00068/10/FR
WP 172

Rapport 01/2010 sur la deuxième action commune de contrôle de l'application de la législation UE:

Respect au niveau national par les fournisseurs de télécommunications et les fournisseurs de services Internet (FSI) des obligations découlant de la législation nationale sur la conservation des données relatives au trafic, sur la base juridique des articles 6 et 9 de la directive 2002/58/CE «vie privée et communications électroniques» et de la directive 2006/24/CE sur la conservation des données la modifiant

Adopté le 13 juillet 2010

Résumé

- Cette action de contrôle de l'application de la législation UE par le groupe de travail «article 29» a été décidée en vue de contrôler le respect des dispositions introduites par la directive 2006/24/CE, compte tenu des recommandations et des préoccupations exprimées par le groupe de travail dans ses précédents avis sur la question.

- L'application de la directive sur la conservation des données par les fournisseurs de services de communications électroniques et de services Internet est par nature associée à un niveau de risque élevé, qui exige des mesures de sécurité techniques et organisationnelles appropriées. Cela tient au fait que la disponibilité des données relatives au trafic permet la divulgation de préférences, d'opinions et de comportements, et peut donc aller à l'encontre du principe de respect de la vie privée des utilisateurs et avoir une incidence non négligeable sur la confidentialité des communications et les droits fondamentaux tels que la liberté d'expression.

- Sur la base d'un questionnaire et de contrôles sur place, auxquels ont été soumis les principaux opérateurs et FSI nationaux afin de couvrir une importante partie du marché, l'action révèle un patchwork de mesures d'application, notamment en ce qui concerne les mesures de sécurité en place.

- Il existe de grandes différences dans la conservation des catégories de données relatives au trafic Internet, et les durées de conservation varient elles aussi sensiblement d'un État membre à l'autre. En ce qui concerne la conservation des catégories de données relatives aux communications téléphoniques, le tableau semble plus uniforme. Il est à noter que la législation nationale de nombreux États membres semble privilégier des durées de conservation plus courtes que les durées maximales autorisées par la directive.

- À ce propos, le groupe de travail «article 29» s'inquiète de constater que la directive ne semble pas avoir été appliquée d'une manière uniforme au niveau national. Il semble notamment qu'elle ait été interprétée par les États membres comme laissant à leur appréciation les limites de son champ d'application; en effet, la directive a-t-elle pour objet de permettre de déroger à l'obligation générale d'effacer les données relatives au trafic dès qu'elles ne sont plus nécessaires à la transmission d'une communication, ou bien de rendre obligatoire la conservation de toutes les données que les fournisseurs sont déjà autorisés à stocker aux fins de l'article 6, paragraphe 2, de la directive 2002/58? Le groupe de travail «article 29» soutient cette seconde interprétation, qui a également été retenue dans le récent arrêt de la CEJ dans l'affaire *Irlande contre Commission* (C-301/06).

- Les mesures de sécurité semblent varier en fonction de la taille des opérateurs; les mesures de sécurité logiques ne sont pas toujours adaptées à la protection des informations extrêmement sensibles contenues dans les données relatives au trafic. Il importe également de noter que les procédures de transfert applicables aux données réclamées par les services répressifs sont très hétérogènes, présentant une vaste palette de solutions et des niveaux très différents de sécurité de la transmission.

- En outre, l'action révèle, d'une part, que seuls quelques États membres ont fourni à la Commission les statistiques qu'elle leur avait demandées concernant l'utilisation des données relatives au trafic conservées en vertu de la directive et, d'autre part, que

l'externalisation constitue une pratique courante chez les plus petits opérateurs, ce qui jette un doute quant au respect effectif des exigences en matière de protection des données.

- Faute de statistiques suffisantes, il est très difficile d'apprécier dans quelle mesure la directive a atteint son objectif. Les conclusions du rapport révèlent un manque évident d'harmonisation et de grandes disparités dans l'application au niveau national. Dans l'attente de la décision de la Commission européenne relative à l'éventuelle modification ou abrogation de la directive[1], le groupe de travail estime nécessaire de formuler une série de recommandations afin d'assurer une meilleure harmonisation, une transmission des données plus sûre et des procédures de transfert normalisées.

- Ces recommandations concernent, en particulier, les points suivants:

  - ***Catégories de données à conserver**:* la liste des données relatives au trafic qui doivent être conservées à titre obligatoire doit être considérée comme exhaustive. En conséquence, aucune obligation supplémentaire de conservation de données ne peut être imposée aux fournisseurs en vertu de la directive sur la conservation des données.
  - ***Durées de conservation:*** afin de parvenir à une plus grande harmonisation, il convient de réduire la durée maximale de conservation des données et de fixer une durée unique, plus courte, applicable à l'ensemble des fournisseurs de l'UE, comme l'a indiqué le groupe de travail «article 29» dans son avis WP113. Dans une perspective plus large, c'est la sécurité générale des données relatives au trafic «en soi» qui doit être reconsidérée par la Commission.
  - ***Mesures de sécurité techniques et organisationnelles:*** des mesures supplémentaires spécifiques (telles que la mise en place d'un système d'authentification solide et l'établissement d'un journal détaillé des accès) ont été détaillées, et une proposition de norme pour le transfert de données aux services répressifs a été élaborée aux fins de transferts rapides et plus fiables, permettant la collecte d'informations statistiques ainsi qu'un accès aux données responsable. À ce propos, la notion d'«infraction grave» semble devoir être clarifiée au niveau des États membres, et la liste des entités autorisées à accéder aux données devrait être communiquée à toutes les parties concernées.

[1] À cet égard, le groupe de travail Article 29 sur la protection des données rappelle ses précédents avis concernant cette directive.

I. Contexte – Contrôle de l'application de la législation UE

À la suite du premier rapport sur la mise en œuvre de la directive relative à la protection des données en mai 2003, la Commission européenne a invité le groupe de travail «article 29» à réfléchir au lancement d'enquêtes sectorielles au niveau européen et à tenter de définir des normes en la matière. Dans sa déclaration du 25 novembre 2004, le groupe de travail «article 29» a indiqué que la promotion d'une application uniforme et d'une conformité harmonisée était l'un de ses objectifs stratégiques et permanents.

Après la première action commune de contrôle de l'application de la législation UE relative aux sociétés d'assurance-santé privées (rapport 1/2007 adopté le 20 juin - WP137) et sur la base de l'expérience acquise à cette occasion, le groupe de travail «article 29» a décidé de lancer une deuxième action commune et a choisi d'examiner la question du respect au niveau national par les fournisseurs de télécommunications et les fournisseurs de services Internet (FSI) des obligations découlant de la législation nationale sur la conservation des données relatives au trafic[2], sur la base juridique des articles 6 et 9 de la directive 2002/58/CE «vie privée et communications électroniques» et de la directive 2006/24/CE sur la conservation des données. Cette action s'inscrit dans le cadre des priorités fixées dans le programme de travail du groupe, en vue de vérifier l'application uniforme des principes de protection des données au niveau européen.

En juillet 2008, le groupe de travail «article 29» a demandé au sous-groupe «application de la législation» de planifier et de mettre en œuvre les mesures nécessaires à la réalisation de cette action, conformément au mandat détaillé dans le document WP152.

La combinaison des différents critères mentionnés dans la déclaration WP101 a mené au choix de ce sujet, même si le groupe de travail était bien conscient du fait que le processus de transposition de la directive sur la conservation des données n'était pas terminé (que ce soit en raison de retards au niveau national ou des différentes échéances imposées aux États membres pour l'introduction des obligations en matière de conservation, notamment à l'égard des données relatives au trafic Internet).

Cette décision a été prise en raison du fait que le champ d'action de la directive 2006/24/CE est très spécifique et déroge au principe général défini dans la directive 2002/58/CE «vie privée et communications électroniques», dont l'article 6, paragraphe 1, dispose que: «les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur […] d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication […] ». La seule obligation générale de conservation des données relatives au trafic figure à l'article 6, paragraphe 2, et concerne les données qui sont «nécessaires pour établir les factures des abonnés et les paiements pour interconnexion»; ce n'est néanmoins autorisé que «jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement.» Il convient de rappeler que l'objectif poursuivi par la directive 2006/24/CE (voir son article 1er) est d'«harmoniser les dispositions [...] en matière de conservation de certaines données qui sont générées ou traitées par les fournisseurs de services communications électroniques de accessibles au public ou de réseaux publics de communication». Les données en question

[2] Dans un souci de clarté, les «données relatives au trafic» couvrent, dans le présent avis, les données auxquelles il est fait référence à l'article 5 de la directive 2006/24/CE.

peuvent être conservées «aux fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne».

