Réforme de la protection des données de l'UE: vers une protection des données plus efficace et plus cohérente dans l'ensemble de l'UE[1]

Peter Hustinx
Contrôleur européen de la protection des données

Aujourd'hui, je souhaiterais vous informer sur les grandes lignes de l'actuelle révision du cadre juridique de l'UE relatif à la protection des données. Après une brève introduction, j'aborderai les principaux motifs de la révision, les éléments clés des propositions de la Commission soumises en janvier 2012, et les prochaines étapes probables du processus de réforme.

L'aspect le plus important de mon exposé concerne l'instauration d'une protection des données «plus efficace et plus cohérente» dans l'ensemble de l'UE. La protection des données n'est utile *que* si elle est appliquée *dans la pratique*, et sa valeur concrète dépend de la *protection* qu'elle est capable d'assurer. À cet égard, il nous reste encore des efforts à accomplir dans un environnement de plus en plus conditionné par les technologies et de mondialisation croissante. La nécessité d'une protection efficace et cohérente sera donc un thème récurrent dans les différentes étapes de mon allocution.

Rôle du CEPD

Permettez-moi tout d'abord de décrire, en quelques mots, le rôle du Contrôleur européen de la protection des données (CEPD). Il s'agit d'une autorité indépendante, clairement distincte de la Commission européenne, chargée d'un certain nombre de tâches spécifiques par rapport à la Commission et aux autres institutions de l'UE. Le CEPD est un organe à part entière de l'UE. Sa première mission est de contrôler la Commission et les autres institutions de l'UE et de s'assurer qu'elles respectent la législation de l'UE en matière de protection des données lorsqu'elles traitent des données à caractère personnel. Le CEPD est investi à cet effet de pouvoirs étendus en matière de contrôle et d'application.

---

[1] Version révisée de la conférence tenue à l'occasion de la 5e Journée suisse du droit de la protection des données qui s'est déroulée le 15 juin 2012 à l'Université de Fribourg (Suisse). Publiée dans: Astrid Epiney /Tobias Fasnacht (Hrsg./ed.), «*Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes und Implikationen für die Schweiz*» / «Le développement du droit européen en matière de protection des données et ses implications pour la Suisse», Zürich 2012, p. 15-21.

Sa deuxième mission consiste à conseiller la Commission, le Conseil et le Parlement sur toute nouvelle législation ayant un impact en matière de protection des données. Dans certains cas, il peut aussi demander à la Cour de justice qu'il soit autorisée à intervenir et à exprimer son point de vue sur un dossier donné, présentant des aspects intéressants en matière de protection des données. Vous trouverez différents exemples de ce type sur notre site internet. En l'occurrence, le CEPD ne peut compter que sur la pertinence de ses arguments.

Sa troisième mission consiste à coopérer avec d'autres autorités chargées de la protection des données, principalement au niveau national, en vue d'améliorer la cohérence de la protection des données dans l'UE. Dans ce domaine, le CEPD doit faire preuve d'autorité et de diplomatie pour exercer sa mission, étant donné que toutes les autorités nationales chargées de la protection des données sont indépendantes et que le CEPD n'est compétent qu'au niveau de l'UE. Ces différentes fonctions du CEPD sont fondées sur le règlement (CE) n° 45/2001 qui, en substance, met en œuvre la directive 95/46/CE sur la protection des données au niveau de l'UE.

La révision du cadre juridique de l'UE relatif à la protection des données est un sujet qui relève de toute évidence des missions de conseil et de coopération du CEPD. Nous avons donc été consultés au sujet des propositions de la Commission, et nous avons travaillé avec nos collègues nationaux en vue de fournir une contribution et des commentaires à la Commission, à différentes étapes du processus. Vous trouverez plus de renseignements relatifs à ces activités sur notre site web.

