COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 17 novembre 2016 CODEXTER (2016) 18rev2

COMITE D'EXPERTS SUR LE TERRORISME

(CODEXTER)

GROUPE DE REDACTION SUR LES TECHNIQUES SPECIALES D'ENQUETE

PROJET D'EXPOSE DES MOTIFS

DE LA RECOMMANDATION RELATIVE AUX « TECHNIQUES SPECIALES D'ENQUETE »

EN RELATION AVEC DES INFRACTIONS GRAVES Y COMPRIS DES ACTES DE TERRORISME

Secrétariat de la Division Anti-Terrorisme
Direction de la société de l'information et de la lutte contre la criminalité, DG I

codexter@coe.int - www.coe.int/terrorism

Projet d'exposé des motifs
Recommandation relative aux « techniques spéciales d'enquête » en relation avec des infractions graves y compris des actes de terrorisme

Le texte reproduit ci-dessous correspond à la version du projet d'exposé des motifs de la Recommandation relative aux « techniques spéciales d'enquête » en relation avec des infractions graves y compris des actes de terrorisme, mise à jour par le groupe de rédaction TSE lors de sa 2e réunion (Rome, 13-14 juin 2016) et par le bureau du CODEXTER lors de sa 8e réunion (Paris, 29-30 octobre 2016).

_____

Introduction

1. Le 20 avril 2005, lors de la 924e réunion des Délégués des Ministres, le Comité des Ministres a adopté la Recommandation Rec(2005)10 du Comité des Ministres aux Etats membres relative aux « techniques spéciales d'enquête » en relation avec des infractions graves y compris des actes de terrorisme.

2. Les 14 et 15 mai 2013, le Conseil de l'Europe a accueilli à Strasbourg la conférence internationale sur le thème « L'utilisation des techniques spéciales d'enquête pour lutter contre le terrorisme et les autres formes d'infraction graves », organisée en étroite coopération avec la Direction exécutive du Comité contre le terrorisme (CTED) du Conseil de sécurité des Nations Unies, l'Organisation pour la sécurité et la coopération en Europe (OSCE) et la Ligue des Etats arabes. Les participants ont reconnu que pour protéger la société contre le terrorisme et la criminalité organisée, les forces de l'ordre devaient recourir à des méthodes d'enquête modernes comme les « techniques spéciales d'enquête » (TSE). La conférence a été l'occasion d'attirer l'attention sur le fait que depuis l'adoption de la Recommandation Rec(2005)10, la technologie internet et informatique avait progressé à grands pas et offrait de nouvelles possibilités aux criminels et aux terroristes mais aussi aux forces de l'ordre et a donc fait observer qu'une actualisation des normes et des lignes directrices applicables à l'utilisation des TSE s'imposait.

3. Sur la base de son mandat pour 2014 – 2015, le Comité d'experts sur le terrorisme (CODEXTER), lors de sa 25e réunion plénière (23-24 octobre 2013), a examiné un document contenant des propositions de domaines prioritaires pour ses travaux en 2014-2015. Ces propositions incluaient notamment la création d'un sous-groupe du Comité consacré aux « techniques spéciales d'enquête ».

4. Lors de sa 26e réunion plénière (6 – 7 mai 2014), le CODEXTER a convenu de créer un groupe de rédaction, composé de membres du CODEXTER, du Comité européen pour les problèmes criminels (CDPC), du Comité directeur sur les médias et la société de l'information (CDMSI), du Comité d'experts sur l'évaluation des mesures de lutte contre le blanchiment des capitaux et le financement du terrorisme (MONEYVAL), du Comité de la Convention Cybercriminalité (T-CY) et du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatique des données à caractère personnel (T-PD), chargé d'élaborer une série de propositions de modification de la Recommandation Rec(2005)10.

5. Lors de la 5e réunion de son Bureau (le 15 septembre 2014), le CODEXTER a convenu de charger le Secrétariat d'inviter 13 membres à rejoindre ce groupe de rédaction. Il a été décidé que le CODEXTER désignerait 7 de ces membres (parmi lesquels le président du groupe de rédaction), le CDPC 2 autres et les autres comités un membre chacun. Il a également demandé au Secrétariat de prévoir au moins deux réunions avec le futur groupe de rédaction.

6. Lors de sa 27e réunion plénière (13-14 novembre 2014), le CODEXTER a confirmé la décision du Bureau de nommer M. Nicola PIACENTE (Italie) président du groupe de rédaction. Préalablement à cette réunion, un appel à candidatures a été lancé aux membres du CODEXTER justifiant d'une expérience concrète liée à l'application des techniques spéciales d'enquête pour les six sièges restants du groupe de rédaction réservés au CODEXTER.

7. Bien que le CODEXTER ait convenu de débuter par le thème des « techniques spéciales d'enquête » (TSE) et de s'y consacrer dès la fin 2014 et tout au long de l'année 2015, il a dû différer ses activités prévues après que le Secrétaire Général du Conseil de l'Europe a demandé, lors de la 27e réunion plénière du CODEXTER, que celui-ci joue un rôle clé dans la mise en œuvre satisfaisante de la Résolution 2178 (2014) des Nations Unies sur les menaces contre la paix et la sécurité internationales relevant du droit

pénal dans les délais prévus. Le Comité a notamment été encouragé à adopter le mandat d'un comité ad hoc chargé de préparer et de négocier un projet de protocole additionnel à la Convention du Conseil de l'Europe sur la prévention du terrorisme. Le 22 janvier 2015, le Comité des Ministres, sur proposition du CODEXTER, a adopté le mandat du Comité sur les combattants terroristes étrangers et les questions connexes (CODCTE), lequel a élaboré le protocole dans les délais prévus. Celui-ci a été adopté par le Comité des Ministres en avril 2015 et ouvert à la signature à Riga le 22 octobre 2015.

8. Lors de sa 29e réunion plénière (17-18 novembre 2015), le CODEXTER a convenu que les travaux sur les modifications de la Recommandation Rec(2005)10 commenceraient début 2016.