Le groupe de travail «article 29» a en outre publié trois avis sur la directive sur la conservation des données et les projets ayant précédé l'instrument final.[3] Dans ces avis, en particulier dans les documents WP113 et WP119, le groupe de travail a fait part de ses réserves, eu égard aux conséquences considérables des dispositions de la directive sur tous les citoyens européens et leur vie privée; la décision d'obliger les fournisseurs de services de téléphonie et Internet à conserver les données relatives au trafic de tous leurs abonnés et utilisateurs étant en effet sans précédent. Elle empiète sur la vie quotidienne de tout un chacun et pourrait menacer les valeurs et libertés fondamentales dont jouissent tous les citoyens européens et auxquelles ils tiennent. En conséquence, le groupe de travail, dans ses avis, «estime capital que les dispositions de la directive soient interprétées et appliquées de manière harmonisée, de sorte à garantir aux citoyens européens un degré de protection identique dans toute l'Union européenne».

L'objectif relativement vague de «répression des infractions graves» a constitué un sujet de préoccupation pour le groupe de travail «article 29», compte tenu de l'absence de définition commune de la notion d'infraction grave. De même, le groupe de travail s'est inquiété du manque de lignes de conduite spécifiques relatives aux services habilités à accéder aux données conservées et des mécanismes de conservation mis en place par les fournisseurs pour limiter l'accès aux informations qu'aux fins prévues par la directive 2006/24. Le groupe de travail «article 29» a demandé que des garanties soient introduites, du moins en ce qui concerne la description de la finalité, la limitation de l'accès, la limitation des données au minimum nécessaire, l'interdiction d'exploration des données, le contrôle juridictionnel/indépendant de l'autorisation d'accès, l'interdiction pour les fournisseurs d'utiliser à d'autres fins les données conservées uniquement pour des raisons d'ordre public conformément à la directive sur la conservation des données - et, par extension, la séparation des systèmes et la définition de normes minimales pour les mesures de sécurité que doivent prendre les fournisseurs.

Les données relatives au trafic qui ont été conservées permettent de reconstituer et de contrôler l'ensemble du réseau relationnel d'un utilisateur, ainsi que de suivre ses déplacements et les outils utilisés à cette fin. Toute limitation du droit des citoyens à la protection des données et de la vie privée doit constituer 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, la défense et la sécurité publique, ou pour assurer la recherche, la détection et la poursuite d'infractions pénales. Au strict minimum, de telles limitations doivent respecter les droits, libertés et principes établis dans la Charte des droits fondamentaux de l'Union européenne ainsi que dans la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

Examiner la manière dont la directive a jusqu'à présent été mise en œuvre dans les différentes législations nationales constituait, dans cette optique, un moyen de vérifier dans quelle mesure les réserves exprimées par le groupe de travail et les besoins d'harmonisation avaient été, à ce jour, pris en considération.

[3] Avis 9/2004, 4/2005 et 3/2006

Bien que le processus de transposition doive encore être achevé au sein de l'UE, les conclusions de cette enquête permettent d'ores et déjà au groupe de travail «article 29» de fournir des informations utiles à la Commission, dont le rapport d'évaluation est attendu pour le 15 septembre 2010.

II. Le cadre juridique

Comme il a déjà été précisé, l'objectif poursuivi par la directive 2006/24/CE sur la conservation des données est d'harmoniser les dispositions nationales relatives aux obligations en matière de conservation de certaines données. À ce propos, référence peut être faite aux articles 5, 6 et 7 de ladite directive, qui définissent respectivement les catégories de données à conserver, les durées de conservation applicables et les mesures de protection et de sécurité des données. Il convient également de rappeler que les effets de l'obligation introduite par la directive peuvent varier, et varient, selon la manière dont son article 3 est interprété et appliqué, à savoir s'il est établi que la directive déroge au principe général en vertu duquel les données relatives au trafic doivent être effacées lorsqu'elles ne sont plus nécessaires à la transmission d'une communication (en vertu de l'article 6, paragraphe 1, de la directive 2002/58), ou plutôt qu'elle se borne à introduire une durée de conservation obligatoire pour ces données, qui sont déjà collectées et stockées par les fournisseurs aux fins mentionnées à l'article 6, paragraphe 2, de la directive 2002/58 («établir les factures des abonnés et les paiements pour interconnexion»).[4]

Partant de ce principe, il convient de rappeler que les dispositions des articles susmentionnés doivent être appliquées de manière restrictive par les États membres, c'est-à-dire que ces derniers ne peuvent adopter de dispositions législatives nationales pour transposer la directive qu'à la condition qu'elles soient strictement conformes aux exigences de la directive sur la conservation des données.

Il doit également être souligné qu'en vertu de la directive sur la conservation des données, chaque État membre est tenu de désigner une autorité publique qui est chargée de surveiller l'application des dispositions des directives 95/46/CE et 2002/58/CE, ainsi que des mesures de protection et de sécurité des données mentionnées à l'article 7 de la directive sur la conservation des données. Les mesures de sécurité mentionnées à l'article 7 doivent être considérées comme le minimum requis devant être assuré par chaque État membre. Il est à noter que la directive sur la conservation des données établit clairement à l'article 9 que les autorités publiques en question peuvent être les autorités nationales de protection des données et qu'elles doivent exercer cette surveillance en toute indépendance.

---

[4] Dans l'*avis 1/2003 sur le stockage des données relatives au trafic à des fins de facturation, adopté le 29 janvier 2003*, le groupe de travail Article 29 a émis des recommandations en vue d'harmoniser la période durant laquelle les données relatives au trafic peuvent légalement être traitées à des fins de facturation. La durée maximale de stockage des données à des fins de facturation doit être de 3 à 6 mois. Seules les données qui sont adéquates, pertinentes et non excessives pour établir les factures et les paiements pour interconnexion peuvent être traitées. Les autres données relatives au trafic doivent être supprimées ou rendues anonymes.

Toute pratique non conforme à ces principes, ou qui n'est pas clairement autorisée par une disposition législative aux conditions fixées à l'article 15 de la directive 2002/58/CE est, de prime abord, incompatible avec les exigences du droit européen de la protection des données.

En outre, la directive sur la conservation des données stipule que la Commission est tenue de présenter au Parlement européen et au Conseil, pour le 15 septembre 2010, une évaluation de son application et de ses effets afin de déterminer s'il y a lieu de la modifier en ce qui concerne, notamment, les catégories de données et les durées de conservation. Dans cette évaluation, la Commission doit tenir compte des observations transmises par les États membres et le groupe de travail «article 29», ainsi que des statistiques sur la conservation des données que les États membres sont tenus de lui transmettre annuellement conformément à l'article 10 de ladite directive. Ces statistiques doivent comprendre notamment les cas dans lesquels des informations ont été transmises aux services répressifs, du laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités ont demandé leur transmission, et les cas dans lesquels des demandes de données n'ont pu être satisfaites.

Une fois encore, rappelons qu'à la date à laquelle nous avons établi ce rapport, tous les États membres n'avaient pas encore transposé la directive sur la conservation des données. Dans certains États membres (Allemagne et Roumanie), la Cour constitutionnelle ou suprême a jugé que les mesures de transposition étaient contraires à des principes constitutionnels.

III. L’action de contrôle de l'application de la législation UE

A. Fondement

L’objectif de la présente action de contrôle de l'application de la législation UE était d’évaluer la manière dont les fournisseurs de services de communications électroniques et de services Internet avaient transposé les obligations découlant de la directive sur la conservation des données en ce qui concerne la catégories de données à conserver (article 5), les durées de conservation (article 6) et les mesures de sécurité techniques et organisationnelles (article 7). Pour les États membres qui n’avaient pas encore transposé la directive dans leur droit interne, il a été tenu compte des obligations imposées aux fournisseurs susmentionnés par la législation nationale en vigueur en application de la directive «vie privée et communications électroniques» (directive 2002/58/CE), tout particulièrement au regard des articles 6 et 9 de ladite directive. Référence a également été faite aux garanties minimales proposées dans l’avis 3/2006 (WP 119).

En vertu des directives 2006/24/CE et 2002/58/CE, la sécurité des données à caractère personnel doit être proportionnée aux risques inhérents au traitement et aux caractéristiques des données en question. De ce point de vue, il est incontestable que la mise en œuvre de la directive sur la conservation des données comporte des risques spécifiques pour les personnes concernées, en raison de la nature des données. C'est pourquoi, l’enquête menée par les membres du groupe de travail «article 29» était plus particulièrement destinée à recueillir des informations concrètes quant à ces risques, afin de déterminer si les préoccupations exprimées par le groupe en des occasions antérieures étaient toujours d’actualité.