Protection des données dans l'UE

À présent, permettez-moi de vous rappeler que la «protection des données à caractère personnel» est un concept distinct mais également étroitement lié au droit au «respect de la vie privée» visé à l'article 8 de la Convention européenne des droits de l'Homme (CEDH). Les principes de base de la protection des données ont été énoncés dans la Convention du Conseil de l'Europe sur la protection des données, également connue comme la Convention 108, ratifiée par plus de 40 États européens, y compris la Suisse. Cette convention permet de protéger les données à caractère personnel de

manière plus systématique et dynamique, car elle est applicable en principe à toutes les données à caractère personnel, indépendamment du droit à la vie privée.

Les principes de la Convention 108 ont été mis en œuvre dans les législations nationales. Le risque de voir apparaître des divergences entre les législations nationales a incité l'UE à s'impliquer, ce qui s'est soldé par l'adoption de la directive 95/46/CE et d'un certain nombre d'instruments plus spécifiques tels que la directive 2002/58/CE, connue également comme la directive «vie privée et communications électroniques». Une étape plus récente, en 2008, a été l'adoption de règles générales dans le domaine de la coopération policière et judiciaire en matière pénale. En d'autres termes, le cadre juridique de l'UE relatif à la protection des données englobe d'autres instruments que la directive 95/46.

Charte et traité de Lisbonne

Il conviendrait de mentionner deux autres éléments: premièrement, l'adoption de la Charte des droits fondamentaux de l'Union européenne en 2000, limitée dans un premier temps à un document politique. Bien qu'elle soit fondée sur la Convention européenne des droits de l'Homme, elle contient également des innovations, notamment la reconnaissance d'un droit à la protection des données à caractère personnel (article 8), ainsi qu'un droit au respect de la vie privée et familiale (article 7).

Deuxièmement, l'entrée en vigueur d'un ensemble de nouveaux traités de l'UE (traité de Lisbonne), à la fin 2009, qui ont transformé la Charte en un document juridiquement contraignant et introduit une base juridique horizontale pour la législation sur la protection des données, ne dépendant plus des besoins du marché intérieur, mais reflétant pleinement la nature de la protection des données en tant que droit fondamental, avec des caractéristiques spécifiques dans une société moderne de l'information (article 16 TFUE). Cela a marqué la confirmation d'une évolution juridique de près de quatre décennies.

Motifs de la révision à l'échelle de l'UE

Revenons à présent à l'actuelle révision du cadre juridique de l'UE relatif à la protection des données. Pourquoi cette révision? Pour trois grandes raisons. La

première est la nécessité de mettre à jour le cadre actuel, et en particulier la directive 95/46/CE, qui en constitue toujours la pierre angulaire. En l'occurrence, «mettre à jour» revient à faire en sorte que cette directive demeure efficace dans la pratique.

Lorsque la directive a été adoptée, l'internet en était encore à ses balbutiements. Aujourd'hui, dans un monde de plus en plus numérisé, nous avons également besoin de garanties plus solides permettant une protection plus efficace. Les défis que constituent les nouvelles technologies et la mondialisation nous incitent immanquablement à faire preuve d'imagination pour proposer des innovations en vue d'une protection plus efficace.

La deuxième raison, c'est que le cadre actuel a renforcé la diversité et la complexité, ne fût-ce que parce qu'une directive doit, par nature, être transposée en droit national. Nous en sommes donc arrivés à 27 versions différentes de principes fondamentaux identiques. C'est tout simplement excessif, et induit des coûts, sans oublier la perte d'efficacité que cela engendre.

En d'autres termes, nous devons accélérer l'harmonisation en renforçant le système et en le rendant plus efficace dans la pratique, mais aussi plus cohérent. Ainsi, nous pourrons réduire cette diversité et cette complexité *qui ne mènent à rien*.

