RESUME

Cette étude est une des dix études de domaine du projet ACTIF. Elle présente la particularité d'être **une étude transverse**, impactant potentiellement sur l'ensemble des domaines fonctionnels couverts par l'architecture. . Le plan du document reprend les trois phases suivantes : état des lieux, analyse de cas concrets, conclusions :retour sur l'architecture ACTIF et recommandations.

Le droit à la protection de la vie privée constitue une liberté fondamentale dans un Etat démocratique. En France, la protection de la vie privée est issue des principes de la déclaration des droits de l'Homme et du Citoyen de 1789. Les nouvelles technologies de l'information et de la communication (NTCI), dont font appel les Systèmes de Transports Intelligents (STI), donnent une importance particulière à la protection de la vie privée. En effet, les nouveaux moyens techniques rendent plus faciles les atteintes aux informations d'ordre privée. L'objectif est d'éviter le phénomène « Big Brother » dont l'opinion publique est de plus en plus sensible.

L'analyse de l'architecture-cible, notamment l'étude des flux d'informations et des bases de données a permis d'identifier des données à caractère personnel. Ainsi, cette étude a pour but d'orienter l'architecture d'ACTIF afin qu'elle puisse s'intégrer dans le cadre juridique lié au respect de la vie privée. L'étude a volontairement été limitée à la protection de la vie privée, et des aspects « protection des informations commerciales » ou « respect de la concurrence » ont été volontairement écartés. Ils relèvent néanmoins de la même préoccupation : protéger des informations sensibles

A partir d'entretiens avec la CNIL (Commission Nationale Informatique et Liberté), et sur la base d'une analyse bibliographique des principaux textes de loi français, européens et mondiaux, l'état des lieux a permis d'identifier les exigences et les contraintes qu'engendrent le recueil, le stockage et le traitement d'informations à caractère personnel. Cette démarche a également été entreprise pour ce qui concerne l'utilisation de vidéo-surveillance dans les lieux publics. Il apparaît que l'utilisation d'informations à caractère personnel est autorisé dans un cadre précis, imposant au maître d'ouvrage des devoirs. Volontairement réducteur, l'énoncé des exigences à respecter peut être le suivant :

- Obligation de déclaration de la création d'un fichier,
- Obligation de sécuriser ce fichier,
- Principe de spécialité des données collectée pour une finalité identifiée,
- Obligation de maîtriser la durée de conservation des données vis-à-vis de la finalité,
- Droit de la loyauté de la collecte des données,
- Droit d'opposition pour des raisons légitimes au traitement des données personnelles,
- Droit d'information sur la finalité des traitements,
- Droit d'accès et de rectification,
- Droit à l'oubli.

A ces droits s'ajoute un encadrement strict pour pouvoir traiter des données nominatives qui feraient apparaître les origines raciales ou les opinions politiques, philosophiques, ou religieuses ou les appartenances syndicales ou les orientations sexuelles (ce qu'on appelle les données sensibles).

La phase 2 a étudié différents cas concrets vis-à-vis de cette problématique. La doctrine de la CNIL, ainsi que l'analyse des textes législatif et européens, montrent clairement les limites dans l'utilisation qui peut être faîte de ces données personnelles. Il est à noter qu'une analyse juridique s'appuie principalement sur des éléments concrets, qu'ils soient techniques ou fonctionnels. La mise en œuvre concrète d'un projet où des informations personnelles seraient concernés est donc essentielle pour émettre un avis motivé. Chaque application doit être étudiée spécifiquement.

La phase 3 précise en premier lieu qu'il est recommandé, compte-tenu des contraintes légale et des impacts sur l'architecture, de **limiter au strict nécessaire** l'utilisation de données à caractère nominatif. En second lieu, les recommandations se déclinent en 4 axes :

1. Compte-tenu de l'architecture-cadre telle qu'elle est spécifiée, la recommandation majeure est le respects de 2 exigences : D'associer à chaque fichier constitué un responsable unique, et une ou plusieurs finalités définies, compatible avec les attributions du responsable.Ces deux contraintes ont un impact non négligeable sur l'architecture, sachant que la modélisation a spécifié des fichiers importants, partagés par plusieurs responsables et attachés à des finalités différentes. Ce modèle va donc à l'encontre des règles élémentaires quant au respect de la vie privée.
2. Conscient de la difficulté d'appréhendé des textes de loi, 4 fiches de sensibilisations et d'informations ont été rédigées :
   Respect de la vie privée : règles à suivre
   Démarche pour déclarer un système automatisé d'informations nominatives
   Vidéo-surveillance : règle à suivre
   Démarche pour déclarer un système de vidéo-surveillance
3. Le stockage des informations nominatives nécessitent de par la loi une sécurisation adapté. Dans ce but, les principales fonctions de sécurisation de tels fichiers ont été précisées, et devront être implémentées autant que de besoins.
4. Enfin, le respect de la vie privée est un axe particulier de la notion de Sécurité Informatique. Un système d'information, à contrario des systèmes d'information fédérés et échangeant des informations, traite des informations sensibles d'une autre nature (données commerciales, secrets industriels, …), et qui sont la cible de plusieurs autres menaces visant à atteindre la confidentialité, l'intégrité et la disponibilité des données et des traitements. Afin d'éviter une perte de confiance des acteurs, entraînant une limitation de leurs échanges d'information (condition indispensable à la réussite de l'architecture), un axe de travail consisterait à établir une « charte », voire une norme, de sécurité auquel devrait adhérer les différents acteurs pour être en conformité avec l'architecture cadre. Elle s'appuierait sur une analyse structurée des menaces, des enjeux et définirait les mesures à adopter.