Comme indiqué précédemment, la disponibilité des données relatives au trafic permet la divulgation de préférences, d’opinions et de comportements et peut donc aller à l’encontre du principe de respect de la vie privée des utilisateurs et par là même compromettre dangereusement la confidentialité des communications et des droits fondamentaux tels que la liberté d’expression. Ces cas de figure sont malheureusement susceptibles de se présenter, que ce soit en raison d’activités intentionnelles ou de mécanismes de conservation peu performants. L’accès à ou la divulgation non autorisés d’informations liées aux communications électroniques (par exemple, des données de localisation) peuvent porter gravement atteinte à la vie privée des personnes concernées. À la lumière des éléments précités, il apparaît que la mise en œuvre de la directive sur la conservation des données par les fournisseurs de services de communications électroniques et de services Internet présente un niveau de risque nécessairement élevé et exige dès lors l'adoption de mesures de sécurité techniques et organisationnelles appropriées.

S’agissant des risques, il convient de rappeler que la directive interdit la conservation de données relatives au contenu des communications; de plus, la simple disponibilité des données relatives au trafic (c'est-à-dire celles visées à l’article 5 de la directive sur la conservation des données) permet de reconstituer divers éléments d’information à caractère personnel (y compris des informations sensibles) à partir du tableau général (par exemple, le profil comportemental d’un utilisateur) pouvant être déduit de ses interactions sociales. Ces informations peuvent être replacées dans un contexte spatial et temporel et classées de manière très précise à l’aide d’outils d’extraction des données exploitant toute la puissance informatique qu'offrent à l'heure actuelle les serveurs et les ordinateurs personnels. Ces techniques se révèlent particulièrement efficaces dans le cas de grandes quantités de données relatives au trafic couvrant une longue période de temps. Quant aux services Internet, ils

peuvent générer d'autres risques que ceux qui sont inhérents aux communications téléphoniques parce que des informations telles que l'adresse IP de destination peuvent révéler le contenu lui-même, le graphique social ou encore des informations relatives aux préférences les plus intimes des personnes concernées. L'un des objectifs de cette action de contrôle de l'application de la législation UE était par conséquent d'évaluer dans quelle mesure les fournisseurs de services de communications téléphoniques et de services Internet sont conscients de ces risques spécifiques et respectent les garanties mises en place pour les éviter.

B. Méthodologie et étapes

L'enquête a été réalisée par les autorités de protection des données des pays suivants: *Allemagne, Belgique, Bulgarie, Chypre, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Liechtenstein, Luxembourg, Lituanie, Malte, Pays-Bas, Pologne, République slovaque, République tchèque, Roumanie, Royaume-Uni et Slovénie*. Il convient de rappeler que l'Agence suédoise des postes et télécommunications ainsi que la Commission européenne ont également présenté des observations sur les conclusions de l'enquête.

Sur la base de l'expérience acquise lors de la première action de contrôle de l'application de la législation UE ainsi que des suggestions figurant dans le rapport final relatif à cette action, le groupe de travail «article 29» a décidé que la deuxième action se déroulerait en deux étapes: d'abord la diffusion d'un questionnaire, et ensuite l'évaluation des réponses par les autorités chargées de la protection des données, notamment au moyen d'inspections sur place.

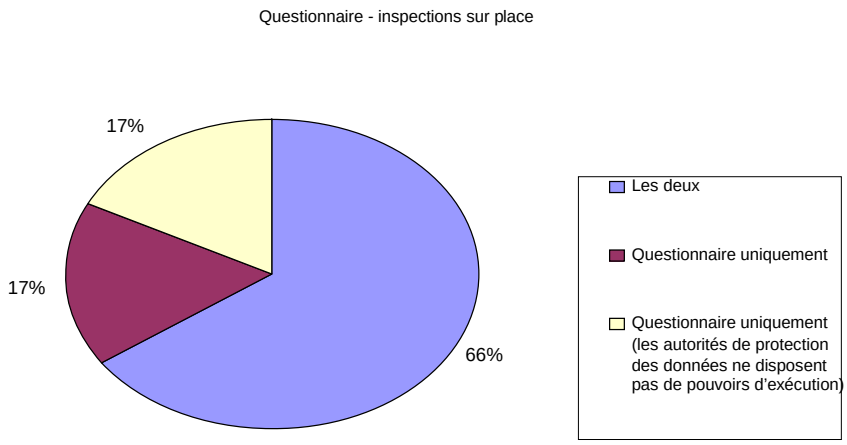
Un questionnaire type (adopté par le groupe de travail en décembre 2008) a été remis, accompagné d'une lettre type à tous les fournisseurs de services de communications électroniques et de services Internet qui avaient été préalablement sélectionnés dans chaque État membre, la sélection ayant été effectuée selon des critères de positionnement sur le marché (téléphonie fixe contre téléphonie mobile, opérateurs convergents, fournisseurs exclusifs de services Internet) et de taille (petits fournisseurs et gros opérateurs de télécommunications) afin de couvrir une part importante du marché national.

Le questionnaire comportait dix parties couvrant le type de données conservées, les durées de conservation et les solutions technologiques mises en œuvre aux fins de la conservation, ainsi qu'une série d'aspects importants pour la conservation des données (sécurité informatique, protection logique, authentification/autorisation, fichiers «journal», cryptage, protocoles de divulgation/transmission, protection physique, récupération de la sauvegarde/d'urgence, etc.). Le nombre de questions a été limité au maximum et leur contenu énoncé aussi clairement que possible, compte tenu des éléments signalés à la suite de la première action, notamment à l'égard des critères de sélection des opérateurs interrogés.

Lorsque les autorités de protection des données l'ont jugé nécessaire, elles ont procédé à des inspections sur place, en vertu des pouvoirs d'inspection qui leur sont conférés par les législations nationales et en fonction de la disponibilité du personnel expérimenté. Ces inspections avaient pour objectif d'évaluer la fiabilité des réponses au questionnaire et d'obtenir des informations plus détaillées sur la mise en œuvre. Elles se sont révélées cruciales pour l'évaluation du respect des exigences applicables par les responsables du traitement.

Un rapport national a ensuite été rédigé par chacune des autorités de protection des données participantes afin de faire le point sur la situation et les principales critiques à formuler pour chaque État membre concerné. Un tableau résumant les informations fournies par les autorités participantes peut être consulté à l'annexe 1 du présent rapport.

Le diagramme ci-dessous représente la ventilation statistique des autorités de protection des données qui ont procédé à des inspections sur place, par rapport à celles qui se sont occupées du questionnaire et à celles qui ne disposent pas des pouvoirs de contrôle requis.



C. Conclusions[5]

D'une manière générale, les réponses au questionnaire ont révélé un patchwork de mesures d'exécution, notamment en ce qui concerne les mesures de sécurité en place (voir annexe 1, colonnes P et Q). Des inspections sur place approfondies ont permis d'établir que certaines des réponses étaient inexactes et/ou imprécises, ce qui a abouti à l'adoption de sanctions *ad hoc* et de mesures techniques et organisationnelles spécifiques.

Compte tenu de la différence de valeur existant entre les informations recueillies lors d'inspections et celles obtenues par le biais de questionnaires, les autorités de protection des données habilitées à procéder à des inspections doivent être particulièrement conscientes des risques inhérents à une obligation générale de conservation des données relatives au trafic, en recommandant des campagnes de sensibilisation et, le cas échéant, en poursuivant leur surveillance des systèmes dans les locaux des fournisseurs de services de communications électroniques et de services Internet; en outre, il conviendrait de veiller à ce que les activités de contrôle des autorités de protection des données ne soient pas limitées par certaines contraintes, notamment celles liées au secret industriel/des affaires, lorsque ces contraintes risquent d'être invoquées par lesdits fournisseurs pour ne pas divulguer les informations demandées. Il est nécessaire de conférer aux autorités de protection des données d'amples pouvoirs d'exécution, dont celui d'exiger l'accès aux

[5] Voir le tableau à l'annexe 1 du rapport pour une vue d'ensemble détaillée des réponses fournies par les États membres.

secrets industriels/d'affaires. Autrement, il sera difficile d'obtenir un tableau complet de la situation.

i. Catégories de données à conserver

En ce qui concerne les catégories de données relatives au trafic soumises à l'obligation de conservation, il apparaît que les données téléphoniques conservées par les fournisseurs (annexe 1, colonnes I et J) sont généralement conformes à celles visées à l'article 5 de la directive sur la conservation des données. En revanche, des divergences considérables ont été constatées pour les données relatives au trafic Internet (annexe 1, colonne K).