La troisième raison concerne le nouveau cadre juridique de l'UE. Le traité de Lisbonne a placé instamment l'accent sur les droits fondamentaux. L'article 8 de la Charte des droits fondamentaux consacre une disposition spéciale à la protection des données à caractère personnel, tandis que l'article 16 TFUE propose une nouvelle base juridique horizontale garantissant une protection complète dans tous les domaines d'action de l'UE, que ce soit le marché intérieur, l'application des lois ou pratiquement tous les autres composants du secteur public.

La révision du cadre vise donc à mettre en place une protection des données à caractère personnel renforcée, plus efficace, plus cohérente et plus exhaustive.

Deux propositions essentielles au moins sont à l'étude: une directive relative à l'application de la loi et un règlement directement contraignant remplaçant la

directive 95/46/CE et portant sur les domaines commerciaux et le secteur public autre que les autorités chargées de l'application de la loi.

L'architecture même de ce train de propositions met en évidence leur manque d'exhaustivité. Et à y regarder de plus près, c'est effectivement là que le bât blesse: le niveau de protection est sensiblement plus faible dans la proposition de directive que dans la proposition de règlement.

Il est possible d'analyser la situation au cas par cas, mais l'échange de données entre des entités publiques et privées, par exemple les autorités chargées de l'application de la loi et les banques, la téléphonie, les voyages, etc. est en pleine expansion, et un déséquilibre aura des conséquences concrètes à une échelle plus large.

Continuité et changement

En ce qui concerne le règlement, il importe que vous gardiez à l'esprit quelques messages essentiels.

Tout d'abord, en dépit de son caractère novateur, le règlement se caractérise par une forte continuité. Tous les concepts et principes fondamentaux actuels sont maintenus, malgré certaines clarifications et innovations. Par exemple, le texte insiste à présent davantage sur la minimisation des données, c'est-à-dire sur la nécessité de ne pas traiter plus de données que nécessaire. De même, le respect de la vie privée dès la conception («privacy by design») est désormais reconnu comme un principe général.

L'innovation majeure consiste en «une protection des données plus efficace dans la pratique». Comme nous le verrons, il s'agit d'insister fortement sur la mise en œuvre des principes et sur l'exécution des droits et des obligations, pour veiller à ce que la protection soit assurée dans la pratique.

En même temps, le règlement prévoit la simplification et la réduction des coûts. Un exemple typique est la suppression de la notification préalable des traitements. Elle reste nécessaire dans les seules situations qui présentent un risque spécifique. Le règlement instaure également un guichet unique pour les entreprises disposant de

sièges dans différents États membres, ce qui suppose l'instauration d'une autorité centrale chargée de la protection des données.

Un règlement directement contraignant offrira évidemment aussi une harmonisation nettement plus large – en principe: une seule règle applicable dans tous les États membres – et une plus grande cohérence. En soi, il permet également aux entreprises actives dans différents États membres de simplifier leurs obligations et de réduire considérablement leurs coûts.

Portée générale

Permettez-moi d'insister sur le fait que la proposition de règlement a une portée générale: elle s'appliquera au secteur privé comme au secteur public. Ceci est tout à fait en phase avec ce qui est prévu par la directive actuelle (directive 95/46/CE). La possibilité d'opérer une distinction systématique entre secteur public et secteur privé dans cette directive avait été explicitement examinée et rejetée.

Cette approche globale de la directive actuelle a été rendue possible par le fait que certaines dispositions (en matière de missions publiques) concernent davantage les pouvoirs publics, tandis que d'autres (en matière de contrats ou d'intérêts légitimes) concernent davantage les acteurs privés.

Dans l'arrêt *Rechnungshof* (mai 2003), la CJUE a clairement expliqué que la directive actuelle s'appliquait également au secteur public d'un État membre. Elle a toutefois souligné que le droit national ne peut constituer un motif légitime justifiant le traitement que s'il respecte les droits fondamentaux.

