Avis n° 31/2012 du 12 septembre 2012

Objet : demande d'avis relatif à l'avant-projet de loi portant création du cadre pour le déploiement de systèmes de transport intelligents ("loi-cadre STI") (CO-A-2012-023)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après la "LVP"), en particulier l'article 29 ;

Vu la demande d'avis du Secrétaire d'État à la Mobilité, reçue le 21/05/2012 ;

Vu le rapport de Monsieur De Schutter ;

Émet, le 12 septembre 2012, l'avis suivant :

I. OBJET ET CONTEXTE DE L'AVIS

1. Le Secrétaire d'État à la Mobilité sollicite l'avis de la Commission sur l'avant-projet de loi transposant la Directive 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 *concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport*, ci-après "l'avant-projet de loi".

2. Le présent avant-projet de loi s'inscrit dans le cadre d'un contexte européen plus large qui comprend un Plan d'action de la Commission européenne[1] (ci-après le Plan d'action STI), la Directive 2010/40/UE (ci-après la "Directive STI") et des points de vue antérieurs pertinents d'autorités européennes et étrangères, parmi lesquels :
   - un avis du Contrôleur européen de la protection des données (ci-après "CEPD")[2] ;
   - des avis du Groupe de travail Article 29 sur la protection des données (concernant un système harmonisé d'appel d'urgence paneuropéen embarqué à bord des véhicules ("eCall"), basé sur le numéro d'appel d'urgence unique européen 112) [3] et sur la géolocalisation des dispositifs mobiles intelligents[4] ;
   Il y avait également auparavant un avis du Groupe de Berlin[5].

3. Étant donné qu'il est également question d'une matière régionale[6], il y aura également une transposition de la Directive STI au niveau régional. Un avant-projet de décret[7] flamand a entre-temps été adopté, lequel entend transposer la Directive STI au niveau flamand. La Commission a appris que ce projet serait officiellement soumis à l'avis de la Vlaamse Toezichtcommissie (Commission de contrôle flamande) et a consulté cette dernière à cet égard afin de parvenir à un point de vue concerté.

4. La Commission européenne (DG MOVE) a confié à un consortium privé[8] la réalisation d'une étude sur la protection des données dont la publication est attendue en septembre. Les premiers résultats de cette étude ont été expliqués lors d'un atelier le 13 juin 2012. Les applications STI visées par cette étude sont les suivantes : tachygraphe numérique, e-Call, tarification à l'usage (Road user Charging), télébillettique dans les transports publics, paiement de services de stationnement, assurances basées sur le comportement routier

---

[1] Plan d'action de la Commission européenne du 16 décembre 2008 pour le déploiement de systèmes de transport intelligents en Europe, COM(2008) 886 final, publié sur :
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0886:FIN:FR:PDF.

[2] Voir l'Avis du contrôleur européen de la protection des données *concernant la communication de la Commission sur le plan d'action pour le déploiement de systèmes de transport intelligents en Europe et la proposition de directive du Parlement européen et du Conseil établissant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport* du 22 juillet 2009, JO, C 47/6 du 25 février 2010, publié à l'adresse suivante :
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_FR.pdf.

[3] Voir le Document de travail WP 125 du 26 septembre 2006 *sur la protection des données et le respect de la vie privée dans l'initiative "eCall"*, publié à l'adresse suivante :
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp125_fr.pdf.

[4] Voir le document WP 185 *sur les services de géolocalisation des dispositifs mobiles intelligents*, publié à l'adresse suivante :
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_fr.pdf.

[5] Document de travail du 4-5 avril 2011 relatif aux "Event Data Recorders (EDR) on Vehicles ; Privacy and data protection issues for governments and manufacturers", publié à l'adresse suivante :
http://www.datenschutz-berlin.de/attachments/795/675.42.10.pdf?1308146250.

[6] Les transports constituent principalement une matière régionale.

[7] *Relatif au cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport*.

[8] Sous la direction de l'entreprise néerlandaise Rapp Trans.

("Pay-As-You-Drive"), contrôle de vitesse par tronçon (Section Speed Control), gestion de flotte (Fleet monitoring), traitement de données de trafic (Traffic Data Collection) et systèmes coopératifs (Cooperative systems de types tels que C2C, C2I et I2C[9]).

5. L'objectif de la Directive STI est décrit comme étant le fait d' "*assurer le déploiement coordonné et cohérent de systèmes de transport intelligents interopérables dans l'Union*"[10].

6. "*Les systèmes de transport intelligents (STI) sont des applications avancées qui, sans pour autant comporter de processus intelligent à proprement parler, visent à fournir des services innovants liés aux différents modes de transport et à la gestion de la circulation et permettent à différents utilisateurs d'être mieux informés et de faire un usage plus sûr, plus coordonné et plus "intelligent" des réseaux de transport*"[11.] À cet égard, "*les STI associent les télécommunications, l'électronique et les technologies de l'information à l'ingénierie des transports afin de planifier, concevoir, exploiter, entretenir et gérer les systèmes de transport. L'application des technologies de l'information et de la communication au secteur du transport routier et à ses interfaces avec d'autres modes de transport contribuera grandement à améliorer les performances environnementales, l'efficacité, notamment énergétique, la sécurité et la sûreté du transport routier, y compris le transport de marchandises dangereuses, la sécurité publique, et la mobilité des passagers et des marchandises, tout en assurant le bon fonctionnement du marché intérieur et en améliorant les niveaux de la compétitivité et de l'emploi.* (…)"[12].

7. Les STI sont déjà lancés et développés depuis quelques années, toujours à petite échelle, dans différents projets de transport au niveau européen ou dans les États membres, dont le transport aérien (SESAR[13]), la navigation intérieure (RIS[14]), le transport par voie ferrée (ERTMS[15]) et par l'intermédiaire de sociétés de transports publics (MOBIB, NAVIGO[16]), la navigation (grands projets et systèmes tels que VTMIS[17], AIS[18], LRIT[19]), et le transport routier (eToll[20] et eCall[21]).

---

[9] Où le C signifie voiture (car) et le I infrastructure.
[10] Considérant 23 de la Directive STI.
[11] Considérant 3 de la Directive STI.
[12] Considérant 4 de la Directive STI.
[13] http://www.sesarju.eu/.
[14] http://ris.vlaanderen.be/html_nl/wat_is_ris/wat_algemeen.html.
[15] http://ec.europa.eu/transport/rail/interoperability/ertms/ertms_en.htm.
[16] http://www.cnil.fr/en/la-cnil/actu-cnil/article/article/2eme-controle-des-passes-anonymes-navigo/?tx_ttnews%5BbackPid%5D=91&cHash=1126ea84e899268aa04dd05017940670.
[17] Vessel Traffic Management Information System
http://www.transport-research.info/web/projects/project_details.cfm?id=101.
[18] L'Automatic Identification System, en abrégé AIS, est un système basé sur la technologie transponder augmentant la sécurité de la navigation maritime en mer et en eaux intérieures. Il entend offrir un aperçu et des informations via une interaction entre les navires et avec les instances à quai. Il a été introduit en 2003 dans la navigation maritime. Pour la navigation intérieure, on utilise l'Inland-AIS qui constitue un complément à la gestion actuelle du trafic de postes de circulation.

8. Il s'agit ici de services en partie publics et en partie commerciaux (par exemple, des informations de trafic en temps réel, eFreight, eCall[22], eToll, réservation d'espaces de parking[23] et le nouveau type de tachygraphe numérique avec interface STI[24]), où différents acteurs sont actifs dans la promotion des STI (par exemple, des compagnies d'assurance voiture, des entreprises de location de voitures[25], …). Ce sont surtout les services commerciaux qui sont en progression ces dernières années parce que de plus en plus de véhicules sont équipés de la navigation par satellite et de la technologie de communication mobile (réseaux sans fil et connexion Internet), permettant de collecter des données de trafic sans utiliser les systèmes en bordure de route gérés par les gestionnaires routiers[26].

9. D'après le Groupe de Berlin[27], cette tendance technologique aura pour conséquence que les véhicules intelligents (tout comme les compteurs intelligents) feront à terme partie de ce qu'on appelle l' "Internet des objets". De nouveaux concepts et de nouvelles tendances comme les "voitures connectées" (voitures "intelligentes et sociales") et la "mobilité coopérative" s'inscrivent dans ce cadre via la connexion Internet, le GPS et les réseaux locaux. De ce fait, de nouveaux services ou applications ("Apps") apparaîtront pour améliorer la sécurité, réduire les embouteillages et la pollution et accroître le confort personnel[28]. Apparaîtront également la gestion des batteries pour voitures électriques, la gestion des moteurs, la musique à la demande dans la voiture[29] et des services de marketing basés sur le contexte et la connectivité. Des inconvénients sont toutefois également liés au profilage croissant des personnes concernées en raison des risques accrus potentiellement propres à l'augmentation du traitement de données (par exemple, le piratage de l'ouverture à distance de portes, la désactivation du système d'alarme du véhicule[30], des violations de sécurité, la délimitation de cibles pour les délits, …).

---

[19] Long-range identification and tracking (LRIT).
[20] Péage électronique ou tarification à l'usage.
[21] Voir le point 3 de l'avis du CEPD qui renvoie au Plan d'action de la Commission européenne. Voir le document de travail précité du Groupe 29 relatif à l'eCall.
[22] Voir la page : http://www.nxp.com/wcm_documents/news/meet-nxp/shows-and-events/ecall/presentations/eCall_trial_end_release.pdf.
[23] Voir le point 8 de l'avis du CEPD.
[24] Voir le point 5 de l'avis du 5 octobre 2011 du Contrôleur européen de la protection des données *sur la proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CEE) n° 3821/85 du Conseil concernant l'appareil de contrôle dans le domaine des transports par route et modifiant le règlement (CE) n° 561/2006 du Parlement européen et du Conseil*, JO C 37/6 du 10 février 2012, publié à l'adresse suivante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:037:0006:0013:FR:PDF.
[25] Voir la page 5 du document de travail précité WP 125 relatif à l'e-Call du Groupe 29.
[26] Voir la page : http://www.rapptrans.nl/nl/its_pr_verkeers_reizigersinformatie.php.
[27] Voir le point 2 du document de travail précité du Groupe de Berlin.
[28] Voir la page : http://www.tue.nl/?id=17796.
[29] Voir par exemple la "MOG App" intégrée par les nouveaux modèles de différents fabricants de voitures (http://www.fastcompany.com/1839441/mog-and-ford-voice-control-music-technology-for-cars et http://www.fastcompany.com/1805641/why-cars-the-worlds-worst-mobile-devices-are-hurting-music-services-like-spotify-pandora).
[30] http://www.businessweek.com/articles/2012-06-07/is-detroit-buying-verizon-s-lte-connected-car-vision.

