

Entretiens européens: «Le droit européen de la protection des données»

Délégation des Barreaux de France, Bruxelles, le 15 mars 2013

Peter Hustinx

Contrôleur européen de la protection de données

«La protection des données et la justice pénale – Le point de vue du CEPD»

Je suis heureux de pouvoir prendre la parole à l'occasion de cette conférence. Le thème de celle-ci est un excellent exemple de l'évolution graduelle du droit européen et de la façon dont il interagit avec les législations nationales. Il est également particulièrement opportun en ce qui concerne la réforme du cadre juridique de l'UE pour la protection des données qui fait actuellement l'objet de débats au Parlement et au Conseil.

Rôle du CEPD

Tout d'abord, permettez-moi d'expliquer brièvement mon rôle. Le contrôleur européen de la protection des données (CEPD) est une autorité indépendante au niveau de l'UE, comme la CNIL en France. Il a trois tâches principales:

- 1) contrôler les institutions et organes de l'UE lorsqu'ils traitent des données personnelles et ce, afin de garantir le respect des principes de protection des données;
- 2) conseiller la Commission, le Parlement européen et le Conseil sur les nouvelles législations qui pourraient avoir un impact sur la protection des données personnelles; et
- 3) coopérer avec les autorités de contrôle nationales, telles que la CNIL et les organes similaires au sein d'autres États membres, pour améliorer la cohérence de la protection des données au sein de l'UE.

La mission de contrôle est peut-être moins pertinente aujourd'hui mais, étant donné l'intérêt particulier pour cet aspect de cette partie de la conférence, permettez-moi d'indiquer que nous contrôlons également les organes de l'UE qui ont un lien évident avec la justice pénale, tels que l'Office européen de lutte antifraude (OLAF). Nous jouons également un rôle de plus en

plus important au sein de l'«espace de liberté, de sécurité et de justice», qui englobe l'immigration et l'asile, ainsi que la coopération sur le terrain de la police et de la justice pénale.

Les deux autres tâches principales sont plus pertinentes aujourd'hui. Cela vaut tout d'abord pour notre rôle consultatif dans le cadre des propositions pour une réglementation générale relative à la protection des données et une directive distincte pour la protection des données dans l'application du droit pénal. Mais plus généralement, une grande majorité des propositions législatives pour lesquelles nous avons émis des recommandations au cours des huit dernières années étaient associées, directement ou indirectement, à l'application du droit pénal. Cela inclut également la directive sur la conservation des données qui a été abordée par l'orateur précédent.

Cependant, la coopération avec les autorités de contrôle nationales est également pertinente. Par exemple, en collaboration avec celles-ci, nous garantissons un contrôle coordonné des systèmes d'information de grande envergure dans le cadre de l'espace de liberté, de sécurité et de justice, au sein duquel les États membres et la Commission jouent un rôle important. Ce modèle s'appliquera également bientôt au système d'information Schengen de deuxième génération (SIS II).

Traité de Lisbonne

Il est également important de mentionner le traité de Lisbonne, tout d'abord parce qu'il place l'accent sur les droits fondamentaux. En raison de l'entrée en vigueur du traité de Lisbonne à la fin de l'année 2009, la Charte européenne des droits fondamentaux est maintenant un instrument contraignant, non seulement pour les institutions et les organes de l'UE mais également pour les États membres lorsqu'ils agissent dans le cadre du droit de l'Union européenne. Cela s'applique également aux articles 7 et 8 de la Charte sur le respect de la vie privée et la protection des données sur lesquels je reviendrai dans un instant.

Le traité de Lisbonne est également pertinent car il a introduit une base juridique générale pour des «règles relatives à la protection des données» dans l'article 16 du traité sur le fonctionnement de l'Union européenne. Cette disposition sert maintenant de base pour l'examen actuel du cadre juridique de l'UE sur la protection des données, notamment dans des domaines impliquant l'ancien «troisième pilier» de l'UE.

Il existe une troisième raison de mentionner le traité de Lisbonne: pour souligner les rôles de la Commission et du Parlement européen dans l'adoption des règles relatives à l'ancien «troisième pilier» de l'UE. Cela signifie que le Parlement européen fait maintenant partie intégrante du corps législatif de l'UE, notamment dans des domaines politiques affectant l'application du droit pénal, comme dans le cas de la protection des données.

