette question avec Mme Agnes Callamard, directrice exécutive d'ARTICLE 19 (Londres) et Mme Dunja Mijatovic, représentante de l'Organisation pour la sécurité et la coopération en Europe (OSCE) pour la liberté des médias, qui a été organisé par sa sous-commission des médias et accueilli par le Parlement suédois à Stockholm, le 12 septembre 2011.

3. D'importants travaux ont été menés par l'ARTICLE 19 et d'autres organisations non gouvernementales pour définir des principes communs en matière de liberté d'expression et d'information dans le contexte de la sécurité nationale. Il convient de mentionner tout particulièrement les Principes de Johannesburg du 1^{er} octobre 1995² ainsi que les Principes de Tshwane du 12 juin 2013³. Ces derniers ont largement inspiré le rapport de M. Arcadio Díaz Tejera (Espagne, SOC) établi au nom de la commission des questions juridiques et des droits de l'homme.

4. La divulgation récente d'informations secrètes par deux citoyens américains, Bradley Manning et Edward Snowden, a grandement attiré l'attention de la communauté internationale sur les restrictions à la liberté d'information pour des raisons de sécurité nationale conformément aux articles 8 et 10 de la Convention. Par conséquent, le 27 juin 2013, l'Assemblée parlementaire a tenu un débat d'actualité sur l'ingérence de l'Etat dans la vie privée sur internet. Le rapport de la commission des questions juridiques et des droits de l'homme est donc tout à fait opportun et important.

5. La Cour européenne des droits de l'homme a eu l'occasion de préciser le degré de protection de la vie privée et de la correspondance garanti au titre de l'article 8 de la Convention européenne des droits de l'homme dans le contexte d'une surveillance secrète pour des raisons de sécurité nationale. Dans l'affaire *Klass et autres c. Allemagne* (Requête n° 5029/71)⁴, la Cour a déjà jugé que «caractéristique de l'Etat policier, le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques. (...) En évaluant l'étendue de la sauvegarde offerte par l'article 8, la Cour ne peut que constater deux faits importants: les progrès techniques réalisés en matière d'espionnage et parallèlement de surveillance; en second lieu, le développement du terrorisme en Europe au cours des dernières années. Les sociétés démocratiques se

2. Voir www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf.

3. Voir

www.opensocietyfoundations.org/sites/default/files/Global%20Principles%20on%20National%20Security%20and%20the%20Right%20to%20Information%20%28Tshwane%20Principles%29%20-%20June%202013.pdf.

4. Voir <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510>.

trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'Etat doit être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire. La Cour doit donc admettre que l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète de la correspondance, des envois postaux et des télécommunications est, devant une situation exceptionnelle, nécessaire dans une société démocratique à la sécurité nationale et/ou à la défense de l'ordre et à la prévention des infractions pénales. Quant au choix des modalités du système de surveillance, la Cour relève que le législateur national jouit d'un certain pouvoir discrétionnaire. Elle n'a sûrement pas qualité pour substituer à l'appréciation des autorités nationales une autre appréciation de ce que pourrait être la meilleure politique en ce domaine. Elle souligne néanmoins que les Etats contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée. Quel que soit le système de surveillance retenu, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus. Cette appréciation ne revêt qu'un caractère relatif: elle dépend de toutes les circonstances de la cause, par exemple la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne».

6. En 1984, la Commission des droits de l'homme des Nations Unies a examiné les Principes de Syracuse concernant les dispositions du Pacte international relatif aux droits civils et politiques qui autorisent des restrictions ou des dérogations⁵; ces principes comportent les recommandations suivantes au sujet de la sécurité nationale:

- La sécurité nationale ne peut être invoquée pour justifier des mesures restreignant certains droits que lorsqu'il s'agit de mesures prises pour protéger l'existence de la nation, son intégrité territoriale ou son indépendance politique contre l'emploi ou la menace de la force.
- La sécurité nationale ne peut être invoquée comme un motif pour introduire des restrictions lorsqu'il s'agit de prévenir des menaces de caractère local ou relativement isolées contre la loi et l'ordre.
- La sécurité nationale ne peut servir de prétexte pour imposer des restrictions vagues ou arbitraires et elle ne peut être invoquée que lorsqu'il existe des garanties adéquates et des recours utiles contre les abus.
- La violation systématique des droits de l'homme compromet la sécurité nationale et peut mettre en péril la paix et la sécurité internationales. L'Etat à qui la responsabilité en incombe n'invoquera pas la sécurité nationale pour justifier des mesures visant à supprimer l'opposition à cette violation systématique ou à soumettre sa population à des pratiques répressives.

7. Dans son dernier rapport adressé à l'Assemblée générale des Nations Unies, M. Frank La Rue, Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, a mis tout particulièrement l'accent sur les questions de droits de l'homme en rapport avec la surveillance des communications, notamment pour des raisons de sécurité nationale. Il a conclu, entre autres, que la surveillance des communications par l'Etat devait être soumise au contrôle d'une autorité judiciaire indépendante, que les Etats devaient ériger en infraction la surveillance illicite effectuée par des acteurs publics ou privés et que les traités d'assistance judiciaire mutuelle devaient réglementer l'accès aux données relatives aux communications détenues par des entreprises étrangères⁶.

5. Voir www.refworld.org/cgi-bin/tehis/vtx/rwmain?docid=4672bc122.

6. Voir www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.