10. En Belgique aussi, le projet le plus concret et visible pour le grand public est probablement Mobib, outre un projet pilote de tarification à l'usage à Leuven[31] et l'utilisation de systèmes "fleetlogger" dans les voitures de service des services de police, ainsi que dans les véhicules de location et dans le transport professionnel. Les résultats du test à Leuven prouvent, d'après les acteurs concernés, que la "mobilité intelligente" marque des orientations, du fait que conformément à la politique de mobilité de la ville, il y a eu moins de détournements de trafic et que l'on a davantage roulé en période creuse[32].

II. CONSIDÉRATION PRÉALABLE GÉNÉRALE RELATIVE AU CARACTÈRE ABSTRAIT DE LA DIRECTIVE STI ET DE L'AVANT-PROJET SUR LEQUEL PORTE LA MISSION D'AVIS

11. La Commission voit sa mission légale d'avis compliquée par la trame très générale et très abstraite de la Directive STI que l'avant-projet entend transposer. La Directive STI et l'avant-projet donnent trop peu d'explications sur les applications et les systèmes STI concrets visés par l'Europe ainsi que sur les finalités visées, bien que plusieurs de ces systèmes soient néanmoins déjà connus de l'Europe car ils sont déjà déployés ou prêts à l'être[33].

12. L'Europe oblige les États membres à prendre "les dispositions législatives, réglementaires et administratives nécessaires" pour satisfaire à la Directive STI dans délai de transposition très bref (27 février 2012)[34]. D'autre part, tant les règles européennes[35] que nationales relatives à la protection de la vie privée[36] exigent que le législateur national rédige une législation concrète et claire au niveau de la définition des ingérences concrètes dans la vie privée en général et des traitements de données à caractère personnel en particulier. Le Plan d'action STI de la Commission européenne comportait des imprécisions analogues à celles de la Directive STI et avait déjà essuyé la critique du CEPD[37] sur certains points considérés comme très (trop) abstraits.

---

[31] Depuis septembre 2011, via la coopération entre IBM, NXP, Mobistar, Touring et la ville de Leuven.
[32] Source : http://www.its.be/Default.aspx?alias=www.its.be/tinc#FR.

[33] Voir la note de bas de page n° 7 ci-avant.

[34] Voir l'article 18 de la Directive STI.

[35] Voir la jurisprudence de la Cour européenne des droits de l'Homme concernant l'exigence de prévisibilité visée à l'article 8 de la CEDH, voir notamment Cour eur. D. H., 4 mai 2000, Rotaru, § 52.

[36] Voir la jurisprudence de la Cour constitutionnelle concernant l'article 22 de la Constitution.

[37] Voir les points 5 et 14 de l'avis précité du 22 juillet 2009. 5. "*Toutefois, on ne voit pas clairement les finalités spécifiques pour lesquelles les STI seront utilisés dans ces domaines (...)".* 14. "*Toutefois, le CEPD note que le cadre juridique proposé est trop large et trop général pour répondre adéquatement aux préoccupations en matière de respect de la vie privée et de protection des données que soulève le déploiement des STI dans les États membres.*"

13. Vu l'importance des systèmes et des applications STI pour notre société et l'impact que l'utilisation des technologies de géolocalisation peut avoir sur la liberté de se déplacer dans l'anonymat, la Commission estime inopportun de se limiter à émettre un avis très succinct et abstrait en la matière.

14. Afin d'assister le législateur au maximum dans l'élaboration d'un cadre légistique général approprié en matière de protection de la vie privée et des données lors de la transposition de la Directive STI, la Commission joint en annexe au présent avis une proposition concrète de texte intégrant les diverses remarques formulées dans le présent avis et tenant compte d'un précédent au niveau européen, à savoir dans le secteur de l'énergie.

15. Vu le caractère régional de la matière[38] et afin de veiller à l'unité de la réglementation relative aux garanties requises en matière de STI en Belgique vis-à-vis des divers acteurs, la Commission est favorable à la conclusion d'accords de coopération entre l'autorité fédérale et les autorités régionales dans cette matière. Elle souligne le pouvoir normatif de tels accords et attire l'attention sur le fait que la conclusion de tels accords sera également obligatoire, vu les dispositions contraignantes de la loi spéciale de réformes institutionnelles du 8 août 1980[39].

16. La Commission et la Vlaamse toezichtscommissie ont, notamment de ce fait, travaillé en étroite collaboration. Il est en effet difficilement concevable pour le citoyen au niveau régional ou national que la protection des données à caractère personnel diffère d'une région à une autre.

17. Il en va de même pour les citoyens de l'Union européenne. La Commission est dès lors également favorable à une proposition européenne de texte en la matière, étant donné que la Directive STI reste somme toute trop vague sur le plan de la protection des données, comme l'avait déjà fait remarquer le CEPD[40].

---

[38] Voir le point 3.

[39] Voir l'article 92*bis*, § 2, a) de la loi spéciale de réformes institutionnelles du 8 août 1980.

[40] Voir l'avis susmentionné du 22 juillet 2009.

III. CONTENU DE L'AVANT-PROJET

A. Finalité de l'avant-projet

18. L'objectif de l'avant-projet de loi est double (article 2 de l'avant-projet). D'une part, on prévoit une transposition de la Directive STI[41]. D'autre part, le législateur veut créer une loi-cadre *"qui d'une part, expose les principes généraux et d'autre part, confie au Roi la possibilité d'élaborer des dispositions d'adaptation et de mise en œuvre ultérieures. Parallèlement, il apparaît utile de mettre sur pied un cadre pour la coopération effective sur les systèmes de transport intelligents et de leur suivi. Outre les différents services publics fédéraux, d'autres acteurs sont également impliqués*."[42]

19. À cet effet, les mesures suivantes sont instaurées :
    - introduction de définitions pertinentes relatives aux STI (chapitre II, article 3) ;
    - champ d'application de la loi sur les applications STI et les services STI (chapitre III, article 4) ;
    - délimitation de domaines de développement et d'application prioritaires (chapitre IV, articles 5 à 6 inclus) ;
    - protection de droits fondamentaux (chapitre V, article 7) ;
    - règlement en matière de responsabilité (chapitre VI, article 8) ;
    - habilitation au Roi à compléter les lois fédérales, à les abroger ou à les remplacer pour les conformer aux exigences requises en matière de STI (chapitre VII, articles 9 à 11 inclus) ;
    - (exécution d'une) coopération en matière de STI par l'autorité fédérale (chapitre VIII, article 12) ;
    - dispositions exécutoires et finales (chapitre IX, articles 13 à 15 inclus).

20. Ce sont surtout les chapitres V et VII (articles 7 et 9 à 11 inclus) qui se révèlent importants pour l'application de la LVP.

21. L'article 7 est énoncé comme suit :

    "§ 1. Nulle disposition de la présente loi ne porte atteinte aux mécanismes de protection légaux et réglementaires en matière de traitement de données à caractère personnel, de sûreté et de réutilisation d'information.

[41] Exposé général de l'avant-projet de loi.
[42] Exposé général de l'avant-projet de loi.

§ 2. En cas de conflit et/ou de contradiction lors de l'application simultanée des mécanismes de protection législatifs visés au § 1er, il est dans le cadre des STI toujours donné priorité aux dispositions légales qui en la matière offrent la protection juridique la plus large aux utilisateurs des STI."

B. Données traitées

22. L'avant-projet n'est pas suffisamment clair quant aux données à caractère personnel qui seront (pourront être) traitées dans les systèmes STI envisagés. L'avant-projet ne contient aucune référence à la limitation des données.

23. Le considérant 12 de la Directive STI dispose que *"Il convient d'appliquer aux applications STI, entre autres, les principes de finalité, de proportionnalité et de limitation des données"*.

24. L'article 10.3 de la Directive STI explique ce que l'on entend par "limitation de données" en indiquant que des données à caractère personnel ne sont traitées *" que dans la mesure où leur traitement est nécessaire pour le bon fonctionnement des applications et des services STI."* (voir ci-après le point 53).

25. Il est d'ores et déjà clair que les STI peuvent concerner les données à caractère personnel les plus diverses qui dépendront (de l'architecture) du système concret et des applications possibles. La question de savoir quelle sera la granularité des données traitées, soit par choix de l'utilisateur, soit par défaut dans le système (ou éventuellement utilisé selon l'application) aura également un impact.

26. L'application du principe souvent appelé "protection des données dès la conception" (ou "privacy by design"[43]) constitue dans ce domaine un point d'attention que le législateur aurait pu aborder, en tenant compte évidemment des coûts de mise en œuvre de chaque système et projet.

27. Par ailleurs, la Commission émet toutefois une réserve quant au lancement du "principe" de limitation de données, lequel ne figure pas en tant que tel dans la Directive 95/46/CE. Elle estime que le législateur doit se montrer prudent lors du lancement de nouveaux "principes" et considère que le fait de ne pas mentionner explicitement le principe de limitation de données dans l'avant-projet ne doit pas poser de problème. Une application du principe de proportionnalité suffit déjà, selon elle (voir ci-après au point F).

---

[43] Pour une définition, voir la proposition de texte annexée au présent avis ainsi que le point III.1 du 22 juillet 2009 du CEPD.

28. La Commission souligne que chaque système concret et chaque application soulèvera néanmoins des questions spécifiques en matière de proportionnalité (voir ci-après), devant toujours être évaluées au cas par cas. La Commission souhaite à cet égard toujours pouvoir jouer pleinement son rôle légal de conseiller indépendant et de contrôleur (articles 29 et suivants de la LVP). Elle demande dès lors que la loi-cadre STI prévoie explicitement que son avis devra obligatoirement être requis pour tout système ou projet STI public ou privé via lequel des données à caractère personnel (sensibles) au sens de l'article 6, 7 ou 8 de la LVP sont traitées, lorsque l'application ou les services donnent lieu à une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ou qui est destinée à évaluer certains aspects de sa personnalité ou qui implique le traitement de données à caractère personnel sans le consentement (libre et spécifique) de la personne concernée.

