

Audition du Comité économique et social européen sur le déploiement
des systèmes de transport intelligents - Ostrava, le 26 mars 2009

Une protection des données intelligente pour les systèmes de transport intelligents

Giovanni Buttarelli

Contrôleur européen adjoint de la protection des données

Remarques préliminaires

- Je me réjouis de me trouver ici aujourd'hui et je voudrais remercier les organisateurs de m'avoir invité.
- Je commencerai par expliquer brièvement pourquoi il est important que le CEPD soit représenté ici aujourd'hui. Le CEPD, qui entame son deuxième mandat quinquennal, est une agence autonome de l'UE chargée principalement de trois missions: contrôler le traitement de données à caractère personnel effectué par les institutions et les organes communautaires (*contrôle*); conseiller les institutions de l'UE sur la législation de l'Union ayant une incidence sur la protection des données à caractère personnel – il peut s'agir de propositions d'instruments légaux, mais aussi de communications et d'autres mesures (*consultation*); coopérer avec d'autres autorités de protection des données instituées tant au niveau national qu'europpéen en vue d'une application et d'une exécution plus uniformes du cadre juridique de l'UE en matière de protection des données (*coopération*).

- Le rôle de consultation et de coopération joué par le CEPD prend tout son sens dans le domaine des systèmes de transport intelligents. En effet, le CEPD a été officiellement consulté par la Commission sur le plan d'action STI et il présentera bientôt un document à ce sujet. En outre, ce n'est pas la première fois que le CEPD et les autorités nationales de protection des données traitent des questions soulevées dans le plan d'action STI. Le CEPD a publié un avis sur la proposition de la Commission visant à faciliter l'application transfrontière de la législation dans le domaine de la sécurité routière en mai 2008 et, avec le GT29, un document de travail sur eCall en septembre 2006. Récemment, le CEPD a également formulé des observations informelles sur un projet de décision de la Commission relative au service européen de télépéage, et il contribue à un mémoire sur le péage rédigé par le groupe de travail international sur la protection des données dans les télécommunications (qui devrait être adopté d'ici la fin du mois d'avril).
- Ce lien étroit entre les systèmes de transport intelligents et la protection des données n'a rien de surprenant. Les systèmes de transport intelligents reposent sur l'utilisation croissante de technologies émergentes de l'information et de la communication, qui nécessitent la collecte et le traitement d'un énorme volume de données. Ils forment dès lors un domaine fortement tributaire des données. Dans de nombreux cas, ces données revêtent un caractère personnel, dans le sens où elles se rapportent à des personnes identifiées ou identifiables. En effet, le concept de données à caractère personnel ne se limite pas aux informations biographiques, mais il inclut, par exemple, les informations liées à la géolocalisation des personnes, à la manière dont elles conduisent, à leur utilisation des systèmes de télécommunications et aux sanctions dont elles pourraient faire l'objet.
- Par conséquent, même quand les objectifs sont licites et qu'ils poursuivent un intérêt public important, comme c'est le cas en l'occurrence, il est crucial de déterminer la manière dont les informations doivent être utilisées.

Principes de la protection des données présentant un intérêt pour les systèmes de transport intelligents

- Dans ce contexte, je voudrais mettre en exergue certains principes et aspects de la protection des données susceptibles de présenter un intérêt particulier pour les systèmes de transport intelligents. Ces principes découlent de la législation européenne en la matière, et en particulier de la directive 95/46 sur la vie privée et de la directive 2002/58 sur la vie privée dans les télécommunications.
- Motifs légaux de traitement. Le traitement des données à caractère personnel doit reposer sur un des motifs légaux prévus par la législation relative à la protection des données, notamment le consentement de la personne concernée ou une obligation légale que le responsable du traitement doit respecter (article 7 de la directive 95/46/CE). Par conséquent, il est essentiel de déterminer clairement si les différentes activités de traitement découlant des initiatives de STI seront effectuées sur une base facultative ou obligatoire, ou sur une combinaison des deux (voir le document de travail du GT29 sur eCall). Une base facultative supposerait que l'utilisateur soit en mesure de donner (et retirer) librement son consentement. Une base obligatoire supposerait que l'obligation de traiter les données soit fixée dans un cadre juridique qui tienne dûment compte des principes de la protection des données. Un système mixte supposerait que certaines activités de traitement soient obligatoires et d'autres laissées au libre choix de l'utilisateur, par exemple en ce qui concerne les services et caractéristiques supplémentaires. Dans tous les cas, même un système basé sur une obligation légale doit tenir dûment compte de la protection des données. Dans ce contexte, il importe de faire en sorte, dans la mesure du possible, que les utilisateurs aient le droit de désactiver leur appareil.
- Principe de la limitation des finalités. Les finalités pour lesquelles des données à caractère personnel peuvent être traitées doivent toujours être clairement définies, compte tenu du fait que l'utilisation à des fins ultérieures incompatibles n'est possible que lorsque des circonstances