9. Les membres du groupe de rédaction du CODEXTER sur les techniques spéciales d'enquête se sont réunis pour la première fois le 18 février 2016. Le comité a examiné le projet et débattu des propositions de modification paragraphe par paragraphe.

10. Lors de la 7e réunion de son Bureau (17 mars 2016), le CODEXTER a examiné l'avant-projet élaboré par le groupe de rédaction et proposé quelques modifications à y apporter.

11. Lors de sa 30e réunion plénière (19-20 mai 2016), le CODEXTER a chargé le Secrétariat de soumettre le projet de recommandation modifiée au CDPC pour avis après la deuxième réunion du groupe de rédaction TSE.

12. Les membres du groupe de rédaction du CODEXTER sur les techniques spéciales d'enquête se sont réunis une seconde fois les 13 et 14 juin 2016.

Observations à caractère général

13. Conformément à la Recommandation Rec(2005)10, l'objectif de la recommandation mise à jour est de promouvoir l'utilisation efficace des techniques spéciales d'enquête par les autorités compétentes essentiellement dans le cadre d'enquêtes pénales portant sur des infractions graves, y compris des actes de terrorisme, tout en garantissant le plein respect des droits et des libertés des individus.

14. Les modifications apportées visent à assurer l'équilibre du texte, d'une part en insistant davantage sur la nécessité de respecter les droits de l'homme dans la mise en œuvre des toutes les techniques spéciales d'enquête et, d'autre part, en tenant compte des nouveaux moyens techniques développés depuis 2005 et de l'inclusion d'enquêtes sur la cybercriminalité et de techniques d'investigation financière visant les personnes physiques, et lorsque la législation nationale le prévoit, les personnes morales, dans les techniques spéciales d'enquête visées par la recommandation.

15. Ainsi, la Recommandation Rec(2005)10 a été mise à jour en conservant la plus grande partie de la version originale du texte et en ajoutant de nouvelles dispositions chaque fois que la mise à jour de la recommandation l'exigeait.

16. Le texte n'a fait l'objet que de révisions structurelles mineures. Dans le préambule mis à jour, les dispositions sont systématiquement présentées par ordre chronologique, exception faite de la référence aux Lignes directrices de 2002 sur les droits de l'homme et la lutte contre le terrorisme. Le chapitre I de l'annexe élargit la définition et le champ d'application des « techniques spéciales d'enquête » et reprend celle des « autorités compétentes ». Il précise par ailleurs la définition et le champ d'application des expressions « investigation financière » et « enquête sur la cybercriminalité ». Le chapitre II « établit ou rappelle un certain nombre de principes communs qui devraient être respectés lorsque les Etats membres réglementent les TSE et lorsque celles-ci sont utilisées par leurs autorités compétentes ». Le chapitre III propose des mesures à prendre en vue d'améliorer la coopération « internationale et nationale » sur les questions relatives à l'utilisation des TSE ».

17. La particularité des TSE tient à leur caractère secret, qui en fait un instrument essentiel de la lutte contre les infractions graves, y compris les actes de terrorisme. Leur utilisation peut toutefois constituer une ingérence dans les libertés et droits fondamentaux, comme le droit à un procès équitable, le droit à la liberté d'expression, à la liberté de communication, la protection du droit de propriété et le droit au respect de la vie privée, y compris le droit à la protection des données à caractère personnel. La recommandation cherche par conséquent à ménager un équilibre entre la nécessité de renforcer l'efficacité de la lutte contre les infractions graves, y compris les actes de terrorisme, en encourageant le recours aux TSE, et la nécessité de garantir la protection des libertés et droits fondamentaux.

18. La recherche d'un équilibre s'inspire d'une approche similaire adoptée par la Cour européenne des droits de l'homme (ci-après « la Cour »). Toute ingérence dans l'exercice d'un droit garanti par la Convention européenne des droits de l'homme (STE n° 5, ci-après « la Convention ») ne peut se produire que dans des conditions exceptionnelles et doit être nécessaire dans une société démocratique, dans l'intérêt, notamment, de la sécurité nationale et/ou de la défense de l'ordre et de la prévention du crime. Les Etats membres ne disposent cependant pas d'une latitude illimitée s'agissant des ingérences dans ces droits liées à l'utilisation des TSE. Toute ingérence doit être proportionnée et nécessaire au regard du but légitime poursuivi. En outre, des garanties appropriées et efficaces contre les abus doivent s'appliquer et l'accès à un recours effectif doit être assuré[1]. Les mesures doivent enfin être soumises à l'autorisation d'une autorité compétente, tel qu'il est prévu au chapitre I, paragraphe 2 de la recommandation, et lorsque le droit national l'exige, au contrôle d'une instance indépendante. A l'heure des nouvelles avancées technologiques, lors du recours aux TSE, il convient d'accorder une attention particulière aux normes pertinentes du Conseil de l'Europe en matière de protection de la vie privée et de la liberté d'expression comme le prévoient, notamment, le cas échéant, les dispositions de la Recommandation 2016(5) sur la liberté d'internet.

19. Plusieurs instruments du Conseil de l'Europe, comme ceux énumérés dans le préambule de la recommandation et au paragraphe 23 du chapitre III, traitent déjà de la question des TSE. Cependant ces instruments ne traitent des questions relatives à l'utilisation des TSE que dans la mesure où ces techniques sont utilisées en relation avec le champ d'application respectif de ces instruments alors que la présente recommandation propose une approche détaillée de l'utilisation des TSE en relation avec toute forme d'infractions graves, y compris des actes de terrorisme.