29. La Commission souligne par ailleurs que le traitement de données de localisation est particulièrement délicat et a déjà fait l'objet d'un règlement légal[44] : "*Comme les données de localisation renvoient à l'identification d'une personne physique dans l'espace, le traitement de ces données à caractère personnel est particulièrement sensible eu égard au fait que ce traitement peut constituer une atteinte aux libertés individuelles (liberté d'aller et venir anonymement, droit au respect de la vie privée et familiale, ...)*"[45].

30. L'enregistrement d'événements dans les véhicules pour les systèmes de sécurité (ce qu'on appelle l' "Event Data Recorder" ou "EDR") permet de traiter par exemple des données telles que le statut technique du véhicule (consommation de carburant, …), le moment de l'accident et le comportement dynamique du conducteur (par exemple, pression du liquide de frein au début et à la fin du freinage, vitesse du véhicule également lors du freinage, vitesse du moteur, utilisation ou non des ceintures de sécurité, pourcentage du régime, …).

31. La Commission attire l'attention sur le fait que de telles données peuvent constituer un traitement de données de profil permettant dresser une carte détaillée du comportement d'une personne concernée. Les fournisseurs concernés de tels systèmes et services STI doivent prendre des mesures visant à protéger les personnes concernées de telles opérations d'observation, comme l'établit déjà le droit européen[46].

---

[44] Voir ci-après les renvois aux articles 122 et 123 de la loi du 13 juin 2005 *relative aux communications électroniques*.
[45] Sénat, Développements du document législatif n° 3-1856/1 *relatif à la proposition de loi modifiant la loi du 13 juin 2005 relative aux communications électroniques, en vue d'assurer une meilleure protection de la vie privée pour les services à données de localisation ou les services de géolocalisation par téléphone portable*, publié à l'adresse suivante : http://www.senate.be/www/?MIval=/publications/viewPub&COLL=S&LEG=3&NR=1856&PUID=50335286&LANG=fr

[46] Voir la recommandation CM/Rec(2010)13 du 23 novembre 2010 du Conseil des Ministres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage, publié sur http://www.coe.int/t/dghl/standardsetting/dataprotection/CMRec_2010_13F.pdf.

IV. EXAMEN GÉNÉRAL

A. Applicabilité de la LVP

32. "*Les STI fonctionnent sur la base de la collecte, du traitement et de l'échange d'un large éventail de données provenant de sources tant publiques que privées. Ils font donc un usage intensif de données*"[47], affirme le CEPD. D'après ce dernier, "*le déploiement des STI s'appuiera dans une large mesure sur les technologies de géolocalisation, par exemple les systèmes de positionnement par satellite et les technologies sans contact telles que les RFID, qui faciliteront la fourniture de toute une gamme de services de positionnement publics et/ou privés (par exemple, informations en temps réel concernant la circulation, eFreight, eCall, eToll, réservation d'espaces de parking, etc.). Certaines informations traitées par les STI sont agrégées — ainsi, celles concernant la circulation, les accidents et les possibilités — et ne concernent pas une personne en particulier, alors que d'autres informations se rapportent à des personnes identifiées ou identifiables et constituent donc des données à caractère personnel au sens de l'article 2, point a), de la directive 95/46/CE.*"

33. Le Groupe 29 et la Commission ont déjà émis plusieurs avis concernant des Technologies telles que la géolocalisation[48], la RFID[49], …

34. L'avant-projet de loi porte dès lors sur des traitements de données à caractère personnel et tombe ainsi dans le champ d'application de la Directive 95/46/CE et de la LVP. Il en résulte que les différents responsables du traitement devront respecter un certain nombre de principes de la LVP (voir ci-après).

---

[47] Voir le point 8 de l'avis précité du CEPD.

[48] Voir l'avis n° 12/2005 du 7 septembre 2005 *relatif à la proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée*, publié à l'adresse suivante : http://www.privacycommission.be/sites/privacycommission/files/documents/avis_12_2005_0.pdf.
Voir l'avis WP 185 du Groupe 29 du 16 mai 2011 *sur les services de géolocalisation des dispositifs mobiles intelligents*, publié à l'adresse suivante : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_fr.pdf.

[49] Avis d'initiative n° 27/2009 du 14 octobre 2009 *relatif à la RFID*, publié à l'adresse suivante : http://www.privacycommission.be/sites/privacycommission/files/documents/avis_27_2009_0.pdf.
Voir l'avis du Groupe 29 WP 180 du 11 février 2011 *sur la proposition révisée des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID)*, publié à l'adresse suivante : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_fr.pdf.

B. Applicabilité de la loi relative aux communications électroniques

35. Certaines formes de STI utilisent un réseau de télécommunications public[50], ce qui permet l'application de la loi du 13 juin 2005 *relative aux communications électroniques* à de tels systèmes et applications. Le champ d'application de la loi du 13 juin 2005 étant toutefois limité aux réseaux et services de communications électroniques publics, la protection de la loi du 13 juin 2005 ne sera souvent pas d'application. C'est le cas si les acteurs offrant des services de géolocalisation ne sont pas opérateurs (par exemple les fabricants de systèmes GPS) et s'il s'agit de services et d'applications de localisation offerts sur la base d'une combinaison de données station de base, Wifi et GPS (lesdits "services de la société de l'information" ne sont pas des "services de communications électroniques"[51] et ne sont par conséquent pas protégés par la loi du 13 juin 2005). Si la loi du 13 juin 2005 ne s'applique pas, les mesures de protection de la LVP restent néanmoins d'application.

C. Examen de l'article 7 de la loi-cadre STI

36. La Commission estime qu'il n'est pas suffisant d'affirmer à l'article 7 de la loi-cadre STI : "*Nulle disposition de la présente loi ne porte atteinte aux mécanismes de protection légaux et réglementaires en matière de traitement de données à caractère personnel, de sûreté et de réutilisation d'information* (…)". Non seulement la loi-cadre STI mais aussi les systèmes, applications et services STI doivent être conformes à la législation en matière de protection de la vie privée (et de communications électroniques). L'article 10 de la Directive STI mentionne d'ailleurs que *"le traitement des données à caractère personnel dans le cadre de l'exploitation des applications et services STI* (doit être) *conforme aux règles de l'Union protégeant les libertés et les droits fondamentaux des personnes, en particulier la directive 95/46/CE et la directive 2002/58/CE.*"

37. La Commission constate quand même que la Directive STI confirme clairement et explicitement[52] l'applicabilité de la Directive 2002/58/CE, tandis que l'avant-projet de loi ne comporte pas un tel renvoi. L'exposé des motifs de l'article 7 de l'avant-projet mentionne uniquement ce qui suit : "*Le § 1 garantit le niveau minimum de protection exigé par l'article 10 de la Directive STI en matière de traitement des données à caractère personnel de sûreté et de réutilisation des informations.*"

---

[50] Voir le point 2 "Principe du système eCall" dans le document de travail précité WP 125 du Groupe 29.
[51] Voir le point 4.2.1. de l'avis 13/2011 *sur les services de géolocalisation des dispositifs mobiles intelligents*, publié à l'adresse suivante : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_fr.pdf.
[52] Voir les considérants 12 et 13 de la de Directive STI et l'article 10 de la Directive STI.

38. Par analogie avec la Directive STI, la Commission demande au législateur de reprendre un renvoi plus clair à la LVP et à la réglementation en matière de communications électroniques dans l'exposé des motifs et à l'article 10 de l'avant-projet de loi.

D. Principe d'un traitement légitime

39. L'article 5 de la LVP mentionne cinq cas dans lesquels un traitement de données à caractère personnel peut être réalisé.

40. Le CEPD a affirmé ce qui suit[53] : "*La proposition ne détermine pas clairement le moment auquel débutera le traitement de données à caractère personnel une fois que des STI auront été intégrés dans un véhicule ni la base juridique sur laquelle s'appuiera ce traitement. Les exploitants peuvent se fonder sur différentes bases juridiques aux fins du traitement des données, par exemple le consentement exprès des utilisateurs, un contrat ou une obligation légale à laquelle le responsable du traitement devra se conformer. Il convient d'harmoniser la base juridique du traitement de données par les STI afin d'assurer le bon fonctionnement des systèmes dans toute l'Europe et de faire en sorte que les utilisateurs ne soient pas affectés par des divergences entre les modalités de traitement dans les différents États membres de l'UE.*"

41. Au niveau européen, on accorde entre-temps davantage d'attention à ce qu'il y ait une bonne base de légitimation pour chaque application[54].

42. Dans la mesure où il s'agit de traitements de données à caractère personnel qui peuvent s'inscrire dans le cadre de l'article 12, cela signifie que pour (l'exécution de) la coopération en matière de STI par l'autorité fédérale, on peut se référer à l'article 5 e) de la LVP (l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement).

43. Tous les systèmes et applications ne seront toutefois pas obligatoirement mis en œuvre. Les applications commerciales non obligatoires réalisées par des tiers requièrent un autre fondement de légitimité comme le consentement de la personne concernée (article 5 a) de la LVP), la nécessité de conclure un contrat (article 5 b) de la LVP), ou une situation où il est question d'un intérêt pondéré (article 5 f) de la LVP).

---

[53] Voir le point 16 de l'avis du CEPD.
[54] Élément de l'étude mentionnée au point 3 qui a sélectionné 10 applications STI.

44. Dans certains cas, le consentement de l'abonné sera déjà requis légalement, comme pour les systèmes et applications STI qui traitent des données de localisation[55] via des réseaux de télécommunications publics, par un service de communication électronique d'un opérateur ("applications hotspot" dans la voiture). Un grand nombre d'applications STI n'en feront pas partie en tant que "service de la société de l'information".

45. À l'instar du CEPD[56] et comme dans le secteur des compteurs intelligents, la Commission soutient quand même l'option privilégiée de ne proposer que sur base volontaire les autres services STI offerts par des acteurs privés. À ce niveau, le législateur pourrait disposer explicitement que "les utilisateurs doivent pouvoir consentir librement à l'utilisation du système et aux finalités spécifiques pour lesquelles il sera utilisé", par exemple s'il s'agit de données de localisation traitées via la navigation par satellite.