Respect de la vie privée et protection des données

L'article 7 de la Charte contient un droit au *respect*, pour tous, de la vie privée et familiale, du domicile et de la correspondance, qui ressemble fortement à celui prévu à l'article 8 de la Convention européenne des Droits de l'Homme (CEDH). Il s'agit d'un droit fondamental classique contre toute *interférence* avec la vie privée, sauf quand une telle interférence est prévue par la loi et est nécessaire dans une société démocratique pour un objectif légitime soigneusement défini. Ces critères servent de base pour la jurisprudence maintenant bien développée de la Cour européenne des droits de l'homme de Strasbourg dans le domaine de la vie privée, de la qualité d'une législation prévoyant l'interférence, la nécessité et la proportionnalité de cette interférence, et du besoin de garanties satisfaisantes contre les éventuels abus.

L'article 8 de la Charte contient un droit à la *protection* des données personnelles qui confirme et consolide les développements juridiques intervenus en Europe au cours des deux dernières décennies. Le concept de la protection des données a été introduit en 1981 dans une Convention du Conseil de l'Europe (Convention 108) et avait pour objectif de fournir des garanties structurelles au sein d'une société de l'information susceptible de dépendre toujours davantage de l'utilisation des technologies de l'information. Cette Convention a été ratifiée par 44 pays, notamment tous les États membres de l'UE. Elle recèle encore les principes de base de la protection des données, quelque soient leur nature ou leur contexte. La Convention a également servi de base à l'actuelle directive 95/46/CE relative à la protection des données, bien que la directive ait apporté des éclaircissements à bien des égards.

Les mêmes principes de base concernant la protection des données sont désormais également présents dans l'article 8 de la Charte:

- les données personnelles doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi;

- toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification;
- le respect de ces règles est soumis au contrôle d'une autorité indépendante.

Pertinence pour l'application de la loi

Il convient de rappeler ce cadre juridique aujourd'hui, non seulement pour souligner la nature différente du droit au *respect* de la vie privée prévue à l'article 7 de la Charte et la *protection* des données personnelles prévue à l'article 8, qui s'assimile plus à un «système de contrôle et d'équilibre», consistant en des droits et des obligations, des procédures et un contrôle institutionnel. Il est également extrêmement pertinent en raison de ses conséquences pour l'application du droit pénal.

Tout d'abord, cela signifie que toute compétence juridique particulière en matière d'application du droit pénal ou toute disposition pratique visant à cette application interférant avec le droit au respect de la vie privée, devra respecter les dispositions de la jurisprudence de la Cour européenne des droits de l'homme, conformément à l'article 8 de la Convention européenne des droits de l'homme. Ces dispositions seront maintenant (très probablement) appliquées par la Cour de justice européenne à Luxembourg conformément à l'article 7 de la Charte.

Ensuite, cela signifie que les principes généraux de protection des données énoncés dans l'article 8 de la Charte s'appliquent également à la protection des données dans le domaine de l'application du droit pénal, à moins qu'il soit évident que des intérêts spécifiques en jeu dans ce domaine nécessitent de faire exception à ces principes. Cela devra évidemment faire l'objet d'une justification convaincante.

En outre, toute disposition législative relative à la protection des données dans ce domaine qui interfère avec le respect de la vie privée devra respecter les mêmes dispositions que toute autre interférence avec ce droit. En d'autres termes, elle doit être claire, précise et prévisible, nécessaire et proportionnée aux intérêts légitimes qui sont en jeu.

Étudions maintenant les sujets spécifiques abordés aujourd'hui. Dans ce contexte, permettez-moi de commencer par quelques remarques sur la directive relative à la conservation de données, puis sur l'examen du cadre juridique de l'UE pour la protection des données.

Directive sur la conservation de données

La directive sur la conservation de données, adoptée en mars 2006, a suscité la controverse dès le début. Elle impose à tous les fournisseurs de services électroniques de communication de stocker les données relatives au trafic et à la localisation des communications de *tous les citoyens* pendant une période comprise entre six mois et deux ans, pour une éventuelle utilisation à des fins répressives. Il s'agit d'un bon exemple de mesure qui *interfère* avec le droit à la vie privée et qui nécessite une justification convaincante.

