

**Conférence de printemps de la Commission autrichienne des juristes**

**"Tout est sous contrôle?", Weissenbach am Attersee, 21 mai 2009**

---

**"Les enjeux actuels de la protection des données en Europe"**

*Peter Hustinx*

*Contrôleur européen de la protection des données*

Mesdames, Messieurs,

Je tiens tout d'abord à vous remercier de m'avoir invité à participer à cette conférence annuelle de printemps, qui porte sur un sujet très intéressant, qui me tient particulièrement à cœur, à savoir le droit fondamental au respect de la vie privée et à la protection des données et la tendance croissante des pouvoirs publics à exiger l'accès aux données à caractère personnel pour des motifs d'intérêt public de plus en plus nombreux.

Le sujet de votre conférence est d'une très grande importance car la protection des données à caractère personnel est un sujet qui revêt lui aussi une importance croissante. Le respect de la vie privée et la protection des données à caractère personnel ont été reconnus comme des droits fondamentaux à part entière par les articles 7 et 8 de la Charte des droits fondamentaux de l'UE, qui deviendra contraignante avec l'entrée en vigueur du traité de Lisbonne. Ce dernier renforcera de plusieurs manières le droit à la protection des données à caractère personnel.

Cette étape très importante confirme l'évolution du droit au cours de ces dernières décennies en Europe. Le droit à la protection des données à caractère personnel est devenu, au cours de cette période, un système de règles et de principes permettant une approche plus structurée des questions auxquelles notre société de l'information doit faire face. Parallèlement, nos sociétés dépendent de plus en plus de technologies de l'information et de la communication omniprésentes, ce qui entraîne inévitablement

un traitement de volumes considérables de données à caractère personnel dans la quasi-totalité des domaines de notre vie.

En d'autres termes, bien que la protection des données à caractère personnel soit un *droit fondamental de plus en plus important*, elle constitue également un enjeu majeur en ce qui concerne la *protection effective* des données à caractère personnel *dans la pratique*. Cela peut paraître paradoxal, pourtant les droits fondamentaux ne concernent pas seulement les situations simples.

Dans ce contexte, je souhaiterais évoquer certains des enjeux actuels en matière de protection des données en Europe. Comme vous pourrez le constater, je suis persuadé que nous aurons des occasions majeures d'améliorer la protection des données, comme notamment le traité de Lisbonne, que j'ai déjà mentionné, à condition que celui-ci soit ratifié par l'ensemble des États membres d'ici à la fin de l'année.

### **Pertinence et caractère sensible**

En raison de l'importance croissante de la protection des données, diverses questions liées au respect de la vie privée ont, elles aussi, acquis une plus grande importance politique et un caractère plus sensible. Il n'est pas exagéré de dire que le respect de la vie privée est un sujet de plus en plus "brûlant". Cela saute aux yeux dans le processus actuel de révision de la directive sur la protection de la vie privée dans le secteur des communications électroniques, qui fait partie d'un ensemble plus vaste d'instruments relatifs aux télécommunications. On le constate également à l'intérêt croissant pour d'autres thématiques liées au respect de la vie privée sur Internet, en particulier le commerce en ligne, sur lesquelles plusieurs membres de la Commission sont en concurrence pour se voir confier la responsabilité de fixer le programme pour les initiatives futures.

Cette importance croissante et ce caractère de plus en plus sensible s'illustrent également dans l'intérêt croissant que suscite l'avenir de la directive 95/46/CE, c'est-à-dire le cadre principal en matière de protection des données, adopté en 1995, qui a fait cette semaine l'objet d'une première conférence organisée par la Commission européenne, afin de recueillir les points de vue et faire le bilan de la situation.

Il en va de même dans le domaine de la justice et des affaires intérieures au niveau de l'UE ainsi que dans la préparation du programme pour les cinq prochaines années, communément appelé "Programme de Stockholm", dont l'adoption devrait intervenir dans le courant de l'année, sous la présidence suédoise. La même constatation s'impose dans un contexte plus large, principalement au niveau transatlantique, où des évolutions fondamentales pourraient avoir lieu dans les années à venir.

