Conférence sur la «Sécurité de l'e-administration»
Parlement européen, Bruxelles, le 19 février 2013

«Le rôle de la législation en matière de protection des données»

Peter Hustinx
Contrôleur européen de la protection des données

Comme l'affirme très justement l'invitation à cette conférence, *«l'e-administration est au cœur des politiques de réforme du secteur public menées actuellement dans le monde entier, où l'utilisation des technologies de l'information et de la communication vise à numériser les transactions, à fournir un meilleur service public et à tirer parti de l'innovation dans le secteur public»*. Elle mentionne également quelques-uns des défis qui se posent actuellement: *«comment garantir un niveau de sécurité adéquat et protéger la vie privée des citoyens?»*.

La présente note introductive s'intéresse aux défis liés à la protection de la vie privée, et plus particulièrement au regard de la législation actuellement en vigueur et de la législation qui le sera très probablement bientôt dans le domaine de la protection des données. Elle ne vise nullement à constituer le «clou du spectacle», mais à contribuer à surmonter certains problèmes et à trouver la meilleure voie possible.

À cette fin, cette note présente d'abord brièvement certaines caractéristiques pertinentes de ce que l'on appelle communément l'«e-administration» (1), et les liens qui existent entre sécurité et vie privée (2). Elle aborde ensuite un certain nombre de défis majeurs liés au respect de la vie privée et à la protection des données[1] (3), et examine l'impact sur ces questions de la révision du cadre juridique européen en matière de protection des données (4). La note se termine par quelques conclusions et pistes de réflexion importantes (5).

1. L'e-administration

Le terme «e-administration» couvre (beaucoup) plus d'aspects que la simple utilisation – systématique – des TIC pour la fourniture de services publics. En effet, si l'e-administration se limitait à cela, cette conférence aurait porté sur l'efficacité ou sur les économies d'échelle. En revanche, *la réforme actuelle du secteur public* englobe plusieurs autres dimensions qui sont reliées entre elles et que l'on peut résumer de la manière suivante:

[1] Le respect de la vie privée et la protection des données sont des notions juridiques étroitement liées mais différentes, qui sont reconnues comme des droits fondamentaux par le droit de l'UE, et visées dans deux dispositions distinctes dans la charte des droits fondamentaux de l'UE: d'un côté, le droit au respect de la vie privée et familiale (article 7), et, de l'autre, le droit à la protection des données à caractère personnel (article 8). Ce dernier est également mentionné à l'article 16 du traité sur le fonctionnement de l'Union européenne, ainsi qu'une base juridique générale pour l'adoption de règles contraignantes en matière de protection des données, non seulement pour les institutions et les organes de l'UE, mais également pour les États membres, dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union. L'article 16 du traité FUE sert de base principale pour la révision actuelle du cadre juridique de l'UE en matière de protection des données.

- redistribution des missions publiques: l'utilisation des TIC non seulement permet, mais exige également souvent, de redéfinir les missions et les services publics susceptibles de faire intervenir différents organismes publics ou différents niveaux de l'administration publique, ou d'impliquer des acteurs privés dans divers rôles («front office» ou «back office»);
- infrastructures communes: la redéfinition des missions et services publics entraîne fréquemment la mise en place d'infrastructures communes pour un usage multifonctionnel ou pour la fourniture de services partagés;
- fourniture de services en ligne: les nouvelles infrastructures permettent non seulement la fourniture de services en ligne, mais aussi à travers des services et organismes publics, créant ainsi des interfaces plus ou moins indépendantes avec les citoyens (usagers, clients, etc.).

La plupart des réformes actuelles du secteur public concernent le *niveau national*, même si les expériences sont partagées avec des projets similaires dans d'autres pays. Le nombre de systèmes transfrontaliers (tels que le système d'information du marché intérieur) demeure très limité.

2. Sécurité et respect de la vie privée

Les infrastructures de TIC destinées aux services d'e-administration requièrent incontestablement un niveau de sécurité extrêmement élevé et solide, afin d'en garantir en permanence la disponibilité, l'intégrité et la confidentialité. C'est d'autant plus vrai si l'on tient compte du risque et de l'impact potentiel de cyber-attaques. Dans ce contexte, il est donc fort possible qu'une infrastructure multi-niveaux soit nécessaire afin d'assurer un niveau de sécurité adéquat.

Toutefois, il convient de ne pas confondre «sécurité» et «vie privée». De la même façon, le «respect de la vie privée » et la « protection des données» ne doivent pas être traités comme une simple sous-catégorie de la sécurité.[2] Au contraire, ces concepts doivent être considérés comme distincts et ne se chevauchant que partiellement. En bref, si bonne sécurité ne rime pas forcément avec bonne protection de la vie privée et des données, une bonne sécurité est indispensable pour une protection adéquate de la vie privée et des données.[3]