En ce qui concerne les services téléphoniques, à quelques exceptions près (en particulier le cas d'un État membre dans lequel il est apparu que le contenu des messages sms était conservé et restait accessible pendant plusieurs mois pour faciliter le travail des services de sécurité), les données conservées sont les données nécessaires pour identifier la source et la destination des communications, en déterminer le début et la fin, ainsi que les services et terminaux employés par les utilisateurs. La conservation des données de localisation constitue toutefois un sujet de préoccupation, lorsque ces données sont collectées de manière continue au cours d'un appel téléphonique ou d'une session Internet et pourraient, dès lors, permettre de suivre les mouvements des utilisateurs.

La situation est différente en ce qui concerne la conservation des données relatives au trafic Internet. Dans certains cas, des catégories de données autres que celles visées à l'article 5 de la directive sont conservées; elles n'entrent donc pas dans le cadre réglementaire actuel et concernent le contenu des communications (voir annexe 1, colonne K). On peut mentionner ici l'adresse IP de destination et les URL des sites internet, l'objet des messages envoyés par courrier électronique, la liste des destinataires mis en copie, et le numéro de port attribué aux utilisateurs par le FSI.

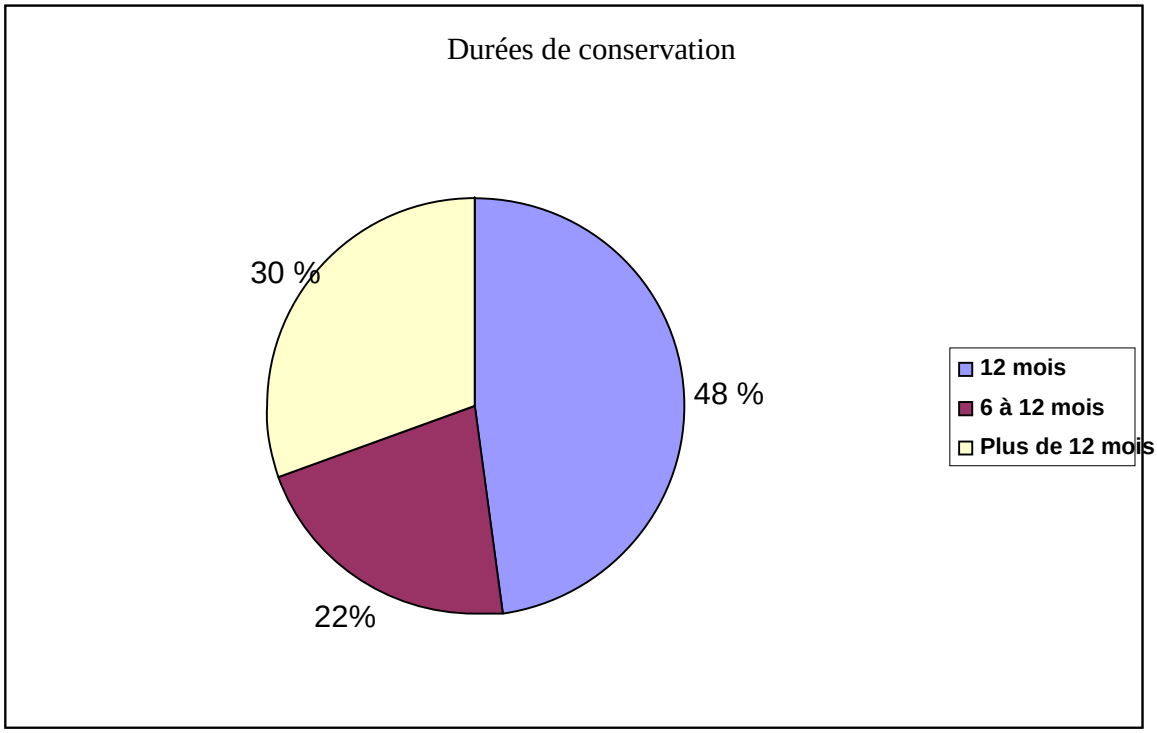
À cet égard, il convient de rappeler que la directive 2006/24/CE déroge aux dispositions de la directive 2002/58/CE et que la liste des données relatives au trafic à conserver obligatoirement doit être considérée comme exhaustive, ce qui signifie qu'aucune obligation supplémentaire de conservation de données ne peut être imposée aux fournisseurs en vertu de la directive sur la conservation des données.

Par ailleurs, le groupe de travail «article 29» est conscient des problèmes qui pourraient découler de l'éventuelle extension en droit national du champ d'application de la directive sur la conservation des données, en particulier la question de savoir si les services répressifs ne peuvent recueillir que les données relatives au trafic que les fournisseurs sont autorisés à conserver en vertu de l'article 6, paragraphe 2, de la directive 2002/58/CE, ou s'ils peuvent également en recueillir d'autres qui ne sont pas mentionnées dans les dispositions pertinentes de cette directive.

ii. Durées de conservation

Aux fins de cette analyse et sur la base des résultats obtenus par l'action de contrôle de l'application de la législation UE, les durées de rétention potentielles (6 à 24 mois) ont été divisées en trois catégories: a. conservation pendant une période de 12 mois; b. conservation pendant une période inférieure à 12 mois; et c. conservation pendant une période supérieure à 12 mois. Il est apparu que 48 % des fournisseurs interrogés conservaient les données pendant

une période de 12 mois, avec un pourcentage non négligeable pour les «données récentes» (groupe b, 22 %) et les «données anciennes» (groupe c, 30 %). Le schéma ci-dessous indique la distribution statistique pour les États membres de l'UE:



Il est également apparu que les durées de conservation fixées par les législateurs nationaux aux fins de la transposition de la directive sur la conservation des données variaient de manière considérable en fonction des États membres (voir annexe 1, colonnes L, M et N), bien que de nombreux pays (voir diagramme ci-dessous) aient semblé préférer une durée de conservation plus courte que la durée maximale autorisée, ce qui laisse entendre que les durées minimale et maximale autorisées par la directive peuvent être encore davantage harmonisées.

À cette fin, ***il serait préférable d'envisager de réduire la durée de conservation maximale autorisée et de fixer une durée unique plus courte, applicable à l'ensemble des fournisseurs de l'UE, comme l'a indiqué le groupe de travail «article 29» dans son avis WP113***.[6]

Sur la base des résultats de cet exercice de contrôle de l'application de la législation UE, les fournisseurs contactés et/ou ayant fait l'objet d'une inspection ou d'un audit se sont conformés aux obligations de conservation susmentionnées. Toutefois, dans de très rares cas, la situation sur le terrain s'est révélée bien différente en raison des pratiques de stockage et/ou obligations appliquées aux données relatives à des fins commerciales, revenant à stocker ces données pendant des durées plus longues que celles prévues par la directive sur la conservation des données, jusqu'à 36 mois dans plusieurs cas et jusqu'à 10 ans dans un cas.

[6] WP 113: «En tout état de cause, il est indispensable de fixer une durée générale de conservation. Cette durée doit être la plus courte possible et se rapprocher au maximum de la période de conservation qui avait été fixée pour atteindre l'objectif initial pour lequel les fournisseurs de services avaient stocké ces données.»

En outre, il est apparu que dans de nombreux cas, aucune procédure automatique d'effacement des données n'était prévue à l'expiration de la durée de conservation applicable. Il faut rappeler à cet égard que les procédures manuelles ou engagées manuellement ne sont pas considérées comme conformes à la directive sur la conservation des données, car elles permettent d'allonger les durées de conservation du temps indéterminé qui s'écoule entre l'expiration du délai de conservation et le début de la procédure manuelle d'effacement. Des procédures automatiques doivent également être appliquées aux copies de sauvegarde.

Il convient également de souligner ici que les fournisseurs de services de communications électroniques et de services Internet stockent les données relatives au trafic dans plusieurs systèmes et les utilisent à des fins d'exploitation et de gestion très diverses, qui dans certains cas sont prévues par la loi et régies par des accords de niveau de service et des contrats de fourniture de services. De plus, toutes les données stockées dans les systèmes accessibles aux services répressifs l'ont également été au préalable dans d'autres systèmes, accessibles quant à eux à des fins diverses telles que la résolution de problèmes, la détection de la fraude, la facturation, etc. et par différentes entités au sein de l'organisation du fournisseur qui sont le plus souvent soumises à des contrôles moins stricts.

