Conseil des barreaux européens
Council of Bars and Law Societies of Europe
Association internationale sans but lucratif
Rue Joseph II, 40 /8 – 1000 Bruxelles
T. : +32 (0)2 234 65 10 – F. : +32 (0)2 234 65 11
Email : ccbe@ccbe.eu – www.ccbe.eu

Recommandations du CCBE concernant l'annulation de la directive sur la conservation des données

12/09/2014

Introduction

Le Conseil des barreaux européens (CCBE) représente les barreaux de 32 pays membres et 13 pays associés et observateurs, soit plus d'un million d'avocats européens

Le CCBE publie dans la présente les recommandations qu'il préconise à ses barreaux membres concernant l'annulation récente de la directive sur la conservation des données (2006/24/CE) par la Cour de justice de l'Union européenne (CJUE) le 8 avril 2014 (dans les affaires jointes C-293/12 et C-594/12).

Lors de l'adoption législative de la directive sur la conservation des données, le CCBE a exprimé vigoureusement ses préoccupations concernant, entre autres, le secret professionnel dont relèvent les communications entre l'avocat et son client, l'autorisation judiciaire préalable à l'accès aux données, la durée et l'objet de la conservation des données.

La directive, qui est en vigueur depuis le 3 mai 2006, devait être transposée par les États membres dans leur droit national avant le 15 septembre 2007, avec la possibilité de différer jusqu'au 15 mars 2009 son application en ce qui concerne les données communiquées par Internet (les données relatives au trafic).

En septembre 2006, le CCBE a publié un ensemble de recommandations à ses membres vis-à-vis de la transposition de la directive dans le droit national. Compte tenu de l'arrêt récent, la question se pose de savoir dans quelle mesure ces législations nationales respectent le principe de proportionnalité auquel se réfère la CJUE.

Aperçu de l'arrêt de la CJUE

Ingérence grave dans les droits au respect de la vie privée et à la protection des données à caractère personnel

La Cour observe que les données à conserver permettent : (1) de savoir avec quelle personne et par quel moyen un abonné ou un utilisateur inscrit a communiqué ; (2) de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu ; (3) de connaître la fréquence des communications. Ces données, prises dans leur ensemble, sont susceptibles de fournir des indications très précises sur la vie privée des personnes dont les données sont conservées, comme les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités réalisées, les relations sociales et les milieux sociaux fréquentés.

La Cour estime qu'en imposant la conservation de ces données et en en permettant l'accès aux autorités nationales compétentes, **la directive s'immisce de manière particulièrement grave dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel**.

En outre, le fait que la conservation et l'utilisation ultérieure des données sont effectuées sans que l'abonné ou l'utilisateur inscrit en soit informé est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante.

Le manquement au respect du principe de proportionnalité et l'incompatibilité possible avec les obligations du secret professionnel

La Cour estime que la conservation des données en vue de leur transmission éventuelle aux autorités nationales compétentes répond effectivement à un objectif d'intérêt général, à savoir la lutte contre la criminalité grave ainsi que, en définitive, la sécurité publique.

Si la conservation des données imposée par la directive peut être considérée comme apte à réaliser l'objectif poursuivi par celle-ci**, l'ingérence vaste et particulièrement grave de cette directive dans les droits fondamentaux en cause n'est pas suffisamment encadrée afin de garantir que cette ingérence soit effectivement limitée au strict nécessaire**.

En effet, premièrement, la directive couvre de manière généralisée l'ensemble des individus, des moyens de communication électronique et des données relatives au trafic sans qu'**aucune différenciation, limitation ou exception** soit opérée en fonction de l'objectif de lutte contre les infractions graves. À cet égard, la Cour rappelle qu'en général, le fait que toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au **secret professionnel**.