20. Parce qu'ils traitent du recours aux TSE non seulement en relation avec le terrorisme mais plus généralement en relation avec les infractions graves, y compris les actes de terrorisme, les principes énoncés dans la recommandation sont applicables dans un contexte plus général. Le Comité a toutefois choisi de ne pas définir les termes « infractions graves » estimant que, aux fins de cette recommandation, il était plus approprié de laisser aux Etats membres une marge d'appréciation pour fixer les seuils de gravité d'une infraction. Comme il est précisé dans l'exposé des motifs de la Recommandation Rec(2005)10, l'article 2 (b) de la Convention des Nations Unies contre le crime organisé transnational disposant que «l'expression « infraction grave » désigne un acte constituant une infraction passible d'une peine privative de liberté dont le maximum ne doit pas être inférieur à quatre ans ou d'une peine plus lourde », peut cependant servir d'indicateur pour permettre aux Etats qui le souhaitent de définir plus précisément cette notion. En tout état de cause, la notion d'« infraction grave » recouvre les infractions liées au terrorisme et à la criminalité organisée.

Commentaire sur les dispositions de la Recommandation

Préambule

21. Le 4e paragraphe recense trois instruments juridiques adoptés par la Commission européenne pour la démocratie par le droit du Conseil de l'Europe (Commission de Venise) présentant un intérêt pour les STE. Dans son « Avis sur la protection des droits de l'homme dans les situations d'urgence », la Commission fait observer que la sécurité de l'Etat et de ses institutions démocratiques « représentent des intérêts publics et privés capitaux qui méritent d'être protégés, si nécessaire à un prix élevé ». En effet les mesures de protection peuvent aussi comporter, ou se traduire par, des restrictions justifiées de certaines libertés et droits fondamentaux non seulement des personnes ayant commis, soupçonnées d'avoir commis ou d'envisager de commettre des actes contre la sécurité publique mais également de toute personne, même d'éventuelles victimes d'actes terroristes. La deuxième source à laquelle le paragraphe 8 fait référence est le Rapport sur le contrôle démocratique des services de sécurité qui porte, notamment, sur les différentes formes de contrôle judiciaire et d'autorisation des « mesures spéciales d'enquête ». Pour finir, la recommandation renvoie au Rapport sur les mesures de lutte contre le terrorisme et les droits de l'homme qui considère que l'intérêt national et la sécurité publique peuvent justifier les restrictions imposées à l'exercice de certains droits fondamentaux non seulement des auteurs d'actes terroristes ou des personnes soupçonnées d'avoir commis de tels actes, mais également de la population au sens large, y compris des victimes avérées ou éventuelles d'actes terroristes ».

[1] Cour européenne des droits de l'homme, Klass et autres c. Allemagne, requête n° 5029/71, arrêt du 6 septembre 1978 ; la Cour a rappelé ces principes à plusieurs reprises, y compris dans l'affaire Gillan et Quinton c. le Royaume-Uni, requête n° 4158/05, 12 janvier 2010; Uzun c. Allemagne, Requête n° 35623/05, arrêt du 2 septembre 2010; R.E. c. Royaume-Uni, Requête n° 62498/11, 27 octobre 2015; l'exemple le plus récent dans ce domaine est l'affaire Karabeyoğlu c. Turquie, requête n° 30083/10, arrêt, 7 juin 2016.

22. Le 7e paragraphe fait référence aux travaux du Conseil de l'Europe dans le domaine du crime organisé transnational (COT). Le Livre blanc du CDPC comporte une liste de recommandations visant à définir les mesures qui devraient être appliquées dans les domaines clés parmi lesquels les techniques spéciales d'enquête. Sur ce point, le Livre blanc fait observer que ces techniques sont indispensables pour déceler les cas de COT et en poursuivre les auteurs mais que leur application doit être contrebalancée par des mesures adéquates, qui garantissent la protection des droits de l'homme et permettent d'éviter les abus. Il attire l'attention sur le fait que l'absence de règles appropriées et d'harmonisation de la législation en matière de TSE entrave le transfert transfrontière des éléments de preuve[2]. Il identifie dès lors deux ensembles de mesures qui pourraient être prises en matière de lutte contre le COT et d'utilisation des TSE : (i) intensifier la réglementation et l'utilisation efficace de ces techniques, tout en acquérant une connaissance globale de la législation en vigueur dans les États membres du Conseil de l'Europe et (ii) renforcer la protection des droits de l'homme lors du recours à ces mesures d'enquête intrusives.

23. Dans le 8e paragraphe, il est fait référence au Plan d'action pluriannuel sur « La lutte contre l'extrémisme violent et la radicalisation conduisant au terrorisme » adopté par le Comité des Ministres le 19 mai 2015. La mise à jour de la Recommandation Rec(2005) s'inscrit dans la lignée des objectifs du Plan d'action, à savoir : 1. renforcer le cadre juridique contre le terrorisme et l'extrémisme violent ; 2. et prévenir et combattre la radicalisation violente par des mesures concrètes dans le secteur public, en particulier dans les établissements scolaires et les prisons, et sur internet.

24. Le 9e paragraphe renvoie aux travaux du Conseil de l'Europe dans le domaine de la protection des données, de l'utilisation d'internet et de la neutralité du réseau, qui sont des éléments essentiels des TSE. Le Guide 2014 des droits de l'homme pour les utilisateurs d'internet est un outil destiné aux utilisateurs d'internet visant à les aider à connaître leurs droits fondamentaux en ligne, leurs limites possibles et les recours disponibles concernant ces limites. Il rappelle que la loi n'autorise la violation de la confidentialité des données personnelles que dans des circonstances exceptionnelles, par exemple dans le cadre d'enquêtes pénales mais fait toutefois observer que « des informations accessibles, claires et précises devraient être mises à votre disposition pour vous permettre de connaître les règles et la législation en vigueur, ainsi que vos droits à cet égard ». La recommandation de 2016 sur la protection et la promotion du droit à la liberté d'expression et du droit à la vie privée en lien avec la neutralité du réseau réaffirme que l'utilisation de techniques de gestion du trafic internet capables d'analyser le contenu des communications devrait respecter la législation en vigueur sur le droit à la vie privée et à la protection des données à caractère personnel et être contrôlée par une autorité compétente au sein de chaque Etat membre afin de vérifier le respect de la législation. Il est également fait référence à la recommandation sur la liberté d'internet adoptée par le Comité des Ministres le 13 avril 2016.