46. La Commission souhaite que le législateur prévoie que la notion de consentement pour les autres services STI doive être comprise conformément aux dernières évolutions du droit de protection des données, qui évolue[57] vers une exigence de manifestation de volonté explicite et spécifique basée sur des informations préalables suffisamment claires (donc pas de consentement implicite).

47. En outre, un tel choix pour le "consentement" de la personne concernée en tant que fondement juridique (par exemple en cas de services avancés proposés par des entreprises de location de voitures) implique que le système doit pouvoir être aisément activé ou désactivé par l'utilisateur, sans pression externe ou conséquence négative pour la personne concernée en cas de désactivation (par exemple, des frais ou efforts supplémentaires)[58] (voir la définition de consentement à l'article 1, § 8 de la LVP et l'accent mis sur le fait de prévoir un consentement révocable). On observe à cet égard que des services sont souvent lancés comme une option libre mais qu'ils se développent petit à petit vers une situation où aucune véritable alternative n'existe en raison de la qualité inférieure du service classique "désuet" (par exemple, la télébillettique pour les transports publics où l'option papier classique devient plus onéreuse et plus complexe ou même disparaît). Le secteur financier (le virement classique sur papier vs. l'e-banking, …) présente des précédents à cet égard.

---

[55] Voir ci-après le renvoi à l'article 9 de la Directive 2002/58/CE et les articles 122 et 123 de la loi du 13 juin 2005 *relative aux communications électroniques*.
[56] Voir le point 18 de l'avis du CEPD.
[57] Voir la proposition de Règlement européen relatif à la protection des données de la Commission européenne du 25 janvier 2012, publiée à l'adresse suivante : http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf.
[58] Voir la page 4, point 3.1. du document de travail WP 125 du Groupe 29.

48. Le recours au consentement libre de la personne concernée ne sera pas non plus évident pour toutes les applications STI. Le consentement n'est par ailleurs pas requis pour la sauvegarde d'un intérêt vital de la personne concernée (article 5 d) de la LVP), qui pourra être utilisé comme fondement légal pour certaines applications STI.

E. Principe de finalité

49. Le principe de finalité a été défini à l'article 4 de la LVP, qui oblige le responsable du traitement à ne collecter des données que pour des finalités déterminées, explicites et légitimes et à ne traiter ces données que de manière compatible avec ces finalités.

50. La directive mais aussi l'avant-projet de loi transposant la directive poursuivent des finalités politiques générales (voir supra les points 3, 5 et 6) que vise le déploiement des STI.

51. Il est clair que la loi-cadre, tout comme le Plan d'action de la Commission européenne pour la période 2009-2014 et la Directive STI, se limitent à déterminer des finalités politiques et domaines prioritaires très généraux. L'objectif premier n'était pas de déterminer toutes les finalités d'utilisation concrètes des données à caractère personnel. Cependant, la Commission se voit contrainte, à l'instar du CEPD[59], de répéter l'obligation des acteurs de définir les finalités d'utilisation concrètes (article 4, § 1, 2° de la LVP et article 22 de la Constitution). La détermination de finalités précises constitue en effet un élément essentiel de la réglementation relative à la protection des données à caractère personnel[60].

52. Pour l'heure, le cadre législatif proposé est en effet *"trop large et trop général pour répondre adéquatement aux préoccupations en matière de respect de la vie privée et de protection des données que soulève le déploiement des STI* (…)"[61].

53. La loi-cadre aurait au moins pu signifier aux acteurs l'obligation de définir clairement toutes les finalités d'utilisation concrètes des systèmes et applications.

---

[59] Voir le point 21 de l'avis précité du CEPD.
[60] Voir l'avis n° 45.459 du 14 novembre 2008 relatif à un avant-projet de décret "relatif au fichier central d'adresses de référence" (décret "CRAB"), Parlement flamand, 2008-2009, 2067, publié à l'adresse suivante : http://docs.vlaamsparlement.be/docs/stukken/2008-2009/g2067-1.pdf.
[61] Voir le point 14 de l'avis précité du CEPD.

54. Il convient également d'accorder davantage d'attention au fait que le principe STI de compatibilité et d'interopérabilité des systèmes (article 4, § 2 de l'avant-projet) est modéré par le principe de finalité de l'article 4, § 1, 2° de la LVP et l'exigence de sécurité des traitements (article 16 de la LVP). Une compatibilité et une interopérabilité intégrales des systèmes ne peut dès lors pas constituer une finalité en soi, vu les risques inhérents au détournement de finalité.

55. Par analogie avec sa recommandation relative aux compteurs intelligents[62], la Commission estime de nouveau qu'il est important que le législateur impose une distinction plus claire entre des finalités de base connues propres aux systèmes qui sont développés et soutenus par le législateur européen en tant que priorité ou obligation (par exemple, l'eCall), des systèmes déjà lancés où l'utilisateur n'a souvent aucun choix comme en matière de transports publics (par exemple, MOBIB), et ensuite les applications qui peuvent être développées par des tiers en réutilisant potentiellement les données disponibles dans des systèmes STI existants dans les véhicules (par exemple, dans le secteur des assurances) ou d'autres applications basées au-delà de la finalité primaire de navigation par satellite (fabricants de GPS). Cette distinction est pertinente tant du point de vue de l'utilisateur qu'au niveau de la base réglementaire (article 4, § 1, 2° de la LVP).

F. Proportionnalité

F.1. Systèmes et applications STI et articles 4, § 1, 3° de la LVP - anonymisation ou pseudonymisation

56. Les données à caractère personnel doivent être "*adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement*" (article 4, § 1, 3° de la LVP). Lorsque le responsable du traitement détermine les moyens du traitement qui lui permettent de réaliser la finalité qu'il envisage, il doit également veiller à choisir les moyens qui portent le moins atteinte à la vie privée des personnes concernées. Une ingérence dans le droit à la protection des données des personnes concernées doit en effet être proportionnelle au regard de l'utilité et de la nécessité du traitement pour le responsable du traitement.

[62] Voir les points 31 et suivants de la recommandation n° 04/2011 du 15 juin 2011, publiée à l'adresse suivante : http://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_04_2011_0.pdf.

57. Si certains systèmes et applications de base ne nécessitent dès lors aucun traitement de données à caractère personnel, il faut déterminer clairement qu'il n'y a aucun besoin de traiter des données à caractère personnel (par exemple le fait de voyager de manière anonyme dans les transports publics est traité de la même manière que le fait de voyager de manière non anonyme). La Commission remarque dans ce cadre que le législateur ne transpose pas l'article 10.3 de la Directive STI. Cet article impose aux États membres d'encourager l'usage de données anonymes pour les applications STI, lorsque cela s'y prête. Le considérant 13 de la Directive STI dispose également de manière très claire ce qui suit : "*Il y a lieu d'encourager l'anonymisation comme l'un des principes visant à renforcer la protection de la vie privée des individus*".

58. La Commission estime que sur ce point, l'avant-projet doit exécuter la Directive STI, ou doit du moins transposer la logique de l'article 10.3 de la Directive STI.

59. Pour rappel, la Commission souligne que les "données anonymes" sont strictement définies à l'article 1, 5° de l'arrêté royal du 13 février 2001. Il ne sera toutefois pas toujours possible ou souhaitable de garantir une véritable anonymisation pour certaines applications de base STI (par exemple e-Call). Dans ce cas, la pseudonymisation sera un choix plus indiqué[63].

F.2. Mécanisme de conservation et effacement des données

60. En vertu de l'article 4, § 1, 5 de la LVP, le délai de conservation des données traitées ne peut excéder la durée nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues.

61. Vu la complexité de nombreux systèmes et applications STI, il ne sera pas évident de fixer un délai de conservation des données simple (par exemple effacement des données après facturation dans le cas des systèmes E-toll).

62. Pour les données traitées et échangées entre les acteurs habilités, il faut au moins définir une politique de conservation, comportant pour les différentes applications des éléments tels que les délais de conservation pertinents des données (ou des méthodes de calcul pour calculer le délai de conservation requis en fonction de facteurs pertinents), les modalités de

[63] Voir par analogie la communication de la Commission européenne COM(2007) 228 final du 2 mai 2007 visant à *promouvoir la protection des données par les technologies renforçant la protection de la vie privée*, publiée à l'adresse suivante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:FR:PDF. Cette communication définit clairement les mesures visant à limiter autant que possible le traitement de données à caractère personnel et à recourir si possible à des données anonymes ou à des pseudonymes, plus particulièrement en soutenant le développement de technologies renforçant la protection de la vie privée et en faisant utiliser ces technologies par les responsables du traitement de données à caractère personnel et par les particuliers.

conservation en ce qui concerne la forme (par exemple la conservation sous forme anonyme ou codée avec ou sans pseudonyme ou via une autre méthode), le lieu de stockage (stockage central, local comme dans la voiture ou auprès de certains acteurs, ou une combinaison de ces éléments), les méthodes de suppression de données désuètes ou devenues non pertinentes et le contrôle interne de cette suppression, …

F.3. Traitement de données de localisation

63. Il convient de veiller à ce qu'il n'y ait pas d'enregistrement permanent de données de localisation et que soit les systèmes de géolocalisation puissent être configurés à un niveau de granularité élevée, soit qu'ils soient désactivés pour tous les traitements qui ne sont pas basés sur une obligation légale ou réglementaire (article 5, c) de la LVP) ou sur une mission d'intérêt public (article 5 e) de la LVP).

G. Responsable(s) du ou des traitement(s)

64. L'avant-projet ne contient aucun règlement explicite désignant le ou les responsables du ou des traitements ni de répartition des rôles (article 1, § 4 de la LVP) dans le contexte de systèmes et d'applications STI coopératifs ou non. Il s'agit d'un obstacle au respect de la LVP, car souvent, on ne pourra pas déterminer clairement "*ceux qui sont responsables du traitement des données et doivent par conséquent assurer le respect des obligations en matière de protection desdites données. Les exploitants de STI devront faire face à des problèmes considérables si les dispositions législatives concernées ne répondent pas à ces questions, puisqu'ils seront en dernier ressort responsables d'appliquer les mesures énoncées dans la directive proposée.*"[64]

65. Les systèmes et applications STI de nature coopérative impliqueront quoi qu'il en soit l'intervention de différents acteurs[65] comme le concepteur et le fournisseur du système, le fournisseur du système d'exploitation et de certaines applications, l'intégrateur de données, … Ce faisant, il faudra, pour chaque système et projet, une réponse très claire à la question de savoir qui est le responsable de quel(s) traitement(s). Il en va du respect de la LVP.