Cette tendance est aussi manifeste dans différents États membres, notamment en Allemagne, où les citoyens et les consommateurs sont de plus en plus engagés dans les questions liées au respect de la vie privée. On le voit aussi lorsque les autorités chargées du respect de la vie privée et de la protection des données sont plus actives et plus fermes en matière de répression. Enfin on le constate par le fait que tous les niveaux de juridiction, tant nationaux qu'europeens, traitent de plus en plus souvent de questions liées au respect de la vie privée et rendent des arrêts qui pourraient amener les professionnels du droit à jouer un rôle plus actif en la matière.

### **Le respect de la vie privée sur Internet**

J'aimerais maintenant m'intéresser de plus près à certains de ces domaines, en commençant par la révision de la directive sur la protection de la vie privée dans le secteur des communications électroniques et d'autres questions relatives au respect de la vie privée sur Internet.

Cette révision s'inscrit dans le cadre d'un ensemble plus large de mesures concernant le secteur des télécommunications, domaine essentiel à la reprise économique. Malgré l'urgence, ces mesures sont actuellement bloquées entre le Conseil et le Parlement européen à cause d'un point. Il s'agit en fait d'un conflit entre la protection de la vie privée sur Internet et la protection des droits de propriété intellectuelle contre le téléchargement illégal. Certains pays ont adopté des mesures autorisant un contrôle par les fournisseurs de services de l'utilisation d'Internet et le blocage de l'accès Internet des utilisateurs soupçonnés d'infractions répétées. La question est de savoir si de telles mesures devraient être autorisées à l'avenir.

Si la directive révisée est finalement adoptée, de nouveaux éléments intéressants verront le jour en matière de protection des données. L'un d'eux est l'obligation de signaler les violations de la sécurité. Ces violations sont un problème de plus en plus

grave, que l'on constate davantage dans certains États membres, comme le Royaume-Uni, où plus de 300 cas sont rapportés en un an. Mais d'autres États membres sont également concernés, comme l'Allemagne, où plusieurs scandales ont récemment éclaté. Il me semble qu'il s'agit là d'un problème structurel, qui risque de saper la confiance de l'opinion dans notre société de plus en plus "électronico-dépendante" si nous n'agissons pas efficacement. J'estime qu'une meilleure gestion des données et une plus grande responsabilisation sont nécessaires. Les plus hauts niveaux de direction des organisations doivent s'y impliquer et assumer leurs responsabilités quant au respect de la vie privée et à la mise en œuvre de mécanismes de sécurité plus efficaces.

Il existe en principe deux options. La première consiste à interpréter l'article 17 de la directive actuelle sur la protection des données, qui prévoit des "mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre un traitement illicite", comme exigeant également que des mesures adéquates soient prises pour la gestion interne des données. L'autre possibilité consiste à introduire une obligation de notification en cas de violation de la sécurité, ce qui pourrait, au bout du compte, avoir le même effet. L'un des principaux avantages de cette deuxième solution est qu'elle constituerait une forte incitation à l'adoption de mesures visant à renforcer la sécurité dans les organisations. Le principal défi à relever à ce jour est de développer un modèle de notification en cas de violation de la sécurité qui soit le plus efficace possible dans la pratique, c'est-à-dire de définir correctement la notion de "violation de la sécurité" et les normes de notification à l'intention des utilisateurs et des autorités. Dans un premier temps, cette obligation concernera uniquement la directive sur la protection de la vie privée dans le secteur des communications électroniques, mais il n'y a pas de raison de ne pas aller plus loin et d'en faire une règle générale de la législation en matière de protection des données. Je pense d'ailleurs que c'est exactement ce vers quoi nous devons aller.