Cette position est renforcée par l'article 8 de la Charte des droits fondamentaux, qui prévoit désormais la reconnaissance explicite du droit à la protection des données à caractère personnel, et par l'article 16 TFUE, qui prévoit une base juridique horizontale explicite pour l'adoption de règles sur la protection des données à caractère personnel, au niveau européen comme dans les États membres, lorsque ceux-ci agissent dans le champ d'application du droit de l'UE.

Parallèlement, une analyse plus pointue de la relation entre le droit de l'Union européenne et le droit national sur la base de la proposition de règlement s'impose. Croire que le règlement remplacera purement et simplement la législation nationale en la matière est une erreur. Le droit national et le droit européen coexisteront et interagiront d'au moins quatre manières différentes. Pensons notamment au fait que le règlement complétera le droit national d'une manière sensiblement identique à ce qui s'est passé dans l'affaire *Rechnungshof*. Il convient sans doute d'accorder plus de place à l'interaction entre le droit de l'UE et le droit national.

S'agissant de la substance du règlement, celui-ci renforce le rôle des partenaires principaux, à savoir, les personnes concernées, l'organisation responsable et les autorités de réglementation.

Contrôle des utilisateurs

La première perspective peut également être perçue comme un renforcement du contrôle des utilisateurs. Les droits actuels des personnes concernées ont été préservés mais surtout consolidés et étendus.

L'exigence relative au consentement a été précisée: *quand* il est exigé, le consentement doit être réel et solide. Le droit d'opposition est consolidé. Les moyens mis en œuvre pour veiller au respect de ces droits dans la pratique sont également renforcés et la transparence mise en exergue. Par ailleurs, une disposition introduit non pas un recours collectif à l'américaine, mais une action en nom collectif, à savoir que des organisations pourront intervenir au nom de leurs membres ou de leurs groupes constitutifs.

Vous avez certainement entendu parler à maintes reprises du «droit à l'oubli», qui à une analyse plus approfondie, consiste principalement à effacer les données lorsqu'il n'existe pas de raison suffisante de les conserver. De même, le droit à la portabilité des données est fondamentalement une spécification du droit actuel de demander une copie de toute donnée à caractère personnel, dans un format particulier.

Responsabilité

L'accent est principalement placé sur la responsabilité réelle des organisations chargées de la gestion des données. La responsabilité n'est pas une notion qui n'intervient qu'à la fin, en cas de problème. Il s'agit au contraire d'une obligation de développer une gestion correcte des données dans la pratique. Cette responsabilité est traduite dans des expressions telles que *prendre toutes les mesures qui s'imposent afin de veiller à la mise en œuvre* et *vérifier et démontrer que ces mesures sont toujours efficaces.*

Il s'agit là de l'une des principales évolutions. Cela implique aussi que la charge de la preuve incombe dans la plupart des cas à l'organisation responsable qui doit, en d'autres termes, prouver l'existence d'une base juridique adéquate, la réalité du consentement et l'efficacité continue des mesures.

Le règlement prévoit également un certain nombre d'exigences spécifiques telles que la nécessité d'une analyse d'impact relative à la vie privée, l'établissement de documentation et la désignation d'un délégué à la protection des données. Certaines de ces dispositions, notamment celles qui concernent la documentation, sont à mon sens trop détaillées et doivent être modifiées pour être plus appropriées. Quelques exceptions figurant dans ces mêmes dispositions ne se justifient peut-être pas tout à fait. Un meilleur équilibre de cette partie de la proposition pourrait sans doute résoudre ces deux problèmes.

Une disposition générale sur la notification des violations de la sécurité est également prévue. Le droit de l'Union européenne limite désormais cette notification aux seuls fournisseurs de télécommunications.

Surveillance et contrôle de l'application

Un troisième point majeur du règlement concerne la nécessité de renforcer la surveillance et le contrôle de l'application. Les garanties prévues pour l'indépendance complète des autorités chargées de la protection des données ont été renforcées, conformément à l'arrêt de la CJUE dans l'affaire Commission/Allemagne.

