

I

(Résolutions, recommandations et avis)

AVIS

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Avis du Contrôleur européen de la protection des données sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE)

(2011/C 279/01)

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES, vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ⁽¹⁾,

vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ⁽²⁾,

vu le règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données ⁽³⁾, et notamment son article 41,

A ADOPTÉ L'AVIS SUIVANT

I. INTRODUCTION

I.1. Publication du rapport

1. Le 18 avril 2011, la Commission a présenté son rapport d'évaluation concernant la directive sur la conservation des données (ci-après le «rapport d'évaluation») ⁽⁴⁾. Le rapport d'évaluation a été envoyé à titre d'information au CEPD à cette même date. Pour les raisons exposées à la section I.2 ci-dessous, le CEPD émet le présent avis de sa propre initiative, conformément à l'article 41 du règlement (CE) n° 45/2001.

⁽¹⁾ JO L 281 du 23.11.1995, p. 31.

⁽²⁾ JO L 201 du 31.7.2002, p. 37 tel que modifié par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009, JO L 337 du 18.12.2009, p. 11.

⁽³⁾ JO L 8 du 12.1.2001, p. 1.

⁽⁴⁾ COM(2011) 225 final.

2. Avant l'adoption de la communication, le CEPD a eu la possibilité de formuler des commentaires informels. Le CEPD est heureux de constater que plusieurs de ces commentaires ont été pris en compte par la Commission lors de la rédaction de la version finale du document.

3. La Commission a préparé le rapport d'évaluation en vue de satisfaire à son obligation énoncée à l'article 14 de la directive sur la conservation des données et consistant à évaluer l'application de la directive et ses effets sur les opérateurs économiques et les consommateurs, afin de déterminer s'il y a lieu de modifier les dispositions de la directive ⁽⁵⁾. Le CEPD est heureux de constater que, bien que l'article 14 ne l'exige pas au sens strict, la Commission a également tenu compte dans le rapport des «effets de la directive sur les droits fondamentaux, compte tenu des critiques formulées, de manière générale, à l'encontre de la conservation des données» ⁽⁶⁾.

I.2. Raisons et finalité du présent avis du CEPD

4. La directive sur la conservation des données constituait une réponse de l'UE à des défis de sécurité urgents, après les attentats terroristes de Madrid en 2004 et de Londres en 2005. Malgré la finalité légitime de la mise en place d'un système de conservation des données, des voix se sont élevées contre l'impact considérable que la mesure pouvait avoir sur la vie privée des citoyens.
5. L'obligation de conserver les données conformément à la directive sur la conservation des données permet aux autorités nationales compétentes de retracer le comportement téléphonique et internet de tous les individus dans l'UE utilisant le téléphone ou l'internet, et ce pendant une période de deux ans.

⁽⁵⁾ La directive sur la conservation des données (directive 2006/24/CE) a été adoptée le 15 mars 2006 et publiée au JO L 105 du 13.4.2006, p. 54. La date limite pour l'élaboration du rapport avait été fixée au 15 septembre 2010, voir article 14, paragraphe 1, de la directive sur la conservation des données.

⁽⁶⁾ Voir p. 1 du rapport d'évaluation.

6. La conservation des données de télécommunications va clairement à l'encontre du droit à la vie privée des personnes concernées tel qu'énoncé à l'article 8 de la Convention européenne des droits de l'homme (ci-après dénommée «CEDH») et à l'article 7 de la Charte des droits fondamentaux de l'Union européenne.
7. La Cour européenne des droits de l'homme (ci-après dénommée la «Cour européenne») n'a eu cesse de rappeler que «le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 [CEDH]»⁽⁷⁾. S'agissant des données téléphoniques en particulier, la Cour européenne a déclaré que la «divulgaration de ces informations à la police sans le consentement de l'abonné équivaut aussi [...] à une ingérence au sens de l'article 8 [CEDH]»⁽⁸⁾.
8. Il découle de l'article 8, paragraphe 2, de la CEDH et de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne qu'une ingérence peut se justifier pour autant que cette ingérence soit prévue par la loi, qu'elle serve un but légitime et qu'elle soit nécessaire dans une société démocratique pour atteindre ce but légitime.
9. Le CEPD a reconnu que la disponibilité de certaines données de trafic et de localisation peut être cruciale pour les services répressifs dans la lutte contre le terrorisme et d'autres infractions graves. Toutefois, dans le même temps, le CEPD n'a eu de cesse d'exprimer des doutes concernant les raisons justifiant la conservation de données dans une telle mesure à la lumière des droits au respect de la vie privée et de la protection des données⁽⁹⁾. Ces doutes ont été partagés par de nombreuses organisations de la société civile⁽¹⁰⁾.
10. Depuis 2005, le CEPD suit de près la création, la mise en œuvre et l'évaluation de la directive de différentes manières. Le CEPD a rendu un avis critique en 2005, après la publication de la proposition de directive par la Commission⁽¹¹⁾. Après l'adoption de la directive, le CEPD est devenu membre du groupe d'experts en matière de conservation des données, dont il est question au considérant 14 de la directive sur la conservation des données⁽¹²⁾. En outre, le CEPD participe au travail du groupe de travail «Article 29», qui a publié plusieurs documents sur le sujet, le plus récent étant un rapport de juillet 2010 sur la manière dont la directive a été appliquée en pratique⁽¹³⁾. Enfin, le CEPD a agi en tant que partie intervenante dans une affaire portée devant la Cour européenne de justice, dans laquelle la validité de la directive était contestée⁽¹⁴⁾.
11. L'importance du rapport d'évaluation et du processus d'évaluation ne peut être surestimée⁽¹⁵⁾. La directive sur la conservation des données constitue un exemple frappant d'une mesure de l'UE visant à assurer la disponibilité pour des activités répressives des données générées et traitées dans le contexte des communications électroniques. Maintenant que la mesure est en place depuis plusieurs années, une évaluation de son application pratique devrait véritablement prouver la nécessité et la proportionnalité de la mesure à la lumière des droits au respect de la vie privée et de la protection des données à caractère personnel. À cet égard, le CEPD a baptisé l'évaluation «le moment de vérité» pour la directive sur la conservation des données⁽¹⁶⁾.
12. L'actuel processus d'évaluation a également une incidence sur d'autres instruments réglementant la gestion des informations, notamment le traitement de quantités importantes de données à caractère personnel, dans le domaine «liberté, sécurité et justice». Dans une communication de 2010, la Commission a conclu que les mécanismes d'évaluation des divers instruments étaient extrêmement variés⁽¹⁷⁾. Le CEPD estime que la procédure d'évaluation actuelle devrait être utilisée pour guider l'évaluation d'autres instruments de l'UE et pour assurer que seules les mesures véritablement justifiées restent en place.
13. Dans ce contexte, le CEPD souhaite partager ses réflexions sur les conclusions présentées dans le rapport d'évaluation par le biais d'un avis public. Cet avis intervient à un stade précoce du processus, afin de fournir une contribution efficace et constructive aux discussions à venir, le cas échéant dans le contexte d'une nouvelle proposition législative telle que celle mentionnée par la Commission dans le rapport d'évaluation⁽¹⁸⁾.