Cet argument peut également être formulé d'une autre manière: si des mesures de sécurité sont nécessaires pour protéger contre «la diffusion ou l'accès *non autorisés*» ou «toute autre forme de traitement *illicite*»[4], le respect de la vie privée et la protection des données posent surtout la question de savoir si une diffusion ou un accès donné, ou toute autre forme de traitement, doivent ou non être *autorisés* ou s'ils sont *licites*. Ce dispositif juridique prévoit également un certain nombre de droits pour les personnes concernées, ainsi que la mise en place de certaines mesures de surveillance institutionnelle.[5]

---

[2] Le terme «protection des données» est apparu dans les années 1980, d'après le terme allemand «Datenschutz». Toutefois, il ne désigne pas la protection des données en tant que telle, mais la protection des personnes concernées contre la collecte et l'utilisation inappropriées des données à caractère personnel les concernant. Voir l'article 1 de la directive 95/46/CE relative à la protection des données: «*Les États membres assurent [...] la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.*»

[3] Les articles 16 et 17 de la directive 95/46/CE traitent de la «confidentialité» et de la «sécurité des traitements».

[4] Article 17, paragraphe 1, de la directive 95/46/CE: *«Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite. [...]»*

[5] L'article 8 de la charte des droits fondamentaux dispose:

3. Défis liés au respect de la vie privée et à la protection des données

Une brève présentation de la législation actuelle en matière de protection des données, telle qu'elle s'applique à l'e-administration, nous amène à nous pencher sur les principaux points suivants.

Champ d'application

Les lois nationales mettant en œuvre la directive 95/46/CE s'appliquent au traitement des «données à caractère personnel», c'est-à-dire *«toute information concernant une personne physique identifiée ou identifiable»* dans le secteur privé ou public.[6] Bien que ces lois reposent sur les mêmes concepts et principes de base, en conformité avec la directive, elles ont tendance à différer légèrement sur de nombreux points importants. Chaque loi nationale devrait s'appliquer à l'ensemble des traitements effectués *«dans le cadre des activités d'un établissement du responsable du traitement»* sur le territoire de l'État membre concerné.[7] En principe, cela signifie que l'e-administration, dans un État membre particulier, est régie par les lois de cet État membre. Il s'agit le plus souvent de la loi générale sur la protection des données de l'État concerné, qui peut être complétée ou non par une loi spécifique applicable dans ce domaine.

Responsabilité

La responsabilité de la conformité avec les exigences de protection des données incombe au «responsable du traitement», c'est-à-dire *«la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel»*.[8] Dans le secteur public, le responsable du traitement est normalement l'organisme public légalement responsable de la fourniture du service. Toutefois, dans le domaine de l'e-administration, il est de plus en plus fréquent que d'autres acteurs publics ou privés interviennent également, ce qui peut conduire à l'apparition de différents dispositifs de contrôle commun. La nature et le champ d'application de ces dispositifs peuvent poser problème.

Le responsable du traitement doit être soigneusement distingué du «sous-traitant», c'est-à-dire *«la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement»*.[9] Les sous-traitants ont des obligations particulières, notamment en ce qui concerne la confidentialité et la sécurité des traitements, mais l'accent est principalement mis sur le responsable du traitement. Cette terminologie n'exclut pas d'autres sous-traitants ou sous-traitants ultérieurs. Cependant, la nécessité de garantir la responsabilité globale du responsable du traitement reste entière.

---

1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données 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. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

[6] Article 2, point a), et article 3 de la directive 95/46/CE.

[7] Article 4 de la directive 95/46/CE.

[8] Article 2, point d), de la directive 95/46/CE.

[9] Article 2, point e), de la directive 95/46/CE.

Traitement licite

Les principes fondamentaux de la protection des données posent un certain nombre de conditions essentielles de licéité des traitements. Les exigences de base relatives à la qualité des données[10] sont que les données personnelles doivent être:

a) *traitées loyalement et licitement;*
b) *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités [...];*
c) *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;*
d) *exactes et, si nécessaire, mises à jour [...];*
e) *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement [...].*

Les conditions relatives à la légitimité[11] les plus pertinentes dans ce contexte prévoient que le traitement de données à caractère personnel ne peut être effectué que si:

a) *la personne concernée a indubitablement donné son consentement; ou*
b) *[...]*
c) *il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis; ou*
d) *[...]*
e) *il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées; ou*
f) *[...].*

Le respect de ces conditions requiert une analyse minutieuse et en temps utile de l'ensemble des éléments pertinents, aux différents stades du traitement des données à caractère personnel auquel ils s'appliqueront, notamment en ce qui concerne la *détermination des finalités, l'utilisation compatible et la nécessité des données à caractère personnel*. Il appartient au responsable du traitement de s'assurer du respect de ces conditions.[12]

Il est intéressant de noter que les dispositions relatives à la sécurité des traitements mentionnées plus haut requièrent la mise en œuvre de *«mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre [...] toute [...] forme de traitement illicite. Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger».*[13] Cette législation fixe un niveau d'exigence élevé pour la plupart des projets d'e-administration pertinents.