25. Le paragraphe 11 est repris dans son intégralité. Les Lignes directrices sur les droits de l'homme et la lutte contre le terrorisme de 2002 restent un instrument d'actualité et de référence en matière d'utilisation des TSE. Cela a notamment été souligné dans le document de réflexion qui envisageait la possibilité de prendre en considération, en particulier, les dispositions I (Obligation des Etats de protéger toute personne contre le terrorisme), V (Collecte et traitement de données à caractère personnel par toute autorité compétente en matière de sécurité de l'Etat), VI (Mesures d'ingérence dans la vie privée), IX (Procédures judiciaires) et XVI (Respect des normes impératives du droit international et des normes du droit international humanitaire) des Lignes directrices.

26. Le paragraphe 14 vise à souligner plus encore l'importance du cadre juridique en insistant sur la disposition XVI des Lignes directrices précitées, qui rappelle la nécessité de lutter contre le terrorisme dans le respect des normes impératives du droit international et des normes du droit international humanitaire, lorsqu'il y a lieu.

27. Dans son nouveau libellé le paragraphe 20, qui adresse les recommandations aux Etats membres, fait également référence à la nécessité de continuer à renforcer la coopération internationale et nationale en matière pénale, notamment en ce qui concerne l'échange d'informations et de bonnes pratiques sur le plan opérationnel.

[2] Le Livre blanc du CDPC fait observer page 27 que « l'absence de réglementation globale et/ou le fait que le droit interne varie d'un État membre à l'autre accroissent évidemment les difficultés de la coopération transnationale et du transfert des éléments de preuve ; la réglementation différente de certaines techniques d'enquête peut par ailleurs entraver leur utilisation dans un cadre transfrontière. Ainsi, le fait de mener des enquêtes secrètes et d'effectuer des livraisons contrôlées sur le territoire d'un autre État n'est pas une tâche facile, en raison des différences entre les législations, les systèmes répressifs et les priorités institutionnelles. »

Annexe à la recommandation

Chapitre I. Définitions et champ d'application

28. Le paragraphe 1 du chapitre I est reproduit dans son intégralité. Toutefois, dans son nouveau libellé, la version mise à jour élargit le champ d'application des techniques spéciales d'enquête qui visent désormais également à prévenir les infractions graves et à poursuivre et réprimer leurs auteurs. Les TSE, y compris dans le cadre des investigations financières et des enquêtes sur la cybercriminalité, désignent des techniques appliquées par les autorités compétentes dans le cadre d'enquêtes pénales. La conséquence de cette précision est double: cela signifie tout d'abord que l'utilisation des TSE dans un contexte différent, comme celui de la sécurité nationale, ne relève pas du champ d'application de la recommandation ; deuxièmement, il en découle que les STE qui sont utilisées dans le cadre d'enquêtes pénales sont couvertes par la recommandation indépendamment du titre ou de l'identité des autorités qui ont participé à la décision, au contrôle ou à l'utilisation de ces techniques. La référence à la « prévention » dans le paragraphe 1 ne vise pas à couvrir les actions des services de renseignement dans le domaine de la sécurité nationale : elle renvoie à la situation où une infraction grave est en préparation mais n'a pas encore été commise (voir aussi la formulation du paragraphe 9 de la recommandation). Le texte du paragraphe 2 éclaircit le sens du terme « autorités compétentes » en référence au contexte des enquêtes pénales.

29. Comme il est précisé dans l'exposé des motifs de la Recommandation Rec(2005)10, les TSE sont des techniques utilisées « de telle sorte que les personnes visées ne soient pas alertées ». Le recours à l'usage des TSE serait superflu, et pourrait même être contre-productif, si les personnes visées étaient prévenues du fait que de telles techniques étaient utilisées en vue de rassembler des informations sur leurs actions ou activités. Par conséquent, les TSE ont souvent un caractère secret, caractère qui se manifeste dès lors que l'on tente de dissimuler qu'une enquête pénale est en cours.

30. Aux fins de cette recommandation, les TSE peuvent comprendre, par exemple : les opérations d'infiltration (y compris les enquêtes sous couvert); les opérations front-store (telles que des entreprises sous couverture) ; les informateurs ; les livraisons surveillées ; l'observation (y compris l'observation transfrontalière); la surveillance électronique de cibles spécifiques ; les interceptions de communications ; les poursuites transfrontalières ; les pseudo-achats ou autres « pseudo-crimes », la surveillance secrète des opérations financières et des consultations sur internet, tels que définis par la législation nationale.

31. Les paragraphes 3 et 4 renvoient à la définition des termes « investigations financières » et « enquêtes sur la cybercriminalité ». Ces modifications visaient à inclure les TSE utilisées dans le cadre des investigations financières et des enquêtes sur la cybercriminalité relevant du domaine de la présente recommandation. Elles étaient essentielles pour inclure expressément dans les TSE visées par la recommandation ces techniques d'enquête visant des personnes physiques et, lorsque la législation nationale le prévoit, des personnes morales. Les techniques d'investigation financière permettent aux enquêteurs de mettre au jour et de perturber les activités des associations et/ou groupes criminels et terroristes et de confisquer leurs avoirs. Les enquêtes sur la cybercriminalité reconnaissent le rôle central que joue le cyberespace en tant qu'environnement par lequel, et au sein duquel, les activités criminelles, y compris terroristes, peuvent à la fois s'exercer et être dépistées.