1.3. Structure de l'avis

14. Le présent avis analysera et débattrà du contenu du rapport d'évaluation du point de vue du respect de la vie privée et de la protection des données à caractère personnel. L'analyse tentera de déterminer si la directive sur la conservation des données satisfait aux exigences définies par ces deux droits fondamentaux. L'analyse tentera également de déterminer si la nécessité de la conservation des données telle qu'arrêtée par la directive a été suffisamment démontrée.

15. Le présent avis est organisé comme suit. La section II présentera le contenu principal de la directive sur la conservation des données et son lien avec la directive 2002/58/CE

⁽⁷⁾ Voir à titre d'information Cour européenne des droits de l'homme, 4 décembre 2008, *S. et Marper contre Royaume-Uni*, 30562/04 et 30566/04, paragraphe 67.

⁽⁸⁾ Voir Cour européenne des droits de l'homme, 2 août 1984, *Malone contre Royaume-Uni*, A-82, paragraphe 84.

⁽⁹⁾ Voir l'avis du CEPD du 26 septembre 2005, JO C 298 du 29.11.2005, p. 1. Lors d'une conférence organisée par la Commission en décembre 2010, le CEPD a qualifié l'instrument comme étant «sans aucun doute l'instrument le plus préjudiciable au respect de la vie privée jamais adopté par l'Union européenne eu égard à son ampleur et au nombre de personnes qu'elle touche», voir le discours du 3 décembre 2010, consultable sur le site web du CEPD (<http://www.edps.europa.eu>) sous «Publications» >> «Discours & Articles» >> «2010».

⁽¹⁰⁾ Voir à ce sujet la lettre datée du 22 juin 2010 d'un groupe important d'organisations de la société civile aux commissaires Malmström, Reding et Kroes (http://www.vorratsdatenspeicherung.de/images/DRletter_Malmstroem.pdf).

⁽¹¹⁾ Voir l'avis du CEPD cité à la note de bas de page 9.

⁽¹²⁾ Voir en outre la décision de la Commission du 25 mars 2008, JO L 111 du 23.4.2008, p. 11.

⁽¹³⁾ Voir WP 172 du 13 juillet 2010, rapport 1/2010 sur la deuxième action commune de contrôle de l'application de la législation UE.

⁽¹⁴⁾ Voir Cour de justice européenne, 10 février 2009, *Irlande contre Parlement et Conseil*, C-301/06. Voir également point 29 ci-dessous.

⁽¹⁵⁾ Dans son avis de 2005, le CEPD avait déjà souligné l'importance d'évaluer l'instrument (voir note de bas de page 9, points 72-73).

⁽¹⁶⁾ Voir le discours du 3 décembre 2010 cité à la note de bas de page 9.

⁽¹⁷⁾ COM(2010) 385 du 20 juillet 2010, *Présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice*, p. 24. Voir l'avis du CEPD du 30 septembre 2010 sur cette communication, consultable sur le site web du CEPD (<http://www.edps.europa.eu>) sous «Consultation» >> «Avis» >> «2010».

⁽¹⁸⁾ Voir p. 32 du rapport d'évaluation.

concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (ci-après la «directive vie privée et communications électroniques») ⁽¹⁹⁾. La section III exposera brièvement les changements apportés par le traité de Lisbonne, puisque ceux-ci sont particulièrement importants pour le sujet en question et qu'ils ont des conséquences directes sur la manière dont les règles de l'UE doivent être perçues, évaluées et éventuellement révisées. La section la plus longue de l'avis, la section IV, contient l'analyse de la validité de la directive sur la conservation des données, à la lumière des droits à la vie privée et à la protection des données à caractère personnel et par rapport aux conclusions présentées dans le rapport d'évaluation. La section V présentera les éventuelles pistes à suivre. L'avis s'achève par une conclusion, la section VI.

II. LES RÈGLES DE L'UE SUR LA CONSERVATION DES DONNÉES

16. Dans le contexte du présent avis, la conservation des données désigne l'obligation des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications de conserver les données relatives au trafic et les données de localisation ainsi que les données connexes nécessaires à l'identification de l'abonné ou de l'utilisateur pendant une certaine période. Cette obligation est énoncée dans la directive sur la conservation des données, qui spécifie dans son article 5, paragraphe 1, les catégories de données à conserver. En vertu de l'article 6 de la directive, les États membres veillent à ce que ces données soient conservées pendant une durée minimale de six mois et maximale de deux ans à compter de la date de la communication.
17. Les données doivent être conservées dans la mesure où elles sont générées ou traitées dans le cadre de la fourniture des services de communications concernés par des fournisseurs de services de communications électroniques (article 3). Ces données incluent également les données relatives aux appels téléphoniques infructueux. Aucune donnée révélant le contenu de la communication ne peut être conservée au titre de la directive (article 5, paragraphe 1).
18. Les données sont conservées en vue de garantir la disponibilité de ces données à des fins de «recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne» (article 1, paragraphe 1).
19. La directive sur la conservation des données ne contient aucune règle supplémentaire sur les conditions en vertu desquelles les autorités nationales compétentes peuvent accéder aux données conservées. Ceci est laissé à la discrétion des États membres et est considéré comme ne relevant pas du champ d'application de la directive. L'article 4 de la directive souligne que ces règles nationales doivent être conformes aux exigences de nécessité et de proportionnalité, telles qu'énoncées, en particulier, dans la CEDH.
20. La directive sur la conservation des données est étroitement liée à la directive sur la vie privée et les communications électroniques. Cette directive, qui particularise et complète la directive générale sur la protection des données à caractère personnel 95/46/CE, stipule que les États membres doivent préserver la confidentialité des communications et

les données relatives au trafic ⁽²⁰⁾. La directive sur la vie privée et les communications électroniques dispose que ces données relatives au trafic générées par l'utilisation des services de communication électronique doivent, en principe, être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication, hormis si et uniquement aussi longtemps qu'elles sont nécessaires à la facturation ⁽²¹⁾. Sous réserve du consentement des utilisateurs ou des abonnés, certaines données peuvent être traitées pour la durée nécessaire à la fourniture d'un service à valeur ajoutée.