Deuxièmement, la directive ne prévoit aucun critère objectif qui permettrait de garantir que les autorités nationales compétentes aient **accès aux données** et ne puissent les utiliser qu'aux seules fins de prévenir, détecter ou poursuivre pénalement des infractions susceptibles d'être considérées, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux en question, comme suffisamment graves pour justifier une telle ingérence. Au contraire, la directive se borne à renvoyer de manière générale aux « infractions graves » définies par chaque État membre dans son droit interne. De plus, la directive ne prévoit pas les conditions matérielles et procédurales dans lesquelles les autorités nationales compétentes peuvent avoir accès aux données et les utiliser ultérieurement. L'accès aux données n'est notamment pas subordonné au contrôle préalable d'une juridiction ou d'une entité administrative indépendante.

Troisièmement, s'agissant de **la durée de conservation** des données, la directive impose une durée d'au moins six mois sans opérer une quelconque distinction entre les catégories de données en fonction des personnes concernées ou de l'utilité éventuelle des données par rapport à l'objectif poursuivi. En outre, cette durée se situe entre 6 mois au minimum et 24 mois au maximum, sans que la directive ne précise les critères objectifs sur la base desquels la durée de conservation doit être déterminée afin de garantir sa limitation au strict nécessaire.

La Cour constate par ailleurs que **la directive ne prévoit pas de garanties suffisantes** permettant d'assurer une protection efficace des données contre les risques d'abus ainsi que contre l'accès et l'utilisation illicites des données. Elle relève entre autres que la directive autorise les fournisseurs de services à tenir compte de considérations économiques lors de la détermination du niveau de sécurité qu'ils appliquent (notamment en ce qui concerne les coûts de mise en œuvre des mesures de sécurité) et qu'elle ne garantit pas la destruction irrémédiable des données au terme de leur durée de conservation.

La Cour critique enfin le fait que la directive n'impose **pas une conservation des données sur le territoire de l'Union.** Ainsi, la directive ne garantit pas pleinement le contrôle du respect des

exigences de protection et de sécurité par une autorité indépendante, comme cela est pourtant explicitement exigé par la charte. Or, un tel contrôle, effectué sur la base du droit de l'Union, constitue un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel.

En conséquence, la Cour est d'avis qu'en adoptant la directive sur la conservation des données, le législateur de l'Union a **dépassé les limites imposées par le respect du principe de proportionnalité**.

Effets de l'invalidation

Étant donné que la directive sur la conservation des données a été invalidée dans son intégralité, le texte est réputé n'avoir jamais existé. La Cour n'ayant pas limité l'effet de son arrêt dans le temps, la déclaration d'invalidité prend effet à la date à laquelle la directive sur la conservation des données est entrée en vigueur. Elle n'est donc plus applicable. L'arrêt ne s'applique toutefois pas aux lois mises en œuvre à l'échelle nationale il reste à voir à ce stade quelles mesures seront prises en réponse à l'arrêt par les institutions de l'UE ainsi que par les États membres.

La Commission européenne a pour l'instant indiqué dans une foire aux questions (FAQ) publiée sur la date de l'arrêt que la législation nationale ne doit être modifiée qu'à l'égard des aspects qui deviennent contraires au droit de l'UE après un arrêt de la Cour européenne de justice. En outre, la déclaration d'invalidité de la directive sur la conservation des données n'annule pas la possibilité qu'ont les États membres en vertu de la directive « vie privée et communications électroniques » (2002/58/CE) d'imposer la conservation des données.

Il semble néanmoins probable que la décision de la CJUE ouvre la porte à des contestations judiciaires contre la collecte de données dans les juridictions nationales, en particulier vis-à-vis du principe de proportionnalité que mentionne la CJUE.