Parmi les autres questions importantes en ce qui concerne Internet figurent la conservation des données par les moteurs de recherche, l'utilisation croissante des réseaux sociaux et la collecte d'informations à des fins de démarchage publicitaire en ligne. Ces questions sont très clairement liées entre elles et sont donc hautement stratégiques. En effet, la publicité en ligne est aujourd'hui le principal modèle d'affaires sur Internet et présente un grand intérêt pour les fournisseurs de moteurs de recherche et de réseaux sociaux. Plus il y a de données sur les utilisateurs, plus la

publicité est ciblée et plus le modèle devient rentable. C'est pourquoi le Groupe Article 29 s'est récemment intéressé tout particulièrement aux moteurs de recherche et aux réseaux sociaux et devrait proposer des lignes directrices pour la publicité en ligne.

Ce mois-ci, la Commission européenne a publié une recommandation sur l'utilisation de l'identification par radiofréquence (RFID) en tant que pierre angulaire de "l'Internet des objets". Dans un proche avenir, de plus en plus d'objets de notre quotidien seront interconnectés et pourront échanger des données concernant leurs utilisateurs. Compte tenu de ces évolutions, il est essentiel que nous abordions la technologie de telle manière que les questions relatives au respect de la vie privée soient intégrées dès le début du processus de développement ("Privacy by Design"). Il s'agit d'une démarche prometteuse, qui est également inscrite à l'ordre du jour de votre conférence.

### **L'avenir de la directive 95/46/CE**

Tout ceci m'amène à aborder l'avenir du principal cadre européen en matière de protection des données, qui est fixé dans la directive 95/46/CE. Jusqu'à récemment, l'accent était clairement placé sur une meilleure mise en œuvre du cadre juridique existant, ce qui impliquait plusieurs lignes d'action, y compris la clarification de plusieurs notions et principes. Le Groupe Article 29 a publié un avis sur la notion de "données à caractère personnel" et s'intéresse à présent aux notions de "responsable du traitement" et de "sous-traitant". La première notion est un élément fondamental pour délimiter la portée des garanties en matière de protection des données. Les deux autres points jouent un rôle essentiel dans la répartition des responsabilités pour ce qui du respect des règles et principes régissant la protection des données et ont aussi des répercussions importantes au niveau des législations nationales applicables, ce qui explique pourquoi il a été décidé de les analyser.

La possibilité d'instaurer des procédures d'infraction contre certains États membres représente une autre ligne d'action. Il s'agit désormais d'une réalité dans l'affaire engagée devant la Cour européenne de justice contre l'Allemagne en ce qui concerne le principe de "contrôle indépendant". L'article 28 de la directive prévoit que les autorités de contrôle exercent "en toute indépendance leurs fonctions". Ce principe est également inscrit dans la Charte des droits fondamentaux et dans le traité de Lisbonne. L'arrêt que rendra la Cour dans l'affaire contre l'Allemagne pourrait donc

avoir des conséquences très importantes sur les dispositions institutionnelles, tant en Allemagne que dans d'autres États membres.

Je suis tout à fait favorable à ce que l'accent soit mis sur une meilleure mise en œuvre du cadre juridique existant. Parallèlement, j'ai déjà dit, il y a de cela plusieurs années, qu'il est inévitable de réviser la directive 95/46/CE. L'argument principal en faveur d'une telle révision est qu'elle est nécessaire afin de garantir que la directive reste efficace dans un monde qui change. Cette démarche exige d'être soigneusement préparée et planifiée. À cet égard, il est intéressant de constater que la Commission va dans le même sens. Cette semaine, elle a organisé à Bruxelles une première conférence visant à recueillir les points de vue et à faire le bilan de la situation. Prochainement, la Commission lancera également une vaste consultation publique sur l'avenir du cadre juridique existant.

Si l'on envisage les différentes options à ce stade, il est justifié de penser qu'une révision nécessitera plusieurs années. En effet, je considère qu'il faudra à la nouvelle Commission au moins deux ans pour compiler les résultats de la consultation publique et en tirer ses propres conclusions. En d'autres termes, je ne serais pas surpris que la Commission ne soumette pas de proposition avant 2012. L'examen de la révision de la directive au Parlement européen et au Conseil pourrait aisément prendre deux ou trois ans et durer ainsi jusqu'en 2015.