21. Conformément à l'article 15, paragraphe 1, de la directive sur la vie privée et les communications électroniques, il est possible pour les États membres de prendre des mesures législatives pour limiter la portée des obligations ci-dessus lorsqu'il s'agit d'une mesure «nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour des raisons spécifiques d'ordre public, à savoir pour sauvegarder la sécurité nationale (c'est-à-dire la sûreté de l'État), la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales [...]». La question de la conservation des données est explicitement mentionnée à l'article 15, paragraphe 1, de la directive sur la vie privée et les communications électroniques. Les États membres peuvent «adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée» lorsque cela est justifié par un des motifs énoncés.
22. La directive sur la conservation des données avait pour objet d'aligner les initiatives des États membres en vertu de l'article 15, paragraphe 1, en ce qui concerne la conservation des données pour la recherche, la détection et la poursuite d'infractions pénales. Il convient de souligner que la directive sur la conservation des données constitue une exception à l'obligation générale consacrée dans la directive sur la vie privée et les communications électroniques d'effacer les données lorsqu'elles ne sont plus nécessaires ⁽²²⁾.
23. Avec l'adoption de la directive sur la conservation des données, un paragraphe supplémentaire 1 a) a été inséré à l'article 15 de la directive sur la vie privée et les communications électroniques précisant que l'article 15, paragraphe 1, n'est pas applicable aux données dont la conservation est exigée par la directive sur la conservation des données aux fins précisées à l'article 1, paragraphe 1, de cette directive.
24. Le rapport d'évaluation note, comme il sera plus amplement débattu dans la section IV.3 ci-dessous, que l'article 15, paragraphe 1, et l'article 15, paragraphe 1, point b), ont été utilisés par plusieurs États membres pour utiliser les données conservées au titre de la directive sur la conservation des données à d'autres finalités également ⁽²³⁾. Le CEPD a qualifié cette situation de «vide juridique» dans le cadre juridique, ce qui entrave l'objectif de la directive sur la conservation des données, à savoir celui de créer des conditions égales pour les entreprises ⁽²⁴⁾.

⁽¹⁹⁾ Cf. note 2.

⁽²⁰⁾ Voir article 5 de la directive sur la vie privée.

⁽²¹⁾ Voir articles 6 et 9 de la directive sur la vie privée.

⁽²²⁾ Voir également WP 29 dans le rapport du 13 juillet 2010, dont il est question à la note de bas de page 13, p. 1.

⁽²³⁾ Voir p. 8 du rapport d'évaluation. Voir également à cet égard le considérant 12 de la directive sur la conservation des données.

⁽²⁴⁾ Voir le discours du 3 décembre 2010 dont question à la note de bas de page 9, p. 4.

III. LE CONTEXTE JURIDIQUE DE L'UE A CHANGÉ APRÈS LISBONNE

25. Le contexte juridique général de l'UE pertinent pour la directive sur la conservation des données a changé considérablement avec l'entrée en vigueur du traité de Lisbonne. Un grand changement a été l'abolition de la structure en piliers, qui avait établi différentes procédures législatives et mécanismes de révision pour les différents domaines relevant de la compétence de l'UE.
26. La structure antérieure en piliers suscitait régulièrement des discussions sur la base juridique appropriée d'un instrument de l'UE lorsqu'un sujet particulier relevait de la compétence de différents piliers. Le choix d'une base juridique était on ne peut plus important puisqu'il débouchait sur des procédures législatives différentes eu égard, par exemple, aux exigences de vote au Conseil (majorité qualifiée ou unanimité) ou l'implication du Parlement européen.
27. Ces discussions étaient extrêmement importantes pour la conservation des données. Puisque la directive sur la conservation des données visait à harmoniser l'obligation des opérateurs, et donc à éliminer les obstacles au marché interne, la base juridique pouvait se trouver à l'article 95 de l'ancien traité instituant la CE (l'ancien premier pilier). Cependant, la question aurait pu être abordée du côté répressif, en faisant valoir que l'objectif de la conservation des données était de combattre les infractions graves, dans le cadre de la coopération policière et judiciaire en matière pénale dans l'ancien traité de l'UE (l'ancien troisième pilier) ⁽²⁵⁾.
28. À cette occasion, la directive sur la conservation des données a été adoptée sur la base de l'article 95 de l'ancien traité instituant la Communauté européenne, régissant uniquement les obligations des opérateurs. La directive ne comportait pas de règles sur l'accès et l'utilisation des données conservées par les autorités répressives.
29. Après son adoption, la validité de la directive a été contestée devant la Cour de justice européenne. Il a été dit que la directive aurait dû être basée sur le troisième pilier plutôt que le premier pilier, puisque l'objectif pour lequel les données devaient être conservées (la recherche, la détection et la poursuite des infractions graves) relevait de la compétence de l'UE au troisième pilier ⁽²⁶⁾. Toutefois, puisque les activités des autorités compétentes ont été explicitement exclues du champ d'application de la directive, la Cour de justice a conclu que la directive était basée à juste titre sur le traité instituant la Communauté européenne ⁽²⁷⁾.
30. Dès le départ, le CEPD a affirmé que si l'UE devait adopter un instrument sur la conservation des données, elle devait réglementer cette obligation des opérateurs, ainsi que l'accès et l'utilisation par les autorités répressives. Dans son avis de 2005 sur la proposition de la Commission, le CEPD a souligné que l'accès et l'utilisation ultérieure par les autorités nationales compétentes constituait une part essentielle et inséparable de cette question ⁽²⁸⁾.
31. Comme nous le développerons plus avant, les effets négatifs de la réglementation partielle de la question par l'UE ont été confirmés par le présent rapport d'évaluation. La Commission conclut que les divergences en droit national concernant l'accès et l'utilisation ultérieure par les autorités nationales compétentes ont créé des «difficultés considérables» pour les opérateurs ⁽²⁹⁾.
32. Avec l'abolition de la structure en piliers après l'entrée en vigueur du traité de Lisbonne, les deux domaines relevant de la compétence de l'UE ont été rassemblés dans le traité sur le fonctionnement de l'Union européenne, qui permet l'adoption de la législation de l'UE sous réserve de la même procédure législative. Ce nouveau contexte permettrait l'adoption d'un nouvel instrument unique sur la conservation des données réglementant les obligations pour les opérateurs ainsi que les conditions d'accès et d'utilisation ultérieure par les autorités répressives. Comme nous l'expliquerons dans la section IV.3 ci-dessous, les droits à la vie privée et à la protection des données à caractère personnel requièrent, lorsqu'une mesure révisée de l'UE sur la conservation des données est considérée, qu'elle régleme au moins la question dans sa globalité.
33. Le traité de Lisbonne a non seulement aboli la structure en piliers, mais il a aussi accordé à la Charte des droits fondamentaux de l'Union européenne, anciennement non-contraignante, et qui incluait les droits à la vie privée et à la protection des données dans ses articles 7 et 8, la même valeur juridique que celle des traités ⁽³⁰⁾. Un droit subjectif à la protection des données a en outre été inclus à l'article 16 du traité sur le fonctionnement de l'Union européenne, créant une base juridique distincte pour les instruments de l'UE sur la protection des données à caractère personnel.
34. La protection des droits fondamentaux est depuis longtemps une pierre angulaire de la politique de l'UE, et le traité de Lisbonne a renforcé l'engagement envers ces droits dans le contexte de l'UE. Les changements induits par le traité de Lisbonne ont poussé la Commission à annoncer en octobre 2010 la promotion d'une «culture des droits fondamentaux» à toutes les étapes du processus législatif et à déclarer que la Charte des droits fondamentaux de l'Union européenne «doit être un guide pour les politiques de l'Union» ⁽³¹⁾. Le CEPD estime que le processus d'évaluation actuel offre à la Commission une bonne occasion de prouver cet engagement.