En outre, le règlement confère aux régulateurs des pouvoirs d'exécution renforcés dans tous les États membres. Les amendes administratives s'élevant à des millions d'euros, des montants faramineux, attirent beaucoup l'attention, mais le message est le suivant: aux grands maux les grands remèdes. De cette manière, la protection des données figurera en tête des priorités à l'ordre du jour des conseils d'administration des entreprises: pareille évolution mérite d'être saluée.

Par ailleurs, le règlement prévoit plusieurs mesures afin de veiller à une application plus stricte de ses dispositions: sanctions correctives, amendes administratives et responsabilités civiles renforcées.

La coopération internationale entre les autorités chargées de la protection des données est vivement encouragée et facilitée. L'instauration d'une autorité principale pour les entreprises possédant plusieurs sites est accueillie positivement, même si ladite autorité n'agira pas seule mais au sein d'un réseau, en étroite collaboration avec d'autres autorités compétentes.

Un changement très important est l'instauration d'un mécanisme de contrôle de la cohérence dans le cadre du comité européen de la protection des données, qui doit s'inspirer de l'actuel groupe de travail «Article 29». Ce mécanisme garantira la cohérence des résultats de la surveillance et du contrôle de l'application dans tous les États membres. Son secrétariat sera assuré par le CEPD.

Protection globale de la vie privée

Enfin, un dernier élément doit être relevé: la dimension internationale élargie du règlement, dans les deux directions. Le champ d'application du règlement a été précisé et étendu. À présent, les dispositions s'appliqueront non seulement à tous les traitements relatifs à un site établi dans l'Union européenne, mais aussi aux livraisons de biens et prestations de services sur le marché européen à partir d'un pays tiers ou aux modalités de contrôle en ligne du comportement des Européens.

Il s'agit d'une réalité dans le monde actuel de l'internet. En même temps, cette approche réaliste s'appuie sur une réflexion commune accrue en matière de protection des données aux quatre coins du globe.

Quant aux autres aspects internationaux, les dispositions relatives aux transferts de données vers les pays tiers ont été étendues, mais aussi rationalisées et simplifiées à certains égards. Une disposition spécifique relative aux règles d'entreprise contraignantes a été introduite et prévoit également plusieurs simplifications.

Permettez-moi également d'ajouter que les autorités chargées de la protection des données mettent en œuvre une coopération internationale à plus grande échelle – par exemple, entre la Commission fédérale du commerce (*Federal Trade Commission*) aux États-Unis et les autorités chargées de la protection des données dans l'UE – au sein d'un réseau mondial (GPEN). Grâce à ce réseau, il sera davantage possible de collaborer avec les acteurs mondiaux sur l'internet. Ce phénomène s'explique aussi par une convergence croissante des principes et des pratiques de protection des données dans le monde.

Conclusions

Pour conclure, cette proposition mérite, à mon sens, d'être accueillie favorablement, pour autant que certains éléments essentiels soient quelque peu améliorés.

Outre le déséquilibre actuel entre le règlement et la directive en matière d'application des lois, j'ai évoqué la nécessité éventuelle d'accorder plus de place à l'interaction entre le droit européen et le droit national ainsi que la nécessité de reconsidérer certaines des exceptions en l'espèce, notamment concernant les petites et moyennes entreprises. Il est *essentiel*, selon moi, que les dispositions générales soient *évolutives* par nature. Des spécifications inadéquates n'entraînent que des exceptions inutiles.

Un mot, enfin, sur la procédure: le débat est en cours au sein du Conseil et du Parlement. Quelques mois ne suffiront pas. Je ne pense pas qu'une décision sera prise avant l'année prochaine, probablement sous la présidence irlandaise.

Quoi qu'il en soit, il est probable que ce texte sera adopté d'ici 2014. Gageons que le règlement deviendra réalité, moyennant, bien sûr, certaines améliorations indispensables.