Un tel calendrier a deux conséquences importantes. Tout d'abord, il convient de continuer, dans l'intervalle, à mettre l'accent sur une mise en œuvre plus efficace des dispositions existantes. Il serait en effet des plus regrettables que nous réduisions nos efforts visant à garantir le respect des règles en vigueur en matière de protection des données à un moment où l'importance de ces règles est indéniable. Ensuite, le débat concernant une révision devrait porter principalement sur les besoins réels en matière de protection en 2015 et au-delà. Pour cela, des solutions créatives seront nécessaires pour continuer de garantir une protection des données efficace dans un environnement qui évolue. L'une des manières de relever ce défi consiste à se concentrer davantage sur les résultats que sur le détail des procédures et à veiller à ce que les responsables du traitement soient responsables du respect des règles et à ce qu'ils soient davantage tenus de rendre des comptes. Dans ce contexte, les autorités chargées de la protection des données devraient disposer des compétences nécessaires et de ressources suffisantes pour assurer leur mission de manière indépendante et efficace et devraient être en mesure de fixer leurs propres priorités.

Toutefois, il est fort possible qu'une partie de la réponse réside dans l'adoption de mesures supplémentaires de portée plus limitée, qui pourraient être liées aux dispositions générales de la directive sur la protection des données. Ce modèle existe déjà dans la directive sur la protection de la vie privée dans le secteur des communications électroniques. Il pourrait également se révéler utile pour l'introduction d'une obligation de notification en cas de violation de la sécurité d'une manière plus horizontale. De même, il est possible que des mesures spécifiques soient nécessaires en ce qui concerne le RFID ou, pour mentionner encore un autre domaine, il est possible que soient adoptées des mesures concernant les services relatifs au respect de la vie privée, tels que l'audit en matière de respect de la vie privée, la certification en matière de respect de la vie privée et d'autres activités similaires.

En d'autres termes, si nous réfléchissons à l'architecture de la législation en matière de protection des données, il ne faut pas croire qu'une seule approche sera suffisante pour répondre à tous les besoins et à tous les cas de figure. Permettez-moi également de souligner que la concurrence, tant entre les responsables du traitement compétents qu'entre les fournisseurs de services de différentes catégories, pourra également être à l'avenir un élément intéressant du paysage de la gouvernance en matière de protection des données.

### **Respect de la vie privée et répression**

D'autres questions importantes se posent en ce qui concerne la répression. L'octroi de pouvoirs spéciaux dans ce domaine doit toujours être scrupuleusement évalué afin de garantir un juste équilibre entre les besoins en matière de répression et ceux liés au respect de la vie privée et de la protection des données. Le cadre légal de cette évaluation a été établi par l'article 8 de la Convention européenne des droits de l'homme. Toute interférence avec le droit relatif au respect de la vie privée devrait avoir une base juridique claire et précise. Toute mesure de ce type devrait être *nécessaire* dans une société démocratique pour répondre à un besoin social impérieux et s'accompagner de garanties appropriées contre tout abus éventuel.

Le principe de *proportionnalité* a été récemment illustré dans l'arrêt rendu par la Cour européenne des droits de l'homme dans l'affaire *Marper*. Bien que, à proprement

parler, cette affaire ne concernait que la conservation des données ADN des suspects d'un crime, le message de la Cour peut aisément être compris dans un sens plus large. En fait, ce serait une bonne chose que nous l'appliquions non seulement aux nouvelles mesures, mais également pour vérifier si les mesures adoptées par le passé satisfont encore aux conditions de légalité visées à l'article 8. C'est également vrai pour la directive 2006/24/CE sur la conservation des données de communication, qui fera prochainement l'objet d'une évaluation.

De nouvelles questions se posent dans le contexte des systèmes d'information utilisés pour l'échange de données des services répressifs entre États membres. Certains de ces systèmes existent déjà, comme le Système d'information Schengen (SIS I), qui est en cours d'adaptation afin d'être étendu à d'autres pays participants et doté de fonctionnalités supplémentaires (SIS II). D'autres systèmes sont soit en cours de développement soit prévus dans les prochaines années. J'estime qu'il serait opportun que le programme de Stockholm établisse un cadre clair pour le développement de tels systèmes. Ce cadre devrait reposer notamment sur la prise en compte du respect de la vie privée dès la conception ("Privacy by Design"). Clairement, une vision à long terme est également nécessaire car les initiatives dans ce domaine ont trop souvent été motivées par des considérations ad hoc.