⁽²⁵⁾ Une première proposition pour une réglementation de l'UE sur la conservation des données (une décision cadre) était basée sur l'ancien traité de l'UE, présentée par la France, l'Irlande, la Suède et le Royaume-Uni. Voir le document du Conseil 8958/04 du 28 avril 2004. Cette proposition a été suivie par une proposition de la Commission basée sur le traité instituant la Communauté européenne. Voir COM(2005) 438 du 21 septembre 2005.

⁽²⁶⁾ Cet argument était basé sur l'arrêt rendu par la Cour de justice dans les affaires «Passenger Name Record», voir Cour européenne de justice, 30 mai 2006, *Parlement européen contre Conseil de l'Union européenne et Commission des Communautés européennes*, C-317/05 et C-318/04.

⁽²⁷⁾ Voir Cour européenne de justice, 10 février 2009, *Irlande contre Parlement européen et Conseil de l'Union européenne*, C-301/06, points 82-83.

⁽²⁸⁾ Voir l'avis de 2005, point 80. Voir également à ce sujet la section IV.3 du présent avis.

⁽²⁹⁾ Voir p. 31 du rapport d'évaluation.

⁽³⁰⁾ Voir article 6, paragraphe 1, du traité sur le fonctionnement de l'Union européenne.

⁽³¹⁾ COM(2010) 573 du 19 octobre 2010, *Stratégie pour la mise en œuvre effective de la Charte des droits fondamentaux par l'Union européenne*, p. 4.

IV. LA DIRECTIVE SUR LA CONSERVATION DES DONNÉES EST-ELLE CONFORME AUX EXIGENCES EN MATIÈRE DE VIE PRIVÉE ET DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL?

35. Le rapport d'évaluation met en évidence plusieurs faiblesses de la présente directive sur la conservation des données. Les informations fournies dans le rapport montrent que la directive n'a pas réussi à atteindre son objectif principal, à savoir harmoniser les législations nationales en matière de conservation des données. La Commission note des différences «sensibles» entre les mesures de transposition régissant la limitation des finalités, l'accès aux données, les durées de conservation, la protection et la sécurité des données, et les statistiques⁽³²⁾. D'après la Commission, les différences sont partiellement dues au degré de variance expressément prévu par la directive. La Commission affirme, cependant, qu'au-delà de ce degré de variance, «les divergences dans l'application nationale de la conservation des données ont créé des difficultés considérables pour les opérateurs» et que «l'insécurité juridique demeure pour le secteur»⁽³³⁾. Il va sans dire qu'un tel manque d'harmonisation ne peut qu'être préjudiciable à toutes les parties concernées: les citoyens, les chefs d'entreprise ainsi que les autorités répressives.
36. Du point de vue de la vie privée et de la protection des données à caractère personnel, le rapport d'évaluation arrive également à la conclusion que la directive sur la conservation des données ne satisfait pas aux exigences imposées par les droits à la vie privée et à la protection des données à caractère personnel. Plusieurs défauts ont été relevés: la nécessité de la conservation des données telle qu'arrêtée par la directive sur la conservation des données n'a pas été suffisamment démontrée, la conservation des données aurait pu, dans tous les cas, être réglementée d'une manière moins intrusive dans la vie privée, et la directive sur la conservation des données manque de «prévisibilité». Ces trois points seront développés plus avant.

IV.1. La nécessité de la conservation des données telle qu'arrêtée par la directive sur la conservation des données n'a pas été suffisamment démontrée

37. Une ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel est autorisée pour autant que la mesure soit nécessaire à la réalisation d'un but légitime. La nécessité de la conservation des données en tant que mesure répressive a toujours fait l'objet de discussions majeures⁽³⁴⁾. Dans la proposition de directive, il est dit que les limitations prévues sur les droits à la vie privée et à la protection des données à caractère personnel étaient «nécessaires pour atteindre les objectifs, généralement reconnus, de prévention de la criminalité et du terrorisme et de lutte contre ces phénomènes»⁽³⁵⁾. Toutefois, dans l'avis de 2005, le CEPD a indiqué ne pas être convaincu par cette déclaration, puisqu'elle nécessitait d'autres éléments de preuve pour déterminer si tel est réellement le cas⁽³⁶⁾. Néanmoins, sans l'apport d'éléments de preuve supplémentaires, le considérant 9 de la directive sur

la conservation des données dispose que «la conservation des données s'est révélée être un outil d'investigation nécessaire et efficace pour les enquêtes menées par les services répressifs dans plusieurs États membres».

38. En raison d'un manque d'éléments de preuve suffisants, le CEPD a affirmé que la directive sur la conservation des données reposait uniquement sur la supposition que la conservation des données telle qu'arrêtée par la directive constituait une mesure nécessaire⁽³⁷⁾. Le CEPD a dès lors appelé la Commission et les États membres à profiter du rapport d'évaluation pour fournir des éléments de preuve supplémentaires venant confirmer la nécessité de la mesure de conservation des données et que la manière dont elle était réglementée dans la directive sur la conservation des données était bel et bien correcte.
39. Sur ce point, la Commission affirme dans le rapport d'évaluation que «les États membres estiment pour la plupart que les règles de l'Union relatives à la conservation des données demeurent nécessaires à la mission des services répressifs, à la protection des victimes et aux systèmes de justice pénale». On estime en outre que la conservation des données joue un «rôle capital» dans les enquêtes judiciaires, qu'elle est «au moins utile et, dans certains cas, indispensable», et que sans elle, certaines infractions pénales «seraient restées impunies»⁽³⁸⁾. La Commission conclut que l'UE devrait par conséquent «encourager et réglementer la conservation des données en tant que mesure de sécurité»⁽³⁹⁾.
40. Il est très discutable, cependant, que la Commission puisse conclure que les États membres pour la plupart estiment la conservation des données comme un outil nécessaire. Il n'est nulle part indiqué quels sont les États membres composant la majorité, laquelle, dans une UE de 27 États membres, devrait être d'au moins 14 pour pouvoir parler de la plupart des États membres. Le nombre d'États membres mentionnés au chapitre 5, et sur lequel se basent les conclusions, est de neuf tout au plus⁽⁴⁰⁾.
41. En outre, il semble que la Commission se base principalement sur des déclarations des États membres sur leur perception de la conservation des données comme étant un outil nécessaire aux fins de la répression. Ces déclarations, cependant, indiquent plutôt que les États membres concernés sont heureux d'avoir des règles de l'UE sur la conservation des données, mais ne peuvent en soi établir la nécessité de la conservation des données en tant que mesure répressive, encouragée et réglementée par l'UE. Ces déclarations sur la nécessité doivent être corroborées par des éléments de preuve suffisants.
42. Certes, démontrer la nécessité d'une mesure intrusive dans la vie privée n'est pas chose aisée. Et surtout pas pour la Commission, qui dépend largement des informations fournies par les États membres.
43. Toutefois, si une mesure est déjà en place, telle que la directive sur la conservation des données, et qu'une expérience pratique a été acquise, il devrait y avoir suffisamment d'informations qualitatives et quantitatives disponibles

⁽³²⁾ Voir p. 36 du rapport d'évaluation.