spécifiques sont réunies. En principe, une conservation massive de données à caractère personnel «au cas où», par exemple à des fins répressives, doit être exclue.

- Limitation/nécessité des données. Les systèmes de transport intelligents sont «alimentés» par des données – et en particulier des données de géolocalisation – et ne sauraient exister sans elles. Les caractéristiques spécifiques doivent toutefois être analysées en détail en fonction des finalités poursuivies. Ainsi, en ce qui concerne les différents systèmes de transport, et en particulier les transports routiers, les informations générales – telles que le trafic, les accidents, les opportunités – doivent être distinguées des informations spécifiques se rapportant à des individus et parfois à des personnes morales. Si les informations ne sont pas sélectionnées avec précision, il y a un risque réel de collecte massive et disproportionnée de données à caractère personnel. Dans ce contexte, il importe de souligner que les informations se rapportant à des véhicules identifiables et à des numéros d'immatriculation sont des données à caractère personnel.
- Anonymisation. Conformément aux principes de la protection des données, si des données à caractère personnel ne sont pas nécessaires – ou si elles ne le sont qu'à un stade précoce –, elles ne peuvent être collectées ou elles doivent être anonymisées dès que possible. Si des données sont utilisées ultérieurement à des fins statistiques ou d'analyse du marché, elles doivent être anonymisées. Par exemple, lorsqu'il s'agit de fournir des informations utiles au public à partir de données agrégées (comme les itinéraires de rechange, les conditions du trafic, etc.), il est nécessaire de supprimer le lien avec des individus identifiables, surtout si l'on tient compte du fait que les données agrégées sont souvent dérivées d'informations sensibles, comme le trafic téléphonique et la géolocalisation. À cet égard, il convient de souligner que le cryptage de données n'équivaut pas à lui seul à une anonymisation, dans la mesure où des données peuvent être reliées à un individu identifiable.

- Proportionnalité. Les activités de traitement doivent être proportionnées aux finalités poursuivies. Ce principe recouvre toute une série d'éléments tels que la quantité et la nature des données collectées et échangées, les périodes de conservation, les modalités et l'architecture des systèmes. Par exemple, les données seront-elles poussées de l'utilisateur au système ou tirées directement du système? Dans quelle mesure les personnes concernées contrôleront-elles l'échange de données? Où les données liées aux paiements seront-elles stockées?
- Information des utilisateurs. Les utilisateurs doivent être dûment informés des principaux éléments des activités de traitement et de leurs droits. Ainsi, ils doivent savoir si le traitement des données à caractère personnel (et lequel) est obligatoire ou facultatif et être informés des possibilités et des risques pouvant résulter du traitement de leurs données à caractère personnel. Ces informations peuvent être fournies par un contrat unique ou par plusieurs contrats. Cette dernière option peut toutefois présenter un risque de fragmentation, c'est-à-dire que les utilisateurs n'ont plus une image globale de la manière dont leurs données sont traitées.
- Droits des personnes concernées. Certains droits fondamentaux des utilisateurs du système doivent être garantis, comme le droit d'avoir accès à leurs données à caractère personnel, de les faire rectifier ou de s'opposer à leur traitement dans certains cas.
- La sécurité de l'information est également un élément clé, et je me réjouis de voir que la sécurité des données est explicitement mentionnée dans le plan d'action. La sécurité ne signifie pas seulement l'intégrité du système, mais aussi la disponibilité des informations et la stabilité du système. À ce propos, il importe de garantir la sécurité non seulement pendant le fonctionnement du système (c'est-à-dire lorsqu'un véhicule circule sur une route), mais aussi au-delà du fonctionnement du système (en empêchant l'usage impropre et les effets collatéraux des appareils: garantir, par exemple, que les appareils nomades sont inaccessibles aux tiers non