Dès lors, il semble nécessaire de souligner la nécessité pour la Commission et les autres institutions chargées d'évaluer le fonctionnement de la directive sur la conservation des données, de prendre en compte le caractère sensible que revêtent par nature les données relatives au trafic et de reconsidérer l'ensemble des mesures de sécurité qui les entourent, (indépendamment de la question de savoir si elles sont stockées dans des systèmes et à des fins autres que celles prévues par la directive), aux fins de l'évaluation générale de l'application de cette directive. Permettre que les systèmes contenant les catégories de données visées par la directive fassent l'objet de mesures de sécurité et de durées de conservation différentes de celles appliquées aux systèmes qui contiennent des données utilisées à d'autres fins, d'ordre commercial, revient à baisser le niveau de sécurité général des données relatives au trafic et à déroger, au final, aux exigences de la directive, à savoir que ces données doivent être conservées pendant des durées limitées et accessibles uniquement sous réserve de certaines contraintes.

iii. Mesures de sécurité techniques et organisationnelles

L'article 7, point b), de la directive sur la conservation des données exige que les données conservées fassent l'objet de mesures de sécurité techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites.
La directive sur la conservation des données n'exige pas de mesures de sécurité supplémentaires par rapport à celles qui sont prévues par les directives 2002/58/CE et 95/46/CE. Néanmoins, comme le groupe de travail «article 29» l'a déjà fait remarquer dans les avis précités, c'est le niveau élevé de risque inhérent aux données relatives au trafic qui exige que des normes de sécurité strictes et adaptées soient appliquées, compte tenu de la nature de ces données, de la quantité des données stockées et des durées de conservation.
À ce sujet, l'action de contrôle de l'application de la législation UE a démontré que les mesures de sécurité techniques et organisationnelles mises en œuvre par les fournisseurs de services de communications électroniques et de services Internet reflétaient leur perception du/des risques liés aux données relatives au trafic téléphonique et Internet. Si aucune ligne de

conduite n'est indiquée ou si les risques sont sous-estimés, il est très probable que des mesures inappropriées seront prises.

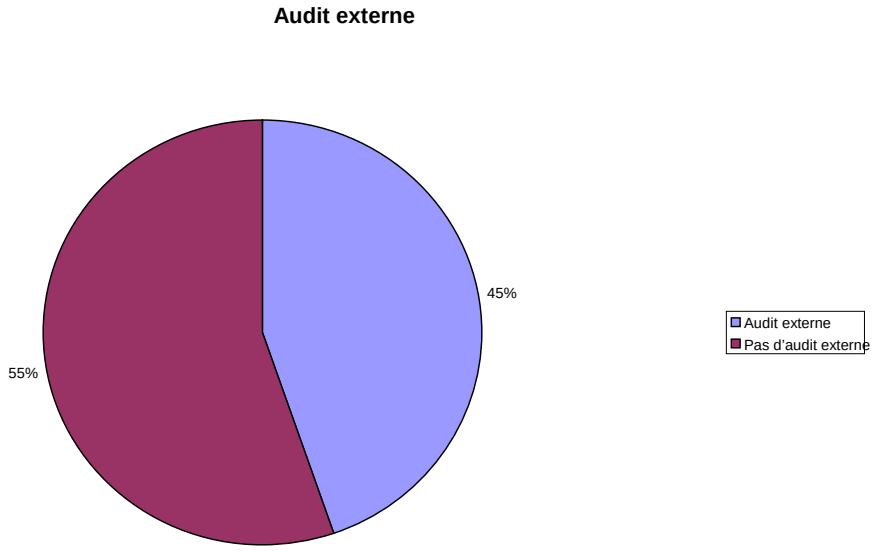
Pour se conformer aux exigences de la directive sur la conservation des données, les fournisseurs de services de communications électroniques et de services Internet doivent évaluer les risques liés aux données relatives au trafic de manière régulière et aussi objective que possible, afin de déterminer tous les facteurs de risque pertinents et leurs effets éventuels, et en accordant une attention particulière au contrôle de l'accès et à la disponibilité des données. Des audits externes réguliers peuvent contribuer à une évaluation des risques indépendante et objective.

En ce qui concerne la sécurité des informations, l'exercice de contrôle de l'application de la législation UE n'a pas permis de dresser un tableau homogène de la situation; en effet, en se basant sur les réponses au questionnaire (voir annexe 1, colonnes P et Q) et les inspections sur place, on constate que les mesures de sécurité varient en fonction de la taille des fournisseurs.

Des niveaux élevés de sécurité ont été constatés en matière d'accès physiques aux systèmes de conservation des données (voir annexe 1, colonne Q). À l'exception de quelques différences mineures, la majorité des fournisseurs de services de communications électroniques et de services Internet ont recours à la vidéo surveillance, à un personnel de surveillance spécialisé, à des systèmes de contrôle d'accès et à des procédures de retour au service normal en cas d'urgence pour assurer une surveillance ininterrompue desdits systèmes.

S'il est apparu que les grands fournisseurs déployaient des mesures de sécurité techniques et organisationnelles propres à assurer un niveau de sécurité approprié pour les données conservées, les petits fournisseurs semblent se contenter de normes de sécurité plus modestes. En effet, la majorité d'entre eux (principalement en raison de stratégies de contrôle des coûts) ne sont pas en mesure de mettre en œuvre des solutions informatiques de premier ordre, protégeant les données relatives au trafic avec le même degré de complexité que les leaders du marché. Les tâches confiées au personnel chargé du traitement des données en question pouvant se chevaucher, certains membres de ce personnel peuvent avoir accès à différents systèmes de stockage des données à des fins diverses. La nécessité d'assurer des niveaux de sécurité appropriés pour les données relatives au trafic n'a pas toujours été prise en compte lors de la conception ou de la mise en œuvre des systèmes de traitement de ces données à des fins commerciales. Il semble que les risques liés à la conservation des données relatives au trafic soient perçus de manière très diverse.

En ce qui concerne, en particulier, la phase préliminaire d'évaluation des risques, il a été établi qu'il s'agissait en règle générale d'une tâche accomplie en interne par les entreprises; ce qui peut entraîner un manque d'impartialité et un risque de sous-estimation des points faibles. Le diagramme ci-dessous montre la proportion de fournisseurs ayant recours à des audits externes et/ou à la certification par des tiers en matière de sécurité, par rapport au nombre total de fournisseurs pris en compte.



Les données relatives au trafic doivent être considérées comme très sensibles par nature. Elles doivent par conséquent bénéficier d'un traitement comparable à celui des catégories particulières de données visées à l'article 8 de la directive 95/46/CE. Si la conservation des données doit être adaptée à leur caractère sensible, l'accès à celles-ci par les services répressifs et leur transfert ultérieur à ces services doivent aussi faire l'objet d'une attention particulière. Pour ce faire, les conditions d'accès et de transfert ultérieur des données conservées doivent être clairement spécifiées par la loi. La directive sur la conservation des données, qui a été élaborée dans les années qui ont précédé le traité de Lisbonne, se base sur une répartition différente des compétences légales et ne prévoit aucune règle spécifique sur ce point, bien que le groupe de travail «article 29» ait déjà appelé à la définition de telles règles. On pourrait en outre ajouter que dans ce domaine, l'autorégulation ne suffit pas, principalement en raison du déséquilibre de pouvoirs qui existe entre les fournisseurs et les services répressifs. Les fournisseurs de services ne sont pas en mesure de «faire respecter» leurs propres politiques de sécurité lorsqu'ils traitent avec les services répressifs.