---

[64] Voir le point 14 de l'avis du CEPD.
[65] Pour MOBIB, il s'agit, pour la gestion, d'un consortium de THV Prodata Systems, Prodata Mobility Systems Fabricom GDF Suez (source : http://www.mobimix.be/inhoud/2011/8/18/2574), outre les sociétés de transport connues (De Lijn, MIVB, TEC et SNCB).

66. La Commission estime qu'il est recommandé de prévoir un point de contact central (appelé "single point of contact") par système, auprès duquel les personnes concernées peuvent s'adresser pour exercer leur droit d'accès, de rectification, d'opposition, de suppression, etc.

67. Cela est d'ailleurs sans rapport avec la question générale de la responsabilité juridique de chaque acteur qui, sur la base de l'obligation générale de précaution, devra suivre les dernières évolutions du droit européen en matière de protection des données en tenant compte des principes de sécurité et d'un niveau de protection suffisamment élevé pour les personnes concernées via la protection de la vie privée dès la conception (ce qu'on appelle le "privacy by design")[66] et la protection des données par des paramètres par défaut ("privacy by default")[67].

68. À l'instar d'autres dossiers (par exemple IMI, compteurs intelligents, …), le législateur aurait de manière générale pu attirer davantage l'attention sur cet aspect, en reprenant par exemple le renvoi suivant : "*l'attribution de différentes responsabilités aux autorités et acteurs doit se faire conformément à la LVP.*"

H. Principe de transparence et obligation d'information des personnes concernées

69. L'obligation légale d'information du responsable du traitement est l'une des obligations de base prescrites par la LVP (article 9 de la LVP). L'expérience des pays voisins a mis en évidence qu'un problème de perception et d'acceptation sociale de plusieurs systèmes et applications STI peut apparaître. Dès lors, il vaut mieux encourager le législateur à prévoir une sensibilisation et une information du grand public encore plus larges que ce que prescrit l'article 9 de la LVP.

70. L'article 9 de la LVP impose à tout responsable du traitement d'informer les personnes dont les données sont traitées quant aux finalités du traitement, à l'identité du responsable du traitement et des destinataires (ou catégories de destinataires) des données ainsi qu'à l'existence d'un droit d'accès et de rectification pour la personne concernée.

---

[66] Voir la définition ci-après dans la proposition de texte.

[67] Voir la définition ci-après dans la proposition de texte.

71. En ce qui concerne les données de localisation, l'avant-projet fait l'impasse sur un quelconque renvoi à l'obligation d'information spécifique en application de l'article 9 de la Directive 2002/58/CE[68].

72. Les projets STI auxquels le grand public a été confronté (surtout les transports publics[69]) ont toujours été dépeints de manière négative dans la presse[70] ces dernières années à cause de problèmes (supposés ou non[71]) en matière de vie privée. Il semble ainsi de bon ton de "récompenser" chaque application de télébillettique par un "Big Brother Award". Il est dès lors très important que le législateur insiste comme il se doit pour encourager davantage de transparence à l'égard des utilisateurs au sens large, même en ce qui concerne les informations pertinentes qui, au sens strict, ne sont pas reprises à l'article 9 de la LVP mais qui sont de nature à encourager la confiance et l'acceptation des utilisateurs vis-à-vis de ces nouvelles applications.

73. Il est conseillé d'imposer une plus large information que le Roi pourrait préalablement encourager (éventuellement par l'intermédiaire de codes de conduite) pour les systèmes et applications. Parmi les éléments de cette information plus large, on pourrait retrouver :
    - le droit applicable (vu la mobilité européenne des systèmes STI intégrés dans les voitures personnelles) ;
    - les données à caractère personnel traitées (mention des données qui ne sont pas traitées, du fait qu'il y a anonymisation ou pseudonymisation). L'enregistrement dans le système du modèle de mobilité détaillé de la personne concernée ne sera pas requis pour chaque application. En ce qui concerne les systèmes eToll, les acteurs peuvent toujours compter sur l'intérêt des services de police et de sécurité, ce qui donne lieu à

---

[68] *"1. Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. Les utilisateurs ou les abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données de localisation autres que les données relatives au trafic.*
2. Lorsque les utilisateurs ou les abonnés ont donné leur consentement au traitement des données de localisation autres que les données relatives au trafic, ils doivent garder la possibilité d'interdire temporairement, par un moyen simple et gratuit, le traitement de ces données pour chaque connexion au réseau ou pour chaque transmission de communication.
3. Le traitement des données de localisation autres que les données relatives au trafic effectué conformément aux paragraphes 1 et 2 doit être restreint aux personnes agissant sous l'autorité du fournisseur du réseau public de communications ou service de communications électroniques accessible au public ou du tiers qui fournit le service à valeur ajoutée, et doit se limiter à ce qui est nécessaire pour assurer la fourniture du service à valeur ajoutée."

[69] Voir la presse en ce qui concerne la carte à puce néerlandaise, MOBIB en Belgique et NAVIGO en France.

[70] Voir un "Big Brother award" pour NAVIGO en France (http://bigbrotherawards.eu.org/article646.html), OV-Chip aux Pays-Bas (http://www.ov-chipkaart.nl/nieuws/laatstenieuws/big_brother_award) et MOBIB (http://www.brusselnieuws.be/article/mivb-krijgt-big-brother-award-voor-mobib-kaart).

[71] Plusieurs infractions ont déjà été constatées par d'autres Commissions vie privée comme dans le cas de Tomtom (http://www.cbpweb.nl/Pages/pb_20120112_tomtom-geolocatie-persoonsgegevens.aspx).

des questions inutiles si le système n'est pas conçu pour enregistrer certaines données. La personne concernée doit savoir si des aspects liés au comportement sont collectés (par exemple, un comportement dangereux au volant) ;

- les finalités d'utilisation (distinction entre les finalités de base du système et les applications dérivées de tiers qui requièrent une autre base comme le consentement de la personne concernée) ;
- une description de qui a (ou non) accès aux données (vise-t-on une utilisation de données en vue d'un profilage par des tiers comme les compagnies d'assurance et/ou le marketing direct de produits par des tiers qui n'offrent pas eux-mêmes des services de transport), ou des garanties offertes à cet égard (voir le droit d'opposition à l'article 12 de la LVP) ;
- le délai de conservation (la politique ou le schéma de conservation des données du système, éventuellement en fonction des diverses applications) ;
- le mode de protection contre des accès non autorisés (hacking, …) et l'accès à ses propres données ;
- le mode d'accès à ses propres données ;
- les données de contact du responsable pour toute information complémentaire concernant les droits de la personne concernée (accès et rectification, …).

I. Droits d'accès et de rectification – point de contact central et coopération internationale

74. Vu la complexité des systèmes et applications, il est recommandé de mettre à la disposition des personnes concernées un mécanisme simple et facilement accessible via un point de contact central (voir ci-avant le point 57) afin qu'elles puissent exercer facilement et dans leur propre langue leurs droits d'accès et de rectification à l'égard des traitements.

75. En outre, la Commission demande d'accorder davantage d'attention à l'impact du caractère transfrontalier de certaines applications. Le législateur devra dès lors prévoir l'instauration de mécanismes (de coopération) avec d'autres acteurs à l'étranger pour aider les citoyens dans leur propre langue en cas d'éventuelles demandes d'accès, de rectification, … lorsque des problèmes transfrontaliers sont causés (ou se posent simplement) par des données provenant de l'étranger[72]. Le fait de prévoir un point de contact central national par les divers responsables devrait permettre dans ce cas aider le citoyen dans sa propre langue au lieu de renvoyer la personne concernée ailleurs.

[72] Par exemple si des données erronées ne se trouvent qu'à l'étranger et pas en Belgique.

J. Principe de sécurité lors d'un traitement

76. Des éléments de protection des données et de sécurité de l'information doivent être intégrés dans les STI avant d'être déployés et intensivement utilisés. De tels éléments peuvent renforcer le contrôle des personnes concernées sur le traitement de leurs données à caractère personnel, réduire le risque de détournement de finalité et d'abus et au moins lever la perception d'un problème.

77. Une de ces mesures est le modèle d'enregistrement local (ce qu'on appelle le "distributed processing" ou la répartition de l'enregistrement de données au travers de l'ensemble de la chaîne STI (par exemple dans la voiture) de manière à éviter un enregistrement central de toutes les données STI à un seul endroit auprès d'un acteur, mais chaque acteur ne dispose que d'une partie de l'ensemble du modèle de mobilité détaillé de la personne concernée).

78. Le responsable du traitement et le cas échéant son sous-traitant doivent prendre les mesures de sécurité [73] techniques et organisationnelles nécessaires pour protéger les systèmes STI et les données traitées par leur intermédiaire contre la destruction accidentelle, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel. À cet égard, la Commission se réfère pour information aux normes de sécurité qu'elle a établies et qui, à ses yeux, doivent être applicables, selon le cas, à un traitement de données à caractère personnel[74.]

K. Analyses d'impact sur la protection des données ("Privacy Impact Assessment" ou "PIA")

79. La Commission constate que lors du lancement de nouvelles technologies et de nouveaux systèmes, le risque existe que des responsables tiennent compte beaucoup trop tard de tous les risques en matière de protection des données et de la réglementation relative à la protection des données. La protection de la vie privée via des mesures telles que les analyses d'impact (appelées privacy impact assessment ou "PIA") sur la protection des données ou la protection de la vie privée dès la conception ne peut pas être expédiée comme une formalité et/ou des mesures inutiles qui n'ont pour effet que d'augmenter les coûts. La Commissions constate en effet dans divers dossiers nationaux qui lui sont soumis que si des responsables attendent le déploiement de systèmes et d'applications pour introduire des modifications motivées par la protection des données, cela entraîne des frais

[73] Article 16 de la LVP.
[74] Voir la page : http://www.privacycommission.be/sites/privacycommission/files/documents/01.01.04.06-mesures_de_reference_en_matiere_de_securite_applicables_a_tout_traitement_de_donnees_a_caractere_personnel.pdf.

d'adaptation (encore) plus élevés et nuit à la réputation des acteurs. Une étude européenne[75] effectuée en 2010 dans divers États membres à la demande de la Commission européenne confirme également les avantages économiques de prévoir la protection de la vie privée dès la conception, du moins si les systèmes et les projets sont examinés au cas par cas[76].