32. La définition de l'expression « investigation financière » trouve son origine dans la Recommandation 30 (Responsabilités des autorités de poursuite pénale et des autorités chargées des enquêtes) des Recommandations de 2012 du Groupe d'action financière (GAFI), un organisme intergouvernemental indépendant dont l'objectif est d'élaborer et de promouvoir des politiques et des normes internationales pour protéger l'intégrité du système financier mondial contre le blanchiment de capitaux, le financement du terrorisme et le financement de la prolifération des armes de destruction massive[3]. Le 17 avril 2015, MONEYVAL a présenté son « Rapport de typologies sur le blanchiment des produits de la criminalité organisée », lequel relève qu'il n'existe pas au niveau des Etats de définition communément admise (ou utilisée) des termes « analyse financière » ou « investigation financière » et que leur interprétation va des activités élémentaires de collecte de renseignements à l'identification de réseaux relationnels et flux de capitaux complexes et au profilage financier visant à déceler une richesse inexpliquée ou des revenus disproportionnés par rapport au mode de vie et aux ressources affichés. Dans ce contexte, MONEYVAL reconnaît que les Lignes directrices de 2012 du GAFI sur les enquêtes financières constituent « un outil

[3] La note interprétative de la Recommandation 30 du GAFI donne la définition suivante : « L'expression *enquête financière* désigne un examen des affaires financières liées à une activité criminelle, visant à: (i) identifier l'ampleur de réseaux criminels et/ou le degré de criminalité; (ii) identifier et dépister le produit du crime, les fonds terroristes et tout autre bien soumis ou susceptible d'être soumis à confiscation; établir des preuves susceptibles d'être produites dans des procédures pénales ».

précieux pour définir la stratégie en matière d'enquête, ses objectifs, les mesures spécifiques, les ressources nécessaires, la formation des enquêteurs et l'utilisation des instruments juridiques existants pour mener des investigations financières efficaces de façon exhaustive, novatrice, cohérente et déterminée ».

33. Aux fins de la présente Recommandation, on entend par « enquête sur la cybercriminalité » une enquête qui vise à prévenir et à déceler toute infraction grave, y compris un acte de terrorisme, ainsi que toute infraction pénale définie par la Convention du Conseil de l'Europe pour la prévention du terrorisme (STCE n° 196) et son Protocole additionnel (STCE n° 217), à enquêter à son sujet et à poursuivre et réprimer ses auteurs.

34. Tant les investigations financières que les enquêtes sur la cybercriminalité visées par la présente recommandation sont des outils à utiliser dans les limites définies au paragraphe 13 du Préambule à la recommandation.

Chapitre II. Utilisation des TSE au niveau national

a) Principes généraux

Paragraphe 5 :

35. Au cours des dernières années, il a été demandé à la Cour d'examiner l'utilisation des TSE dans le cadre de l'article 8[4]. Cette jurisprudence a fixé un ensemble de principes clairement définis régissant le recours aux TSE, qui sont largement pris en compte dans le texte modifié de la recommandation.

36. Le paragraphe 5 rappelle qu'une ingérence ne peut se justifier que si elle est prévue par la loi de manière suffisamment claire. Cette formulation requiert que la mesure incriminée soit accessible à la personne concernée et prévisible quant à ses effets Dans ce contexte, la législation nationale doit être suffisamment « précise » et « accessible » pour qu'un individu puisse être en mesure de prévoir, avec un degré de certitude raisonnable, les conséquences de ses actes ou les circonstances et conditions dans lesquelles les autorités peuvent prendre certaines mesures. A cet égard, la Cour a affirmé :

« Il faut d'abord que la 'loi' soit suffisamment accessible : le citoyen doit pouvoir disposer de renseignements suffisants, dans les circonstances de la cause, sur les normes juridiques applicables à un cas donné. En second lieu, on ne peut considérer comme une "loi" qu'une norme énoncée avec assez de précision pour permettre au citoyen de régler sa conduite ; en s'entourant au besoin de conseils éclairés, il doit être à même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé. »[5]

37. Lorsqu'elles réglementent une TSE ou décident d'y avoir recours, les autorités nationales doivent garder à l'esprit que leur utilisation peut affecter, non seulement les droits de la personne suspectée d'avoir commis ou préparé l'infraction, mais aussi, directement ou indirectement, les droits d'autres personnes physiques ou morales. A cet égard, le caractère approprié d'une TSE particulière peut dépendre, entre autres, de son caractère intrusif pour les droits de ces autres personnes.

38. En ce qui concerne plus précisément l'interception des communications, la loi doit au minimum définir les catégories de personnes dont les communications sont susceptibles d'être interceptées, la nature des infractions justifiant le recours à cette interception, la durée de la mesure, la procédure d'établissement des procès-verbaux consignant les communications interceptées, les précautions à prendre pour veiller à l'intégrité des communications aux fins d'un contrôle et d'un examen éventuels par les autorités judiciaires et les parties, ainsi que les circonstances de l'effacement permanent des informations (notamment après un non-lieu ou une relaxe).

39. De manière plus générale, en ce qui concerne la compatibilité des TSE avec les exigences de l'article 8, la Cour a eu à examiner un certain nombre de situations, telles que les suivantes :

[4] Aux termes de l'article 8 : « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. 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 ».

[5] Cour européenne des droits de l'homme, *Sunday Times c. Royaume-Uni*, requête n° 6538/74, arrêt du 26 avril 1979, paragraphe 49.

A) Concernant les écoutes téléphoniques :

La Cour a affirmé le principe de légalité des écoutes en considérant que les écoutes « sauvages », à des fins tant judiciaires que de sécurité nationale, sont interdites.

B) Concernant l'interception des correspondances :

La Cour a admis que l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète de la correspondance et des envois postaux puisse être une nécessité dans le cadre de la lutte contre le terrorisme si des garanties adéquates et suffisantes contre les abus sont prévues. L'appréciation que porte la Cour dépend de la nature, de l'étendue et de la durée des mesures éventuelles, des raisons requises pour les ordonner, des autorités compétentes pour les permettre, les exécuter et les contrôler ou encore du type de recours prévu par le droit interne. Une protection supplémentaire est accordée s'agissant de la correspondance échangée avec un avocat, l'ingérence touchant ici aussi aux droits de la défense.

La correspondance électronique a créé une situation nouvelle : si la recherche des infractions pénales ou la protection de l'ordre public constituent des motifs légitimes d'ingérence, un cadre légal bien défini s'impose. La particularité de l'ingérence tient ici au fait que l'on vise non seulement le secret de la correspondance mais aussi le secret des communications et le respect de la vie privée au domicile[6].