Toutefois, l'avis du CEPD publié en septembre 2005 sur la proposition de la Commission a été un des premiers avis à émettre une conclusion *négative*. Il a conclu que la nécessité et la proportionnalité de la mesure proposée étaient sujettes à caution et qu'il existait un manque évident de garanties adéquates. Toutefois, suite aux attaques terroristes de Madrid et de Londres, la proposition a été adoptée, sans modification majeure, après une procédure législative relativement brève.

Pour moi, le fait que la mise en œuvre de la directive au niveau national engendre des problèmes n'a pas été une surprise. Dans certains États membres, l'adoption d'une législation nationale de transposition s'est heurtée à des réticences. Dans d'autres, une décision a été prise en faveur d'une durée de conservation la plus brève possible. La législation nationale a cependant tout de même été remise en question par les cours constitutionnelles de plusieurs États membres. À ce stade, des cours nationales ont envoyé au moins trois demandes de décision préjudicielle à la Cour de justice européenne concernant la compatibilité de la directive avec la Charte des droits fondamentaux.

J'ai déclaré publiquement que l'évaluation de la directive doit être considérée comme *le moment de vérité*. Après plusieurs années d'examen de la mise en pratique de la conservation des données, il doit être possible de fournir des preuves convaincantes pour illustrer l'importance et l'efficacité de la mesure pour l'application de la loi. On a toutefois constaté avec étonnement qu'il était *très difficile* pour la Commission de collecter *des preuves fiables* auprès des États membres.

Rapport d'évaluation

Après une analyse approfondie du rapport d'évaluation présenté par la Commission en avril 2011, nous avons conclu que la directive ne respecte *pas* les dispositions des droits

fondamentaux en ce qui concerne le respect de la vie privée et la protection des données, notamment pour les raisons suivantes:

- la nécessité de la conservation des données telle que prévue dans la directive n'est pas encore suffisamment démontrée;
- la conservation des données aurait pu être réglementée de façon moins intrusive pour la vie privée;
- la directive actuelle laisse trop de latitude aux États membres pour décider des fins auxquelles les données peuvent être utilisées et de qui peut avoir accès aux données et dans quelles conditions.

Le rapport d'évaluation devait jouer un rôle dans les éventuelles décisions sur l'avenir de la directive. Selon nous, la Commission doit étudier sérieusement toutes les options, y compris la possibilité d'une abrogation de la directive, combinée ou non avec une proposition de mesure alternative, plus ciblée, au niveau européen.

Si, sur la base des nouvelles informations, la nécessité d'un instrument européen sur la conservation des données était démontrée, nous pensons que trois dispositions fondamentales devraient être respectées:

- il doit établir des règles globales et doit véritablement harmoniser les obligations de conservation des données, ainsi que d'accès et d'utilisation ultérieure de ces données par les autorités compétentes;
- il doit être *exhaustif*, ce qui signifie qu'il doit fixer un objectif clair et précis qui ne peut pas être contourné;
- il doit être *proportionné* et ne pas aller au-delà de ce qui est nécessaire.

Toutefois, la Commission semble avoir reporté une éventuelle décision à une date indéterminée. Cela signifie que la Cour de justice peut très bien être la première à décider de l'avenir de la directive et des conditions pouvant s'appliquer à une éventuelle révision.

Examen de la protection des données

Dans le cadre de l'examen actuel du cadre juridique de l'UE sur la protection des données, nous avons accueilli favorablement les propositions de la Commission présentées en janvier 2012. Cela s'applique plus spécifiquement au règlement sur la protection des données qui constitue un progrès énorme en offrant une protection des données plus efficace et plus cohérente dans un monde de plus en plus régi par l'utilisation des technologies de

l'information dans tous les domaines de la vie. De plus en plus de citoyens sont aujourd'hui connectés pratiquement en permanence et ils ont besoin d'une protection plus efficace et plus cohérente.