En plus des mesures de sécurité déjà en place, plusieurs mesures peuvent être proposées et adoptées en toute conformité avec le principe de neutralité technologique afin de garantir que l'accès aux données n'est effectué que par un personnel spécifiquement autorisé, conformément à l'article 7, point c), de la directive sur la conservation des données. Ces mesures ne sont pas actuellement appliquées par les fournisseurs en question:

- ***un contrôle strict de l'accès aux données conservées, par la définition de responsabilités et de profils d'utilisateur avec des droits d'accès différents;***
- ***une solide procédure d'authentification lors de l'accès, basée sur un double contrôle (par exemple, mot de passe + élément biométrique, ou mot de passe + jeton d'accès) et visant à garantir la présence physique du responsable du traitement des données;***
- ***un suivi détaillé des opérations d'accès et de traitement, par la conservation des fichiers «journal» consignant, au minimum, l'identité de l'utilisateur, l'heure d'accès et le fichier consulté;***

- ***la mise en place de solutions de gestion des fichiers «journal» visant à garantir l'intégrité de ces derniers par le cryptage ou des mesures de protection équivalentes;***
- ***la séparation logique avec d'autres systèmes de traitement des données à des fins commerciales;***
- ***toute mesure supplémentaire requise pour garantir la confidentialité des données.***

De plus, sur le plan de l'organisation et de la gestion, une importance particulière doit être accordée aux administrateurs des systèmes dans lesquels les données relatives au trafic sont stockées à des fins répressives; ***les rôles et fonctions de ces administrateurs doivent être détaillés, y compris au moyen de documents d'orientation ad hoc, et toutes les activités de maintenance réalisées sur ces systèmes doivent faire l'objet de contrôles approfondis***.

Pour améliorer les mesures de sécurité applicables aux données relatives au trafic, des actions multiples et coordonnées sont nécessaires; ***leur mise en œuvre par les fournisseurs peut être facilitée si à la fois les règles internes à l'entreprise et les mesures technologiques au sens strict sont intégrées à un programme de certification en matière de sécurité, à exécuter à intervalles réguliers (de préférence par un tiers), conformément aux normes internationales d'évaluation de l'efficacité des mesures prises pour faire face à l'évolution des risques et des points faibles. D'autres mesures peuvent se révéler efficaces dans ce domaine, comme par exemple permettre aux autorités chargées de la protection des données de réaliser des audits ou mettre des rapports d'audit à leur disposition***.

Un respect inégal des obligations en matière de mesures de sécurité techniques et organisationnelles constitue une entrave à la réalisation de l'objectif d'harmonisation de la directive. Il influe sur les coûts supportés par les acteurs du marché en fonction de leur taille et de leur positionnement, et affecte la dynamique du marché, ce qui en définitive se traduit par une application non harmonisée de la directive sur la conservation des données et empêche les citoyens européens de bénéficier d'un niveau égal de protection.

Le cas de l'article 7, point d), de la directive sur la conservation des données - L'article 7, point d), de la directive sur la conservation des données prévoit une exception applicable aux données auxquelles les services répressifs ont pu accéder, qui peuvent *de facto* être conservées pour une durée supplémentaire indéterminée.

On pourrait se demander s'il conviendrait d'exiger des fournisseurs de services de communications électroniques et de services Internet qu'ils mettent en place des mesures de sécurité supplémentaires pour cette catégorie particulière de «données auxquelles on a pu accéder», puisqu'aucune exigence spécifique n'est prévue dans la directive, ou si ces données doivent être incluses dans les dossiers correspondants et faire l'objet des mesures de sécurité applicables confiées aux autorités compétentes (ce qui semble être le cas). Les données en question présentent un niveau de risque extrêmement élevé, car elles peuvent révéler des informations importantes sur les utilisateurs (voire des informations sensibles).

Un accès massif aux données relatives au trafic et une prolongation de leur durée de conservation pour de trop longues périodes peuvent être considérés comme des mécanismes de contournement des obligations définies dans la directive. ***La nécessité d'envisager des durées de conservation plus longues pour les données auxquelles on a pu accéder doit être évaluée selon des critères bien définis qui, dans tous les cas, doivent prévoir la suppression de ces données conformément aux exigences fixées par la directive 95/46/CE et les***

instruments internationaux (y compris la recommandation R(87)15 du Conseil de l'Europe).

iv. Procédures de transfert

Il est apparu que les procédures de transfert applicables aux données relatives au trafic demandées par les services répressifs étaient extrêmement diverses. Les réponses au questionnaire et les inspections sur place ont fait état d'une vaste palette de solutions (y compris des procédures de transfert basées sur des documents manuscrits, des envois classiques ou par coursier) et de niveaux de sécurité très variables, allant de l'envoi de messages par courrier électronique ou par fax à l'utilisation de canaux de transmission dédiés protégés par cryptage. ***Une importance particulière doit être accordée à l'objectif d'harmonisation dans ce domaine, par la mise au point de procédures normalisées de transfert des données pour les services répressifs***.

À cet égard, il convient de rappeler que la directive sur la conservation des données comprend une liste exhaustive des données pouvant être transmises aux services répressifs par les fournisseurs, ces données constituant un ensemble fini d'éléments; en outre, la législation nationale doit clairement spécifier quelles sont les infractions graves pouvant motiver une demande de transfert, et fournir une liste précise et exhaustive des entités (autorités judiciaires) habilitées à autoriser l'accès à ces données et des possibilités spécifiques d'accès prévues par la loi.

Une procédure informatique type pourrait être élaborée à partir d'un protocole d'échange des données basé sur les considérations susmentionnées, alors que cette question est actuellement laissée à l'appréciation des parties prenantes – du moins d'après les informations disponibles. Définir une procédure de transfert type, qui prenne en compte la directionnalité du transfert (qui doit être basé sur un modèle PUSH), permettrait des transferts de données plus rapides, plus fiables et moins onéreux pour toutes les parties concernées (fournisseurs et services répressifs); en effet, ces dernières pourraient bénéficier de solutions normalisées conçues sur la base d'un cadre de référence unique et appliqué à grande échelle. Ceci constituerait une avancée considérable par rapport aux solutions actuellement disponibles sur le marché, qui sont à la fois de nature différentes et plus coûteuses.

- Notons que spécifier de manière claire qui sont les parties prenantes et quelles sont les données qu'elles peuvent échanger pourrait considérablement améliorer le niveau de sécurité général de la procédure de transfert, et ceci pour plusieurs raisons: cela permettrait une authentification mutuelle; les conditions préalables seraient réunies pour la mise en place de connexions cryptées et de canaux de communication sécurisés et fiables basés sur des échanges de certificats de clé et de signature numérique garantissant l'intégrité, la confidentialité et la non-répudiation des transferts de données; le risque d'interception illicite (interception et saisie et/ou duplication des données au cours de leur transfert) serait réduit au minimum; tous les outils nécessaires pour rendre compte efficacement de l'accès aux données seraient introduits; les parties concernées pourraient classer les différentes demandes par objet ou par catégorie de données demandées, ce qui devrait faciliter l'établissement de rapports statistiques comparables dans les États membres. Toutes ces options, une fois mises en œuvre, auraient pour conséquence de réduire le nombre d'accès inappropriés

aux données et permettraient aux autorités chargées de la protection des données de contrôler efficacement l'accès aux données. Les autorités judiciaires devraient elles aussi intervenir dans le processus de transfert, en leur qualité d'institutions de confiance habilitées à décider au cas par cas pour quelles données et dans quelles circonstances l'autorisation d'accès peut être accordée aux services répressifs. Le motif devrait être tiré d'une liste connue d'infractions graves, de manière à refléter fidèlement la procédure de communication des données relatives au trafic prévue par la directive.

Pour toutes les raisons susmentionnées, une norme de transfert paneuropéenne pourrait comporter les éléments suivants:

- un point de contact unique pour chaque fournisseur;
- un format unique de transfert des données incluant, au moins, les champs suivants permettant de garantir un échange de données entre les parties concernées ou un accès aux données sécurisé et fiable:
    - o les données utilisateur, comportant un nombre connu et fini de champs relatifs à l'abonnement de l'utilisateur et aux terminaux mis à sa disposition;
    - o les données relatives au trafic, comportant un nombre connu et fini de champs relatifs à la transposition nationale de la liste de données visées à l'article 5 de la directive sur la conservation des données;
    - o le code fournisseur, contenant un identifiant européen unique du fournisseur de services de communications électroniques ou de services Internet;
    - o le code du service répressif, contenant un identifiant du service autorisé à accéder aux données;
    - o le code judiciaire, contenant un identifiant européen unique de l'autorité judiciaire habilitée à autoriser l'accès aux données;
    - o un horodateur et le numéro de la demande, afin de déterminer la date et l'ordre des demandes d'accès et des autorisations respectives;
    - o le type de demande, précisant la catégorie de données demandées (par exemple par type d'infraction ou par quantité de données demandées).

La mise en place d'un protocole d'échange des données répondant aux caractéristiques énumérées ci-dessus permettrait de réduire au minimum certains des problèmes soulevés par les autorités chargées de la protection des données au cours de la présente action de contrôle de l'application de la législation UE, comme par exemple la pression exercée par les services répressifs sur les fournisseurs en vue d'obtenir des données utilisateur non visées par la directive sur la conservation des données, ou encore les demandes d'accès ne présentant pas toutes les garanties formelles ou émanent d'entités non autorisées (c'est-à-dire autres que les services répressifs).