Recommandations

Compte tenu des conclusions de l'arrêt de la CJUE, le CCBE recommande de prendre les mesures nécessaires suivantes :

1. Si la législation nationale ne répond ni au principe de proportionnalité mentionné par la CJUE ni aux préoccupations du CCBE concernant :
   - le secret professionnel des communications entre l'avocat et son client ;
   - l'autorisation judiciaire préalable à l'accès aux données ;
   - la durée et l'objet de la conservation des données.

il est proposé que les membres du CCBE prennent les mesures suivantes :

   a) Identifier les stratégies permettant un changement dans la législation nationale lorsque cela s'avère nécessaire (par exemple en faisant pression auprès des parlementaires ou en lançant une campagne de sensibilisation auprès du public, etc.)

   b) Faire connaitre les affaires dans lesquelles des clients/avocats sont touchés de manière négative par le manquement au principe de proportionnalité et obtenir des conseils juridiques sur les recours possibles en mentionnant l'arrêt de la CJUE.

   c) Porter le manquement au principe de proportionnalité à l'attention des organes gouvernementaux (autorités de protection des données, ministères et services gouvernementaux, etc.) responsables de la protection des données. En outre, si cela s'avère nécessaire, les membres du CCBE devraient chercher à contester toute législation nationale pouvant être jugée contraire à l'arrêt de la CJUE, en particulier en soutenant les

avocats et les cabinets dans ces contestations judiciaires (par exemple en soumettant des mémoires d'amicus curiae si possible).

d) Mentionner spécifiquement l'arrêt de la CJUE dans tout document, toute déclaration publique et lettre au gouvernement et aux élus concernant la question de la protection des données dans le cadre de la conservation des données.

e) Exprimer les préoccupations auprès de la Commission européenne (DG Justice - Direction C Droits fondamentaux et citoyenneté de l'Union – 3 Protection des données) et du groupe de travail établi en vertu de l'article 29 de la directive 95/46/E[1], du commissaire national à la protection des données ou du contrôleur européen de la protection des données[2].

f) Informer le CCBE de l'état d'avancement de la mise en œuvre de la directive sur la conservation des données dans leur État membre et indiquer comment le CCBE peut aider ses membres à prendre des mesures vers un changement de la législation nationale si nécessaire.

g) Envisager les contestations possibles de la loi mettant en œuvre la directive sur la conservation des données devant l'organe constitutionnel concerné (par exemple le conseil constitutionnel ou tout autre organe constitutionnel concerné, les tribunaux ordinaires, etc. tel que prévu par le droit local) ou tout autre tribunal compétent.

2. À la lumière des conclusions de l'Étude comparative du CCBE sur la surveillance gouvernementale des données des avocats hébergées dans le nuage, le CCBE invite également la Commission européenne à s'assurer que, quel que soit le régime de réglementation en place dans un État membre vis-à-vis de l'interception des communications, ledit régime garantit l'inviolabilité des données et d'autres éléments de preuve relevant du secret professionnel.

En conséquence :

a) Un niveau minimal de protection du secret professionnel devrait exister, quelles que soient les données relatives au trafic, les métadonnées ou les données relatives au contenu, quel que soit l'organe gouvernemental qui exige l'accès à des données et que ce soit ou non pour des motifs de sécurité nationale ou de lutte ou de prévention vis-à-vis de la criminalité.

b) Le niveau minimal de protection des communications relevant du secret professionnel devrait être le même dans le monde électronique que dans le monde papier.

c) Ce niveau minimal de protection doit garantir au sein des États membres une protection plus explicite et plus cohérente du secret professionnel dans le cadre des communications entre l'avocat et son client par le biais d'une autorisation judiciaire préalable et des exigences claires quant à l'objet et à la durée des données.

3. À la lumière de la résolution du Parlement européen du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI)), le CCBE invite également le Parlement européen à agir de toute urgence pour établir « un habeas corpus numérique européen protégeant les droits fondamentaux à l'ère numérique » comprenant la protection de la confidentialité des relations entre l'avocat et son client, tel que stipulé dans l'action 6 de la résolution.

---

[1] European Commission: DG JUST - Justice, Marie-Helene.Boulanger@ec.europa.eu (Head of Unit - Data protection), +32 229-69408. Art.29 Working Group: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

[2] For contact details of the national data protection commissioner, please see : http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_fr.htm ; Contact details of the European Data Protection Supervisor: http://ec.europa.eu/justice/data-protection/bodies/supervisor/index_fr.htm.