Droits de la personne concernée

Le responsable du traitement doit également garantir aux personnes concernées la possibilité d'exercer un certain nombre de droits spécifiques. Hormis les informations adéquates à fournir aux personnes concernées lors de la collecte des données les concernant, afin de garantir un traitement transparent, les personnes concernées ont le droit d'accès, de

[10] Article 6, paragraphe 1, de la directive 95/46/CE.
[11] Article 7 de la directive 95/46/CE.
[12] Article 5, paragraphe 2, de la directive 95/46/CE.
[13] Article 17, paragraphe 1, de la directive 95/46/CE.

rectification et d'effacement, ainsi que le droit de s'opposer au traitement, sous réserve seulement de quelques exceptions assez strictes.[14]

Contrôle

Le développement de l'e-administration est non seulement soumis au contrôle et à l'intervention éventuelle d'une autorité de contrôle indépendante dans chaque État membre, mais il peut aussi faire l'objet de contrôles préalables à différents stades de projets pertinents. Ces contrôles peuvent également comprendre la consultation préalable de l'autorité de contrôle sur des lois spécifiques instaurant certaines mesures d'e-administration.[15]

4. Révision du cadre juridique européen

En janvier 2012, la Commission européenne a présenté une proposition de règlement général sur la protection des données[16] destinée à remplacer la directive 95/46/CE, qui fait actuellement l'objet de discussions au Parlement européen et au Conseil. Les aspects suivants apparaissent comme les plus pertinents pour l'e-administration.

Champ d'application

La proposition de règlement sera directement applicable dans tous les États membres et remplacera les lois nationales en vigueur, sauf en ce qui concerne les spécificités nationales pour lesquelles une certaine souplesse est accordée. Le degré de flexibilité dans le secteur public est un point de discussion important, notamment au Conseil. Cependant, le règlement devrait en principe prévoir un seul ensemble de règles applicable dans tous les États membres. Son champ d'application s'étendrait également aux acteurs établis dans des pays tiers, lorsqu'ils exercent leurs activités sur le marché européen.[17] Ce règlement aurait un impact significatif sur la fourniture de services d'informatique en nuage.

Responsabilité

La proposition de règlement prévoit des responsabilités accrues pour les responsables du traitement et de nouvelles obligations pour les sous-traitants.[18] En général, les responsables du traitement doivent prendre des mesures appropriées pour garantir, et être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect du règlement. Le règlement comporte aussi un certain nombre d'obligations spécifiques, comme l'adoption de mesures appropriées pour «la protection des données dès la conception» et «par défaut», et la nécessité de réaliser des «analyses d'impact relatives à la protection des données», autant de mesures qui semblent être pertinentes pour l'e-administration. Cela met en évidence la nécessité d'identifier clairement le responsable du traitement et de mettre en place, si nécessaire, des dispositifs de contrôle partagé très solides.

Traitement licite

Les conditions essentielles de licéité des traitements continueront à s'appliquer sous leur forme actuelle, avec, éventuellement, une certaine souplesse en ce qui concerne la nécessité d'une utilisation compatible.[19] Toutefois, dans la mesure où il s'agit d'un élément clé de la protection des données, qui est également mis en avant dans la charte des droits fondamentaux de l'UE, le degré de souplesse sera limité.

[14] Articles 10 à 14 de la directive 95/46/CE.
[15] Articles 18 à 21, et article 28 de la directive 95/46/CE.
[16] COM (2012) 11 final.
[17] Article 3 de la proposition de règlement.
[18] Articles 22 à 34 de la proposition de règlement.
[19] Articles 5 et 6 de la proposition de règlement.

Droits de la personne concernée
Les conditions de transparence ont été améliorées, et tous les droits existants ont été renforcés,[20] avec l'ajout de nouveaux éléments comme le «droit à l'oubli numérique» et le «droit à la portabilité des données», qui pourraient, dans une certaine mesure, être également pertinent pour le secteur public. Le responsable du traitement sera également tenu de mettre en place des mécanismes et des procédures permettant aux personnes concernées d'exercer leurs droits. Ce règlement fera donc partie intégrante du développement de l'e-administration.

Contrôle
Les autorités de contrôle seront investies de pouvoirs beaucoup plus importants[21]. L'autorité de contrôle aura notamment le pouvoir d'infliger de lourdes sanctions financières en cas de violation de la proposition de règlement et d'imposer des mesures spécifiques lorsque des obligations d'ordre général ne sont pas respectées. Des mesures seront également prises pour garantir la coopération et la cohérence de la protection des données dans toute l'UE.[22]

5. Conclusions
La révision du cadre juridique européen vise à renforcer les règles de protection des données, à les rendre plus efficaces en pratique et à garantir une meilleure cohérence au sein de l'UE. L'adoption d'un ensemble unique de règles permettra de faciliter les projets transfrontaliers, mais fera également monter les enjeux pour l'e-administration.

La responsabilité de la fourniture de services d'e-administration nécessitera une répartition très claire des responsabilités et la mise en place de mécanismes de transparence et de responsabilisation solides, y compris en ce qui concerne la protection des données dès la conception, les analyses d'impact et le suivi régulier des résultats dans la pratique.

[20] Articles 11 à 21 de la proposition de règlement.
[21] Articles 46 à 54, et article 79 de la proposition de règlement.
[22] Articles 55 à 63 de la proposition de règlement.