80. Par analogie avec le droit en vigueur dans le secteur de l'énergie[77], il convient de déjà prévoir des analyses d'impact sur la protection des données concernant des applications et des systèmes intelligents,. Ces analyses doivent permettre, en tenant compte des coûts de mise en œuvre, d'évaluer au plus vite (de préférence avant le développement de l'architecture du système STI, donc lors de l'analyse préalable), dès le début de la conception de nouveaux systèmes, les risques au niveau de la protection des données. Sans cette approche, le lancement efficace de systèmes ou d'applications est tôt ou tard compromis.

81. Le législateur doit contraindre les différents acteurs à procéder à une analyse d'impact. La Commission recommande à cet égard de charger le Roi de définir le contenu d'une telle analyse d'impact, à condition que le projet d'arrêté royal soit soumis à son avis préalable. Lors d'une analyse d'impact, il faudra tenir compte de la nature et de la finalité du système et de l'application, de l'échelle d'application, de la reconnaissance officielle ou non au niveau européen d'un système comme étant prioritaire ou imposé légalement, des évolutions attendues du système à l'avenir, de l'éventuelle diversité des applications qui peuvent être associées à un système (architecture ouverte[78] ou plus fermée). Tout ceci bien sûr en tenant compte des coûts de mise en œuvre de chaque projet.

82. Les analyses d'impact doivent par ailleurs être effectuées à temps. Le législateur doit prévoir une obligation, pour tous les acteurs STI, de procéder à une analyse d'impact relative à la protection des données au moment où les systèmes, services ou applications STI sont développés, en tenant compte des coûts de mise en œuvre (protection de la vie privée en tant que composante de ce que l'on appelle une "analyse coût-bénéfice").

---

[75] Voir la page 7 et suivante de l'étude de juillet 2010 sur les avantages économiques de technologies de protection de la vie privée réalisée par London Economics à la demande de la DG Justice, publiée sur http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf

[76] *"The complexity of the issue of economic benefits makes it impossible to quantify the economywide benefits to data controllers of PETs deployment. Rather, the evidence suggests that the net economic benefit of PETs deployment needs to be assessed on a case-by-case basis."*

[77] Voir la recommandation 2012/148/UE de la Commission européenne du 9 mars 2012 *relative à la préparation de l'introduction des systèmes intelligents de mesure*, publiée à l'adresse suivante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:FR:PDF.

[78] On s'attend à ce que des appareils embarqués dans les voitures soutiennent plusieurs services. C'est moins évident pour d'autres services STI comme le péage.

83. Enfin, la Commission estime nécessaire que de telles analyses d'impact soient toujours tenues à la disposition des contrôleurs concernés (Commission, IBPT, …), et ce dès le stade (d'analyse) initial, c'est-à-dire avant même le début du développement des systèmes et applications. Cela peut se faire, le cas échéant, sous la forme d'une annexe à une déclaration éventuelle (article 17 de la LVP) et/ou d'une demande d'autorisation du responsable.

L. Dispositions exécutoires – Principe de légalité

84. L'article 9 de l'avant-projet dispose que le Roi est habilité, "*sous les conditions mentionnées dans le présent article, à compléter les lois fédérales, à les abroger ou à les remplacer pour les conformer aux exigences requises en matière de STI.*"

85. Vu l'article 22 de la Constitution[79], cette habilitation au Roi montrera inévitablement ses limites.

M. Dispositions exécutoires – Principe d'examen préalable (avis de la Commission)

86. Étant donné que des avis précédents (géolocalisation, RFID, …) ont quand même fait apparaître clairement que les STI comportent "potentiellement des risques spécifiques pour les droits et libertés individuels" auxquels s'applique le principe européen d'examen préalable[80], la Commission demande que toutes les dispositions exécutoires des articles 9 à 11 inclus concernant le traitement de données à caractère personnel soient toujours prises après un avis préalable obligatoire de la Commission (article 29 de la LVP).

87. Les articles 9 à 11 inclus doivent être adaptés en conséquence.

V. CONCLUSION

88. La Commission constate qu'en matière de STI, il y a de grandes analogies avec d'autres systèmes et applications "intelligents" ("Internet des objets"), et des technologies et projets assimilés déjà abordés précédemment ou ailleurs (MOBIB, RFID, géolocalisation, …).

---

[79] *Une délégation à un autre pouvoir n'est pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur.* (Voir les arrêts de la Cour constitutionnelle n° 202/2004 du 21 décembre 2004, considérant B.6.2, et 29/2010 du 28 mars 2010, considérant B.16.1). Voir aussi l'avis du Conseil d'État n° 38.385 du 3 octobre 2005 *relatif à un projet d'arrêté royal réglementant le statut des gardes champêtres particuliers*, publié à l'adresse suivante : http://www.emis.vito.be/EMIS/Media/Legislation_Docs/sb240206-1-a.pdf

[80] Article 20 de la Directive 95/46/CE. Par exemple s'il s'agit de systèmes et applications qui dressent en détail ou même en intégralité le modèle de mobilité de personnes ou de véhicules.

Elle recommande au législateur de bien vouloir tenir compte des avis, points de vue ou analyses d'impact sur la vie privée existants dans des domaines comparables (en particulier en ce qui concerne les compteurs intelligents) au niveau national et européen.

89. Les STI sont en réalité une "notion globale" pour l'utilisation de technologies à bord et dans le domaine des "véhicules intelligents" dont les risques en matière de protection de la vie privée ont été commentés précédemment, souvent sur des aspects partiels. La Commission européenne a estimé précédemment que les nouvelles questions non résolues concernant la vie privée et la protection des données "*constituent l'un des principaux obstacles à la généralisation des STI* "[81].

90. L'avant-projet ne tient manifestement pas compte de la préoccupation européenne explicite du Plan d'action STI et de la Directive STI concernant la protection des données. L'article 7 de l'avant-projet ("Protection des droits fondamentaux") ne donne à ce sujet pas suffisamment d'éléments pour résoudre les questions précitées à l'égard des acteurs et personnes concernées. D'une part, l'avant-projet ne transpose pas les dispositions pertinentes et explicites de la Directive STI en matière de vie privée et de protection des données (par exemple l'obligation pour tous les systèmes et projets de ne traiter que les données qui sont adéquates, pertinentes et non excessives) et d'autre part, non seulement la loi-cadre STI mais aussi tous les systèmes, applications et services STI doivent être conformes à la législation en matière de vie privée (et de communications électroniques).

91. La Commission estime que l'avant-projet est trop abstrait pour concrétiser son objectif de coopération efficace en matière de STI. L'avant-projet nécessite un encadrement général au niveau de la protection des données en se référant à quelques principes généraux (de protection des données) et au contexte européen en évolution depuis 2010[82]. Sans cet encadrement, la mise en œuvre aisée de systèmes STI belges prioritaires risque d'être entravée plutôt que facilitée.

92. Le législateur doit également tenir compte du fait que pour chaque système et application, une analyse particulière en matière de vie privée sera toujours requise, la Commission souhaitant être en mesure d'accomplir son rôle de conseiller et de contrôleur prévu légalement.

---

[81] Voir le point 10 de l'avis du CEPD.
[82] La publication de l'impact assessment relatif au plan d'action européen est attendue en septembre ; perception et attention médiatique négatives quant à des projets STI concrets.

93. La Commission a par ailleurs estimé qu'il aurait été approprié (dans l'exposé des motifs) de se référer davantage à des systèmes et applications concrets déjà connus (voir la liste au point 3) pour modérer le caractère très abstrait et général pour le destinataire de la norme et accroître la prévisibilité des ingérences de la réglementation STI à l'égard de la vie privée (article 8 de la CEDH).

94. Les principes et garanties concrets auxquels le législateur aurait pu se référer sont les suivants :
    - l'applicabilité de la loi du 13 juin 2005 *relative aux communications électroniques* et de la LVP ;
    - la présence du bon fondement de légitimité en fonction du système et de l'application STI concrète ;
    - la modération du principe européen dans la directive STI d'interopérabilité par les principes de protection des données de finalité, proportionnalité et sécurité des traitements ;
    - l'intégration du principe d'anonymisation ou pseudonymisation dans la loi-cadre STI, comme l'impose la Directive STI sur la base des principes de proportionnalité, de protection de la vie privée dès la conception ("privacy by design") et de l'exigence européenne de prévoir des technologies de protection de la vie privée (appelées "privacy enhancing technologies" ou "PETS")[83] ;
    - la définition de l'obligation de conservation ;
    - une répartition des rôles obligatoire en tant que responsable ou sous-traitant au sens de la LVP, surtout pour les systèmes STI plus complexes de nature coopérative ;
    - une obligation légale de large sensibilisation et de transparence des systèmes et applications, outre l'obligation d'information de l'article 9 de la LVP et de la loi du 13 juin 2005 ;
    - le développement de mécanismes simples et facilement accessibles pour l'exercice des droits d'accès et de rectification par les personnes concernées ;
    - le mode de protection contre un accès non autorisé et l'accès aux propres données par des mesures techniques et organisationnelles pour modérer le risque d'abus (par exemple une répartition de l'enregistrement des données à plusieurs endroits comme pour la télébillettique, le paiement de places de stationnement, …) ;
    - l'imposition à tous les acteurs des STI de réaliser des analyses d'impact sur la protection des données ("Privacy Impact Assessment" ou "PIA"), basées sur un modèle d'analyse d'impact défini par un arrêté royal ;

[83] Voir concernant cette notion la communication de la Commission européenne du 2 mai 2007 au Parlement européen et au Conseil concernant la promotion de la protection des données par les technologies renforçant la protection de la vie privée, COM(2007) 228 final, publiée sur http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:FR:PDF.

- l'application de la règle européenne d'examen préalable en prévoyant l'obligation d'avis au sujet de tous les projets de réglementation en soumettant à l'avis préalable de la Commission d'éventuelles modifications législatives via des pouvoirs spéciaux au Roi ou des dispositions exécutoires par le Roi en vertu des articles 9 à 11 inclus.

