Protection des données personnelles lors de l'utilisation d'appareils AIS Intérieur

Rapport de synthèse : état des lieux des règlementations nationales au 15 avril 2014

1. Etat des lieux de la réglementation actuelle en matière de protection des données en lien avec l'AIS intérieur

1.1. En Suisse, la protection des données est réglementée au niveau fédéral par la loi fédérale du 19 juin 1992 sur la protection des données (LPD), RS 235.1) et par l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD), RS 235.11). Cette loi vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données. Comme l'AIS Intérieur n'émet pas de données personnelles au sens de la loi suisse, et de ce fait, ne produit pas de profils de personnalité, la LPD n'est pas applicable pour les données émises par les appareils AIS Intérieur.

De même, les données émises par les appareils AIS Intérieur ne font pas l'objet d'une règlementation spécifique en Suisse.

En revanche, le Code pénal suisse contient plusieurs dispositions qui pourraient être évoquées par des conducteurs de bateau si des tiers interceptaient ou utilisaient de façon frauduleuse les données émises par l'appareil AIS Intérieur sans leur accord. Les principaux articles pouvant être invoqués sont :

- L'article 143 qui réprime « *la soustraction des données* ».

  Cela signifie que celui qui, dans le dessein de se procurer ou de procurer à un tiers un enrichissement illégitime, aura soustrait, pour lui-même ou pour un tiers, des données enregistrées ou transmises électroniquement ou selon un mode similaire, qui ne lui étaient pas destinées et qui étaient spécialement protégées contre tout accès indu de sa part, sera puni d'une peine privative de liberté de cinq ans au plus ou d'une peine pécuniaire. La soustraction de données commise au préjudice des proches ou des familiers ne sera poursuivie que sur plainte.

- L'article 143bis qui condamne « *l'accès indu à un système informatique* ».

  Il prévoit que quiconque s'introduit sans droit, au moyen d'un dispositif de transmission de données, dans un système informatique appartenant à autrui et spécialement protégé contre tout accès de sa part est, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

- L'article 144bis qui sanctionne « *la détérioration de données* ».

  Le chiffre 1 de cet article précise notamment que celui qui, sans droit, aura modifié, effacé, ou mis hors d'usage des données enregistrées ou transmises électroniquement ou selon un mode similaire sera, sur plainte, puni d'une peine privative de liberté de trois ans au plus ou d'une peine pécuniaire.

1.2. En France, les données à caractère personnel bénéficient d'une protection particulière, notamment lorsqu'elles font l'objet d'un traitement, en d'autres termes lorsqu'elles sont contenues ou appelées à figurer dans des fichiers. La réglementation en vigueur, protectrice de la liberté personnelle, a ainsi pour objet d'encadrer les conditions dans lesquelles les personnes publiques et les personnes privées peuvent constituer des fichiers contenant des informations de nature personnelle (loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et décret n° 2005-1309 pris pour l'application de la loi précitée). La Commission Nationale de l'Informatique et des Libertés (CNIL), autorité administrative indépendante, assure ce rôle de protection. Elle est consultée sur tout projet de texte relatif à la protection des personnes à l'égard

des traitements automatisés. En outre, elle est saisie préalablement à la mise en œuvre de ce type de traitement, soit pour l'autoriser, soit pour fournir un avis motivé sur le traitement envisagé. Enfin, la CNIL dispose également de pouvoirs d'investigation, de contrôle et de sanction.

1.3. En Belgique, la loi du 8 décembre 1992, relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, a servi de base au texte réglementaire relatif à la protection des données personnelles (Arrêté royal du13 février 2001 en exécution de la Loi du 8 décembre 1992, relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel). Par données à caractère personnel, on entend : « toute information concernant une personne physique identifiée ou identifiable, désignée ci-après « personne concernée » ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. »

Un organe de contrôle indépendant auprès de la Chambre des représentants a été institué le 1er janvier 2004 : la Commission de la protection de la vie privée. Elle a pour mission de veiller à ce que la vie privée soit respectée lors du traitement de données à caractère personnel. Elle examine toute plainte parallèlement à la procédure menée par l'instance judiciaire. Elle accomplira une mission de médiation pour parvenir à une conciliation des parties ou, en l'absence de conciliation, elle émettra un avis.

1.4. Aux Pays-Bas, le dispositif juridique repose sur deux outils : le Code de la circulation maritime et fluviale et la loi relative à la protection des données personnelles (Wbp)

- Les mesures pour les usagers des voies navigables reposent sur le *« Scheepvaartverkeerswet »* (Code de la circulation maritime et fluviale). Il contient une base légale permettant de déléguer la réglementation concernant « *la réception, la conservation et la communication de données relatives à la navigation par des organisations et des personnes qui ne sont pas des acteurs du trafic* ». (Article 4, chiffre 1, lettre E).