⁽³³⁾ Voir p. 36 du rapport d'évaluation.

⁽³⁴⁾ Voir l'avis du CEPD de 2005. Voir également la lettre du 22 juin 2010 d'un groupe important d'organisations de la société civile, citée à la note de bas de page 10.

⁽³⁵⁾ COM(2005) 438 du 21 septembre 2005, p. 3.

⁽³⁶⁾ Voir l'avis de 2005, points 17-22.

⁽³⁷⁾ Voir le discours du 3 décembre 2010 cité à la note de bas de page 9.

⁽³⁸⁾ Toutes les citations sont extraites des p. 26 ou 35 du rapport d'évaluation.

⁽³⁹⁾ Voir p. 35 du rapport d'évaluation.

⁽⁴⁰⁾ République tchèque, Slovaquie, Royaume-Uni, Allemagne, Pologne, Finlande, Pays-bas, Irlande et Hongrie.

permettant d'évaluer si la mesure fonctionne véritablement et si des résultats comparables auraient pu être obtenus sans cet instrument ou avec un moyen alternatif moins intrusif dans la vie privée. Ces informations devraient constituer une preuve authentique et montrer la relation entre utilisation et résultat ⁽⁴¹⁾. En ce qui concerne la directive de l'UE, les informations doivent en outre représenter la pratique d'au moins la majorité des États membres de l'UE.

44. Après une analyse minutieuse, le CEPD estime que, bien que la Commission ait clairement consenti bon nombre d'efforts dans la collecte d'informations auprès des gouvernements des États membres, les informations quantitatives et qualitatives fournies par les États membres ne sont pas suffisantes pour confirmer la nécessité de la conservation des données telle qu'arrêtée par la directive sur la conservation des données. Des exemples intéressants de son utilisation ont été fournis, mais il y a tout simplement trop de lacunes dans les informations présentées dans le rapport pour pouvoir tirer des conclusions générales sur la nécessité de l'instrument. De plus, une recherche plus approfondie sur des moyens alternatifs doit encore être réalisée. Ces deux points seront développés plus avant.

Les informations quantitatives et qualitatives fournies dans le rapport d'évaluation

45. S'agissant des informations statistiques quantitatives présentées principalement au chapitre 5 et à l'annexe du rapport d'évaluation, des informations cruciales font défaut. Par exemple, les statistiques n'indiquent pas les finalités pour lesquelles les données ont été conservées. De plus, les chiffres n'indiquent pas si toutes les données auxquelles l'accès a été accordé étaient des données enregistrées du fait de l'obligation juridique de conserver les données ou dans un but commercial. Par ailleurs, aucune information n'est fournie concernant les résultats de l'utilisation des données. Il est en outre problématique, pour tirer des conclusions, que les informations des différents États membres ne soient pas toujours totalement comparables et que, dans de nombreux cas, les tableaux ne représentent que neuf États membres.
46. Les exemples qualitatifs fournis dans le rapport offrent une meilleure illustration du rôle important joué par les données conservées dans certaines situations spécifiques et des avantages potentiels d'un système de conservation des données. Cependant, rien ne permet d'affirmer avec certitude que l'utilisation des données conservées était le seul moyen de résoudre le crime ou délit en question.
47. Certains exemples illustrent le caractère indispensable de la mesure de conservation des données pour combattre la cybercriminalité. À cet égard, il convient de noter que le principal instrument international dans ce domaine, la convention du Conseil de l'Europe sur la cybercriminalité, n'envisage pas la conservation des données comme une mesure pour lutter contre la cybercriminalité, mais plutôt comme un moyen d'enquête ⁽⁴²⁾.

⁽⁴¹⁾ Voir sur le principe de nécessité et de proportionnalité l'avis du CEPD du 25 mars 2011 sur la proposition «Passenger Name Record» de l'UE, consultable sur le site web du CEPD (<http://www.edps.europa.eu>) sous «Consultation» >> «Avis» >> «2011».

⁽⁴²⁾ Voir également p. 5 du rapport d'évaluation.

48. La Commission semble accorder un poids considérable aux exemples fournis par les États membres dans lesquels les données conservées ont été utilisées pour exclure des suspects des scènes de crime et vérifier des alibis ⁽⁴³⁾. Bien qu'il s'agisse d'exemples intéressants de la manière dont les données sont utilisées par les autorités répressives, ils ne peuvent être avancés comme démontrant la nécessité de la conservation des données. Cet argument doit être utilisé avec précaution car il peut être mal interprété, comme si la conservation des données était nécessaire pour prouver l'innocence des citoyens, ce qui serait difficile de concilier avec la présomption d'innocence.

49. Le rapport d'évaluation ne discute que très brièvement de la conservation des données en rapport avec les évolutions technologiques, et plus précisément l'utilisation des cartes SIM prépayées ⁽⁴⁴⁾. Le CEPD souligne que davantage d'informations quantitatives et qualitatives sur l'utilisation des nouvelles technologies non couvertes par la directive (par exemple le VoIP et les réseaux sociaux) auraient été instructives pour évaluer l'efficacité de la directive.

50. Le rapport d'évaluation est limité car il est essentiellement axé sur les informations quantitatives et qualitatives fournies par les États membres qui ont mis en œuvre la directive sur la conservation des données. Il aurait toutefois été intéressant de voir si des différences tangibles ont été constatées entre ces États membres et les États membres qui n'ont pas mis en œuvre la directive. En particulier pour les États membres dans lesquels la mise en œuvre de la législation a été annulée (Allemagne, Roumanie et République tchèque), il aurait été intéressant de voir s'il existe des preuves d'une hausse ou d'une chute du nombre d'enquêtes criminelles résolues, aussi bien avant qu'après ces annulations.

51. La Commission reconnaît que les statistiques et les exemples fournis dans le rapport d'évaluation sont «limités à certains points», mais conclut néanmoins que les preuves n'attestent «pas moins le rôle capital que les données conservées jouent dans les enquêtes judiciaires» ⁽⁴⁵⁾.

52. Le CEPD estime que la Commission aurait dû être plus critique à l'égard des États membres. Comme expliqué précédemment, les déclarations politiques de certains États membres sur la nécessité d'une telle mesure ne peuvent justifier à elles seules une action de l'UE. La Commission aurait dû insister pour que les États membres produisent des éléments suffisants démontrant la nécessité de la mesure. D'après le CEPD, la Commission aurait dû au moins conditionner son soutien à la conservation des données en tant que mesure de sécurité (voir p. 35 du rapport d'évaluation) à la communication par les États membres de preuves supplémentaires durant l'étude d'impact.

Moyens alternatifs

53. La nécessité de la conservation des données telle qu'arrêtée par la directive sur la conservation des données dépend également de l'existence de moyens alternatifs moins intrusifs dans la vie privée qui auraient pu produire des résultats comparables. Ceci a été confirmé par la Cour de justice dans son arrêt *Schecke* en novembre 2010, par lequel la législation de l'UE sur la publication des noms des

⁽⁴³⁾ Voir p. 27 du rapport d'évaluation.