PAR CES MOTIFS,

La Commission a conscience que le législateur belge se trouve confronté ici à une mission difficile. Cette difficulté résulte du fait que diverses autorités sur le plan fédéral, régional et local sont compétentes pour transposer la Directive STI et/ou pour régler ou soutenir le développement de systèmes et de services STI. À cela s'ajoute toutefois également un manque de prévisibilité dû au caractère trop large et trop général de la Directive STI qui ne tient pas suffisamment compte des exigences de qualité élevées imposées aux législateurs par la réglementation européenne et nationale en matière de protection de la vie privée, ce dans une matière dont les applications concrètes peuvent impliquer des risques élevés pour la protection de la vie privée.

Compte tenu des remarques ci-dessus, la Commission plaide pour la conclusion d'accords de coopération dans cette matière. Elle formule également une proposition concrète de texte, jointe en annexe, afin de pourvoir l'article 7 de l'avant-projet de loi d'un cadre général approprié en matière de respect de la vie privée et de protection des données, conforme au droit européen et belge en la matière. Elle émet un avis positif pour autant que cette proposition de texte soit prise en compte.

Vu l'importance des divers systèmes et applications, la Commission reste à disposition pour une éventuelle concertation ultérieure sur les systèmes ou applications STI et pour la révision et/ou l'exécution des dispositions de l'avant-projet.

L'Administrateur f.f., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere

PROPOSITION DE TEXTE **Article 3 Définitions**	
Proposition de texte	**Exposé des Motifs**
§ 1 (…)	Les définitions sous les points 21, 22 et 23 sont inspirées de celles présentes dans la recommandation 2012/148/UE de la Commission européenne du 9 mars 2012 relative à la préparation de l'introduction des systèmes intelligents de mesure. Elles peuvent être appliquées par analogie.
21. "analyse de l'impact sur la protection des données" : processus systématique pour l'évaluation de l'impact potentiel ainsi que des risques pour les droits et libertés des personnes concernées, plus précisément de par la nature des traitements de données à caractère personnel, leur portée ou leurs finalités ;	Lors du déploiement de systèmes de transport intelligents, il est nécessaire d'accorder la plus grande attention à la sécurité et à la protection des données à caractère personnel qui y sont traitées. Conformément aux dernières évolutions en droit européen en matière de protection des données, l'analyse d'impact sur la protection des données doit permettre d'évaluer, dès le début de la conception de systèmes intelligents, les risques pour la protection des données. Le considérant 9 de la recommandation de la Commission européenne du 9 mars 2012 *relative à la préparation de l'introduction des systèmes intelligents de mesure* impose entre-temps aux États membres une obligation analogue en matière de déploiement dans le secteur de l'énergie. L'obligation doit être exécutée par le responsable du traitement ou par le sous-traitant ou bien par le sous-traitant agissant au nom du responsable du traitement.

22. "protection des données dès la conception" : l'ensemble des mesures techniques et organisationnelles adéquates , de la conception à l'évaluation en passant par l'exécution, afin de satisfaire aux exigences légales et réglementaires visant la protection des droits et des libertés des personnes concernées en ce qui concerne la protection de la vie privée et des données à caractère personnel.	22. La définition au point 22 vise ce que l'on appelle dans le jargon le "privacy by design". Selon une définition européenne[84], il s'agit de la mise en oeuvre, sur la base de technologies modernes et en tenant compte des coûts de mise en oeuvre, à la fois au moment où sont choisis les procédés de traitement et lors du traitement lui-même, des mesures techniques et organisationnelles adéquates, de telle façon que le traitement satisfasse aux exigences établies par la directive 95/46/CE et la loi du 8 décembre 1992. Le texte correspond à l'article 16, § 4, deuxième alinéa de la loi du 8 décembre 1992 qui contient des éléments analogues[85] concernant l'état de la technique et les coûts y afférents.
23. la "protection des données par défaut" : l'obligation de proposer par défaut la meilleure protection de données possible sans que la personne ne doive intervenir elle-même ; .	23. Ce que l'on appelle généralement "la protection des données par défaut" englobe la mise en oeuvre des mécanismes garantissant que, par défaut, seules sont traitées les données à caractère personnel nécessaires pour chaque finalité spécifique du traitement, et qu'en particulier, les données ne sont ni recueillies ni conservées au-delà du minimum nécessaire pour remplir lesdites finalités, à la fois en termes de quantité de données et de durée de stockage ;

[84] Ces éléments proviennent de l'article 3 d'une recommandation existante de la Commission européenne dans le secteur de l'énergie. Voir sur http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:FR:PDF.

[85] "Ces mesures doivent assurer un niveau de protection adéquat, compte tenu, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels."

Article 7 Protection des droits fondamentaux

Proposition de texte	Exposé des Motifs
§ 1. Nulle disposition de la présente loi ne porte atteinte à la protection légale et réglementaire de la vie privée et du traitement de données à caractère personnel. .	§ 1. Cet article contient un règlement de concordance à l'égard des diverses législations en matière de protection de la vie privée et de protection des données à caractère personnel. Étant donné que les lois du 8 décembre 1992 et du 13 juin 2005 concrétisent les normes juridiques internationales et supranationales en matière de protection des données, la présente loi sera d'abord confrontée aux lois du 8 décembre 1992 et du 13 juin 2005. Lors de la rédaction de cet article, il a été tenu compte de la jurisprudence de la Cour constitutionnelle relative à l'article 22 de la Constitution et des avis antérieurs du Conseil d'État[86] concernant cet article. Il ressortait déjà des travaux parlementaires de la Constitution [87] qu'une réglementation régionale et/ou sectorielle sur la base du deuxième alinéa de l'article 22 de la Constitution pouvait offrir davantage de garanties. La législation ne peut toutefois pas, sur la base de l'article 8 de la CEDH, offrir moins de garanties hormis dans des cas très spécifiques où cela s'avérerait nécessaire et en s'appuyant pour cela sur une base légale ou réglementaire spécifique. On peut penser à l'application de l'article 3, § 5 de la loi du 8 décembre 1992, par laquelle les articles 9, 10 et 12 de la loi du 8 décembre 1992 seraient considérés comme

[86] Voir la page 90, points 3.2 et 5 de l'Avis n° 45.459 du 14 novembre 2008 relatif à un avant-projet de décret relatif au Centraal Referentieadressenbestand (fichier central d'adresses de référence) (décret "CRAB"), VI. Parlement, 2008-2009, 2067, publié sur http://docs.vlaamsparlement.be/docs/stukken/2008-2009/g2067-1.pdf.

[87] Rapport fait au nom de la Commission de révision de la Constitution en vue d'y insérer un nouvel article 24*quater* relatif au respect de la vie privée, Doc. Parl., Chambre, 1993-1994, 1278/2, p. 3 et 4, également cité par Degrave, E., o.c., J.T., 366 note de bas de page 6, publié sur http://www.dekamer.be/FLWB/PDF/48/1278/48K1278002.pdf.

	non applicables pour les traitements effectués avec des données STI pour des finalités de police administrative ou judiciaire.
§ 2. En cas de contradiction lors de l'application simultanée des mécanismes de protection légaux et réglementaires visés au § 1er, il est dans le cadre des STI toujours donné priorité aux dispositions légales qui, en la matière, offrent la protection juridique la plus large aux utilisateurs des STI.	Il a également été tenu compte de la possibilité de prévoir, sur le plan régional ou dans des CCT, une protection particulière des personnes concernées sans que cela puisse porter atteinte à la protection de base offerte par les lois du 8 décembre 19992 et du 13 juin 2005, qui sont elles-mêmes la transposition du droit européen en matière de protection de la vie privée et des données, en ce compris les Directives 95/46/CE et 2002/58/CE.
§ 3 Le recours à des données anonymes, éventuellement des données codées, pour des applications STI est prévu par les fournisseurs de services STI et les développeurs de plateformes, d'architecture et d'interfaces.	§ 3. Le § 3 tient compte de la liberté de chacun d'aller et venir dans l'anonymat, comprise dans le droit au respect de vie privée et familiale (cf. le considérant 13 et le premier alinéa de l'article 10.3 de la Directive 2010/40/UE ainsi que la remarque de la Commission de la protection de la vie privée concernant l'article 4, § 1, 3° de la loi du 8 décembre 1992). Les notions de données anonymes et de données à caractère personnel codées sont comprises au sens de l'article 1, 3° et 5° de l'AR du 13 février 2001 portant exécution de la loi du 8 décembre 1992.
§ 4. Il est indiqué qui est le responsable du traitement pour des applications et des services STI.	§ 4. Lors de l'introduction d'applications et de services STI, il convient d'attribuer la responsabilité au sens de l'article 1 de la loi du 8 décembre 1992.
§ 5.La politique interne ou externe de protection de la vie privée stipule à chaque fois quelle est la base de légitimité au sens de l'article 5 de la	§ 5. L'existence d'une base de légitimité appropriée au sens de l'article 5 de la loi du 8 décembre 1992 pour chaque service ou

loi du 8 décembre 1992, disponible pour chaque finalité d'applications et de services STI.	application constitue un point important. Ainsi, le consentement de la personne concernée sera bel et bien requis pour un certain nombre d'applications privées, mais il ne sera pas possible ou souhaitable pour plusieurs autres applications qui visent, par exemple, l'accomplissement d'une tâche d'intérêt général.
§ 6. Les données à caractère personnel ne sont traitées que dans la mesure où leur traitement est nécessaire pour les applications et les services STI.	§ 6. Le § 6 reprend littéralement le deuxième alinéa de l'article 10.3 de la Directive 2010/40/UE. Ce paragraphe réitère clairement l'exigence de nécessité en tant que critère de confrontation pour établir la conformité de projets et de services STI avec l'article 4, § 1, 3° de la loi du 8 décembre 1992. La raison en est le risque de manque d'attention pour la suppression ou le codage en temps voulu dans des applications et des services de données ne présentant plus d'utilité opérationnelle.
§ 7. Les personnes physiques ne peuvent pas être surveillées en permanence et doivent pouvoir désactiver un système de surveillance à moins d'y être obligé en vertu d'une obligation légale ou contractuelle.	§ 7. Voir le point 13 de l'avis de la Commission. Les technologies de localisation sont considérées comme particulièrement dangereuses pour la vie privée et peuvent enfreindre les libertés individuelles. Est concernée en particulier la liberté de se déplacer de manière anonyme. Par conséquent, la possibilité de désactiver le système de traçage doit être offerte afin que les personnes ne soient plus suivies, par exemple pour certaines applications en dehors des heures de travail. Il y a bien une exception de prévue lorsqu'il existe une obligation légale de l'activer ou quand il existe une obligation contractuelle. En ce qui concerne l'obligation contractuelle, il s'agit d'obtenir le consentement visé à l'article 1, § 8 de la Loi vie privée.