Rappelons à ce sujet que ***la liste des infractions graves justifiant la conservation des données en vertu de la directive doit être établie au niveau national conformément à la législation nationale, compte tenu des considérations exposées dans les documents WP113 et WP119 relatives à la nécessité de définir clairement la notion d'«infraction grave». Une liste exhaustive des entités autorisées à accéder aux données conservées conformément à la directive doit être fournie à toutes les parties prenantes concernées.***

Il convient de mentionner à cet égard que l'Institut européen des normes de télécommunications (ETSI) a déjà travaillé efficacement à l'élaboration d'un modèle de référence pour le transfert des données aux services répressifs. Ce modèle peut encore être étudié et évalué.

D. Statistiques visées à l'article 10 de la directive sur la conservation des données

En vertu de l'article 10 de la directive sur la conservation des données, les États membres doivent faire en sorte que des statistiques sur l'utilisation des données conservées conformément aux dispositions applicables soient transmises annuellement à la Commission; l'article 14 stipule que toute modification de la directive doit tenir compte de ces statistiques (mises à disposition par les États membres). À de très rares exceptions près, le respect de cette obligation de notification n'a pu être confirmé.

Seuls quelques États membres ont fourni les informations requises, qui concernaient le nombre de demandes soumises aux fournisseurs, les cas dans lesquels les informations ont été transmises, et ceux dans lesquels les demandes de données n'ont pu être satisfaites, ainsi que le laps de temps écoulé entre la date de stockage des données et la date à laquelle les autorités compétentes ont demandé leur transmission.

Même si les statistiques visées à l'article 10 ne peuvent constituer la seule base à utiliser pour décider de l'avenir de la directive, la disponibilité et l'exactitude des informations en question sont essentielles pour évaluer si les objectifs sous-tendant la directive (y compris l'introduction de principes harmonisés applicables à tous les États membres) ont été atteints, eu égard notamment aux problèmes signalés tout au long des discussions qui ont précédé et suivi son adoption (voir les décisions de certaines Cours constitutionnelles et Cours suprêmes européennes).

Le manque de statistiques fiables pourrait être préjudiciable à l'ensemble de l'exercice, car leur examen constitue une condition préalable à l'éventuelle révision de la directive, en particulier en ce qui concerne la liste des données visées à l'article 5 et les durées de conservation fixées à l'article 6 de ladite directive.

L'utilisation de statistiques partielles ou non comparables pourrait entraîner des décisions ayant des conséquences non négligeables sur le respect de la vie privée des personnes concernées, sans répondre à l'objectif d'harmonisation poursuivi par la directive.

De même, on peut considérer que plusieurs obstacles pourraient être levés si une procédure de transfert normalisée était mise en place. Grâce à la disponibilité de règles de transfert spécifiques, chacun des acteurs pourrait fournir des statistiques comparables à celles des autres parties concernées, ce qui permettrait d'obtenir une vue d'ensemble plus fiable de l'utilisation et de l'efficacité des données relatives au trafic dans le cadre de la poursuite des «infractions graves».

En vue de la première évaluation de l'application de la directive 2006/24/CE que la Commission est tenue d'effectuer pour le 15 septembre 2010, il est fondamental que chacun des États membres qui ont transposé la directive fournisse les statistiques nécessaires. Le groupe de travail «article 29» estime qu'il est indispensable que cette

information soit fournie afin de permettre d'établir de manière objective la nécessité et l'efficacité de la directive sur la conservation des données.

En outre, il est important que ces statistiques comportent des informations concernant l'incidence des données en question, ventilées selon leur ancienneté, sur la lutte contre les infractions graves.

E. Sous-traitance

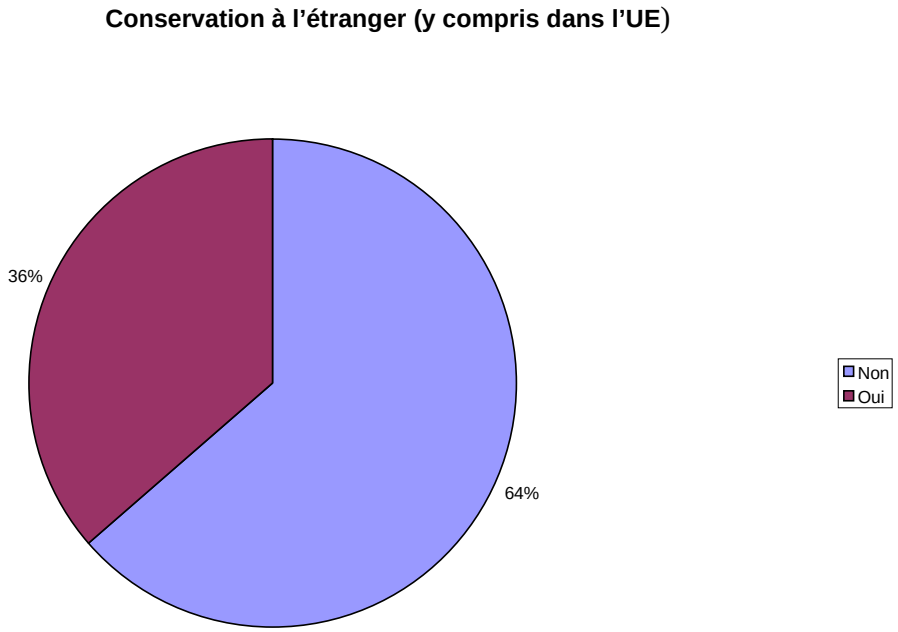
Au cours de la présente action de contrôle de l'application de la législation UE, il est apparu que les sous-traitants étaient de plus en plus sollicités dans le cadre de plusieurs activités liées à la conservation des données relatives au trafic, en particulier par les petits opérateurs obéissant à une politique de maîtrise des coûts. Cette pratique n'est pas toujours compatible avec une définition précise des rôles respectifs de chacun, en particulier en ce qui concerne la conformité avec la législation nationale sur la protection des données et la désignation des sous-traitants et/ou l'attribution des tâches de traitement au personnel en charge.

Il convient de rappeler que le marché des réseaux et services de communications électroniques est constitué d'entités hétérogènes qui disposent de ressources humaines et financières très variables; cette situation constitue clairement un obstacle à l'objectif d'harmonisation poursuivi par la directive sur la conservation des données. Il a par exemple été établi que la taille de l'entité chargée de la conservation des données était dans certains cas plus importante que celle du fournisseur de services de communications électroniques; dans de tels cas, il est évidemment difficile pour ce dernier de contrôler de manière efficace les opérations de traitement des données effectuées par le sous-traitant. Des problèmes supplémentaires surviennent lorsque les données sont conservées à l'extérieur des frontières du pays, ce qui n'est pas une pratique inhabituelle (voir schéma ci-dessous) même si elle se limite principalement aux grands acteurs opérant dans de petits États membres et ayant recours aux services pris en charge par leurs sièges respectifs. C'est également une solution pour laquelle optent parfois les petits fournisseurs et/ou les opérateurs virtuels qui ont recours aux services de multinationales spécialisées dans les technologies de l'information. Dans ces circonstances, les autorités de supervision sont tenues de fournir un niveau accru de coopération et d'assistance mutuelles en vue de permettre l'accès aux données et l'exercice des pouvoirs d'exécution nécessaires.

Afin de répondre aux exigences prévues par la directive tout en limitant les coûts, on peut se référer aux solutions fédérées qui ont déjà été appliquées principalement au niveau national par les petits FSI: l'un des FSI fédérés, ou une tierce partie mandatée, met au point et applique le système de conservation des données, gère les phases d'authentification et répartit la mémoire attribuée à chaque FSI. Cette stratégie doit être considérée favorablement, bien qu'elle requière un ensemble de règles déjà relativement harmonisées, officialisées et détaillées.

Le transfert des données conservées vers d'autres pays doit en tout temps s'effectuer conformément aux conditions fixées par la directive 95/46/CE. Le transfert de données qui sont générées sur le territoire de l'UE et destinées à être utilisées en dehors de ce territoire, en particulier, devra faire l'objet d'une évaluation, conformément à la directive.