⁽⁴⁴⁾ Voir p. 29 du rapport d'évaluation.

⁽⁴⁵⁾ Voir p. 35 du rapport d'évaluation.

- bénéficiaires des fonds agricoles a été annulée⁽⁴⁶⁾. Une des raisons de l'annulation était que le Conseil et la Commission n'avaient pas considéré des modalités alternatives de publication d'informations relatives aux bénéficiaires concernés qui seraient conformes à l'objectif d'une telle publication tout en étant moins attentatoires au droit de ces bénéficiaires au respect de leur vie privée et à la protection de leurs données à caractère personnel⁽⁴⁷⁾.
54. La principale alternative mise en avant dans les discussions entourant la directive sur la conservation des données est le mode de conservation a posteriori («quick freeze» ou gel immédiat et «quick freeze plus» ou gel immédiat plus)⁽⁴⁸⁾. Il s'agit de conserver temporairement ou de «geler» certaines données de trafic des télécommunications et de localisation portant uniquement sur des personnes déterminées soupçonnées d'activités criminelles, qui peuvent par la suite être mises à la disposition des autorités répressives avec une autorisation judiciaire.
55. La conservation des données a posteriori est citée dans le rapport d'évaluation dans le contexte de la Convention sur la cybercriminalité susmentionnée, mais elle est considérée comme étant inappropriée puisqu'elle «ne garantit pas la possibilité de remonter en amont de l'injonction de conservation, pas plus qu'elle ne permet de recueillir des preuves sur les mouvements des victimes ou des témoins d'une infraction, par exemple»⁽⁴⁹⁾.
56. Le CEPD reconnaît qu'un système de conservation des données a posteriori implique moins d'informations qu'un système général de conservation des données. Cependant, c'est précisément grâce à sa nature plus ciblée que la conservation des données a posteriori constitue un instrument moins intrusif dans la vie privée en termes de portée et de nombre de personnes concernées. L'évaluation doit non seulement s'intéresser aux données disponibles, mais également aux différents résultats obtenus avec les deux systèmes. Le CEPD estime qu'une étude plus approfondie de cette mesure s'avère justifiée et indispensable. Cela pourrait se faire dans le cadre de l'étude d'impact dans les mois à venir.
57. À cet égard, il est regrettable que dans les conclusions du rapport, la Commission s'engage à déterminer si une approche européenne à la conservation des données a posteriori peut compléter (et non remplacer) la conservation des données⁽⁵⁰⁾. La possibilité de combiner un quelconque système de conservation avec les garanties procédurales entourant les divers modes de conservation des données a posteriori mérite effectivement que l'on s'y intéresse de plus près. Toutefois, le CEPD recommande à la Commission de considérer aussi lors de l'étude d'impact si un système de conservation des données a posteriori, ou tout autre moyen alternatif, peut totalement ou partiellement se substituer au système actuel de conservation des données.
- IV.2. La conservation des données, telle qu'arrêtée par la directive sur la conservation des données va, dans tous les cas, au-delà de ce qui est nécessaire**
58. D'après le CEPD, les informations présentées dans le rapport d'évaluation ne contiennent pas suffisamment d'éléments de preuve pour démontrer la nécessité de la conservation des données telle qu'arrêtée par la directive sur la conservation des données. Cependant, le rapport d'évaluation permet de conclure que la directive sur la conservation des données a réglementé la conservation des données bien au-delà de ce qui est nécessaire, ou, tout au moins, qu'elle a été incapable de garantir que la conservation des données n'a pas été appliquée de manière abusive. À cet égard, quatre éléments peuvent être soulignés.
59. Primo, la finalité imprécise de la mesure et la notion plutôt large des «autorités nationales compétentes» a donné lieu à une utilisation des données conservées à des fins, et par des autorités, bien trop nombreuses. De plus, les garanties et conditions d'accès aux données manquent de cohérence. Par exemple, l'accès n'est pas conditionné à une approbation préalable par une autorité judiciaire ou une autre autorité indépendante dans tous les États membres.
60. Secundo, la période de conservation maximale de deux ans semble aller au-delà de ce qui est nécessaire. Les informations statistiques de certains États membres dans le rapport d'évaluation montrent qu'une grande majorité des demandes d'accès portent sur des données d'une ancienneté de six mois maximum, à savoir 86 %⁽⁵¹⁾. De plus, seize États membres ont opté pour une période de conservation d'un an ou moins dans leur législation⁽⁵²⁾. Ceci suggère fortement qu'une période de conservation maximale de deux ans va bien au-delà de ce qui est considéré comme nécessaire par la majorité des États membres.
61. En outre, l'absence d'une période de conservation fixée pour l'ensemble des États membres a créé toute une série de législations nationales divergentes, ce qui n'est pas sans poser de problèmes, puisqu'il n'est pas toujours évident de déterminer quelle législation nationale — que ce soit en matière de conservation des données ou de protection des données à caractère personnel — est applicable lorsque les opérateurs stockent des données dans un État membre autre que celui dans lequel les données sont collectées.
62. Tertio, le niveau de sécurité n'est pas suffisamment harmonisé. L'une des principales conclusions du groupe de travail «Article 29» dans son rapport de juillet 2010 épinglait la pléthore de mesures de sécurité mises en place dans les différents États membres. La Commission semble considérer les mesures de sécurité dans la directive actuelle comme suffisantes, puisque «aucun exemple concret d'atteintes graves à la vie privée» n'a été rapporté⁽⁵³⁾. Il semble cependant que la Commission ait uniquement demandé aux gouvernements des États membres de se prononcer sur la question. Afin d'évaluer l'adéquation des présentes règles et mesures de sécurité, une consultation plus large et un examen plus concret des cas d'abus s'avèrent nécessaires. Même si aucun exemple spécifique d'atteinte grave à la vie privée n'est mentionné dans le cadre du rapport, les

⁽⁴⁶⁾ Cour européenne de justice, novembre 2010, *Volker und Markus Schecke*, C-92/09 et C-93/09.

⁽⁴⁷⁾ Cour européenne de justice, *Schecke*, point 81.

⁽⁴⁸⁾ Le «gel immédiat» désigne le «gel» des données de trafic et de localisation portant uniquement sur des personnes déterminées soupçonnées d'une activité criminelle, à compter de la date de l'injonction judiciaire. Le «gel immédiat plus» inclut également le «gel» des données déjà détenues par les opérateurs à des fins de facturation et de transmission.

⁽⁴⁹⁾ Voir p. 6 du rapport d'évaluation.

⁽⁵⁰⁾ Voir p. 37 du rapport d'évaluation.

⁽⁵¹⁾ Voir p. 25 du rapport d'évaluation. Douze pour cent des demandes concernent des données entre six mois et un an et 2 % concernent des données remontant à plus d'un an.

⁽⁵²⁾ Voir p. 16 du rapport d'évaluation.