  Cet article prévoit entre autres la possibilité de réglementer la réception, le traitement et la réutilisation d'informations dans le cadre des Services d'information Fluviale (SIF)[1], également pour des personnes / organisations à terre.

  D'autres règles sont stipulées par règlement d'administration publique, notamment la résolution concernant les formalités déclaratives et le traitement de données de la navigation.

- Le traitement des données personnelles est régi par la loi relative à la protection de données personnelles (Wbp).

1.5. En Allemagne, le dispositif juridique repose essentiellement sur deux niveaux :

- des lois cadres (la loi fédérale relative à la protection des données et les lois correspondantes des Länder)

- des lois relatives à la protection des données qui sont spécifiques au domaine concerné. Le droit applicable à la navigation intérieure comporte également des dispositions relatives à la protection des données qui sont spécifiques à certains domaines, par exemple dans la loi dite *Binnenschifffahrtsaufgabengesetz* (loi fixant l'étendue des obligations en liaison avec la navigation intérieure), qui réglemente plusieurs banques de données (infractions, inventaire de la flotte etc.) mais ne prévoit pas de disposition relative à l'AIS Intérieur. En effet, à ce jour, il n'existe pas encore de réglementation spécifique concernant la protection des données AIS.

---

1 défini en article 1, chiffre 1, lettre p, du Code, par la formulation suivante : « services d'information harmonisés favorisant la gestion du trafic et des transports dans le domaine de la navigation, y compris, dans tous les cas où cela est techniquement possible, les interfaces avec d'autres modes de transport ou d'autres activités commerciales qui ne sont pas des activités commerciales internes entre une ou plusieurs des sociétés concernées. »

- L'autorité compétente au niveau fédéral pour les questions relatives à la protection des données est le "Chargé fédéral pour la protection des données et la sécurité de l'information". En ce qui concerne les sanctions en cas d'utilisation abusive des données, sont compétents les ministères publics compétents ou les services désignés par les différentes lois relatives à la protection des données.

2. Quelles sont les mesures prises pour sécuriser les données personnelles transmises par l'appareil AIS Intérieur et leur utilisation (non commercialisation, traitement…)?

2.1. La délégation suisse suggère d'informer de manière exhaustive la profession sur les données collectées, la durée de conservation et l'usage précis fait de ces données, ceci afin d'obtenir son approbation. Ces aspects devraient par conséquent être pris en compte dans la résolution de la CCNR.

2.2. En France, pour les données des appareils AIS Intérieur, la procédure mise en œuvre est celle de la déclaration « normale » prévue à l'article 23 de la loi n° 78-17 du 6 janvier 1978 qui concerne les traitements d'application courante. Cette déclaration comporte l'engagement que le traitement des données satisfait aux exigences de la loi. Les informations transmises sont précisées par l'article 30 de la loi précitée. Le demandeur peut mettre en œuvre le traitement des données dès réception du récépissé délivré par la CNIL.

D'autres mesures sont prises pour sécuriser les données :

- protection de l'accès physique au traitement,
- mise en œuvre d'un procédé d'authentification des utilisateurs,
- journalisation des connexions,
- traitement des données réalisé sur un réseau interne dédié (non relié à internet),
- le canal de transport est chiffré pour les données échangées sur le réseau internet.

Les structures susceptibles d'être destinatrices des données sont les suivantes : les transporteurs, les chargeurs, les services internes de VNF, les douanes, les services de police fluviale, les services de justice, le tiers autorisé par le marinier lui-même.

2.3. En Belgique, l'article 17 de la loi du 8 décembre 1992 mentionnée au 1.3 prescrit la procédure à respecter lors du traitement de données. Il s'applique donc au traitement des données des appareils l'AIS Intérieur. Le traitement de données doit faire l'objet d'une déclaration auprès de la Commission de la protection de la vie privée. Le § 3 de l'article 17 précise les données devant être mentionnées dans la déclaration.

2.4. Aux Pays-Bas, les mesures prises découlent des deux textes de référence ;

a) Concernant toute information recueillie dans le cadre de l'obligation d'annonce et pour toute information reçue dans le cadre des SIF, les articles 7, 8 et 9 de la résolution concernant les formalités déclaratives et le traitement de données de la navigation stipulent qui peut être destinataire de cette information et dans quelles conditions. D'après ces articles, le gestionnaire de la voie navigable locale est autorisé à utiliser de l'information pour la gestion du trafic. Par contre, il est explicitement exclu que le gestionnaire de la voie navigable ou quiconque se serve de ces données pour contrôler le respect des règlements, à moins qu'il ne soit question d'une suspicion de délit.