C) Concernant la prise de photos et l'enregistrement de films :

La Cour a admis la légitimité de cette technique dans le contexte tout particulier de la lutte contre le terrorisme et lors d'un interrogatoire par les forces de sécurité. Elle a souligné que ce contexte avait une influence sur son appréciation du juste équilibre entre les droits de l'individu et les besoins de la société. Il est cependant clair qu'un cadre juridique prévisible dans son application et un but légitime restent requis. De même, l'utilisation de ces techniques doit être considérée comme ayant été nécessaire dans une société démocratique pour prévenir certaines infractions.

D) Concernant le recours à des indicateurs :

La Cour a admis que les nécessités de l'action policière peuvent imposer le recours à des indicateurs sans que cela ne constitue une violation de l'article 8 de la Convention. La police n'a pas véritablement l'obligation de dévoiler l'identité de ceux qui la renseignent, mais l'utilisation de ces renseignements comme moyen de preuve devant un tribunal devra respecter le droit à un procès équitable garanti par l'article 6 de la Convention.

Paragraphe 6 :

40. Le paragraphe 6 rappelle que l'utilisation des TSE ne peut entraîner des restrictions aux droits garantis par la Convention que dans la mesure où elle poursuit un but légitime et est nécessaire dans une société démocratique. S'agissant de déterminer si une ingérence est « nécessaire dans une société démocratique », il est établi dans la jurisprudence de la Cour que lorsqu'elles mettent en balance l'intérêt de l'Etat défendeur à protéger la sécurité nationale et/ou à maintenir l'ordre ou à empêcher une infraction d'une part, et la gravité de l'ingérence d'autre part, les autorités nationales disposent d'une certaine marge d'appréciation. Cette marge est toutefois soumise à un contrôle de la Cour portant à la fois sur la loi et sur les décisions qui visent à l'appliquer. La Cour doit être convaincue de l'existence de garanties adéquates et effectives contre les abus car un système de techniques d'enquête secrète risque de nuire à la démocratie et à l'Etat de droit.

41. Comme le précise l'exposé des motifs de la Recommandation Rec(2005)10, le paragraphe 6 ne doit pas être interprété comme créant une obligation pour les Etats membres d'introduire des TSE supplémentaires. Les TSE qui devraient être rendues disponibles dépendent de ce qui est considéré comme étant adéquat par les autorités législatives nationales.

Paragraphe 7 :

42. Le paragraphe 7 s'écarte de l'avis de la Cour, selon lequel il est « en principe souhaitable que le contrôle soit confié à un juge en un domaine où les abus sont potentiellement si aisés dans des cas

[6] Cour européenne des droits de l'homme, Roman Zakharov c. Russie, Requête n° 47143/06, arrêt du 4 décembre 2015, paragraphes 227-234

individuels et pourraient entraîner des conséquences préjudiciables pour la société démocratique tout entière »[7].

43. L'examen et le contrôle judiciaires 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 en tant que telle, mais aussi le contrôle qui l'accompagne. Il se révèle donc indispensable que les procédures existantes offrent des garanties appropriées et équivalentes de sauvegarde des droits de l'individu. Pour ne pas dépasser les bornes de la nécessité au sens de l'article 8, paragraphe 2, il faut de surcroît respecter fidèlement, dans les procédures de contrôle judiciaire, les valeurs d'une société démocratique. 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.

44. Comme indiqué dans l'exposé des motifs de la Recommandation Rec(2005)10, les différents types de contrôle peuvent être complémentaires en fonction du degré d'intrusion dans la sphère privée occasionnée par l'utilisation de TSE. Par exemple, dans le cadre d'opérations sous couverture, le contrôle judiciaire peut intervenir tant au début que pendant ou à la fin de l'opération. Au début, le déclenchement de l'opération est subordonné à l'existence de raisons ou d'indices suffisants ; pendant l'opération, des rapports réguliers relatant le déroulement sont établis ; enfin, une description précise du déroulement de l'opération peut permettre un contrôle a posteriori.

Paragraphe 8 :

45. La possibilité pour les personnes physiques et morales de contester l'utilisation des TSE et d'avoir accès à un recours effectif contre une utilisation abusive devant une instance nationale sont des composantes indispensables des droits et des libertés garantis par la Convention, comme énoncé à l'article 13. La recommandation contient une disposition particulière qui reconnaît ce droit en cas d'utilisation abusive des TSE. La Cour a reconnu que le caractère secret des TSE ne doit pas conduire « à ce qu'elles soient en pratique inattaquables et qu'elles échappent au contrôle des autorités judiciaires nationales et de la Cour »[8].

b) Conditions d'utilisation

Paragraphe 9 :

46. Le paragraphe 9 a été reproduit dans son intégralité. Il convient de noter, comme indiqué dans l'exposé des motifs de la Recommandation Rec(2005)10, que la détermination de « raisons suffisantes » présuppose celle de faits ou renseignements propres à persuader un observateur objectif que l'individu en cause peut avoir accompli une infraction. Ce que l'on peut considérer comme « plausible » dépend toutefois de l'ensemble des circonstances.

47. La référence à une infraction qui « est en cours de préparation » couvre les situations où, bien qu'aucune infraction n'ait encore été commise, une personne commet ou a commis un ou plusieurs actes qui peuvent objectivement être considérés comme contribuant à la préparation d'une infraction.

Paragraphe 10 :

48. Ce paragraphe souligne l'importance et le caractère non dérogatoire du principe de proportionnalité lorsqu'il est question de décider d'avoir recours à des TSE.

Paragraphe 11 :

49. Ce paragraphe est reproduit pour encourager les autorités compétentes à utiliser d'autres méthodes d'enquête que les TSE si de telles méthodes permettent de prévenir l'infraction, de la déceler, d'enquêter à son sujet et de poursuivre et réprimer son auteur « avec une efficacité satisfaisante ». L'utilisation des termes « avec une efficacité satisfaisante » indique que l'emploi de techniques autres que les TSE devrait

[7] Cour européenne des droits de l'homme, Klass et autres c. Allemagne, op. cit., paragraphe 56.
[8] Cour européenne des droits de l'homme, Roman Zakharov c. Russie, op.cit., paragraphe 171

être privilégié si, d'une part, elles sont susceptibles de produire les mêmes résultats et que, d'autre part, leur mise en œuvre ne se heurte pas à des obstacles pratiques importants.