autorisés et qu'ils ne sont pas utilisés pour identifier et tracer les personnes pour une finalité étrangère au système).

- En ce qui concerne les garanties, certaines informations peuvent avoir une nature «neutre», tandis que d'autres, même si elles ne sont pas sensibles, peuvent donner lieu au contrôle préalable de l'autorité de protection des données compétente, puisqu'elles révèlent la situation de certaines personnes, la manière dont elles utilisent les systèmes de transport ou même si certains individus devraient faire l'objet de sanctions telles que des amendes.

Conclusions

En examinant le plan d'action STI, le législateur de l'UE, en ce compris le Comité économique et social, a une occasion unique de tenir compte des principes de la protection des données et donc d'élaborer une vision fructueuse du déploiement des systèmes de transport intelligents en Europe; une vision à long terme, qui tient compte non seulement des applications disponibles actuellement, mais aussi des éventuelles évolutions futures des systèmes.

Il importe dès lors de profiter de cette occasion pour déterminer en amont l'architecture de l'infrastructure du système, les flux de données (des véhicules à l'infrastructure et entre les véhicules), les catégories de données et les finalités pour lesquelles elles sont utilisées, les modalités de traitement des informations, la période de conservation des données, la réutilisation éventuelle des informations ainsi que le rôle des différents acteurs dans les systèmes envisagés. Cela est particulièrement important dans les systèmes intégrés, où il est nécessaire de clarifier les rôles et les responsabilités, notamment en ce qui concerne les différents fournisseurs qui contribuent au système et la manière dont ils garantiront la sécurité du réseau.

Il est par conséquent primordial de prendre en compte d'emblée les questions liées à la vie privée, au moment de définir l'architecture des systèmes de transport intelligents («respect de la vie privée dès la conception») et de mettre

en œuvre le système. En outre, l'utilisation des technologies renforçant la protection de la vie privée (PET) doit être encouragée.

À cet égard, je recommande que les questions liées à la protection des données soient traitées de manière plus détaillée au niveau de l'UE par la publication d'orientations adéquates concernant l'application des principes de la protection des données aux systèmes de transport intelligents. Dans le cas contraire, des interprétations nationales différentes et des problèmes non résolus de protection transfrontalière des données pourraient entraver le déploiement et l'interopérabilité du système envisagé.

Si les principes liés à la vie privée ne sont pas pris en considération, il y a des risques élevés non seulement de non-conformité avec la législation, mais aussi d'utilisation impropre du système et, au final, de perte de confiance des consommateurs. Est également en jeu ici la liberté de mouvement interprétée de manière dynamique, c'est-à-dire comme la liberté de se déplacer sans laisser de trace permanente et donc sans perdre le droit de se déplacer anonymement.

La protection des données ne fait pas obstacle à un échange efficace d'informations, ainsi que l'expérience des acteurs de la protection des données l'a montré jusqu'à présent pour ce qui est de l'utilisation des technologies de l'information et de la communication dans d'autres contextes, comme l'internet et l'utilisation de téléphones mobiles. Le CEPD souhaite contribuer de manière constructive à une utilisation efficace et licite des TIC dans le secteur des transports. Le déploiement des systèmes de transport intelligents ne peut toutefois pas avoir comme conséquence que les utilisateurs perdent leur droit à circuler anonymement.

Je souhaite donc souligner le fait qu'une prise en compte adéquate de la protection des données dans l'architecture et la mise en œuvre du système constitue un élément clé du succès des projets de STI: les systèmes de transport intelligents ont besoin d'une protection des données intelligente.