§ 8. Les fournisseurs de services STI et les développeurs de plateformes, d'architecture et d'interfaces appliquent une protection des données dès la conception, conformément à leurs obligations en vertu des lois du 8 décembre 1992 et du 13 juin 2005	§ 8. Cet article concerne la protection des données dès la conception, comme mentionnée à l'article 3, point 22. La possibilité d'introduire des systèmes de transport intelligents est soumise à la condition absolue de trouver des solutions techniques et juridiques appropriées garantissant la protection des données à caractère personnel en tant que droit fondamental, en vertu de l'article 8 de la Charte des Droits fondamentaux de l'Union européenne et de l'article 16 du Traité sur le fonctionnement de l'Union européenne. Particulièrement lors la première phase de l'introduction de véhicules intelligents, les autorités et les parties prenantes doivent veiller à ce que les applications des systèmes dans les transports intelligents fassent l'objet d'un monitoring et à ce que les libertés et droits fondamentaux des individus soient protégés [88] . L'article 10 de la Directive 2010/40/UE dispose que : *"Les États membres veillent à ce que le traitement des données à caractère personnel dans le cadre de l'exploitation des applications et services STI soit conforme aux règles de l'Union protégeant les libertés et les droits fondamentaux des personnes, en particulier la directive 95/46/CE et la directive 2002/58/CE."* Cet article tient en outre compte de la critique émise par la Commission de la protection de la vie privée selon laquelle *"Non seulement la loi-cadre STI mais aussi les systèmes, applications et services STI doivent être conformes à la législation en matière de protection de la vie privée (et de communications électroniques)"*.

[88] Voir le considérant 5 de la recommandation applicable par analogie : Recommandation 2012/148/UE de la Commission européenne du 9 mars 2012 *relative à la préparation de l'introduction des systèmes intelligents de mesure*, publiée à l'adresse suivante : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:FR:PDF.

Les fournisseurs de services STI et les développeurs de plateformes, d'architecture et d'interfaces prévoient la protection des données dès la conception et la protection des données via des paramètres par défaut lors de la planification et des analyses coûts-bénéfices préalables au développement et au déploiement de systèmes, d'applications et de services STI. La protection des données via des paramètres par défaut est exécutée par les fournisseurs de services STI et les développeurs de plateformes, d'architectures et d'interfaces STI de façon à ce que l'option la plus respectueuse des données soit proposée au client en tant que configuration par défaut. § 9. Les fournisseurs de services STI et les développeurs de plateformes, d'architecture et d'interfaces protègent les données à caractère personnel contre les abus, y compris contre l'accès illicite, la modification ou la perte,.	
§ 10. Les fournisseurs de services STI ainsi que les développeurs de plateformes, d'architecture et d'interfaces prennent les mesures nécessaires pour fournir aux personnes concernées des informations qui contiendront au moins les éléments repris à l'article 9 de la loi du 8 décembre 1992 ainsi que les éléments de la gestion des données. § 11. Les fournisseurs de services STI ainsi que les développeurs de plateformes, d'architecture et d'interfaces utilisent des mécanismes adaptés de certification de protection de la vie privée ainsi que des scellés et des marques de	§ 10. Veiller à la transparence est une condition fondamentale pour exercer un contrôle sur des traitements de données à caractère personnel et pour encourager la confiance des personnes concernées dans le développement de systèmes et d'applications STI. Il convient dès lors de recommander que d'autres éléments pertinents qui ne sont pas mentionnés à l'article 9 de la loi du 8 décembre 1992 soient intégrés dans une politique publique de protection de la vie privée. Ces éléments engloblent le droit applicable, les données à caractère personnel traitées (mentionner quelles données ne sont pas traitées, s'il est question d'anonymisation ou de

protection des données, fournis par des parties indépendantes. Le Roi peut, après avis de la Commission de la protection de la vie privée, définir des mécanismes adaptés de certification de protection de la vie privée ainsi que des scellés et des marques de protection des données et fixer les critères pour déterminer les conditions d'indépendance et d'aptitude des parties pouvant analyser l'impact sur la protection de la vie privée de ces mécanismes, scellés et marques.	codage, définir les finalités de base du système et les applications dérivées de parties tierces qui requièrent une autre base telle que le consentement de la personne concernée, définir qui a accès (ou pas) aux données), ou quelles sont les garanties à cet égard, le délai de conservation (la politique ou le schéma de conservation des données du système éventuellement en fonction des différentes applications), les modalités de protection contre l'accès non autorisé (hacking, …) et l'accès à ses propres données, la description des modalités concrètes pratiques de l'accès à ses propres données (droit d'accès en vertu de l'article 10 de la loi du 8 décembre 1992).

§ 12. Les fournisseurs de services STI et les développeurs de plateformes, d'architecture et d'interfaces effectuent une analyse d'impact sur la protection des données avant le développement et le déploiement des plateformes, de l'architecture, des interfaces, des systèmes et des applications. Ils tiennent compte à cet égard des caractéristiques ainsi que de l'analyse globale coûts-bénéfices de chaque projet. Les fournisseurs de services STI et les développeurs communiquent préalablement les analyses d'impact au public et, dès qu'elles sont disponibles, ces analyses sont communiquées au public. Les responsables de systèmes et de services STI informent le plus rapidement possible la	§ 12. La demande d'effectuer une analyse d'impact devra faire partie de l'analyse globale coûts-bénéfices de chaque projet de manière à éviter à temps de coûteuses adaptations postérieures au déploiement de systèmes et d'applications ainsi qu'un risque de dégradation de la réputation suite à une protection défaillante des données. Cette disposition tient également compte de l'observation faite dans l'étude européenne sur les avantages économiques des technologies de promotion de la vie privée selon laquelle une analyse au cas par cas est nécessaire si l'on veut retirer des avantages en matière d'économie et de protection de la vie privée[89].

[89] Voir la page 80 de l'étude précitée publiée sur http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf

Commission de la protection de la vie privée de l'analyse d'impact effectuée, et de toute façon avant le déploiement de plateformes, architectures, interfaces, systèmes, et applications STI. Le Roi peut, après consultation de la Commission pour la protection de la vie privée, déterminer les éléments qui devraient faire partie de l'évaluation de l'impact	
§ 13. Les responsables des systèmes et services STI publics ou privés qui sont déployés ou proposés au niveau fédéral demandent l'avis de: la Commission de la protection de la vie privée dans un ou plusieurs des cas suivants : - lorsque des données à caractère personnel (sensibles) au sens de l'article 6, 7 ou 8 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* sont traitées, lorsque le système STI, l'application STI, - le service STI ou les données STI donnent lieu à une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ou qui est destinée à évaluer certains aspects de sa personnalité ou ; - le traitement de données à caractère personnel sans le consentement (libre et spécifique) de la personne concernée. Le Roi peut étendre la liste précitée de cas où l'avis de la Commission est requis.	§ 13. Cette modification tient compte du point 28 de l'avis de la Commission. La personne concernée a de toute façon le droit, en vertu de l'article 12*bis* de la loi du 8 décembre 1992, de ne pas être soumise à des décisions uniquement fondées sur un traitement automatisé de données qui sont prises à son égard ou qui l'affectent de manière significative. À cet égard, on peut penser à des décisions relatives à une prestation professionnelle, à la fiabilité ou au comportement. Ce paragraphe vise toutefois les situations présentant un risque accru qui ne relèvent pas de l'article 12*bis* de la loi du 8 décembre 1992, par exemple parce que les décisions ont été prises avec une intervention humaine et pas purement sur la base d'un système de décision déjà interdit car entièrement automatisé.
§ 14. Le non-respect des mesures visées aux paragraphes 3, 4, 6, 7, 8, 9 ou 10 par les fournisseurs de services STI et par les développeurs est considéré comme une	§ 14. Cette disposition est une disposition interprétative qui clarifie l'application des dispositions des articles 4, § 1, 1° et 16, § 4 de la loi du 8 décembre 1992 au secteur des systèmes et des services de transports

infraction aux articles 4, § 1, 1° et 16, § 4 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*.	intelligents.
§ 15. Le Roi peut définir des éléments qui devront faire partie de l'analyse d'impact sur la protection des données, après que ceux-ci aient été soumis à l'avis de la Commission de la protection de la vie privée.	§ 15. Lorsque des acteurs tels que des fournisseurs de services STI et des développeurs de plateformes, d'architecture, d'interfaces, etc. au sens de la présente loi effectuent une analyse d'impact sur la protection des données, ils doivent tenir compte des avis des autorités de contrôle indépendantes pertinentes en matière de protection des données sur le plan européen et belge, parmi lesquelles le Groupe de protection des personnes à l'égard du traitement des données à caractère personnel et la Commission de la protection de la vie privée. Par analogie avec le secteur de l'énergie et afin de garantir la qualité et l'indépendance de l'analyse de l'impact, la possibilité a été donnée au Roi d'établir un modèle d'appréciation (privacy impact assessment), après avis préalable de la Commission de la protection de la vie privée. L'absence d'un arrêté royal ne dispense toutefois pas les acteurs de l'obligation d'établir et d'appliquer une analyse de l'impact sur la protection des données.

Article 9 Habilitation au Roi

Proposition de texte	Exposé des Motifs
§ 1. Le Roi est habilité sous les conditions mentionnées dans le présent article, à compléter les lois fédérales, à les abroger ou à les remplacer pour les conformer aux exigences requises en matière de STI.	
§ 2. L'habilitation visée dans le présent article ne peut être utilisée que moyennant le respect des conditions cumulatives suivantes : 1. l'utilisation de l'habilitation doit être nécessaire et proportionnelle. Cette utilisation doit être mentionnée dans un rapport écrit au Parlement au plus tard un mois avant l'établissement des disposition concernées ; 2. Les dispositions pour lesquelles l'habilitation a été utilisée doivent faire l'objet d'un avis préalable de la Commission de la protection de la vie privée.	§ 2. En cas d'utilisation des pouvoirs spéciaux par le Roi, les prescriptions de traitement et notamment les risques pour la protection des données à caractère personnel de la personne concernée et la sécurité y afférente doivent être évalués eu égard à l'article 20 de la Directive 95/46/CE et à l'article 22 de la Constitution.