Paragraphe 12 :

50. La première phrase du paragraphe ne signifie pas que les TSE devraient être exclusivement utilisées dans le but d'obtenir des informations et des éléments pouvant servir de preuves devant un tribunal. Elle vise à assurer que, si nécessaire, ces informations et éléments recueillis grâce à l'utilisation des TSE, puissent être produits en toute légalité lors d'un procès devant des juridictions nationales et appelle les Etats membres à édicter une législation appropriée à cette fin.

51. Comme il ressort de la deuxième phrase de ce paragraphe, les preuves recueillies grâce à l'utilisation des TSE ne devraient pas être produites d'une manière qui risquerait de mettre en péril le droit de l'accusé à un procès équitable garanti par l'article 6 de la Convention. Bien que l'article 6 de la Convention prévoie que la réglementation relative à l'admissibilité des preuves relève au premier chef du droit interne, la Convention exige tout de même que la procédure dans son ensemble, y compris la façon dont les preuves sont produites, soit équitable. Dans ce contexte, il convient de souligner que le paragraphe 7 n'empêche pas les Etats membres d'exclure l'admissibilité en tant que preuves des informations et des éléments recueillis grâce à l'utilisation des TSE dans des circonstances extraordinaires, en particulier lorsque les TSE n'ont pas été utilisées conformément au droit national.

52. Dans certaines affaires, la Cour a considéré qu'une opération surveillée et qu'une opération contrôlée sont compatibles avec les droits des accusés seulement si ces opérations sont menées dans le cadre d'une information judiciaire et que l'identité et le rôle de l'agent infiltré sont connus du juge. A l'inverse, une initiative prise sans contrôle judiciaire constituerait un procédé déloyal qui vicierait la procédure dès le départ.

53. Si la Cour accepte le recours à des agents infiltrés dont le rôle n'est pas totalement passif, elle condamne la provocation à commettre des infractions. Il y a provocation lorsque le comportement des autorités a été déterminant pour la commission de l'infraction. La Cour considère aussi qu'une condamnation fondée essentiellement sur les déclarations des « agents provocateurs » méconnaît le droit à un procès équitable.

54. Le recours à des agents infiltrés, à des informateurs occultes ou à des témoins anonymes entraîne des questions juridiques particulières. Bien que la Convention n'interdise pas le recours à des informateurs occultes au stade de l'enquête préliminaire, l'emploi des informations ainsi obtenues au stade du procès pose un problème d'équité. Dans ce contexte, la Cour part du principe que les moyens de preuve doivent être présentés à l'audience et contradictoirement débattus ; toutefois cela n'interdit pas l'usage devant le tribunal de dépositions faites lors de l'instruction, pourvu que leurs auteurs aient pu être confrontés à la défense avant l'audience. La question du recours à des témoignages anonymes dont les auteurs ne comparaissent pas à l'audience pour des raisons de sécurité et dont l'identité reste inconnue de la défense, et parfois même des juges du fond, doit être examinée. L'admissibilité de tels témoignages anonymes dépend des circonstances de l'affaire et de la réponse à trois questions qui se dégagent de la jurisprudence : l'anonymat est-il justifié par une raison impérieuse ? Les limitations qui en résultent pour l'exercice effectif des droits de la défense ont-elles été assez compensées? La condamnation est-elle fondée exclusivement ou de façon décisive sur ces témoignages anonymes ?

c) Lignes directrices opérationnelles

Paragraphes 15 et 16 :

55. Comme indiqué plus haut, la recommandation définit spécifiquement l'utilisation des TSE dans le cadre des enquêtes financières et attire l'attention sur ce point. Ces investigations peuvent perturber des activités criminelles, en empêchant les auteurs de tirer profit de leur conduite, ou en bloquant l'accès aux fonds utilisés pour favoriser ces activités. En outre, les enquêtes financières peuvent permettre de dépister les produits d'activités criminelles afin de geler, saisir et confisquer les produits et les instruments d'infractions graves, y compris des actes de terrorisme, appartenant à des personnes physiques et, lorsque la législation nationale le prévoit, à des personnes morales.

56. La formulation du paragraphe 15 concernant l'identification et la confiscation des produits et des instruments est adaptée à celle de la Convention du Conseil de l'Europe relative au blanchiment, au

dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme (STCE n° 198).

Paragraphe 17 :

57. De la même façon, la recommandation appelle les Etats membres à utiliser les TSE dans le cadre d'enquêtes sur la cybercriminalité, à la fois pour enquêter sur des infractions commises dans ce domaine, mais aussi pour perturber leur exécution.

Paragraphe 18 :

58. La rétention et la conservation des données relatives au trafic et, lorsque la loi le prévoit, des données à caractère personnel, peuvent être nécessaires dans le cadre des enquêtes pénales portant sur des infractions graves, y compris des actes de terrorisme. Aux fins de cette recommandation, il convient de rappeler que le terme « données relatives au trafic » a été défini à l'article 1 d) de la Convention sur la Cybercriminalité du 23 novembre 2001 (STE n° 185). Il convient aussi de noter que le terme « fournisseur de services » a été défini à l'article 1 c) de cette même convention (STE n° 185).

59. Les Etats membres devraient assurer que l'accès aux données relatives au trafic conservées à d'autres fins par les autorités compétentes est conforme à la législation nationale et aux instruments internationaux, notamment l'article 8 de la Convention européenne des droits de l'homme et la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108).

60. Toutefois, le paragraphe 18 ne saurait être lu ou interprété d'une manière qui imposerait aux Etats membres d'introduire une législation sur la rétention et la conservation des données relatives au trafic qui irait au-delà des exigences déjà prévues par le droit national ou international.