Toutefois, nous avons déjà mentionné que les propositions sont moins exhaustives qu'elles devraient l'être. Premièrement, elles ne s'appliquent pas aux institutions et aux organes de l'UE, bien qu'il soit probable que cela soit le cas ultérieurement. Deuxièmement, elles n'affectent aucune législation spécifique, telle que la directive sur la vie privée et les communications électroniques, qui a un lien avec la directive sur la conservation de données, bien que cela puisse également être le cas plus tard.

Troisièmement, et c'est plus important encore, il existe un manque flagrant d'équilibre entre le règlement proposé sur la protection des données et la directive proposée pour l'application du droit pénal. Tout d'abord, il existe une différence évidente en matière d'instruments, ce qui laisse davantage de latitude aux États membres dans un domaine où la protection de la vie privée et des données personnelles est essentielle et où la nécessité d'une coopération entre les États membres va croissant.

Toutefois, le problème le plus important est que le niveau de protection dans la directive proposée est beaucoup moins satisfaisant que dans le règlement proposé. Cela peut être illustré de nombreuses manières, notamment en indiquant que les autorités répressives (contrairement aux autres autorités et aux entreprises privées) n'auraient pas l'obligation générale de démontrer le respect des dispositions relatives à la protection des données. En outre, les pouvoirs des autorités de contrôle doivent être beaucoup plus limités. Il s'agit d'un signal négatif et d'une occasion ratée de favoriser la confiance envers les autorités répressives.

L'avis du CEPD sur les propositions de réforme a donc suggéré une série d'améliorations pour garantir davantage d'équilibre et de cohérence entre les deux propositions. Ceci est important, non seulement pour les citoyens mais également pour tous les services publics concernés par la limite entre le règlement et la directive. Un des problèmes réside dans le fait que l'échange de données entre les deux secteurs s'accroît et qu'un manque d'équilibre et de cohérence peut avoir des effets négatifs pour toutes les parties prenantes.

Le groupe de travail sur l'article 29 a récemment soulevé un autre problème important: la mesure dans laquelle les autorités répressives seront autorisées à stocker et à conserver des

données personnelles sur des personnes complètement *extérieures* à une enquête ou à des poursuites pénales particulières (en d'autres termes qui ne sont pas suspectes, témoins ou victimes). Les termes actuels de la directive proposée en l'état ne comportent aucune exclusive en ce qui concerne les catégories de personnes pour lesquelles des données personnelles peuvent être collectées et traitées.

Il s'agit d'un bon exemple d'une disposition relative à la protection des données qui interfère avec le respect de la vie privée et qui doit donc respecter les dispositions pertinentes, en d'autres termes, être claire et précise, nécessaire et proportionnée. Le groupe de travail article 29 a élaboré des formulations plus précises pour ce sujet très sensible.

Nous avons été très heureux de constater que le Parlement européen étudie des amendements qui apporteront des améliorations considérables à la directive proposée et nous étudierons les négociations entre le Conseil et le Parlement avec grand intérêt.

Remarques finales

Permettez-moi d'aborder un autre point, dans la mesure où cette conférence est organisée par une association professionnelle d'avocats qui a le devoir professionnel de contribuer au développement de la loi, notamment la législation sur la protection des données, et un intérêt évident à cet égard.

Par principe, je suis d'accord avec le prochain orateur: les avocats peuvent jouer un rôle utile en tant que délégués de la protection des données, extérieurs aux organisations concernées. Ce domaine peut être développé dans un avenir proche, notamment dans le cadre du nouveau règlement. Toutefois, il existe également d'autres options. Dans ce contexte, je voudrais plaider en faveur d'un rôle plus actif de la part des avocats dans l'exploration des droits des personnes concernées et des effets juridiques de la protection des données dans la pratique.

Dans la mesure où la protection des données est une problématique transversale, ces activités peuvent impliquer différents domaines de la pratique juridique, de l'emploi à la concurrence, la procédure pénale étant certainement incluse. Si la protection des données est rendue plus efficace dans la pratique, elle aura également un impact sur les litiges et les avocats représenteront différentes parties au débat.

Je vous remercie pour votre attention et je ne doute pas que le débat sera intéressant.