En ce qui concerne plus spécifiquement la protection des données, il y a lieu de noter que la décision-cadre 2008/977/JAI du Conseil fixe des règles communes pour la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Toutefois, le champ d'application de ces règles n'est pas satisfaisant car elles ne s'appliquent qu'aux transferts de données transnationaux et non aux données exclusivement nationales, bien que la distinction entre ces catégories soit de plus en plus difficile à faire. Un autre problème est le manque de cohérence entre ces nouvelles règles et la directive 95/46/CE. L'échange de données entre le secteur privé et les services répressifs entraînera donc également davantage de difficultés, ce qui signifie que le champ d'application et le contenu de ces nouvelles règles devraient être améliorés dans un avenir proche.

## **Respect de la vie privée et mondialisation**

La nécessité de garanties au niveau mondial est elle aussi de plus en plus forte car les activités ont de plus en plus une dimension mondiale ou sont interconnectées.

Le champ d'application de la législation européenne en matière de protection des données ne se limite pas aux États membres de l'Union européenne, car il s'applique à *tout* traitement de données à caractère personnel effectué dans le *cadre des activités* d'un *établissement* du responsable du traitement situé dans un État membre de l'Union européenne. Cela signifie que l'externalisation d'activités vers un pays tiers est soumise à la législation européenne en matière de protection des données. Le transfert de données vers des pays tiers est lui aussi subordonné au respect de certaines garanties, indépendamment du fait que la responsabilité incombe ou non au responsable du traitement dans l'UE. Ce système de garanties est fondé sur une distinction entre les pays tiers qui disposent d'un niveau de protection approprié et ceux qui n'en disposent pas.

De plus en plus de pays à travers le monde, tant en Amérique du Nord qu'en Amérique latine ou dans la région Asie-Pacifique, se dotent d'une législation en matière de protection des données. Ce sont au total quelque cinquante à soixante pays du monde entier qui sont concernés, parmi lesquels figurent depuis récemment certains pays d'Afrique. On constate également une convergence croissante entre les garanties en matière de respect de la vie privée dans différentes régions du monde.

Différentes initiatives ont été lancées en vue de définir des normes mondiales en matière de respect de la vie privée, et ce afin de simplifier les échanges de données au niveau international. L'une de ces initiatives, parrainée par la Conférence internationale des commissaires à la protection des données et à la vie privée, débouchera sans doute sur la présentation d'une proposition commune de normes internationales lors de la 31<sup>ème</sup> conférence, qui se tiendra à Madrid en novembre 2009. Cette proposition montrera la faisabilité de normes internationales qui pourraient servir de base à une éventuelle convention internationale.

Dans l'intervalle, les normes peuvent également servir de cadre pour des solutions contractuelles et d'autorégulation dans différents secteurs. Le Groupe Article 29 a beaucoup travaillé au développement de "règles d'entreprise contraignantes", qui constituent pour les entreprises multinationales un élément prometteur afin de garantir que leurs activités de traitement de données à travers le monde sont conformes aux normes pertinentes. Il conviendrait bien entendu d'en tenir compte lors d'une éventuelle révision de la directive 95/46/CE.

Des mesures plus ciblées sont également attendues au niveau transatlantique dans les années à venir. Le Groupe de contact à haut niveau, qui réunit des fonctionnaires de l'UE et des États-Unis, a remis l'an dernier un rapport qui fait état d'importants chevauchements entre les garanties européennes et les garanties américaines en matière de respect de la vie privée et de la protection des données. Si les problèmes qui subsistent sont résolus, il devrait être possible de parvenir à un accord international contraignant pour l'échange d'informations provenant des services répressifs. L'un des principaux problèmes est que la législation américaine ne prévoit pas la révision judiciaire des décisions affectant des citoyens non ressortissants des États-Unis et que la loi sur le respect de la vie privée (privacy act) a un champ d'application limité. Toutefois, je ne serais pas surpris que ces obstacles puissent être levés et que des progrès importants puissent être réalisés dans les prochaines années.