⁽⁵³⁾ Voir p. 35 du rapport d'évaluation.

atteintes à la sécurité des données et les scandales dans le domaine des données de trafic et des communications électroniques dans certains États membres constituent des signaux d'alerte clairs. La question ne peut être prise à la légère, puisque la sécurité des données conservées est d'une importance capitale pour un système de conservation des données en tant que tel, puisqu'elle garantit le respect de toutes les autres garanties ⁽⁵⁴⁾.

63. Quarto, le rapport ne permet pas de déterminer si toutes les catégories de données conservées se sont avérées nécessaires. Seules quelques distinctions générales sont établies entre données téléphoniques et internet. Certains États membres ont choisi d'imposer une période plus courte de conservation des données relatives à l'internet ⁽⁵⁵⁾. Toutefois, aucune conclusion générale ne peut être tirée à partir de ces éléments.

IV.3. La directive sur la conservation des données manquant de prévisibilité

64. Une autre lacune de la directive sur la conservation des données a trait à son manque de prévisibilité. L'exigence de prévisibilité provient de l'exigence générale contenue à l'article 8, paragraphe 2, de la CEDH et à l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, qui disposent qu'une ingérence dans la vie privée doit être prévue par la loi. D'après la Cour européenne des droits de l'homme, cela signifie qu'une mesure doit avoir un fondement juridique et qu'elle doit être compatible avec l'État de droit. Ceci implique que la loi soit accessible et prévisible ⁽⁵⁶⁾. La Cour de justice a également statué, dans l'affaire *Österreichischer Rundfunk*, que la loi doit «[être] libellé[e] avec suffisamment de précision pour permettre aux destinataires de la loi de régler leur conduite» ⁽⁵⁷⁾. Le droit doit indiquer de manière suffisamment claire la portée d'un tel pouvoir discrétionnaire conféré aux autorités compétentes ainsi que les modalités de son exercice ⁽⁵⁸⁾.
65. S'agissant de la check-list mentionnée dans la communication de la Commission sur la Charte des droits fondamentaux de l'Union européenne, une des questions qu'il convient de se poser est de savoir si la limitation des droits fondamentaux est formulée «de manière précise et prévisible» ⁽⁵⁹⁾. Dans sa communication sur la présentation générale de la gestion de l'information dans le domaine de la liberté, de la sécurité et de la justice, la Commission a également affirmé que les citoyens «ont le droit de connaître les données à caractère personnel les concernant qui sont traitées et échangées et de savoir par qui elles le sont et à quelle fin» ⁽⁶⁰⁾.
66. Dans le cas d'une directive de l'UE, la responsabilité de la conformité avec les droits fondamentaux, notamment

l'exigence de prévisibilité, incombe principalement aux États membres qui transposent la directive dans leur législation nationale. Il est bien connu qu'une telle transposition doit se faire dans le respect des droits fondamentaux ⁽⁶¹⁾.

67. Également dans le rapport d'évaluation, la Commission souligne que la directive «ne garantit pas en soi que les données conservées seront stockées, extraites et utilisées dans le strict respect du droit à la vie privée et à la protection des données à caractère personnel». Elle rappelle que «la responsabilité de faire respecter ces droits incombe aux États membres» ⁽⁶²⁾.
68. Cependant, le CEPD estime qu'une directive de l'UE devrait dans une certaine mesure satisfaire également à l'exigence de prévisibilité. Ou, pour paraphraser la Cour de justice dans l'affaire *Lindqvist*, le régime arrêté par la directive ne doit pas «manquer de prévisibilité» ⁽⁶³⁾. Ceci est particulièrement vrai lorsqu'il s'agit d'une mesure de l'UE qui exige que les États membres organisent une ingérence à grande échelle dans les droits à la vie privée et à la protection des données à caractère personnel des citoyens. Le CEPD estime que l'UE a la responsabilité d'assurer au moins une finalité clairement définie et une indication précise de qui peut avoir accès aux données et sous quelles conditions.
69. Cette position est appuyée par le nouveau contexte juridique créé par le traité de Lisbonne qui, comme expliqué, a élargi la compétence de l'UE dans le domaine de la coopération policière et judiciaire en matière pénale et renforcé l'engagement de l'UE à faire respecter les droits fondamentaux.
70. Le CEPD souhaite rappeler que l'exigence d'une finalité déterminée et l'interdiction subséquente de traiter des données d'une manière incompatible avec cette finalité («principe de limitation de la finalité») sont d'une importance capitale pour la protection des données à caractère personnel, comme le confirme l'article 8 de la Charte des droits fondamentaux de l'Union européenne ⁽⁶⁴⁾.
71. Le rapport d'évaluation montre que le choix de laisser la définition précise de ce que constitue une «infraction grave» ainsi que des entités devant être considérées comme des «autorités compétentes» à la discrétion des États membres a donné lieu à toute une série de finalités pour lesquelles les données ont été utilisées ⁽⁶⁵⁾.
72. La Commission affirme que «[l]a plupart des États membres qui ont transposé la directive autorisent, dans leur législation, l'accès aux données conservées et leur utilisation pour des finalités dépassant celles couvertes par la directive, comme la prévention et la répression de la criminalité en général et les risques pour la vie humaine» ⁽⁶⁶⁾. Les États membres utilisent le «vide juridique» laissé par l'article 15, paragraphe 1, de la directive sur la vie privée et les communications électroniques ⁽⁶⁷⁾. La Commission considère que cette situation pourrait ne pas répondre suffisamment à

⁽⁵⁴⁾ Voir également l'avis du CEPD de 2005, points 29 à 37. Voir également le discours du Contrôleur adjoint du 4 mai 2011 consultable sur le site web du CEPD (<http://www.edps.europa.eu>) sous «Publications» >> «Discours & articles» >> «2011».

⁽⁵⁵⁾ Voir p. 16 du rapport d'évaluation.

⁽⁵⁶⁾ Voir Cour européenne des droits de l'homme, *S. et Marper*, cité à la note de bas de page 7, point 151.

⁽⁵⁷⁾ Cour européenne de justice, 20 mai 2003, *Österreichischer Rundfunk*, C-465/00, point 77, et Cour européenne des droits de l'homme, *S. et Marper*, cité à la note de bas de page 7, point 95.

⁽⁵⁸⁾ Voir Cour européenne des droits de l'homme, *Malone*, cité à la note de bas de page 8, points 66-68.

⁽⁵⁹⁾ COM(2010) 573, citée à la note de bas de page 31, p. 5.

⁽⁶⁰⁾ COM(2010) 385, citée à la note de bas de page 17, p. 3.

⁽⁶¹⁾ Voir par exemple, Cour européenne de justice, 6 novembre 2003, *Lindqvist*, point 87.

⁽⁶²⁾ Voir p. 36 du rapport d'évaluation.

⁽⁶³⁾ Cour européenne de justice, *Lindqvist*, point 84.

⁽⁶⁴⁾ Voir également l'article 6 de la directive 95/46/CE.

⁽⁶⁵⁾ Voir p. 10 du rapport d'évaluation.

⁽⁶⁶⁾ Voir p. 10 du rapport d'évaluation.