Paragraphe 19 :

61. L'interception des communications est l'une des TSE les plus communément utilisées dans les Etats membres. Le paragraphe 19 prévoit que ces interceptions doivent satisfaire aux « exigences minimales de confidentialité, d'intégrité et de disponibilité ». Ces exigences signifient que l'information ne doit être accessible qu'à certaines personnes autorisées (confidentialité), qu'elle doit être authentique et complète, apportant ainsi un niveau de fiabilité minimum (intégrité), et que le système technique installé pour intercepter les communications doit être accessible chaque fois que cela est nécessaire (disponibilité).

Paragraphe 21 :

62. Le fait d'encourager les Etats membres à envisager de demander des conseils spécialisés au niveau national n'entraîne pas l'obligation de rechercher ces conseils auprès d'organisations non gouvernementales.

Chapitre III. Coopération nationale et internationale

Paragraphe 22 :

63. Le texte de la Recommandation Rec(2005)10 a été modifié pour qu'il mentionne la coopération nationale. Cette modification vise à tenir compte du document de réflexion sur les techniques spéciales d'enquête (CODEXTER (2014)1) dans la mesure où il suggère de déterminer la manière d'améliorer la collecte et le partage des renseignements entre les diverses autorités compétentes participant à la lutte contre le terrorisme tant au niveau international que national.

64. Le terme « accords internationaux », repris dans ce paragraphe, recouvre non seulement les traités et instruments multilatéraux mais également les traités et instruments bilatéraux. De plus, il est fait référence à des accords avec le secteur privé. Ceux-ci doivent être interprétés comme des accords nécessaires pour l'échange d'informations à caractère purement technique concernant l'avènement de nouveaux outils qui pourraient être utilisés pour les techniques spéciales d'enquête et pour garantir une formation actualisée des autorités concernées. Ce terme ne vise pas à désigner des accords d'entraide judiciaire.

65. Les Etats doivent veiller à ce que les autorités compétentes aient accès en temps opportun à des informations sur les enquêtes, notamment des informations issues de la surveillance et des informations

financières sur les personnes visées par l'enquête, par exemple relatives à leurs avoirs, à des personnes physiques ou (si la législation nationale le prévoit) morales et à des transactions de tout type. Les dispositions pertinentes figurent dans la Convention de Varsovie (STCE n° 198) – articles 7, 17, 18 et 19.

66. La mention des questions de compétence liées à l'application des techniques spéciales d'enquête aux investigations sur la cybercriminalité traduit une certaine inquiétude sur le fait que les Etats membres ne devraient pas avoir recours aux TSE pour se soustraire aux mesures traditionnelles de coopération internationale et interférer avec le principe de territorialité et de souveraineté des autres Etats. La Convention sur la cybercriminalité (STE n° 185) prévoit, à l'article 32, deux cas de figure dans lesquels une Partie est autorisée à accéder à des données informatiques stockées sur le territoire d'une autre Partie sans faire une demande d'entraide judiciaire. Les autres situations ne sont cependant ni autorisées ni exclues. Les termes « questions de compétence liées à l'application des techniques spéciales d'enquête sur internet » désignent uniquement les actions entreprises entre des Etats et n'ont aucune incidence sur d'éventuels accords de coopération avec le secteur privé.

Paragraphe 23 :

67. Le texte a été mis à jour afin de prendre en compte les conventions et instruments fondamentaux les plus récents, tels que : la Convention pour la prévention du terrorisme du 16 mai 2005 (STCE n° 196) et son Protocole additionnel du 22 octobre 2015 (STCE n° 217) ; la Convention du Conseil de l'Europe relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme du 16 mai 2005 (STCE n° 198) ; et le Protocole additionnel à la Convention sur la cybercriminalité relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE n° 189). Les Etats membres sont par ailleurs encouragés à prêter attention aux résolutions pertinentes du Conseil de sécurité des Nations Unies, notamment la Résolution 2178, ainsi qu'aux normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération, dont les recommandations du GAFI.

Paragraphe 24 :

68. La référence au « Conseil de l'Europe », qui figure dans ce paragraphe, vise à inviter les Etats membres à accroître leur participation dans les différents comités en place, ou à créer par le Comité des Ministres, mais également dans les futures conférences européennes ou réunions que le Conseil de l'Europe pourrait organiser sur des thèmes en relation avec l'utilisation des TSE. Le texte modifié fait en outre référence à d'autres organisations, institutions, juridictions et instances, partenaires clés du Conseil de l'Europe, qui ont acquis une expérience inestimable dans l'utilisation des TSE en coopération avec les Etats et organisations concernés.

Paragraphe 25 :

69. Ce paragraphe a été modifié pour encourager davantage les Etats membres à échanger des informations spontanément, c'est-à-dire sans demande préalable. Il se fonde sur l'idée que les Etats membres devraient surmonter les problèmes pratiques qui entravent une coopération efficace en renforçant les échanges au niveau opérationnel entre les autorités compétentes. Parmi ces « problèmes pratiques » figurent, par exemple, ceux ayant trait aux procédures de travail, y compris les retards injustifiés, le manque d'informations, le manque de connaissances linguistiques, la bureaucratie injustifiée, les lenteurs dans la transmission d'informations, les points de contact non appropriés, les questions financières et tout autre problème technique pertinent. Ce paragraphe envisage également une assistance et un échange d'informations proactifs et spontanés entre les autorités compétentes et les autres Etats membres, si nécessaire.

Paragraphe 26 :

70. Ce paragraphe s'appuie sur l'idée que des références techniques communes dans le domaine des TSE devraient faciliter la coopération internationale. En ce qui concerne les « normes internationalement acceptées », il conviendrait d'accorder une attention particulière aux travaux menés par l'Institut européen de normalisation des télécommunications (ETSI) et l'Union internationale des télécommunications (UIT) à cet égard[9].

[9] Pour de plus amples informations : http://portal.etsi.org/li/Summary.asp ; www.etsi.org et http://www.itu.int/fr/Pages/default.aspx