### **Traité de Lisbonne**

Cela m'amène au traité de Lisbonne, que j'ai déjà évoqué au début de mon intervention. La ratification de ce traité par tous les États membres et son entrée en vigueur au début de l'année prochaine auraient des conséquences majeures sur la protection des données à au moins deux niveaux.

Au niveau institutionnel, l'entrée en vigueur du traité de Lisbonne mettra fin à la structure en piliers. L'une des conséquences importantes de cette abolition est que la procédure communautaire de prise de décision, dans laquelle interviennent à la fois le Conseil et le Parlement européen, s'appliquera également à des domaines relevant actuellement du troisième pilier, ce qui signifie que le Parlement européen n'aura plus seulement un rôle consultatif, mais qu'il sera pleinement responsable dans le cadre

d'une procédure de codécision. Il s'agit d'une garantie importante qui devrait permettre une prise de décision plus équilibrée et, espérons-le également, des résultats plus équilibrés.

En outre, le traité de Lisbonne aura des conséquences importantes sur la structure de législation de l'UE en matière de protection des données. Cette législation s'est jusqu'à présent développée dans la perspective du marché intérieur et n'est toujours pas très visible dans les différents traités. L'article 286 du traité CE dispose que les actes communautaires relatifs à la protection des données, tels que la directive 95/46/CE, s'appliquent également aux institutions et organes communautaires et constitue ainsi la base pour un contrôle indépendant par le CEPD. L'article 30, paragraphe 1, point b), du traité UE stipule que des garanties appropriées doivent être mises en place pour la protection des données lors de l'échange d'informations dans le cadre de la coopération policière et judiciaire en matière pénale.

Parallèlement, la protection des données est devenue une question horizontale. C'est ce que montre clairement l'arrêt rendu en mai 2003 par la Cour européenne de justice dans l'affaire *Rechnungshof*, également connue sous le nom "*Österreichischer Rundfunk*", qui est le premier arrêt rendu à propos de la directive 95/46/CE. Cette affaire concerne toutefois exclusivement le service public autrichien. Néanmoins, la Cour a profité de cette affaire pour souligner l'étendue importante du champ d'application de la directive. Cette orientation a été confirmée dans l'article 8 de la Charte des droits fondamentaux, qui deviendra contraignante à l'entrée en vigueur du traité de Lisbonne.

Le traité de Lisbonne introduira également, à l'article 16 du traité sur le fonctionnement de l'Union européenne (TFUE), une base juridique horizontale pour la protection des données, qui deviendra un principe général du droit européen. Cet article crée un droit subjectif à la protection des données. Il aura un "effet direct", ce qui signifie que chacun pourra s'en prévaloir devant une juridiction. L'article 16 comporte également une obligation formelle de fixer des règles en matière de protection des données à caractère personnel. Cette obligation s'appliquera non seulement aux institutions et organes de l'Union européenne, mais également aux

États membres lorsqu'ils agissent dans le champ d'application de la législation européenne.

Cette disposition n'aura pas d'effet immédiat en ce qui concerne la directive 95/46/CE, qui continuera de s'appliquer jusqu'à ce qu'elle soit modifiée ou remplacée par un autre acte. Mais elle aura des incidences sur le cadre adopté récemment pour le troisième pilier, car il n'est pas pleinement conforme aux nouvelles exigences et devra donc être remplacé ou modifié par un acte adopté en codécision.

Quoi qu'il en soit, la nouvelle base juridique offrira l'occasion de repenser complètement la législation européenne en matière de protection des données, ce qui pourrait avoir des répercussions dans tous les domaines évoqués aujourd'hui. Un dernier enjeu très important est donc la manière dont nous pouvons mettre à profit les possibilités qui existent pour protéger mieux et plus efficacement les données à l'avenir.

---