⁽⁶⁷⁾ Tel que discuté au point 24 ci-dessus.

«l'exigence de prévisibilité à laquelle est soumise toute mesure législative qui restreint le droit à la vie privée»⁽⁶⁸⁾.

73. Dans ces circonstances, il ne peut être dit que la directive sur la conservation des données, lue en conjonction avec la directive sur la vie privée et les communications électroniques, offre la clarté suffisante pour satisfaire au principe de prévisibilité au niveau de l'UE.

V. LA VOIE À SUIVRE: TOUTES LES OPTIONS DOIVENT ÊTRE ENVISAGÉES

74. L'analyse de la section précédente permet de conclure que la directive sur la conservation des données ne satisfait pas aux exigences imposées par les droits à la vie privée et à la protection des données à caractère personnel. Il est donc évident que la directive sur la conservation des données ne peut continuer à exister dans sa mouture actuelle. À cet égard, la Commission propose, à juste titre, une révision du cadre actuel régissant la conservation des données⁽⁶⁹⁾.

75. Cependant, avant de proposer une version révisée de la directive:

- a) la Commission doit, durant l'étude d'impact, s'atteler à collecter des preuves pratiques supplémentaires auprès des États membres afin de démontrer la nécessité de la conservation des données en tant que mesure au titre du droit de l'UE;
- b) si une majorité des États membres considère la conservation des données comme étant nécessaire, ces États membres doivent tous fournir des preuves quantitatives et qualitatives pour le démontrer;
- c) les États membres qui s'opposent à une mesure de conservation des données doivent fournir à la Commission les informations pertinentes pour permettre une évaluation plus large de la question.

76. Dans l'étude d'impact, il convient en outre d'examiner si des moyens alternatifs et moins intrusifs dans la vie privée auraient pu mener ou pourraient encore mener à des résultats comparables. La Commission devrait adopter une initiative en la matière, soutenue, le cas échéant, par des experts externes.

77. Le CEPD note avec satisfaction que la Commission a annoncé la consultation de toutes les parties prenantes concernées durant l'étude d'impact⁽⁷⁰⁾. À cet égard, le CEPD encourage la Commission à trouver les moyens d'impliquer directement les citoyens dans cet exercice.

78. Il convient de souligner que l'évaluation de la nécessité et l'examen des moyens alternatifs moins intrusifs dans la vie privée ne peuvent être menés équitablement que si toutes les options pour l'avenir de la directive sont laissées ouvertes. À cet égard, la Commission semble exclure la possibilité d'abroger purement et simplement la directive, de façon exclusive ou combinée avec une proposition de mesure alternative de l'UE plus ciblée. Le CEPD appelle donc la Commission à considérer sérieusement ces options dans l'étude d'impact.

⁽⁶⁸⁾ Voir pages 10 et 15 du rapport d'évaluation.

⁽⁶⁹⁾ Voir pages 37-38 du rapport d'évaluation.

⁽⁷⁰⁾ Voir pages 37-38 du rapport d'évaluation.

79. Une future directive sur la conservation des données ne pourra être envisagée que si tout le monde s'accorde sur la nécessité d'une réglementation de l'UE du point de vue du marché interne et de la coopération policière et judiciaire en matière pénale et si, durant l'étude d'impact, la nécessité de la conservation des données, encouragée et réglementée par l'UE, peut être suffisamment démontrée, avec un examen minutieux des mesures alternatives.

80. Le CEPD ne nie pas la valeur des données conservées à des fins de répression ni le rôle capital qu'elles peuvent jouer dans des cas spécifiques. À l'instar du Bundesverfassungsgericht allemand, le CEPD n'exclut pas qu'une obligation bien définie de conservation des données de télécommunications puisse être justifiée sous certaines conditions très strictes⁽⁷¹⁾.

81. Tout instrument futur de l'UE sur la conservation des données devra par conséquent satisfaire aux exigences fondamentales suivantes:

- il doit être global et véritablement harmoniser les règles sur l'obligation de conservation des données, ainsi que sur l'accès et l'utilisation ultérieure des données par les autorités compétentes;
- il doit être exhaustif, ce qui signifie qu'il doit avoir une finalité claire et précise, et que le vide juridique existant à l'article 15, paragraphe 1, de la directive sur la vie privée et les communications électroniques doit être comblé;
- il doit être proportionnel et ne pas aller au-delà de ce qui est nécessaire (voir à cet égard les commentaires formulés à la section IV.2 ci-dessus).

82. Bien entendu, le CEPD examinera minutieusement toute proposition future sur la conservation des données à la lumière de ces conditions fondamentales.

VI. CONCLUSION

83. Le CEPD note avec satisfaction que, bien que l'article 14 ne l'exige pas au sens strict, la Commission a également tenu compte dans le rapport d'évaluation des effets de la directive sur les droits fondamentaux.

84. Le rapport d'évaluation montre que la directive n'a pas réussi à atteindre son objectif principal, à savoir d'harmoniser les législations nationales en matière de conservation des données. Un tel manque d'harmonisation ne peut qu'être préjudiciable à toutes les parties concernées: les citoyens, les chefs d'entreprise ainsi que les autorités répressives.

85. Sur la base du rapport d'évaluation, il peut être conclu que la directive sur la conservation des données ne satisfait pas aux exigences établies par les droits à la vie privée et à la protection des données à caractère personnel, pour les motifs suivants:

- la nécessité de la conservation des données telle qu'arrêtée par la directive sur la conservation des données n'a pas été suffisamment démontrée;
- la conservation des données aurait pu être réglementée d'une manière moins intrusive dans la vie privée;

⁽⁷¹⁾ Voir Bundesverfassungsgericht, 1 BvR 256/08.

- la directive sur la conservation des données manque de prévisibilité.
86. Le CEPD appelle la Commission à envisager sérieusement toutes les options contenues dans l'étude d'impact, notamment la possibilité d'abroger purement et simplement la directive, de façon exclusive ou combinée avec une proposition de mesure alternative de l'UE plus ciblée.
87. Une future directive sur la conservation des données ne pourra être envisagée que si tout le monde s'accorde sur la nécessité d'une réglementation de l'UE du point de vue du marché interne et de la coopération policière et judiciaire en matière pénale et si, durant l'étude d'impact, la nécessité de la conservation des données, encouragée et réglementée par l'UE, peut être suffisamment démontrée, avec un examen minutieux des mesures alternatives. Un tel instrument devra satisfaire aux exigences fondamentales suivantes:
- il doit être global et véritablement harmoniser les règles sur l'obligation de conservation des données, ainsi que sur l'accès et l'utilisation ultérieure des données par les autorités compétentes;
- il doit être exhaustif, ce qui signifie qu'il doit avoir une finalité claire et précise, et que le vide juridique existant à l'article 15, paragraphe 1, de la directive sur la vie privée et les communications électroniques doit être comblé;
- il doit être proportionnel et ne pas aller au-delà de ce qui est nécessaire.

Fait à Bruxelles, le 31 mai 2011.

Peter HUSTINX

Contrôleur européen de la protection des données