Cette protection concerne toutes les données provenant de la navigation, qui sont utilisées pour la gestion du trafic. Il ne s'agit pas uniquement des données des SIF, mais également des informations obtenues par le biais d'annonces, obligatoires ou non, par exemple l'obligation d'annonce visée à l'article 12.01 du RPNR, et les informations obtenues par image radar d'une installation à terre, au moyen desquelles les itinéraires des bateaux sont enregistrés.

Pour conclure, toute infraction à la résolution concernant les formalités déclaratives et traitement de données de la navigation est passible de sanctions au regard de l'article 31, chiffre 4, du Code de la circulation maritime et fluviale. Cette disposition prévoit l'application d'une peine sous forme d'emprisonnement ou d'amende pouvant s'élever au plus à 7 800 euros par contravention.

b) Si des organisations ou personnes n'entrent pas dans le champ d'application de la résolution évoquée au 1.4., ou si les données ne proviennent pas de la gestion du trafic, deux instruments légaux permettent de protéger les données émises par les appareils AIS Intérieur :

- Le premier est le Code pénal. Toute divulgation d'information par une personne qui a obtenu cette information alors qu'elle ne lui était pas destinée est considérée comme en infraction d'après l'article 441 du Code pénal. Selon l'utilisation effective de l'information obtenue (par exemple la communication de l'information), toute utilisation abusive peut être sanctionnée conformément à cet article.

- La loi sur la protection des données personnelles peut également être invoquée dans certains cas. En effet, les informations AIS sont souvent réductibles à des personnes physiques, puisque beaucoup d'entreprises fluviales sont des entreprises unipersonnelles. Dans ce cas, il s'agit de données personnelles. D'après le service juridique du Ministère de l'Infrastructure et de l'Environnement ainsi que du Conseil pour la protection des données à caractère personnel (CPB), les informations AIS sont considérées comme étant des données personnelles, puisque dans un grand nombre de cas dans la navigation intérieure, ces données sont réductibles à des personnes. Aussi, la communication, la vente, etc., sans accord explicite de l'expéditeur, de données AIS – à condition qu'elles soient réductibles à des personnes physiques – sont très probablement régies par la Wbp.

Un grand nombre de dispositions de la Wbp ont pour objet l'intérêt des personnes concernées, comme l'article 8, stipulant les situations dans lesquelles les données personnelles peuvent être traitées. Le CPB pourra infliger une amende ou le juge pénal pourra infliger une amende ou une peine de prison si des organisations ou des personnes à terre ne respectent pas ces exigences lors d'un traitement de données émises par l'AIS Intérieur.

2.5. Selon le droit allemand, les données AIS sont des données personnelles, puisque ces données peuvent être rapportées à une personne. Du point de vue de la protection des données, il en résulte que :

a) Si l'administration souhaite utiliser les données transmises par l'AIS à des fins de gestion du trafic, il est nécessaire de créer une base d'habilitation spécifique au domaine, laquelle fixe de manière détaillée quelles sont les données pouvant être collectées, enregistrées et transmises, ainsi que l'usage qui peut en être fait.

b) En revanche, l'introduction de l'obligation de posséder et d'utiliser l'équipement AIS pour l'auto-signalisation entre les bateliers ne nécessite pas de nouvelle base juridique concernant la protection des données.

c) Des prescriptions déjà en vigueur permettent de protéger les données AIS contre des tiers, étrangers à la navigation, qui souhaiteraient en faire un usage non souhaité. L'article 202b du code pénal sanctionne "l'interception de données" et l'article 43, paragraphe 2, alinéa 1, 44 de la loi fédérale relative à la protection des données protègent les données personnelles qui ne sont pas accessibles à tout un chacun contre la collecte et l'utilisation.

3. Modification / évolution de la réglementation / législation

3.1. Aucune modification / évolution de la règlementation actuelle n'est prévue en Suisse, en France, en Belgique et aux Pays-Bas.

3.2. En Allemagne, le ministère fédéral en charge du transport et de l'infrastructure digitale a prévu de prendre cette année une initiative législative pour la modification de la loi dite Binnenschifffahrtsaufgabengesetz, afin que les données AIS puissent à l'avenir être utilisées par l'administration. Le projet législatif devrait être achevé fin 2014.

3.3. Les délégations française, néerlandaise et belge ont également rappelé que la Directive européenne n°95/46/CE du 24 octobre 1995 constitue le cadre juridique européen actuel en

matière de protection des données. Une réforme actuellement en cours vise à faire évoluer ce cadre en le remplaçant par un Règlement européen d'application directe dans l'ensemble des États Membres de l'Union européenne. Le but de ce texte est de permettre une meilleure harmonisation et de renforcer l'effectivité des règles de protection des données personnelles.

***