En outre, les dispositions de la directive 95/46/CE relatives au transfert de données personnelles vers des pays tiers ne peuvent être dissociées des autres dispositions de cette même directive, en ce compris celles qui régissent les relations entre les responsables du traitement et les sous-traitants.[7]



La question de la sous-traitance doit faire l'objet d'une analyse plus approfondie par les autorités chargées de la protection des données, afin d'évaluer de manière plus précise sa compatibilité avec les exigences de la législation nationale (en ce qui concerne la désignation des sous-traitants, par exemple), y compris des clauses contractuelles - qui doivent prévoir des mesures de sécurité spécifiques et adaptées.

IV. Actions ultérieures et recommandations

À la lumière des résultats de la présente enquête commune, les recommandations ci-dessous peuvent être effectuées pour chacun des problèmes examinés. Si ces recommandations s'adressent principalement aux fournisseurs, qui possèdent les moyens techniques nécessaires à leur mise en œuvre, elles peuvent néanmoins faire entrer en jeu les autorités publiques (dont la Commission européenne, les États membres et les autorités nationales de protection des données), principalement en ce qui concerne la question des coûts, qui peuvent d'une part

[7] Pour une analyse plus approfondie des aspects légaux de la sous-traitance, le groupe de travail Article 29 se réfère au paragraphe 4.6, «Flux de données transfrontaliers» de l'avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT). On peut également se référer à l'avis n° 1/2010 (WP169) du groupe de travail sur les notions de «responsable du traitement» et de «sous-traitant».

empêcher la mise en place de mesures de sécurité et de protection des données, et d'autre part provoquer des distorsions du marché. ***En outre, le groupe de travail souhaite rappeler que l'autorégulation seule ne suffit pas dans ce contexte***, ***principalement en raison du déséquilibre de pouvoirs qui existe entre les fournisseurs et les services répressifs, mais aussi parce que les préoccupations relatives aux coûts et à la concurrence ne permettent pas de mettre en place une stratégie d'autorégulation garantissant un niveau élevé de sécurité.***

- Catégories de données à conserver

Étant donné que la directive 2006/24/CE déroge aux dispositions de la directive 2002/58/CE, la liste de données à conserver obligatoirement doit être considérée comme exhaustive. Dès lors, aucune autre obligation de conservation de données ne peut être imposée aux fournisseurs par la législation nationale sur le fondement de la directive sur la conservation des données. D'autre part, le groupe de travail «article 29» souhaite souligner qu'en vertu de cette même directive, les services répressifs ne sont pas habilitées à demander aux fournisseurs de services de collecter des données qui n'entrent pas dans les catégories visées par la directive.

- Durées de conservation

a. Le manque d'harmonisation révélé par cette enquête dans le domaine des durées de conservation porte gravement atteinte au principe selon lequel les citoyens européens «sont en droit de bénéficier du même niveau de protection dans toute l'Union européenne», en partie parce qu'il peut avoir des conséquences financières considérables pour les parties prenantes et également pour des questions de coûts et de compétitivité. À cet égard, et comme il l'a déjà indiqué dans son avis WP113, le groupe de travail «article 29» considère qu'il serait utile d'envisager de réduire la durée maximale de conservation et de fixer une durée unique plus courte, applicable à l'ensemble des fournisseurs dans toute l'Union européenne.

b. Étant donné l'existence d'objectifs et de durées très variables en matière de conservation des données (finalités commerciales contre finalités répressives), il semblerait approprié de suggérer que la Commission reconsidère la question générale de la sécurité des données relatives au trafic, dans le cadre de l'évaluation globale de l'application de la directive sur la conservation des données. Il ne devrait pas être permis d'appliquer des niveaux de sécurité et des durées de conservation différents en fonction des objectifs recherchés. La directive sur la conservation des données stipule que les données conservées à des fins répressives doivent l'être pour une durée limitée et qu'on ne doit pouvoir y accéder qu' des fins spécifiques et sur une base légale explicite.

- Mesures de sécurité techniques et organisationnelles

a. Les fournisseurs de services de communications électroniques et de services Internet devraient évaluer les risques inhérents aux données relatives au trafic de manière régulière et aussi objective que possible, afin de repérer tous les facteurs de risque et leurs effets éventuels, en accordant une attention particulière au contrôle de l'accès et à la disponibilité des données. Des audits externes réguliers peuvent contribuer à une évaluation des risques indépendante et objective.

b. En plus des mesures de sécurité déjà en place, les mesures suivantes peuvent être proposées et adoptées en toute conformité avec le principe de neutralité technologique afin de garantir que les données ne soient accessibles que par le personnel dûment autorisé, conformément à l'article 7, point c), de la directive sur la conservation des données. Ces mesures ne sont actuellement pas appliquées par les fournisseurs en question:

- un contrôle strict de l'accès aux données conservées, par la définition de responsabilités et de profils d'utilisateur avec des droits d'accès différents;
- une solide procédure d'authentification lors de l'accès, basée sur un double contrôle (par exemple, mot de passe + élément biométrique, ou mot de passe + jeton d'accès) et visant à garantir la présence physique du responsable du traitement des données;
- un suivi détaillé des opérations d'accès et de traitement, par la conservation des fichiers «journal» consignant, au minimum, l'identité de l'utilisateur, l'heure d'accès et le fichier consulté;
- la mise en place de solutions de gestion des fichiers «journal» visant à garantir l'intégrité de ces derniers par le cryptage ou des mesures de protection équivalentes;
- la séparation logique avec d'autres systèmes de traitement des données à des fins commerciales;
- toute mesure supplémentaire requise pour garantir la confidentialité des données.

c. Les rôles et fonctions de ces administrateurs doivent être détaillés, y compris au moyen de documents d'orientation ad hoc, et toutes les activités de maintenance réalisées sur ces systèmes doivent faire l'objet de contrôles approfondis.

d. Pour améliorer les mesures de sécurité applicables aux données relatives au trafic, des actions multiples et coordonnées sont nécessaires; leur mise en œuvre par les fournisseurs peut être facilitée si à la fois les règles internes à l'entreprise et les mesures technologiques au sens strict sont intégrées à un programme de certification en matière de sécurité, à exécuter à intervalles réguliers (de préférence par un tiers), conformément aux normes internationales d'évaluation de l'efficacité des mesures prises pour faire face à l'évolution des risques et des points faibles. D'autres mesures peuvent se révéler efficaces dans ce domaine, comme par exemple permettre aux autorités chargées de la protection des données de réaliser des audits ou mettre des rapports d'audit à leur disposition.

e. La nécessité d'envisager des durées de conservation plus longues pour les données auxquelles on a pu accéder doit être évaluée selon des critères bien définis qui, dans tous les cas, doivent prévoir la suppression de ces données conformément aux exigences fixées par la directive 95/46/CE et les instruments internationaux (y compris la recommandation R(87)15 du Conseil de l'Europe).

- Procédures de transfert

a. En vue d'une meilleure harmonisation, des procédures normalisées de transfert des données pour les services répressifs devraient être mises en place à l'échelle européenne. Une procédure informatique type pourrait être élaborée à partir d'un protocole d'échange des données, en tenant compte de la directionnalité du transfert (qui doit être basé sur un modèle PUSH). Ceci permettrait des transferts de données plus rapides et moins onéreux pour toutes les parties concernées (fournisseurs et services répressifs); une telle norme

devrait permettre de conserver la trace des paramètres ou activités suivants, au moins: données utilisateur, type de données, code fournisseur, code du service répressif, code judiciaire, date et heure, numéro et type de demande.

b. La liste des infractions doit être transposée en droit national, en tenant compte des considérations émises dans les documents WP113 et WP119. Une liste exhaustive des entités autorisées à accéder aux données conservées conformément à la directive doit être fournie à toutes les parties prenantes concernées.

- Statistiques

Les États membres doivent fournir à la Commission les statistiques nécessaires aussi rapidement que possible, et dans tous les cas dans un délai utile avant l'échéance fixée pour le rapport d'évaluation de la directive sur la conservation des données que la Commission est tenue de préparer. Ces statistiques seront éventuellement accompagnées d'informations relatives à l'incidence des données en question, ventilées selon leur ancienneté, sur la lutte contre les infractions graves.

- Sous-traitance

a. La question de la sous-traitance doit faire l'objet d'une analyse plus approfondie par les autorités chargées de la protection des données, afin d'évaluer de manière plus précise sa compatibilité avec les exigences de la législation nationale (en ce qui concerne la désignation des sous-traitants, par exemple), y compris des clauses contractuelles - qui doivent prévoir des mesures de sécurité spécifiques et adaptées.

b. Référence peut être faite aux solutions fédérées qui sont déjà appliquées à l'échelle nationale par les petits FSI.

ANNEXE I

Data Retention_DraftFinall